

DECserver 500

digital

Management

DECLIT
AA
CROSS
HUBOD

Order Number: AA-HU80D-TK

DECserver 500

Management

December 1989

This guide explains both initial and day-to-day management of the DECserver 500 series terminal server. The topics cover everything you need to know to configure ports and to customize the permanent and operational databases of the server. This guide is for the server manager, who should use it with the *DECserver 500 Software Installation* and the *Terminal Server Commands and Messages* manuals.

Supersession/Update Information: This is a revised manual.

Software Version: DECserver 500 V2.0

This manual applies to Version 2.0 of DECserver 500 software and all subsequent maintenance releases up to the next major product release.

digital™


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 only be used or copied 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 or its affiliated companies.

Copyright © 1987, 1989 by Digital Equipment Corporation
All Rights Reserved.
Printed in U.S.A.

The following are trademarks of Digital Equipment Corporation:

DEBNA	DESQA	RSX
DEC	DEUNA	RSX-11M-PLUS
DECconnect		RT
DECnet	LA50 (LA100, et al.)	ThinWire
DECserver	LN01 (LN03, et al.)	UNIBUS
DECUS	LQP02	VAX
DELNI	Micro/RSX	VAXcluster
DELQA	MicroVAX	VMS
DELUA	PDP	VT
DEMPR	Q-bus	Work Processor
DEQNA	RSTS	

IBM is a registered trademark of International Business Machines Corporation.
PC/XT and Personal Computer AT are trademarks of International Business Machines Corporation.

Contents

Preface

1 Introduction to Managing the Server

1.1	What Are the DECserver 500 and DECserver 550 Terminal Servers?	1-1
1.1.1	Models	1-4
1.1.2	Line Cards	1-5
1.2	Server Concepts	1-6
1.2.1	Operating Modes	1-6
1.2.1.1	Local Mode	1-6
1.2.1.2	Service Mode	1-7
1.2.2	Server Databases	1-7
1.2.2.1	Permanent Database	1-8
1.2.2.2	Operational Database	1-8
1.2.2.3	Log-In Database	1-9
1.2.2.4	Changing Values in the Operational Database Versus Changing Values in the Permanent Database	1-10
1.2.3	Log-In Load Balancing	1-11
1.2.4	Automatic Failover	1-11
1.2.5	Groups	1-11
1.2.6	Automatic Node Database Management	1-12
1.3	Port Devices	1-13
1.3.1	Port Speeds	1-15

1.3.2	Port Access	1-15
1.3.3	Terminals	1-15
1.3.3.1	Access to Server Commands	1-15
1.3.3.2	Dedicated Connections	1-16
1.3.3.3	Multiple Sessions	1-16
1.3.3.4	Session Management Terminals (TD/SMP)	1-16
1.3.3.5	3270 Terminals	1-17
1.3.4	Printers	1-18
1.3.4.1	Host-Initiated Requests	1-18
1.3.4.2	Dedicated Printers	1-19
1.3.4.3	Printers Accessed by Personal Computers	1-19
1.3.5	Computers	1-19
1.3.6	Personal Computers	1-20
1.3.7	Modems	1-20
1.4	Offering Printers As Services	1-21
1.4.1	Requirements for Offering Printers As Services	1-22
1.4.2	Advantages of Offering Printers As Services	1-23
1.5	Queuing	1-23
1.6	Security Features	1-26
1.6.1	Security Status	1-27
1.6.2	Passwords	1-27
1.6.3	Limited View	1-27
1.6.4	Modem Control with Non-LAT Hosts	1-28
1.6.5	DSR Logout	1-28
1.7	Down-Line Loading from Load Hosts	1-28
1.7.1	The Server Image	1-28
1.7.2	The Need for Down-Line Loading	1-28
1.7.3	Assigning Load Hosts	1-29
1.8	A Summary of the Server Installation	1-29
1.9	Using Server Management Tools	1-30
1.10	Performing Server Management Tasks	1-31

2 Introducing Server Management Tools

2.1	Server Commands	2-2
2.1.1	Users of Server Commands	2-2
2.1.2	Overview of Server Commands	2-2
2.2	The Terminal Server Configurator (TSC)	2-6
2.3	The Load Host Configuration Procedure (DSVCONFIG)	2-7
2.4	The Remote Console Facility (RCF)	2-8
2.5	The Console Port (Management Port)	2-8
2.6	The Privileged Port	2-10
2.7	Server Security Features	2-11
2.7.1	Security Levels for Server Ports	2-11
2.7.2	Passwords	2-13
2.7.2.1	Privileged Password	2-14
2.7.2.2	Log-In Password	2-14
2.7.2.3	Maintenance Password	2-14
2.7.2.4	Service Passwords	2-16
2.7.2.5	Lock Password	2-16
2.7.3	Modem Control	2-17
2.7.4	DSR Logout	2-17
2.7.5	Limited View	2-17
2.8	On-Line Help	2-18
2.8.1	Server On-Line Help	2-18
2.8.2	TSC On-Line Help	2-20
2.9	Information Displays	2-20
2.10	Troubleshooting Features	2-21
2.11	Terminal Server Manager (TSM)	2-22
2.12	Keyboard Mapping Commands	2-22

3 Identifying and Performing Initial Management Tasks

3.1	Coordinating Your Tasks with Others	3-2
3.2	Establishing Server Security	3-2
3.3	Determining Your Server's Load Hosts	3-4
3.4	Customizing the Server Image on a Load Host Using TSC	3-6

3.4.1	Operating with All Default Values	3-6
3.4.2	Changing the Defaults to Customize Your Server	3-7
3.5	Ensuring That All Load Hosts Have the Same Server Image	3-8
3.6	Down-Line Loading the Customized Server Image	3-9

4 Introducing Day-to-Day Management Tasks

4.1	Coordinating Your Tasks with the Load Host System Manager and Others	4-2
4.2	Customizing the Operational Database	4-2
4.3	Customizing the Log-In Database	4-3
4.4	Customizing the Server Image	4-4
4.5	Down-Line Loading the Customized Server Image	4-4
4.6	Verifying That the Ports Are Operational	4-5
4.7	Maintaining Server Security with Passwords	4-5
4.8	Reconfiguring the Load Host's Node Database	4-6
4.9	Monitoring the Server	4-6
4.10	Helping Server Users	4-6
4.11	Troubleshooting the Server	4-6
4.12	Keyboard Mapping Commands	4-7

5 Performing Day-to-Day Management Tasks

5.1	Maintaining Server Security with Passwords, Password-Related Characteristics, and Security-Related Characteristics	5-2
5.1.1	Setting the Privileged Password	5-2
5.1.2	Setting the Log-In Password	5-3
5.1.3	Setting the Maintenance Password	5-3
5.1.4	Setting and Clearing Service Passwords	5-4
5.1.5	Setting and Clearing a Lock Password	5-4
5.1.6	Setting Other Password-Related Characteristics	5-5
5.1.7	Setting Other Security-Related Characteristics	5-5
5.2	Down-Line Loading the Customized Server Image	5-6
5.2.1	The Initialization Process	5-6

5.2.2	The Different Ways to Initiate a Down-Line Load	5-7
5.2.2.1	How INITIALIZE Works	5-8
5.2.2.2	Resetting the Server by Pressing the Boot Switch	5-10
5.2.2.3	How NCP LOAD Works	5-10
5.2.2.4	How NCP TRIGGER Works	5-14
5.2.3	The Different Ways To Monitor a Down-Line Load	5-17
5.2.4	Preparing for Down-Line Loading	5-17
5.2.4.1	Setting Up DECnet Event Logging	5-17
5.2.4.2	Warning Users	5-18
5.2.4.3	Managing Local Services Before Shutdown	5-20
5.2.5	Initiating a Down-Line Load	5-20
5.2.5.1	Issuing the INITIALIZE Command	5-21
5.2.5.2	Resetting by Pressing the Boot Switch	5-21
5.2.5.3	Issuing the NCP LOAD and TRIGGER Commands	5-21
5.2.6	Monitoring a Down-Line Load	5-21
5.2.6.1	Reading the 900-Series Messages After the Down-Line Load	5-21
5.2.6.2	Reading the Server's LED Displays During the Down-Line Load	5-21
5.2.6.3	Reading Event-Logging Messages After the Down-Line Load	5-22
5.3	Making Use of Groups	5-23
5.3.1	Network Service Groups: Overview	5-24
5.3.2	Assigning Service Groups for Your Server	5-26
5.3.3	Assigning Authorized Groups for Your Ports	5-27
5.3.3.1	Service information	5-27
5.3.3.2	User Information	5-28
5.3.3.3	Adding and Replacing Authorized Groups	5-29
5.3.3.4	Reducing Authorized Groups to Current Groups	5-29
5.4	Managing Local-Access Ports	5-30
5.4.1	Identifying Who Uses the Local-Access Ports	5-32
5.4.2	Session Management Terminal (TD/SMP)	5-32
5.4.3	Educating Users	5-34
5.4.4	User-Oriented Server Characteristics	5-34
5.4.4.1	The Broadcast Feature	5-35

5.4.4.2	The Lock Feature	5-36
5.4.5	User-Oriented Port Characteristics	5-36
5.4.5.1	Assigning a Dedicated Service	5-37
5.4.5.2	Enabling the Log-In Password	5-38
5.4.5.3	Assigning Security Status	5-38
5.4.5.4	Assigning Authorized Groups	5-39
5.4.5.5	Specifying a Session Limit	5-40
5.4.5.6	Enabling Interrupts on Dynamic-Access Ports	5-40
5.4.5.7	Enabling Inactivity Logout	5-40
5.4.5.8	Assigning Permanent User Names	5-41
5.4.5.9	Controlling Access to All Services on the LAN	5-41
5.5	Managing Sessions	5-42
5.5.1	Displaying Session Information	5-42
5.5.2	Terminating Sessions	5-43
5.6	Setting Up and Managing Modem Control	5-44
5.6.1	Introduction to Modem Control	5-44
5.6.2	Modem Control Standards	5-46
5.6.3	Restrictions	5-46
5.6.4	Modem Control Signals	5-47
5.6.5	Modem Control Signaling Sequences	5-49
5.6.6	Implementing Modem Control	5-51
5.6.6.1	Port Characteristics Related to Modem Control	5-51
5.6.6.2	Procedure	5-53
5.6.7	The Monitoring of Modem Control by the Server and TSC	5-54
5.7	Managing Flow Control	5-55
5.7.1	In-Band Flow Control	5-55
5.7.2	Out-Of-Band Flow Control	5-55
5.7.3	Data Transparency Modes for a Local-Access Session	5-56
5.8	Managing Your Server As a Service Node	5-57
5.8.1	Introduction to Local Services	5-57
5.8.2	Commands That Affect Local Services	5-57
5.8.3	Server Characteristics That Affect Local Services	5-58
5.8.3.1	The Name of Your Server As a Service Node	5-59
5.8.3.2	Controlling the Announcement of Local Services	5-60

5.8.3.3	Managing the Multicast Timer	5-60
5.8.3.4	Specifying Service Groups	5-60
5.8.4	Service Characteristics	5-60
5.8.5	Using Service Passwords	5-61
5.8.6	Establishing a Local Service	5-62
5.8.6.1	Prerequisites	5-63
5.8.7	Preventing Remote Access to a Port That Offers a Local Service	5-67
5.8.8	Displaying Information About Local Services	5-68
5.8.9	Controlling Access to Local Services	5-68
5.8.9.1	Controlling Access to All Local Services	5-68
5.8.9.2	Controlling Access to a Specific Local Service	5-68
5.8.10	Clearing Local Services	5-70
5.9	Managing Ports Used for Host-Initiated Requests	5-70
5.9.1	Deciding Whether to Assign a Port Name or Service Name	5-70
5.9.2	Naming the Port or Service	5-71
5.9.3	Reassigning a Port	5-71
5.10	Managing the Connection Queue	5-72
5.10.1	Displaying Server Queue Entries	5-73
5.10.2	Managing the Queue Limit	5-73
5.10.3	Disabling Further Queuing	5-74
5.10.4	Removing Entries from the Queue	5-74
5.11	Managing File Transfers	5-75
5.12	Managing Your Server As Part of the LAT Network	5-76
5.12.1	Distributing Devices on Servers	5-76
5.12.2	Controlling the Number of Known Service Nodes	5-76
5.12.3	Selecting the Value of the Circuit Timer	5-77
5.12.4	Selecting the Value of the Retransmit Limit	5-77
5.12.5	Selecting the Value of the Keepalive Timer	5-77
5.12.6	Controlling Access to Network Services	5-78
5.12.7	The Use of Groups on the Network	5-80
5.13	Setting Up and Managing Ports for 3270 Terminals	5-80
5.13.1	Introduction to the 3270 Terminal Option Card	5-80
5.13.2	Supported Terminals and Keyboard Mapping	5-82

5.13.3	The Effect of Server Power Up on 3270 Terminals	5-82
5.13.4	The Effect of 3270 Terminal Power Up	5-83
5.13.5	The Effect of Power Loss or Line Card Failure	5-83
5.13.6	Image Configuration	5-83
5.13.7	Up-Line Dumping CXM04 Information	5-85
5.14	Line Card Redundancy	5-85

6 Performing Server Management Tasks on the Load Host

6.1	Customizing the Server Image: Using the Terminal Server Configurator (TSC)	6-2
6.1.1	Defining Port, Server, and Service Characteristics	6-3
6.1.1.1	Defining Passwords, Password-Related Characteristics, and Security-Related Characteristics	6-4
6.1.1.2	Defining Other Characteristics	6-6
6.1.2	Using TSC	6-6
6.1.2.1	Overview of TSC Commands	6-7
6.1.2.2	Starting TSC	6-10
6.1.2.3	TSC Problems with Opening Files	6-11
6.1.2.4	Entering TSC Commands	6-12
6.1.2.5	TSC On-Line Help	6-13
6.1.2.6	Executing TSC Commands from a TSC Command File	6-14
6.1.2.7	Updating the Server Image File	6-16
6.1.2.8	Resetting All Values to the Defaults	6-17
6.1.2.9	After Running TSC	6-18
6.2	Down-Line Loading the Customized Server Image	6-18
6.2.1	Setting Up DECnet Event Logging	6-18
6.2.2	Warning Users	6-19
6.2.3	Managing Local Services Before Shutdown	6-19
6.2.4	Issuing the NCP LOAD and TRIGGER Commands	6-19
6.3	Up-Line Dumping	6-21
6.4	Using the Remote Console Facility (RCF)	6-21
6.4.1	RCF and Other Input to Port 0	6-22
6.4.2	Using Remote Management	6-23
6.4.3	Starting a Remote Management Session	6-24

6.5	The Load Host Configuration Procedure: DSVCONFIG	6-26
6.5.1	Overview of DSVCONFIG	6-27
6.5.1.1	Databases Affected by DSVCONFIG	6-28
6.5.1.2	DSVCONFIG Options	6-28
6.5.1.3	Other DSVCONFIG Functions	6-29
6.5.2	Specifying DECnet Characteristics During DSVCONFIG . .	6-29
6.5.2.1	DECnet Node Name	6-30
6.5.2.2	DECnet Node Address	6-30
6.5.2.3	Ethernet Hardware Address	6-31
6.5.2.4	Server Types	6-31
6.5.2.5	Load File (Server Image File)	6-31
6.5.2.6	Dump File Name	6-33
6.5.2.7	Service Circuit	6-33
6.5.3	Preparing to Run DSVCONFIG	6-34
6.5.4	DSVCONFIG Conventions and Requirements	6-35
6.5.5	Running DSVCONFIG	6-35
6.5.5.1	List Known DECservers (Option 1)	6-37
6.5.5.2	Add a DECserver (Option 2)	6-38
6.5.5.3	Swap an Existing DECserver (Option 3)	6-40
6.5.5.4	Delete an Existing DECserver (Option 4)	6-43
6.5.5.5	Restore Existing DECservers (Option 5)	6-43
6.5.6	Restoring with the RESTORE Parameter and from the Load Host's Start-Up Procedure	6-44
6.5.7	After Running DSVCONFIG	6-44
6.6	Keyboard Mapping	6-45
6.6.1	Example of Keyboard Mapping	6-46

7 Configuring Ports for Common Applications

7.1	Cabling Requirements	7-2
7.1.1	Cabling for the CXY08 Line Card (EIA-232-D Interfaces)	7-2
7.1.1.1	Null-Modem Cables	7-2
7.1.1.2	Modem Connections Using Straight-Through Cables	7-3

7.1.2	Cabling for the CXA16 and CXB16 Line Card (EIA-423-A and RS-422-A Interfaces)	7-4
7.1.3	Cabling for the CXM04 Line Card	7-4
7.2	Configuring Physical Port Characteristics	7-4
7.2.1	Local-Access Ports	7-5
7.2.2	Remote-Access or Dynamic-Access Ports	7-6
7.3	Guidelines for Using the Following Application Sections	7-6
7.3.1	Using Examples	7-7
7.3.2	Using Tables	7-7
7.4	A Terminal Capable of Connecting to Many Services	7-9
7.5	A Terminal Using a Dedicated Service	7-12
7.6	A Personal Computer Used As a Terminal and As a Service ...	7-16
7.7	A Printer Configured for Host-Initiated Requests	7-22
7.8	A Printer Used with a Dedicated Service	7-28
7.9	A Non-LAT Host	7-32
7.10	A Dial-Out Modem	7-37
7.11	A Dial-In Modem	7-41
7.12	A Dial-In/Dial-Out Modem	7-45
7.13	A Terminal Switch	7-49
7.14	A Printer Using CTS/RTS Flow Control	7-54
7.15	A Terminal Using DSR/DTR Flow Control	7-56
7.16	A 3270 Terminal Emulating a VT220 Terminal	7-58
7.17	A TD/SMP Session Management Terminal	7-61

8 Specifying Values for Server Characteristics

8.1	Port Characteristics	8-2
8.1.1	Access Characteristics	8-7
8.1.2	Session Initiation Control Characteristics	8-11
8.1.3	Physical Port Characteristics	8-16
8.1.4	Flow Control Characteristics	8-19
8.1.5	Session-Switching Characteristics	8-20
8.1.6	Port Display Control Characteristics	8-22
8.1.7	Modem Support Characteristics	8-23
8.1.8	Port Identification Characteristics	8-25

8.1.9	Remote Modification Control Characteristic	8-26
8.1.10	3270 Terminal Characteristics	8-26
8.2	Server Characteristics	8-27
8.2.1	Network Communications Characteristics	8-29
8.2.2	Local-Access Characteristics	8-31
8.2.3	Server Maintenance Characteristics	8-34
8.2.4	Server Identification Characteristics	8-35
8.2.5	Service Node Characteristics	8-37
8.3	Service Characteristics	8-38
8.4	Devices	8-41
8.4.1	Defining Device TYPE	8-41
8.4.1.1	The CXY08 Line Card	8-42
8.4.1.2	The CXM04 Line Card	8-42
8.4.2	Device STATE	8-43
8.4.3	Device DUMP	8-44
8.5	Defining Languages	8-44

9 Displaying Server Information

9.1	Overview of Display Commands	9-1
9.2	Device Displays	9-5
9.2.1	Device Summary Display	9-5
9.2.2	Device Counters Display	9-8
9.3	Node Displays	9-15
9.3.1	Node Counters Display	9-16
9.3.2	Node Status Display	9-19
9.3.3	Node Summary Display	9-22
9.4	Port Displays	9-24
9.4.1	Port Characteristics Display	9-25
9.4.2	Port Counters Display	9-31
9.4.3	Port Status Display	9-36
9.4.4	Port Summary Display	9-39
9.5	Queue Display	9-42
9.6	Server Displays	9-43
9.6.1	Server Characteristics Display	9-43

9.6.2	Server Counters Display	9-47
9.6.3	Server Status Display	9-54
9.6.4	Server Summary Display	9-58
9.7	Service Displays	9-60
9.7.1	Service Characteristics Display	9-61
9.7.2	Service Status Display	9-62
9.7.3	Service Summary Display	9-64
9.8	Sessions Display	9-67
9.9	Users Display	9-69
9.10	Usage Display	9-70

A MOP System ID Message Format for the DECserver 500 Server

B TSC Defaults Command File

C Setting Up Remote Printers for VMS Systems

C.1	Setting Up the Remote Printer on Your Server	C-1
C.1.1	Example	C-2
C.1.2	Procedure	C-2
C.2	Setting Up the VMS Service Node for the Remote Printer	C-4
C.2.1	Example	C-5
C.2.2	Procedure	C-5
C.2.3	Checkpoint	C-6
C.3	Configuring the Remote Printer Queue on a Service Node	C-7
C.3.1	Example	C-8
C.3.2	Procedure	C-8
C.4	Creating a Remote Printer Command File	C-10
C.5	Setting Up Remote Printing on VAXclusters	C-11

Index

Figures

1-1	The Path of a Host-Initiated Request	1-22
1-2	Server Processing Two Host-Initiated Requests for the Same Service	1-25
1-3	Server Processing the Queue After Service/Port Becomes Available	1-26
5-1	Server Manager Enters LOAD Command at HOST 1	5-12
5-2	Server JUNIOR Asks HOST1 for a Down-Line Load	5-13
5-3	HOST1 Loads Server JUNIOR	5-13
5-4	Server Manager Enters TRIGGER Command at HOST1	5-15
5-5	Server JUNIOR Sends Multicast Message	5-16
5-6	First Load Host to Respond, HOST 3, Loads Server JUNIOR ..	5-16
5-7	Ports Offering a Local Service	5-67
6-1	Remote Management Console on an Ethernet	6-22
7-1	A Terminal Capable of Connecting to Many Services	7-9
7-2	A Terminal Using a Dedicated Service	7-13
7-3	A Personal Computer Used As a Terminal and As a Service ...	7-18
7-4	A Printer Offered As a Service for Host-Initiated Requests ...	7-24
7-5	A Printer Used with a Dedicated Service	7-29
7-6	A Non-LAT Host Offered As a Service	7-34
7-7	A Dial-Out Modem Offered As a Service	7-39
7-8	A Dial-In Modem Used with a Terminal	7-42
7-9	A Terminal Switch Offered As a Service	7-50
7-10	A Terminal Switch Offered As a Front End to a Terminal Server	7-51
9-1	Device Summary Display	9-6
9-2	Device Counters Display	9-9
9-3	Node Display of Local Services	9-15
9-4	Node Counters Display	9-16
9-5	Node Status Display	9-19
9-6	Node Summary Display	9-23
9-7	Port Characteristics Display	9-26

9-8	Port Counters Display	9-32
9-9	Port Status Displays	9-36
9-10	Port Summary Display with Server SHOW Command	9-40
9-11	Port Summary Display with TSC LIST Command	9-40
9-12	Queue Display	9-42
9-13	Server Characteristics Display	9-44
9-14	Server Counters Display	9-48
9-15	Server Status Display	9-54
9-16	Server Summary Display with Server SHOW Command	9-59
9-17	Summary Display with TSC LIST Command	9-59
9-18	Service Characteristics Display for a Service Offered by the Server and for a Service Offered by Another Service Node	9-61
9-19	Service Status Display	9-63
9-20	Service Summary Display with Server SHOW Command	9-65
9-21	Service Summary Display with TSC LIST Command	9-66
9-22	Sessions Display	9-67
9-23	Users Display	9-69
9-24	TSC Usage Display	9-71

Tables

4-1	Summary of TSC Keyboard Mapping Commands	4-8
5-1	Methods of Initiating a Down-Line Load	5-7
5-2	Local-Access Applications Discussed in Chapter 7	5-31
5-3	Local Mode Command Restrictions During Session Management	5-33
5-4	Management Decisions Affecting Local-Access Ports	5-37
5-5	Line Signals Supported by the Server	5-47
5-6	Server and TSC Commands That Affect Local Services	5-58
5-7	Service-Related Applications Discussed in Chapter 7	5-64
7-1	Physical Port Characteristics	7-5
7-2	Using the Tables	7-7
7-3	Port Values for a Terminal Capable of Connecting to Many Services	7-10

7-4	Port Values for a Terminal Using a Dedicated Service	7-13
7-5	Port Values for a Personal Computer Using Dynamic Access . .	7-19
7-6	Port Values for a Printer Configured for Host-Initiated Requests	7-25
7-7	Port Values for a Printer Used with a Dedicated Service	7-29
7-8	Port Values for a Non-LAT Host	7-35
7-9	Port Values for a Dial-Out Modem	7-39
7-10	Port Values for a Dial-In Modem	7-43
7-11	Port Values for a Dial-In/Dial-Out Modem	7-47
7-12	Port Values for a Terminal Switch	7-52
7-13	Port Values for a Printer Using CTS/RTS Flow Control	7-55
7-14	Port Values for a Terminal Using DSR/DTR Flow Control	7-57
7-15	Port Values for a 3270-class Terminal	7-59
7-16	Port Values for a Session Management Terminal	7-61
8-1	Server and TSC Commands Listed by Database	8-2
8-2	Port Characteristics	8-4
8-3	Default Values for Port Characteristics	8-5
8-4	Default Values for Port 0 Characteristics	8-6
8-5	Server Characteristics	8-28
8-6	Default Values for Server Characteristics	8-29
8-7	Service Characteristics with Defaults	8-39
9-1	Display Command Verbs	9-1
9-2	Display Command Verbs, Applicable Entities, Functions	9-3
9-3	Display Types	9-4
9-4	Device Summary/Characteristics Display Fields	9-7
9-5	Device Counters Display Fields	9-10
9-6	CXM04 Counters Display Fields	9-13
9-7	CXM04 Counters Display Fields	9-14
9-8	Node Counters Display Fields	9-17
9-9	Node Status Display Fields	9-20
9-10	Node Summary Display Fields	9-23
9-11	Port Characteristics Display Fields	9-27
9-12	Port Counters Display Fields	9-33
9-13	Port Numbering for a Server with CXM04 Line Cards (Terminals Only) VT Mode — Configuration 8	9-35

9-14	Port Numbering for a Server with CXM04 Line Cards (CCU and Terminals) Configuration 4	9-35
9-15	Port Status Display Fields	9-37
9-16	Port Summary Display Fields	9-41
9-17	Queue Display Fields	9-42
9-18	Server Characteristics Display Fields	9-45
9-19	Server Counters Display Fields	9-49
9-20	Server Status: Error Display Fields	9-55
9-21	Server Status: Resource Display Fields	9-56
9-22	Server Summary Display Fields	9-60
9-23	Service Characteristics Display Fields	9-62
9-24	Service Status Display Fields	9-63
9-25	Service Summary Display Fields	9-66
9-26	Sessions Display Fields	9-68
9-27	Users Display Fields	9-70

Preface

The *DECserver 500 Management* manual presents the information you need for both initial management and day-to-day management of the DECserver 500 terminal server, DECserver 510 terminal server, and the DECserver 550 terminal server. This guide mainly covers software management. Use it in conjunction with the appropriate DECserver 500 series terminal server hardware manuals (depending on your hardware configuration), especially the *DECserver 500 Introduction* and the *DECserver 500 Problem Solving* manuals. The latter book also discusses software troubleshooting.

This guide is written in a tutorial format with some reference material. However, it is not a command reference manual. The *Terminal Server Commands and Messages* manual is the command reference manual for the DECserver 500 system. Also use the *Terminal Server Commands and Messages* manual for explanations of all the error messages generated by the server and the Terminal Server Configurator program (TSC).

Another DECserver 500 manual that you will find helpful is the *DECserver 500 Software Installation* manual. See this guide for operating-system-specific information about starting TSC and the Remote Console Facility (RCF).

The *DECserver 500 Management* manual assumes that you are familiar with using a terminal on a Digital Equipment Corporation terminal server. See the *DECserver 500 Use* manual for information about basic topics such as logging in to and out of the server and entering server commands.

If you have the Terminal Server Manager (TSM) software, an optional network management product available for VMS load hosts, read the documentation for this product before you look at the DECserver 500 documents. TSM affects the way you install and manage servers.

Intended Audience

This guide is for the **server manager**, the person responsible for initializing, maintaining, and managing a DECserver 500 system.

Structure of This Manual

This manual has nine chapters and two appendixes, some tutorial in nature, some mainly reference, and some a combination. In addition, some chapters outline procedural information that is detailed in later sections.

- | | |
|-----------|--|
| Chapter 1 | Introduces server concepts and server management tasks. |
| Chapter 2 | Lists the server management tools to help you with both initial and day-to-day management tasks. It also describes in detail the tools you use on the server. |
| Chapter 3 | Describes the tasks you first perform as manager of a new DECserver 500 server. The initial management tasks are those you undertake after the new system has been installed as described in the appropriate DECserver 500 series hardware installation manual. |
| Chapter 4 | Outlines all the day-to-day server management tasks. This chapter points you to the appropriate sections for more information. |
| Chapter 5 | Fully explains the day-to-day server management tasks, detailing all the major operating features of the server. This chapter helps you customize your server's databases by explaining the server's features and providing the server SET commands to implement these features. |
| Chapter 6 | Explains in detail the server management tasks you perform on a load host and the tools on the load host that help you. This chapter helps you customize your server's permanent database by providing TSC DEFINE command examples. |

- Chapter 7** Shows examples of configuring the server's ports. A separate section is provided for each typical port configuration. In addition, a table of required and recommended values, a diagram of the devices involved, and examples of the commands you use to set up the configuration help you with each configuration.
- This chapter also discusses cabling requirements for each of the DECserver's line cards.
- Chapter 8** Lists and describes the DECserver's characteristics. The changeable values of these characteristics make up the server's databases. This is mainly a reference chapter.
- Chapter 9** Illustrates all the server displays. This chapter has tables to explain the display fields and provides guidelines for using the displays. Chapter 9 also gives you the appropriate **SHOW** or **LIST** command you issue to get each display.
- This chapter helps you customize your server's databases by showing you how first to display the values in the permanent and operational databases. This is mainly a reference chapter.
- Appendix A** Lists and explains Maintenance Operations Protocol (MOP) system ID message formats used by the server.
- Appendix B** Contains a printed version of the TSC and TSM defaults command file for the server. You can use this command file to reset all the server's permanent characteristics to the original default values.
- Appendix C** Describes the procedures that both the server manager and the system manager perform to set up a remote printer.

Using This Manual

If you are familiar with managing Digital terminal servers, you might first want to read Chapter 3 on the initial management tasks, and then go on to Chapter 7 for descriptions of specific port configurations with step-by-step examples. Or, you might find it helpful to refer to Chapter 9 on displaying information before you begin to configure the ports, and then go back to Chapter 7. Next, Chapters 5 and 6 can help you set up and use all of the server's features.

On the other hand, if you have not previously been a server manager, it is a good idea to read the chapters in order.

Conventions Used in This Manual

To use this manual effectively, familiarize yourself with the conventions discussed in this section:

- The RETURN key, which you must press to execute all commands, is assumed in most command examples and therefore not shown on command line displays.
- The Local> prompt, which appears in most examples, is the default server prompt. You can change this prompt to something other than Local> with the SET/DEFINE SERVER PROMPT command.
- All numbers are decimal unless otherwise noted.
- All Ethernet addresses are given in hexadecimal.

Convention	Meaning
<i>Special type</i>	Special type in examples indicates system output or user input.
Red type	Red type in examples indicates user input.
UPPERCASE	Uppercase letters in command syntax indicate keywords that must be entered. You can enter them in either uppercase or lowercase. You can abbreviate command keywords to the first three characters or the minimum unique abbreviation.
<i>italics</i>	Lowercase italics in command syntax or examples indicate variables for which either you or the system supplies a value.
BOLD	In summaries of characteristics, bold type indicates default values.
bold	In text, words appearing in bold type introduce new terms or concepts and can also be found in the Glossary.
{ }	Braces in command syntax statements indicate that the enclosed text is required, and you must specify one (and only one) of the enclosed values. Do not type the braces.
[]	Square brackets in command syntax statements indicate that the enclosed text is optional. You can enter none or one. Default values apply for unspecified options. Do not type the brackets.

key

This symbol means that you should press the specified key. For example, **RET** means that you should press the RETURN key.

CTRL/x

This symbol means that you should hold down the CONTROL key and simultaneously press the key specified by *x*. The server displays this key combination as **^x**.

/

A slash indicates related commands or options. For example, SET/DEFINE PORT refers to the SET PORT and/or DEFINE PORT command(s).

Introduction to Managing the Server

This chapter introduces the DECserver 500 series terminal servers and the tasks you perform to manage these systems. The DECserver 500 series terminal server products are:

- The **DECserver 500 terminal server** — a system that consists of DECserver 500 software and DECserver 500 hardware.
- The **DECserver 510 terminal server** — a system that consists of DECserver 500 software and DECserver 510 hardware.
- The **DECserver 550 terminal server** — a system that consists of DECserver 500 software and DECserver 550 hardware.

Chapter 1 presents an overview of the server's features, discusses the network environment in which the server operates, and outlines server management.

1.1 What Are the DECserver 500 Series Terminal Servers?

The DECserver 500 series terminal servers are a group of Digital Equipment Corporation networking products known as Ethernet communications servers.

A **server** is a computer system, or **node**, where resources shared by the network are located. A server offers these resources to the other nodes. A **communications server** takes over some of the communications tasks required of network nodes. This is the resource it offers.

The DECserver 500 series servers are types of communications servers called a **terminal server**. A terminal server connects to an Ethernet Local Area Network (LAN).

The **DECserver 500 series terminal servers** consist of:

- The DECserver 500, 510, or 550 hardware with corresponding firmware.
- The DECserver 500 distribution software.
- The server image, which is down-line loaded, residing on a load host.

The server also comes with additional software utilities that help maintain the operating product.

The server offers two kinds of benefits to the network:

- It gives the users of its attached interactive devices (for example, terminals and dial-in modems) access to **services** (such as applications programs) offered by other network nodes, known as **service nodes**.
- It offers its own services, called **local services** (for example, printers), to its own users and to users of other terminal servers and systems on the network.

The DECserver 500 and 550 support up to 128 asynchronous devices (up to 32 asynchronous devices for DECserver 510) with EIA-422-A or EIA-423-A data-leads-only communications or 64 asynchronous devices (16 for DECserver 510) with EIA-232-D with modem control. Depending on your configuration, the DECserver 550 terminal server supports either 32 or 64 (8 or 16 for the DECserver 510) 3270-series terminals, allowing each 3270 terminal to emulate a Digital VT220 terminal and access services on the LAN. It also supports mixed configurations of CXM04, CXA16 and CXY08. The server logically connects these devices to the LAN, allowing each device to communicate with the other nodes on that LAN.

The server handles communications over a single Ethernet interface rather than over multiple interfaces at nodes throughout the network.

The server is designed for use on a LAN, which serves a relatively small area, such as an office building or a college campus. The server provides transparent data paths between devices on its ports and other network nodes. The other nodes are computers or other terminal servers on the network that offer resources, or **services**, to the network.

Each server user can maintain up to eight simultaneous connections, or **sessions** per port, to these various services. However, the DECserver 550 or the upgraded DECserver 500 can handle a maximum of 512 simultaneous sessions. The DECserver 510 can handle a maximum of 128 simultaneous sessions.

Response time and throughput are similar to those for terminals directly connected to a computer system. The server also permits properly configured computer systems on the network to share access to asynchronous printers attached to the server's ports.

The server runs a Local Area Transport (LAT) protocol. Nodes that run LAT software and that support the LAT protocol are called **LAT nodes**. LAT nodes can be service nodes, servers, and servers that also perform as service nodes. See the *Local Area Transport (LAT) Network Concepts* manual for a discussion of LAT networks, of LAT software, and of the DECnet Maintenance Operations Protocol (MOP).

1.1.1 Models

Several models of the DECserver 500 series terminal servers are currently available. The rack-mount models are installed in a standard 19-inch equipment rack, while the office models come in a cabinet on castors. Here are the currently available models:

Hardware Component	Order Code
DECserver 500 Rack-Mount Model	
120 Vac	DSRVS-AA
240 Vac	DSRVS-AB
DECserver 500 Office Model	
120 Vac	DSRVS-BA
240 Vac	DSRVS-BB
DECserver 510	
120 Vac	DSRVN-AA
240 Vac	DSRVN-AA
DECserver 550 Rack-Mount Model	
120 Vac	DSRVS-CA
240 Vac	DSRVS-CB
DECserver 550 Office Model	
120 Vac	DSRVS-DA
240 Vac	DSRVS-DB

1.1.2 Line Cards

A **line card** is a hardware module that fits into a physical **slot** on the server hardware. The DECserver 500 and 550 server hardware can have up to ten line cards in any combination, but only eight line cards can be active at the same time. Two slots are initially reserved for standby line cards that can be swapped with active line cards. The server hardware comes with these line cards, in a variety of combinations. The DECserver 510 server hardware can have up to two CXM04 line cards with no other combinations.

Line Card	Description
CXA16	A 16-line, data-leads-only line card that supports EIA-423-A communications. Can be used for locally connected terminals, printers, and PCs up to 1000 feet away. Supports up to 16 devices.
CXB16	A 16-line, data-leads-only line card that supports EIA-422-A communications. Can be used for locally connected terminals, printers, and PCs up to 4000 feet away. Supports up to 16 devices.
CXY08	An 8-line card with modem control that supports EIA-232-D communications. Connects modem signaling equipment and foreign hosts to the server. Can be used for terminals, printers, and PCs. Supports up to 8 devices.

Line Card	Description
CXM04	<p>(DECserver 510 and 550 terminal server models only) The 3270 Terminal Option card. Allows 3270-class terminals to be connected to host systems on an Ethernet LAN (VT mode) or to their IBM CCU (3270 mode). Can be configured so that four 3270 terminals can switch between the two modes of operation. Can also be configured so that eight 3270 terminals operate in VT mode only.</p>

The server provides device support through the use of its **line cards**. Servers with a CXY08 line card have modem control available, which you may enable on a per port basis, or you may choose to make all the associated ports function as data-leads-only ports.

1.2 Server Concepts

The following concepts explain some of the many features and functions of the server.

1.2.1 Operating Modes

The server has two modes of operation: local mode and service mode.

1.2.1.1 Local Mode

In local mode, an interactive user enters server commands to communicate directly with the server. Local mode is distinguished by the server's local mode prompt that appears on the port user's device display. Local> is the default prompt displayed unless you change the prompt to something other than Local> with the SET/DEFINE SERVER PROMPT command.

Here is an example of a command entered in local mode:

```
Local> SHOW PORT CHARACTERISTICS
```

1.2.1.2 Service Mode

In service mode, an interactive user communicates with a service in an active session. The server does not interpret data entered by the user. This data, rather, is passed to the service node.

To the user, it appears that he or she is connected directly to the service node. The user sees the prompt of the operating system or application program, for example, \$, for a VMS service.

Service mode commands are typically those of the service node's operating system. For example, a user in service mode with a VMS service could enter any DCL command, such as:

```
$ DIRECTORY/DATE/SIZE/OUTPUT=DIR.TEMP BOOK.TXT
```

User input is not necessarily a command. If the service is a dial-out modem, for instance, the user might initially enter a phone number to reach a remote dial-in modem.

1.2.2 Server Databases

Each server has a permanent, operational, and log-in database. These databases contain the values for characteristics that the server needs to operate. You can specify values for:

- Port characteristics for each port
- Server characteristics

- Service characteristics for local services
- Device characteristics

1.2.2.1 Permanent Database

The permanent database is part of the server's image file, which resides in the special server directory on each of the server's load hosts. The permanent database values are permanent in that they overwrite the values in the operational database each time the server is reloaded.

The generic server image, with a default value for each characteristic, is one of the server distribution files. During the installation procedures, the software installer uses the distribution image file to create a unique image for your server. This image also has all default values. The load host knows this file as the server's **load file**.

You define, or customize, values in the permanent database by running the Terminal Server Configurator (TSC) utility, or the optional Terminal Server Manager (TSM) utility, on a load host. You change values with **DEFINE PORT**, **DEFINE SERVER**, **DEFINE SERVICE**, and **DEFINE DEVICE** commands. See Section 6.1.2 for a complete discussion of TSC. Refer to the *Guide to TSM* for complete information on TSM.

When one of the load hosts down-line loads the image to the server, the permanent database values immediately replace the parameters in the current operational database on the running server. This occurs each time you initialize the server.

1.2.2.2 Operational Database

The operational database resides on the running server in dynamic memory. The operational database values are temporary in that they are overwritten by the values in the permanent database each time the server is reloaded. The values for the port, server, and service characteristics in the operational database determine how the server functions.

Use server **SET PORT**, **SET SERVER**, **SET DEVICE**, and **SET SERVICE** commands to modify values in the operational database. These changes remain in effect until you modify the values again with additional **SET** commands or until the server requests a down-line load. This happens if you initiate a down-line load, but it also happens automatically if the server experiences failure.

To have your changes in the operational database remain after a down-line load, duplicate them in the permanent database. Preferably, make changes that you intend to be permanent only once — in the permanent database. This avoids duplication of your efforts.

The **SET PORT** command changes the port characteristics in the operational database. However, the port values that you and other server users specify with **SET PORT** commands affect the operational database only until logout from the server or other disconnection:

- **Local-access ports**

For local-access ports, interactive users can make some of these changes. The new values remain in effect only while the port is logged in to the server. At logout, these changes are lost unless you save them (see the discussion in the next section on the log-in database).

- **Remote-access ports**

For remote-access ports, only you can make these changes. The new values stay in effect only during the remote-access session. When the session terminates, these changes are lost unless you save them (see the discussion in the next section on the log-in database).

Before the port logs out (or before the session at the remote-access port terminates), you can issue **SAVE PORT** commands in order to retain port values specified with **SET PORT** commands.

1.2.2.3 Log-In Database

The log-in database resides in dynamic memory on the server. It stores the operational port characteristics.

For local-access ports, the server copies these characteristics to the operational database at port logout, and they become the operational port characteristics starting with the next login. For remote-access ports, the server copies the new values to the operational database whenever a remote-access session terminates.

To retain new port values in the log-in database, follow these steps:

1. Both you and the nonprivileged user can enter SET PORT commands to modify the current port characteristics.
2. You execute the privileged SAVE PORT command to copy those port characteristics to the log-in database.

Without your using SAVE PORT, the values last down-line loaded from the permanent database stay in the log-in database and go back into effect as soon as the user logs out.

The port values in the log-in database remain in effect until the next time the server initializes, unless you duplicate the particular SET PORT commands in the permanent database with their equivalent DEFINE PORT commands.

Note

Other databases are on the server. For example, the directory of available services is a database located elsewhere in dynamic memory.

1.2.2.4 Changing Values in the Operational Database Versus Changing Values in the Permanent Database

The differences between changing values in the operational database and changing values in the permanent database are as follows:

- Making changes to the operational database is faster because they are made on the server at the local mode prompt rather than on a load host. In contrast, making changes to the permanent database requires that you:
 - Log in to your privileged account on a load host.
 - Run TSC or the optional TSM and make your changes.
 - Ensure that all the other load hosts have the new image file.
 - Instruct the current users to end their sessions and log out of the server.
 - Reload the server.

- Your changes to the operational database immediately affect the server's operations. The changes you make to the permanent database, however, take effect only after you down-line load.
- Your changes in the operational database are only temporary. That is, they remain in effect only until the next time the server is reloaded. In contrast, your changes to the permanent database remain in effect regardless of how often the server is loaded. (The only way to modify values in the permanent database is by issuing TSC or TSM DEFINE commands.)

1.2.3 Log-In Load Balancing

When two or more service nodes offer the same service, the server provides log-in load balancing. **Log-in load balancing** is a function that spreads the user load evenly among those service nodes.

The server evaluates the service ratings that the service nodes include in multicast announcements of services. The server ensures that connections to services offered by multiple service nodes are handled in an efficient manner.

1.2.4 Automatic Failover

Automatic failover is a feature that operates when an active session is disconnected unexpectedly from the service due to a failure of the connection at the service node.

If a service node suddenly becomes unavailable, the server automatically searches the service's database for another service node that offers the same service. If the server finds one or more suitable nodes, it attempts to connect to the service on the node with the highest service rating. This process is **automatic failover**.

When used with a VAXcluster, automatic failover provides a flexible terminal connection to the VAXcluster service.

1.2.5 Groups

Establishing groups helps control the size of the databases of the service nodes and servers, controls access to services, and makes some of the information displays easier to read. If it suits your environment, you can also use groups as a security feature. See Section 5.3 for complete information.

The LAT network makes use of several kinds of groups:

- Groups you set up for your users
- Groups you set up for all network users
- Groups set up by other server managers
- Groups set up by the network manager
- Groups set up by nonprivileged users

These groups, called **service groups**, **authorized groups**, **current groups**, and **server groups**, are all related.

Group codes are the primary mechanism for logically subdividing LAT networks, and you should use group codes to manage a terminal server's node database. However, group code management on service nodes can be time-consuming because privileged accounts are required for each service node. Therefore, if a situation arises where there are more service nodes validated for a server than the server can accommodate, the server software initiates automatic node database management (see the following section).

1.2.6 Automatic Node Database Management

On large LAT networks it is possible to have more service nodes validated for a particular server (using group codes) than the server can accommodate, either in terms of node limits or in terms of memory constraints. If too many service nodes become validated for a server to handle, the server software provides automatic node database management until you can adjust groups codes.

Under certain conditions, automatic node database management attempts to purge obsolete nodes from the database when a user requests connection to a service that is unknown to the server. In this way, obsolete nodes are purged from the server database in order to make room for a requested service not present in the database. Obsolete nodes are any nodes in the server's database that are:

- Currently UNKNOWN (no longer multicasting)
- Currently UNREACHABLE (connections have failed)

- Currently REQUESTING (issuing print requests but not accepting connections)
- Currently REACHABLE but have never been connected to by any user on the terminal server

The server initiates the purging procedure when a terminal server user is in the AUTOCONNECT state and the reason for a connection failure is “service not known” or “node not known.” If the server has reached its node limit, the node database is scanned and all obsolete nodes removed.

Then, during a 30-second timer period, new service announcement multicast messages are accepted from valid nodes, allowing the node database to be repopulated. The AUTOCONNECT function, which retries connections every 30 seconds, tries to connect using the new node database.

At the end of 30 seconds, the node database and current port states are reexamined. If there are any ports still autoconnecting to an unknown service, and if the node limit has been reached again, another 30-second purge cycle begins.

The purge cycling continues until the outstanding connection request is satisfied or until the user ends the AUTOCONNECT process. Automatic purging may continue for several cycles before a user request is completed.

1.3 Port Devices

Device support means that the server can exchange data with the device in at least one of the device’s modes of operation. You can configure your server’s ports to use many types of devices.

Configuring ports is described in Chapter 7. See the *DECserver 500 Software Product Description* (SPD) for information about the specific devices that the server supports.

The hardware installer does not connect devices directly to the line cards. Instead, the installer either connects devices directly to the ports or connects devices remotely with modems. The connection method depends upon the type of line card and the type of device. See the appropriate DECserver 500 series hardware manual for details.

The server supports printers and connections to hosts with EIA-232-D or asynchronous communications. With the CXA16 and the CXB16 line cards, you can attach terminals and printers with DECconnect cables.

The server supports these types of devices:

- VT terminals, which allow interactive users to access both the server and the services of the LAN
- 3270 terminals, which allow interactive users to emulate VT220 terminals and to access both the server and the services of the LAN when the 3270 Terminal Option card is used
- Printers, which can be accessed by service nodes and by users of personal computers on LAT terminal servers
- Computers that do not have an Ethernet controller module (non-LAT hosts)
- Personal computers (in terminal-emulation or file-transfer mode), which allow users to access services and to transfer files on the LAN
- Modems (dial-in and dial-out), which allow the LAT network to communicate with remote devices

You can configure any port (except port 0) for terminals, printers, or personal computers. The port and the attached device must implement the same type of communications standard, whether EIA-423-A (DECconnect), EIA-422-A, or EIA-232-D.

You can configure any EIA-232-D port to offer a computer terminal interface line as a local service. You can also configure the EIA-232-D ports to offer dial-out modems as local services. To offer a device as a service, you must first assign the port to a local service.

You must configure a port to match the characteristics of the device on that port. The server supports several data-signaling speeds and split-speed operation. See Section 7.2 for details.

The autobaud feature provides automatic detection of the data signaling speed of ports. Section 8.1.3 discusses the autobaud feature. Flow control options enhance the possibilities of configuring a port to the special needs of the attached devices. See Sections 5.7 and 8.1.4 for details on flow control.

1.3.1 Port Speeds

The distribution software supports the following port speeds (in bits per second) for all types of line cards: 50, 75, 110, 134.5, 150, 300, 600, 1200, 1800, 2000, 2400, 4800, 7200, 9600, 19200, and 38400.

1.3.2 Port Access

Using a server with a variety of devices and applications requires that you specify appropriate access for each port. The type of access required for a specific device depends on its intended application. For example, you might want to configure ports for:

- An interactive function that requires local access
- An applications function that requires remote access
- Alternation between local access and remote access

A session to a port currently used for remote-access is known as a “remote session.”

You can configure a port for any of these types of access or specify no access. See Chapter 7 for an explanation of configuring ports for each possible application and Section 8.1 for information about access types.

1.3.3 Terminals

With local access, a server supports terminals that request services. The terminal can be physically attached to a port or connected to a dial-in modem that is attached to the port.

When configured for an interactive terminal, a port offers access to server commands, dedicated connections, and simultaneous sessions. The *DECserver 500 Use* manual is for users of local-access ports.

1.3.3.1 Access to Server Commands

By default, terminals can access local mode, where the user enters server commands. After starting a session, the user can return to local mode at any time by pressing either the BREAK key or a user-defined switch character. Returning to local mode during a session leaves the session intact but in an inactive state. See Section 2.1 for a discussion of server commands.

1.3.3.2 Dedicated Connections

You can configure a port so that the attached device appears to users to be hard-wired to a specific service. This configuration means dedicating the port to a single service, which is called a **dedicated service**. A port with a dedicated service is called a **dedicated port**.

For a dedicated port, the server establishes only a single session for that port. A dedicated port cannot enter local mode, although you can define log-in and service passwords for the users of a dedicated port. See Sections 5.4.5.1, 7.5, and 8.1.2 for information about dedicated ports.

1.3.3.3 Multiple Sessions

By default, the server supports four simultaneous sessions for a local-access port. You can modify the session limit. For information, see Sections 5.4.5.5, 5.12.6, 8.1.2, and 8.2.2.

1.3.3.4 Session Management Terminals (TD/SMP)

Port users can enable a port characteristic that lets the server communicate with a **session management terminal** using the Terminal Device/Session Management Protocol (TD/SMP). Session management terminals can have more than one interaction, or **terminal session**, with the server, but each terminal session can have only one service session. With session management terminals, TD/SMP maintains the context of a service session when the user switches to another service session. Session data from a service node continues even though the service session is currently inactive. For terminals that do not implement TD/SMP, the server suspends service session data until the user resumes the session.

With session management enabled for a port, the server commands available to the port user have restrictions that do not exist when session management is disabled. For a description of these differences, refer to Section 5.4.2 of this manual or to the *DECserver 500 Use* manual.

1.3.3.5 3270 Terminals

The **3270 Terminal Option card (CXM04)**, a Q-bus option card for the DECserver 510 and 550 terminal servers, provides a means for **IBM 3270 Information Display System terminals** (or Personal Computers that emulate 3270 terminals) to connect to systems on an Ethernet through an Ethernet controller in the DECserver 510 or 550 hardware. This mode of operation is known as **VT mode**. To applications on an Ethernet system, the 3270 terminal appears to be a VT220 terminal. In **3270 mode**, the 3270 terminal can access applications on an **IBM Cluster Control Unit (CCU)** connected to the line card.

The 3270 terminal can operate in VT mode or 3270 mode. You can configure the CXM04 and its associated ports so that the terminal has the capability of switching back and forth between the two modes. In this configuration, the user switches between the two modes by pressing the ALT, then SHIFT keys or, in some cases, an alternate **hot-key sequence**. However, you can also configure a port to restrict a terminal to one mode of operation.

In VT mode, the firmware on the CXM04 emulates a VT220 terminal. To the server, the 3270 terminal appears to be a VT220 terminal. The server's local mode prompt is displayed. From the local mode prompt, the 3270 terminal user can connect to LAT services as a user would from a VT220 terminal.

In 3270 mode, the terminal and the CCU are hard-wired together and communicate directly through the CXM04. The 3270 terminal behaves exactly as if it were connected directly to the CCU.

Note

The term "3270 terminal" refers to the family of 3270 Information Display System terminals that operate in **Control Unit Terminal (CUT) mode**. This term also applies to personal computers that emulate the 3270 terminal in CUT mode.

For information about configuring CXM04 ports for 3270 terminal users, refer to Section 5.13.

1.3.4 Printers

The server can support asynchronous printers, such as the Digital LA120, LN01, and LN03. You can configure both nonkeyboard and keyboard printers. Note that a server can also support printer-like devices, such as plotters. Printers on a server can be accessed in several ways:

- By host-initiated requests from properly configured service nodes
- By establishing a dedicated session with one service node
- By requests from personal computers on servers, if the server offers the printer as a service

It is important that you enable `SIGNAL CHECK` for ports with printers attached. Without `SIGNAL CHECK` enabled, data loss can occur when a printer is powered off. See Section 8.1.7 for details on `SIGNAL CHECK`.

The port configuration for a printer depends on how it is accessed (see Sections 7.7, 7.8, 7.14, and 8.1.1).

1.3.4.1 Host-Initiated Requests

Some service nodes can access a printer by the name of the server port to which the printer is attached. This kind of connection request is called a **host-initiated request**.

If you also assign the printer to a local service, the service node can access the printer by the name of that service.

There are advantages to assigning a local service to the printer. For example, with queuing set up for the service, the time required to connect host-initiated requests to the printer might be shortened and the probability of getting an available printer is higher. In addition, a print job goes to one of two (or more) ports that you assigned to the service without the requesting service node needing to know which ports offer the printer (see Section 1.4).

Section 5.9 discusses how to manage ports used for host-initiated requests.

1.3.4.2 Dedicated Printers

For a service node whose operating system does not contain the LAT V5.1 protocol software, it is still possible for a server to initiate connections between a printer and a service node. Using local-access ports, you can dedicate printers to a single service. This configuration allows a service node offering a dedicated service to maintain a long-term session with a printer.

If you use this method, printers cannot be shared among service nodes. Also, setting up a print queue on the service node is more difficult than on nodes that support LAT V5.1.

1.3.4.3 Printers Accessed by Personal Computers

If a printer on a remote-access port is offered as a service, a personal computer (PC) with a suitable applications program can send printer output in a session. A personal computer on a server can connect to the printer service and temporarily use the printer.

Such applications programs must be supplied by the users of personal computers.

1.3.5 Computers

Using remote-access ports, the server can offer computer systems, including some non-Digital systems, as services. These systems, which do not implement the LAT protocol, are called **non-LAT hosts**.

Acting as a service node, the server provides the service software and the Ethernet interface for computers that do not provide that function. The server provides a logical path to those computers from the users requesting the system as a service. A port on a CXY08 line card and the computer can both use modem control to signal the establishment and the termination of sessions. This is an important security feature.

See Sections 7.9 and 5.6 for information about non-LAT hosts and modem control.

1.3.6 Personal Computers

The server supports file transfers in a session between a personal computer on a local-access port and any compatible computer whose resources are offered as a service. The personal computer user's other sessions are unaffected. A user can move easily back and forth between terminal-emulation and file-transfer functions. See Section 5.11 for information about managing file transfers.

With an appropriate applications program, a personal computer can also use a printer offered as a service by the server. On a remote-access or dynamic-access port, a personal computer can be assigned to a local service and can carry out file transfers with other personal computers.

1.3.7 Modems

The modem control feature of the server requires a CXY08 line card. You can use any of the CXY08's associated ports with full-duplex asynchronous modems. The modem control sequences conform to the EIA-232-D and CCITT V.24 standards. See the *DECserver 500 Introduction* for a list of the modems supported by the DECserver 500 series servers.

A modem connection can be to a leased line or to a private line. The server supports modems that receive calls (dial-in modems), modems that send calls (dial-out modems), and modems that alternate between receiving and sending calls (dial-in/dial-out modems).

You can use a modem on a port set to dynamic access, but dial-in modems are generally used with local access, and dial-out modems are generally used with remote access. However, port access actually operates independently of the direction of a modem, and alternative configurations are possible.

Any autoanswer or autodial modem can be offered as a service on ports set for remote or dynamic access. For example, a dial-in modem might be on a remote-access port to allow users to dial in to a service node after the service node establishes a session with the remote-access port. The session provides a means for a remote modem user to dial in to an applications program running on the service node.

Users connect to a modem offered as a local service by requesting a connection to the service name.

When you are actively managing a modem, it is considered a **local modem**. While a local modem is communicating with another modem, the other modem is considered a **remote modem**. The physical location of the remote modem is irrelevant. It can be on a server, or it can be connected to a terminal or to another device.

See Section 5.6 for information about modem control and Sections 7.10, 7.11, and 7.12 for instructions on configuring ports for modems.

1.4 Offering Printers As Services

The server permits service nodes that support LAT V5.1 to make requests for printers on remote-access server ports. These nodes, configured for host-initiated requests, can access a printer by the name of the server port to which the printer is attached.

If you assign the printer to a local service, the service node can request access to the printer by specifying the name of that service.

These requests are called **host-initiated requests** because they are generated by service nodes that are general-purpose computers (for users of the service node).

Service node users need not know that the printer is on a server. These users might be connected to the node in a server session or might be on a terminal that is physically connected to the service node.

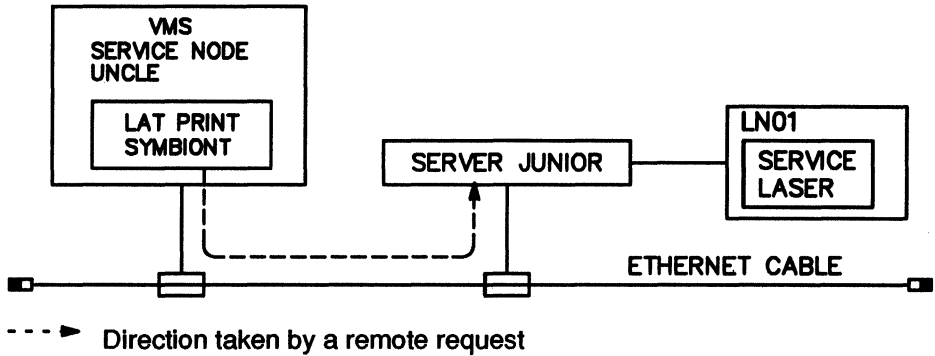
When a service node requires the use of a remote printer, the node multicasts a request for information about the node offering the printer to the LAN. Then, the server transmits a status-of-port message for the port offering the printer.

If the service node acknowledges this message, the server does one of the following:

- Creates a session between the printer and the service node if the port is not busy
- Queues the host-initiated request until a port is free that can satisfy the request

Figure 1–1 illustrates the path of a host-initiated request from the VMS service node UNCLE to the server JUNIOR for the service LASER.

Figure 1-1: The Path of a Host-Initiated Request



LKG-0351-87

A connection established for a host-initiated request is a regular LAT session. For information about handling host-initiated requests by a service node, see the documentation for the operating system of the service node. Check the appropriate *DECserver 500 Software Product Description (SPD)* to see which operating systems support host-initiated connections.

1.4.1 Requirements for Offering Printers As Services

Each host-initiated request is targeted for a printer on a particular server port or for a local service consisting of one or more printers on the server. The printers must be asynchronous, EIA-232-D printers with one of these flow control protocols:

- XON/XOFF
- DSR/DTR
- CTS/RTS

With DECconnect wiring, the printer must support XON/XOFF flow control.

See Section 5.8 on setting up and managing local services, and Sections 7.7 and 7.8 for relevant port configuration information.

1.4.2 Advantages of Offering Printers As Services

Host-initiated requests have these advantages:

- Service node users need not be on terminals connected to servers in order to establish a host-initiated request, increasing access to printers.
- Printers can be shared by all suitably configured service nodes, also increasing access to printers.
- The server, rather than the various service nodes, is responsible for processing host-initiated requests, thus reducing a service node's overhead for connection management.
- If you assign a group of ports to a service so that host-initiated requests can solicit connections by service name, the probability of the requester getting a printer port without being queued is increased.

See Section 5.9 for information about managing ports used for host-initiated requests.

1.5 Queuing

The server maintains a single, internal queue, called the **connection queue**. The queue stores connection requests for a printer or service offered by the server when that printer or service is busy. A connection request can be one of the following:

- A host-initiated request from a service node
- A request made with the server **CONNECT** command from interactive users on other servers that support queued connection requests

Only terminal servers offer queuing. Service nodes that are not terminal servers cannot queue connection requests.

The connection queue, a first-in-first-out (FIFO) queue, has no special priorities. The server begins every search of the queue with the earliest entry (the entry that has currently been queued for the longest period of time). The server examines the queue until it finds the first entry that can be satisfied by a newly available port where the printer or service is offered.

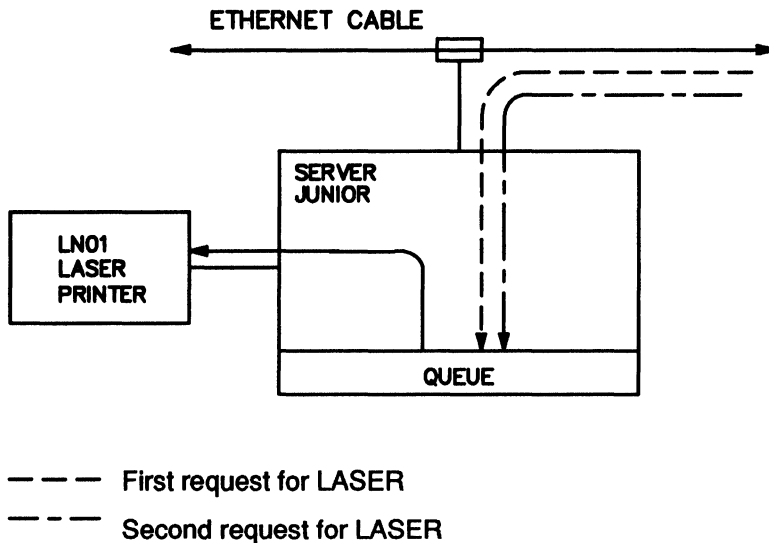
By queuing connection requests, the server can offer fair access to its printers or services when it receives overlapping requests. If queuing is enabled for the service or printer, the server can accept a connection request and place it in the queue behind all existing entries for that printer or service. Thus, the server can temporarily postpone making a connection until the proper resources become available. The server sends messages about queued connection requests to the port user or service node that makes the request.

If you disable the queue and a connection request cannot be immediately processed at any port, the request is refused. The server transmits a message with the reason for the connection failure to the requesting service node or port user.

The server that sends the port connection requests must be configured to exchange queuing messages with the server that offers queuing. You accomplish this by enabling the port characteristic `QUEUING` for the ports that require queuing.

Figure 1-2 shows the server processing two host-initiated requests for the same service. The first request for the service `LASER` is connected immediately. The second request for the same service is queued by the server while the service is still in use.

Figure 1-2: Server Processing Two Host-Initiated Requests for the Same Service

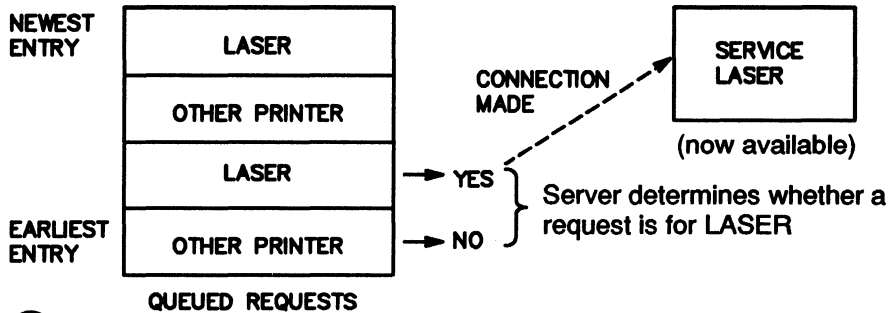


LKG-1012-88
REV. 0

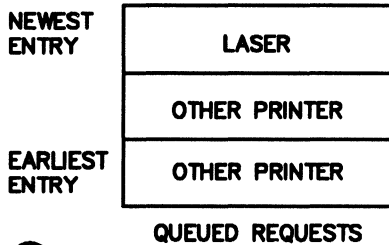
The server **dequeues** the earliest request for the port in question. After dequeuing an entry, the server attempts to establish a connection between its port and the service node or server that initiated the queued request. This connection is established by an automated version of the procedure used for any connection requested by a server user.

A service node or server that makes a connection request may be no longer reachable on the network when its request is dequeued. In this case, the server that processes the request does not make the connection. The service node or the port user on the server must resubmit the connection request. Figure 1-3 shows the server processing the queue.

Figure 1-3: Server Processing the Queue After Service/Port Becomes Available



① Queued request when printer becomes available



② Queued requests after next connection is made

LKG-0353-88

See Section 5.10 for information about managing the connection queue.

1.6 Security Features

The server has several security features: security status, passwords, modem control, and DSRlogout. As server manager, you control security by assigning each user to a particular status class, creating passwords, defining modem control, and enabling DSRlogout and limited view of server information.

1.6.1 Security Status

There are three levels of security status:

- Secure status (most limited)
- Nonprivileged status
- Privileged status (most privileged)

See Section 2.7.1 for information about security status.

1.6.2 Passwords

The server uses five types of passwords:

- Maintenance password (relates to the DECnet service password)
- Privileged password
- Log-in password
- Service passwords (for local services)
- Lock passwords

Except for the lock password, you define these passwords for various security situations. The maintenance and privileged passwords protect your server from users performing unauthorized management operations. The log-in password ensures that unauthorized people do not use the server. Service passwords ensure that unauthorized people do not use the server's local services.

For a discussion of passwords, see Sections 2.7.2 and 4.7, 5.1, 5.4.5.2, 5.8.5, and 6.1.1.1. For information about using lock passwords, see the *DECserver 500 Use manual*.

1.6.3 Limited View

As a security feature, you can use the PORT characteristic **LIMITED VIEW** to prohibit users from executing **SHOW NODES** and **SHOW SERVICES** commands.

1.6.4 Modem Control with Non-LAT Hosts

The server can offer a non-LAT host as a service. Security for a port with this kind of service requires the use of modem control for communications between the server port and the non-LAT host.

Modem control ensures that disconnected sessions are terminated at both ends of the connection. See Section 5.6 for a discussion of how modems improve security.

1.6.5 DSRLogout

If modem control is not enabled at a port, you can use DSRlogout as a security feature. DSRlogout terminates all sessions at the port when the port device is powered off. Sections 2.7.4 and 5.6.6.1 discuss DSRlogout.

1.7 Down-Line Loading from Load Hosts

The server gets its operational software by a process called **down-line loading**.

1.7.1 The Server Image

The operational software is contained in the **server image**. The server image has executable code and the server's permanent database. This image file and several other distribution files make up the **software distribution kit**.

The DECserver 500 series terminal server hardware is delivered without its image. Without this software, the server hardware can run only its ROM-based diagnostics.

1.7.2 The Need for Down-Line Loading

The server image file always resides on the load host, but the server does not support any storage devices. As a result, the server relies on load hosts to down-line load its image. A **load host** is a system that has the server image, several related files for customizing this image, and a node database with entries for specific servers. See Section 6.5 for a definition and discussion of the load host's node database.

A load host can down-line load the server image to the server and can receive up-line dumps from it. Load hosts must be DECnet Phase IV systems on the same Ethernet as the server and must have an operating system that is supported by the server. These operating systems are listed in the *DECserver 500 Software Product Description (SPD)* and the *DECserver 500 Software Installation* manual.

1.7.3 Assigning Load Hosts

- Digital advises the network manager to assign:
- For each server, a minimum of two load hosts
- One load host for every ten servers on a network

Sections 5.2.2 and 8.2.3 explain how the server uses primary load hosts and backup load hosts for down-line loading and up-line dumping.

The *DECserver 500 Software Installation* manual discusses the assignment of load hosts.

1.8 A Summary of the Server Installation

The server **installation** is fully explained in the *DECserver 500 Software Installation* manual and, depending on your server hardware, in the appropriate DECserver hardware installation manual. This summary outlines the server installation:

1. Hardware installation and first part of verification
2. Server distribution software installation on at least one load host
3. Load host installation verification
4. System installation verification

It is helpful to your understanding of the server and of your server management tasks to know a little about the server's combined hardware and software installation. Here are some details:

1. The software installer, usually the load host system manager, installs the server **distribution files** onto the load host.
2. The system manager configures the load host's node database to include the new servers.
3. The hardware installer installs the hardware and powers it up. The server automatically runs its **diagnostic self-test**. The self-test verifies the **hardware installation**. The server requests a down-line load from any load host.

4. A load host down-line loads the server's image with all default values to the server.
5. The load host system manager verifies that his or her system can down-line load the server. He or she reloads the server with the DECnet NCP LOAD command. This procedure is the **software installation verification** and the **load host installation verification**.
6. The load host system manager executes a few selected server commands on the server to make sure that the proper software was down-line loaded and is running. This procedure is **system installation verification**.
7. The hardware installer tells you that the hardware is installed and tested.
8. The software installer informs you that the software is installed, the load host's node database is configured, the system installation verification steps are complete, and your server system is fully functional.

1.9 Using Server Management Tools

The distribution software provides you with several server management tools. These tools help you with both the initial management tasks and your day-to-day management tasks. Some of these tools are on the server and some of them reside on the load host, where you use them.

See Chapter 2 for a description of all the server management tools.

1.10 Performing Server Management Tasks

As server manager, your responsibilities consist of initial management tasks and day-to-day management tasks, some of which overlap.

Your tasks as a server manager begin after server installation. Digital suggests that you begin to manage your server by learning how the hardware and software installers install a server and by understanding the status of your server when system installation is finished. See Chapter 3 for a walk-through of your initial tasks as server manager.

Your day-to-day management tasks are the routine things you do to maintain the server. See Chapter 4 for an introduction to these tasks. For complete conceptual and procedural information about routine server management tasks, see Chapters 5 and 6.

Introducing Server Management Tools

This chapter introduces the server management tools, a combination of server features and load host features. These tools are as follows:

- **Server commands** — Used on the running server
- **Terminal Server Configurator (TSC) commands** — Used on a load host
- **Load host configuration procedure (DSVCONFIG)** — Used on a load host
- **Remote Console Facility (RCF)** — Used on a load host or other DECnet node
- **Physical console port** — Used on the server
- **Privileged port** — Used on the server
- **Security features** — Used on the server and on a load host
- **Server on-line Help** — Used on the server
- **TSC on-line Help** — Used on a load host
- **Information displays** — Used on the server and on a load host
- **Troubleshooting features** — Used on the server and on a load host
- **The Terminal Server Manager (TSM) (optional software)** — Used on appropriately configured VMS load hosts

The server management tools on your server are described in detail in this section. For additional discussion of the tools that you use on the load host, see Chapter 6.

2.1 Server Commands

The server commands help you manage the server and its ports. You use these commands to specify values for every server characteristic that determines how the server operates. When you want to change or to view these values in the server's operational database, use server commands.

To change values in the operational database, you issue SET commands. These commands immediately affect the server but do not affect the server's permanent database. (You change the permanent database on the load host with TSC commands.)

The server commands and the TSC commands have a common command syntax described fully in the *Terminal Server Commands and Messages* manual. See Section 2.2 for an introduction to TSC as a management tool and Section 6.1.2 for a detailed discussion of TSC.

You execute server commands at the server's local mode prompt at a terminal connected to a server port.

2.1.1 Users of Server Commands

In addition to being a management tool, many server commands are also available to all server users. General users issue server commands to connect to LAT services, display status information, set characteristics for their terminal, and control a few port functions.

Since server commands are for both the server manager and other server users, each server command has a particular security level: privileged, nonprivileged, or secure. See Section 2.7.1 for a discussion of security levels.

2.1.2 Overview of Server Commands

This section outlines the server commands. While many examples in this manual illustrate the exact command syntax, use the *Terminal Server Commands and Messages* manual for complete syntax information on all the server commands, keywords, valid ranges of values, and defaults.

Each server command begins with a descriptive verb. These verbs and their meanings are:

- **BACKWARDS** — Resumes the session preceding your current session in the session list
- **BROADCAST** — Sends a message to one or more server ports
- **CLEAR SERVICES** — Deletes specified local services from the operational database
- **CONNECT** — Connects your port to a service
- **CRASH** — Shuts down the server, up-line dumps a copy of server memory, and then reinitializes the server
- **DISCONNECT** — Disconnects one or more sessions on your port
- **FORWARDS** — Resumes the session following your current session in the session list
- **HELP** — Displays the server on-line documentation
- **INITIALIZE** — Reloads the server software after a 1-minute delay
- **INITIALIZE DELAY** — Reloads the server software after a specified period of time
- **INITIALIZE CANCEL** — Cancels a delayed initialization that has not yet begun
- **INITIALIZE DIAGNOSE** — Starts diagnostic testing of the ROM program and then reloads the server software
- **LOCK** — Locks your terminal from unauthorized use while you are temporarily absent
- **LOGOUT** — Logs out one or more ports from the server
- **MONITOR** — Produces continuously updated information displays from the operational database

- **MOVE DEVICE** — Redirects line card operation from an active line card to a standby line card
- **REMOVE QUEUE** — Removes entries from the server queue of host-initiated requests
- **RESUME** — Resumes either the current session or a specified session
- **SAVE PORT** — Retains the current port characteristics after logout
- **SET** — Modifies values in the operational database
- **SET PRIVILEGED** — Sets the port you are using to privileged status so that you can enter privileged commands
- **SET NOPRIVILEGED** — Resets the port you are using to previous status so that nonprivileged users cannot enter privileged commands at that port
- **SHOW** — Displays information in the operational database
- **TEST LOOP** — Tests the physical connections between your server and another Ethernet node on the network
- **TEST PORT** — Sends a test pattern to a port on the server, loopback optional
- **TEST SERVICE** — Tests communications between the server and a service node
- **ZERO COUNTERS** — Resets the specified counters to zero

Of all these commands, the ones you probably use most often as server manager are **SET** and **SHOW**. The **SET** command syntax consists of the following parts:

- The verb **SET**
- A keyword that names the component to modify, for example, **PORT**, **SERVER**, or **SERVICE**
- Parameters, known as **characteristics**, associated with the component, for example, **AUTHORIZED GROUPS**, **PASSWORD**, or **IDENTIFICATION** (Chapter 8 describes all the characteristics.)

- Values for the characteristics, for example, **AUTHORIZED GROUPS 6-19, PASSWORD PLANET, IDENTIFICATION ENABLED**

The following example illustrates a typical SET command:

```
Local> SET PORT 8 AUTHORIZED GROUPS 1,2,6-19,25 ENABLED SESSION LIMIT 3
```

This example contains these parts:

- The verb is **SET**.
- The component is **PORT 8**.
- The characteristics are **AUTHORIZED GROUPS** and **SESSION LIMIT**.
- The values for **AUTHORIZED GROUPS** are **1, 2, 6-19, 25** and **ENABLED**. The value for **SESSION LIMIT** is **3**.

The keywords for the components you can modify are:

- **DEVICE** — Modifies the state of a line card or changes the **DUMP** option for a **CXM04** line card
- **PORT** — Modifies port characteristics, for example, data-signaling speed and character size
- **SERVER** — Modifies operating characteristics, for example, the server's name and identification
- **SERVICE** — Creates or modifies services offered by the server
- **SESSION** — Modifies the amount of data transparency during a particular session

The **SHOW** command syntax consists of the verb **SHOW**, a keyword that specifies the component about which you want information, and a display type, for example:

```
Local> SHOW PORTS ALL SUMMARY
```

The keywords for the components about which you can request information are:

- **DEVICES** — Displays the server's hardware configuration and some diagnostic counters

- **NODES** — Displays information about LAT service nodes, including the server if it offers local services
- **QUEUE** — Displays entries in the queue of host-initiated requests
- **PORTS** — Displays information for ports, including the current characteristics set by users with the nonprivileged SET PORT commands
- **SERVER** — Displays information about the server, including the values set by you with the SET SERVER command
- **SERVICES** — Displays information about services available on the network, both services from other nodes and local services offered by the server
- **SESSIONS** — Displays information about the current sessions
- **USERS** — Displays information about the current users

The MONITOR command is a special version of the SHOW command. You can produce displays for the same components with MONITOR as with SHOW. The difference is that SHOW generates a single display of the values in effect when you issue the command and MONITOR generates a display that is continuously updated on your screen until you either press the BREAK key or enter `CTRL/O`.

See Chapter 9 of this manual and the *Terminal Server Commands and Messages* manual for more information on the SHOW and MONITOR commands.

2.2 The Terminal Server Configurator (TSC)

The Terminal Server Configurator (TSC) utility is another tool that helps you manage the server. As with server commands, you use TSC commands to specify the values for every server characteristic that controls the server. When you want to enter these values in the server's permanent database, use TSC. In addition, TSC commands display status information.

TSC is software that resides on your server's load hosts. See Section 6.1.2 for complete details on using TSC.

2.3 The Load Host Configuration Procedure (DSVCONFIG)

Another tool for managing your server is a configuration command procedure called DSVCONFIG. Use it to reconfigure, when required, your load hosts' node databases. The load host's node database comprises three separate databases, each of which contains an entry for your server. The entry provides information that DECnet software needs to down-line load to your server and up-line dump from it.

Use this management tool if:

- You are installing the distribution software for one or more new servers. You probably have this responsibility if you are also the system manager of one of the assigned load hosts. See the *DECserver 500 Software Installation* manual for the appropriate operating system.
- The network manager asks you to change your server's DECnet node name or DECnet node address.
- Your server hardware is replaced by another server. (Even if you use the same DECnet node name and DECnet node address for the new server, its Ethernet address is different.)
- Your server hardware is replaced with another kind of Digital terminal server.
- The network manager assigns a new load host and asks you to configure that system to perform load-host functions.
- You delete or the system manager accidentally deletes your server's image file and there is not another identical one on another load host to copy.

The DSVCONFIG command procedure is software that resides on your server's load hosts. See Section 6.5 for complete information about DSVCONFIG and how to use it to configure the node database of your server's load hosts. Section 6.5 also describes the three databases of the load host's node database.

2.4 The Remote Console Facility (RCF)

While you are away from your server and any interactive terminal, you might need to log in to the server. Using a management tool called the Remote Console Facility (RCF), you can remotely connect to any server. RCF establishes a logical connection between a terminal on a DECnet node and the management port on the server hardware. This is the same management port as physical port 0, which is also called the console port.

RCF is a tool provided on most DECnet nodes on your LAN, including your server's load hosts. Here is a typical sequence of events you perform at a load host for which RCF is a helpful tool:

1. You run TSC and change a few values in the server's permanent database.
2. You ensure that all the load hosts have the updated image file.
3. You warn current server users that they must log out for 5 minutes with the server INITIALIZE or BROADCAST command: connect to your server using RCF and log in. All the server commands are available to you (with one or two exceptions) including BROADCAST and INITIALIZE.
4. You down-line load the new values in the database with the NCP LOAD NODE command (if you did not use INITIALIZE).

See Section 6.4 for a full discussion on how to use RCF.

2.5 The Console Port (Management Port)

The server hardware unit has a physical console port, which is located on the handle of the CPU module (see the appropriate hardware installation manual for a description and illustration). The console port is port 0 and is exclusively a management tool. This is also the port RCF connects you to when you establish remote management sessions.

Use the console port for help with troubleshooting. You can execute variations of the server diagnostic self-test to help solve hardware-based problems. In addition, this port displays the 900-series of server messages. While the other server messages can be received at any port, only the console port displays the 900 series. These maintenance messages concern down-line loading, fatal errors, and up-line dumping.

The 900-series messages are important during server initialization. If the server passes self-test, the messages show you the status of the server and the down-line loading process.

Ensure that the device attached to the console port can display the 900-series messages. The console port is designed for interactive devices; connect a terminal or a keyboard printer to the port connector (see the appropriate hardware installation manual). The *Terminal Server Commands and Messages* manual lists and explains the 900-series messages.

Port 0 has a few restrictions:

- It can have only local access. You cannot set up the port to remote access or dynamic access and offer a printer, non-LAT host, or any other device as a service.
- Several of its default values are fixed. You cannot modify these port 0 characteristics:
 - ACCESS
 - AUTHORIZED GROUPS
 - AUTOBAUD
 - CHARACTER SIZE
 - DEDICATED
 - DIALUP
 - DSRLOGOUT
 - DTRWAIT
 - FLOW CONTROL
 - GROUPS
 - INPUT SPEED
 - MODEM CONTROL
 - MULTISESSIONS

- OUTPUT SPEED
- PARITY
- SIGNAL CHECK
- SPEED

See the *DECserver 500 Problem Solving* manual for information about using the console port for troubleshooting.

2.6 The Privileged Port

The privileged port is not one, designated, physical port. To the contrary, any user who knows the privileged password can issue the `SET PRIVILEGED` command at any interactive terminal to make it a privileged port. Digital strongly recommends, therefore, that you do not reveal the privileged password to any other users.

Use a privileged port to enter commands to manage the server, in particular, the privileged commands. However, at the privileged port, you can issue all the server commands — privileged, nonprivileged, and secure.

You cannot, however, execute TSC commands (all privileged commands) at the privileged port or at any port of the server hardware unit. Enter TSC commands on a load host (see Section 6.1.2). In addition, you cannot define a port as permanently privileged.

More than one port at a time can be privileged, but if you are the only user who knows the privileged password, there never will be two existing privileged ports if you reset your terminal to nonprivileged when you have finished issuing privileged commands.

Note

When you have finished using privileged commands, or when you leave your terminal, it is important to use `SET NOPRIVILEGED` to return the port to nonprivileged status. You can also log out from the server at this port to reset the port to nonprivileged status.

2.7 Server Security Features

The server has several security features to use as management tools. These features include:

- User security levels
- Passwords
- Modem control
- DSRlogout
- Limited view

As server manager, you control security by assigning each user to a particular security level, creating passwords, enabling/disabling modem control, enabling/disabling DSR logout, and restricting SHOW command information from specified ports.

2.7.1 Security Levels for Server Ports

Choosing security levels for server ports is one tool that helps you manage the server. With this feature, you can limit the use of server commands, in particular, the privileged SET commands that change the operational database.

The server has three levels of security: privileged, nonprivileged, and secure. Usually, this is how you decide on privilege levels for users:

- Server managers can use all server commands including privileged commands.
- Most users can use only nonprivileged commands.
- Users you want to restrict are limited to secure commands.

By default, ports are nonprivileged. Only you or a backup manager, if your server has one, should modify the security status of a port. The three levels of status and how to set them are:

- **Privileged Status**

Lets a port accept all server commands — privileged, nonprivileged, and secure. Privileged status is the only level that allows access to the SET commands that manage the server, its ports, and its services. You set a port to privileged status with the SET PRIVILEGED command (see Sections 3.2 and 5.1).

With the privileged commands, you can:

- Configure ports
- Establish privilege levels for ports
- Customize the operational database
- Establish and manage local services
- Perform tests
- Observe the status of the server, its ports, and the LAT network environment

- **Nonprivileged Status**

Rejects most SET commands and any other command that changes the state of the server.

A port with nonprivileged status has access to all the nonprivileged commands required for accessing and using services, and to a few SET PORT commands. Nonprivileged status also allows access to some SHOW commands. In addition, this status also permits users to use some restricted server features such as broadcasting to other ports. Nonprivileged status is the default.

A user at a nonprivileged port can:

- Establish characteristics for the port
- Obtain a display of available services
- Establish sessions with services

- Switch between sessions
- Display many characteristics of the port and its sessions
- **Secure Status**

Restricts the commands that are available on a port to a subset of the nonprivileged commands. This subset contains only commands that are required for accessing and using services from a particular port and for specifying some port characteristics of that port. For example, secure users can use `SHOW PORT` only for their own port, and they can change only a few port characteristics.

Secure status is useful for isolating port users from the activities of the server and other users. For example, the `SHOW SERVER` command and the broadcast feature are unavailable on secure ports. See Section 5.4.5.3 for a list of secure server commands.

You can define a port as `secure` with the `SET/DEFINE PORT SECURITY ENABLED` command. In addition, you can restrict the `SHOW` command information available to a port by enabling the port characteristic `LIMITED VIEW`. See Sections 2.7.5 and 5.1.7 for information about these security features.

2.7.2 Passwords

The server system uses five types of passwords:

- Privileged password
- Log-in password
- Maintenance password
- Service passwords
- Lock passwords

These passwords are an important management tool. They help you control the server's use and protect the server, its operational database, and the users' efforts.

Except for the lock password, which is a general user tool, the commands that set passwords are privileged and are your responsibility.

2.7.2.1 Privileged Password

The privileged password prevents the misuse of commands designed for server management.

You can change the privileged password in both the operational and permanent databases. If you need to change it quickly, and you decide therefore to do it in the operational database (see Section 5.1.1), repeat the change as soon as possible in the permanent database (see Section 6.1.1.1).

2.7.2.2 Log-In Password

The log-in password prevents unauthorized use of the server. If you enable the log-in password, any potential user trying to log in to the server is prompted for the log-in password. Only if the user correctly specifies the log-in password, does the server complete the log-in sequence.

You can define a log-in password and then enable it on any local-access port. A single log-in password is used for the whole server, although you enable it on a port-by-port basis.

This password is most likely to be useful when you wish to reserve access to public terminals. A log-in password is also highly recommended on ports connected to modems used for dial-in.

You can change the log-in password in both the operational and permanent databases. If you need to change it quickly and you decide therefore to do it in the operational database (see Section 5.1.2), repeat the change as soon as possible in the permanent database (see Section 6.1.1.1).

2.7.2.3 Maintenance Password

The maintenance password prevents unauthorized access to the server by remote maintenance requests, for example the issuing of the `NCP LOAD` and `TRIGGER` commands. If you define a maintenance password in the server's permanent database, anyone, including you, at another node who tries to access the server by issuing a `LOAD` or `TRIGGER` command usually must include this password. See the discussion that follows for the exception to this condition.

Remote maintenance activities are usually performed by the DECnet NCP utility. A load host's DECnet database contains several facts about the server, including the DECnet service password. When you first create or the distribution software installer first creates the server entry in the DECnet database, the value for the DECnet service password is 0.

Note

The DECnet service password is not the same as a server's service password, which has a different purpose (see Section 2.7.2.4).

The server's default maintenance password is 0. A value of 0 means that the server does not check the DECnet service password with remote maintenance requests. Changing the maintenance password to anything other than 0, however, instructs the server to check that the DECnet service password in its permanent database and the maintenance password stored in the load host's DECnet database are identical before the server accepts any remote maintenance activity.

To illustrate, the following example initiates a down-line load from a VMS load host to a server with the DECnet node name ROBIN and with a maintenance password previously defined as FF44:

```
NCP>LOAD NODE ROBIN SERVICE PASSWORD FF44
```

The server checks the password. If the DECnet service password on the command line is absent, or if it differs from the maintenance password defined in the server's database, the server rejects the request. If the passwords are identical, the server accepts the request.

When you enter a command such as the one here and specify the SERVICE PASSWORD (FF44), you actually override the load host's existing DECnet service password value of 0. This allows the service password value to match the maintenance password value.

Even if you define a maintenance password in the server's permanent database for security reasons, as Digital recommends, there is still a way that someone could avoid the password specification with `LOAD` and `TRIGGER` commands. Specifying the password is not required if you have changed the DECnet service password from its default value of 0 in the load host's DECnet database to the same value as the maintenance password in the server's permanent database. In this case, they also match when the server checks a password.

Therefore, to maintain adequate security for the server, Digital strongly advises:

- In the server's permanent database, change the default value of 0 for the maintenance password. Define a new maintenance password.
- Do not store the new maintenance password in the load host's DECnet database.

2.7.2.4 Service Passwords

Service passwords protect the local services that you set up on your server from unauthorized access. You can assign a service-specific password to any local service. If you do, a user must correctly supply this password before the server connects his or her port to that service. When you define a service, there is no default service password.

The service password is particularly useful for unprotected devices such as modems used for dialing out. See Section 5.8.5 for details.

It is a good idea to define a service password for a service when you first establish the service. You can specify a service password for a service in both the operational and permanent databases. If you need to define it or change it quickly, and you decide therefore to do it in the operational database (see Section 5.1.4), repeat the change as soon as possible in the permanent database (see Section 6.1.1.1).

2.7.2.5 Lock Password

Any server user can specify a lock password to prevent unauthorized access to his or her port. The *DECserver 500 Use* manual explains the lock password.

2.7.3 Modem Control

Modem control is a feature that provides security for a non-LAT host that the server offers as a local service.

With modem control enabled on the server, during a session, the host receives a steady series of Data Set Ready (DSR) signals, indicating that the server is maintaining the connection. If the server disconnects from the host, the host detects a loss of DSR. The host can then respond by disconnecting the session at its own end.

In contrast, without the server using modem control, a session that is disconnected only at the server remains active at the host and is accessible by any user connecting to the host service. Therefore, when you use a server port with a non-LAT host, Digital highly recommends that you use the server's modem control features.

Note that other characteristics affect modem control and, after you enable it, modem control does not take effect immediately. Modem control and security for non-LAT hosts are discussed fully in Section 5.6.

2.7.4 DSRlogout

If modem control is not enabled at a port, you can use DSR logout as a security feature. DSRlogout terminates all sessions at the port when the port device is powered off. Without DSRlogout enabled for a port, the sessions at that port remain active when the user turns off his or her terminal. This situation allows another user to access those sessions by simply turning on the terminal again.

DSRlogout requires:

- A port device that sends DSR signals to the server when the device is powered up and drops the signals when powered down
- A device cable that lets the server receive DSR signals from that device
- That you enable the DSRLOGOUT port characteristic

2.7.5 Limited View

By enabling LIMITED [VIEW], you can restrict specified ports from access to the SHOW command information. As a security feature, LIMITED [VIEW] prohibits the user from executing SHOW NODES and SHOW SERVICES.

2.8 On-Line Help

The server offers three types of on-line Help:

Type of Help	Location
Tutorial Help	On the server
Reference Help	On the server
TSC Help	On a load host, part of TSC

2.8.1 Server On-Line Help

Tutorial Help is a brief introduction to using the server. Reference Help displays brief descriptions of the commands available for the current privilege level of the port. Users specify the command for which they want an explanation.

To access tutorial Help, enter one of these commands:

```
Enter username> HELP
```

OR

```
Local> HELP TUTORIAL
```

The server displays a series of screens of tutorial information, always beginning with the first screen. To proceed, follow these conventions:

- To request the next screen, press the RETURN key.
- To restart the tutorial Help at the first screen, enter ? and then press the RETURN key.
- To exit tutorial Help, press **CTRL/Z**.

For reference Help on server commands, enter HELP in response to the local mode prompt:

```
Local> HELP
```

The server responds with a list of command keywords available for the current privilege level of the port and prompts you again:

```
Topic?
```

Note that one of the options is TUTORIAL, which takes you into tutorial Help.

When you enter a command keyword from the list, for example, SHOW or SET, the server gives you a brief description of the function performed by that command and lists any subtopics associated with it. The server then prompts you for a subtopic. Here is an example from a nonprivileged port:

```
Topic? SET 
```

```
SET  
Use SET commands to change characteristics and options stored in the  
server's operational database.
```

```
SET {  
  PRIVILEGED  
  PORT  
  SESSION  
}
```

```
Additional HELP available for:
```

```
PORT          PRIVILEGED          SESSION
```

```
SET Subtopic? PORT 
```

The server lists all SET PORT options and prompts you again for a subtopic.

If you already know the option you want, you can skip these intermediate steps by typing it immediately. For example, to get information about specifying flow control, enter the following command:

```
Local> HELP SET PORT FLOW CONTROL
```

To redisplay the options you can enter in response to Topic?, enter:

```
Topic? ? 
```

Note

Help information employs the graphic conventions [] and { } to indicate command usage. Do not enter these graphic characters in your command lines. All graphic conventions are described in the Preface of this manual.

Alternatively, the server can always display an abbreviated on-line command summary of the DECserver 500 commands by executing the following TSC command:

```
TSC> DEFINE SERVER LIMITED HELP ENABLED
```

When LIMITED HELP is enabled, all help requests display this summary of all server commands.

2.8.2 TSC On-Line Help

On the load host, TSC has on-line Help for all TSC commands. For instructions on starting TSC, see the *DECserver 500 Software Installation* manual for the operating system of the load host at which you will run the program. For information about using TSC to customize the server's permanent database, see Section 6.1.2 of this manual.

To invoke Help for TSC commands, type:

```
TSC> HELP
```

TSC responds with a list of command keywords for which information is available and prompts you again:

```
Topic?
```

The TSC HELP conventions are the same as the ones on the server (see the previous section).

2.9 Information Displays

The server provides many displays that contain information about the server and its ports, the port devices, local and network services, service nodes, the connection queue, sessions, and users. TSC also gives you many information displays. Use these displays at any time to determine values and to make decisions about any new values to define with SET or DEFINE commands.

The server SHOW command displays information in the operational database. The TSC LIST command displays information in the permanent database.

These are some examples of **SHOW** and **LIST** commands to display database information:

```
Local> SHOW DEVICES ALL SUMMARY
```

```
Local> SHOW NODE PEACH COUNTERS
```

```
TSC> LIST USAGE
```

```
TSC> LIST PORT 1 SUMMARY
```

See Chapter 9 for every display command, illustrations of the displays, a discussion of each display, and an explanation of what relationships to look for among the display fields.

2.10 Troubleshooting Features

The server and its load hosts provide features that help you troubleshoot problems affecting the server and the attached devices.

On the server, these features include:

- A **TEST LOOP** command, which tests the physical connections between your server and another Ethernet node on the network
- A **TEST PORT** command, which tests whether ports and their attached devices are operating correctly
- A **TEST SERVICE** command, which can be used to test access to services offered by the server
- The diagnostic self-test program and other ROM-based services
- The **CRASH** command (see Section 6.3)

On load hosts, these troubleshooting features are:

- The **NCP LOOP CIRCUIT** command
- **RCF**
- **TSM**

A complete description of server troubleshooting tools is presented in the *DECserver 500 Problem Solving* manual.

2.11 Terminal Server Manager (TSM)

The Terminal Server Manager (TSM) is an optional software product that helps you remotely monitor and control multiple servers on an extended LAN. TSM runs on suitably configured DECnet VMS Phase IV nodes.

TSM incorporates all the functions of TSC, including the TSC command set. In addition, with TSM you can make changes remotely to the operational database from a centralized site.

Contact your Digital sales representative for information about the operating systems that currently support TSM.

2.12 Keyboard Mapping Commands

The keyboard mapping commands are pertinent only to the DECserver 510 or DECserver 550 on systems with CXM04 line cards installed.

Keyboard mapping commands allow the terminal server manager to tailor the standard keyboard tables by changing the mapping of individual 3270-keyboard keys to Digital VT220 keys.

The keyboard mapping commands are described in detail in Section 6.6 and in *Terminal Server Commands and Messages*.

Identifying and Performing Initial Management Tasks

This chapter describes your first tasks in managing a new server. The main purpose of Chapter 3 is to walk you through the procedures in the appropriate order.

Some of the initial tasks you perform at the server, while others you perform at one of the server's load hosts. As discussed in Chapter 2, both the server and the load host offer management tools to help you.

After the hardware and software are installed and verified, you can assume management of the server. Your initial management tasks are:

- Coordinating your tasks with other people concerned with network operations
- Establishing server security by defining passwords on the running server
- Finding out which systems the network manager designated as load hosts for your server
- Customizing the server image on a load host using TSC
- Ensuring that all the other assigned load hosts for your server have the new image file
- Down-line loading the customized image

The distribution software installer will tell you when your system is fully installed and verified.

3.1 Coordinating Your Tasks with Others

Your role as server manager requires that you coordinate some of your tasks with other people who are also involved with network management:

- The network manager
- The load host system manager
- The software installer
- The hardware installer

3.2 Establishing Server Security

This section presents the actual commands you issue to establish initial security. For a full explanation of the security features, see Section 2.7. For the commands that help you maintain day-to-day security on the running server, see Section 5.1.

To begin managing your server, you need to have privileged status so that you can issue the privileged commands, including the ones that change the passwords from the defaults.

Define passwords as part of establishing server security. At server installation, all the passwords have default values, which are printed in the *Terminal Server Commands and Messages* manual. Follow these steps at an interactive terminal connected to one of the server's ports:

1. Give your port privileged status using the current (default) privileged password:

```
Local> SET PRIVILEGED
Password> SYSTEM (not echoed)
Local>
```

Note

When you leave your terminal or when you have finished issuing privileged commands, remember to enter the **SET NOPRIVILEGED** command to return the port to nonprivileged status:

```
Local> SET NOPRIVILEGED
```

2. Set a new value for the privileged password.

So that other users cannot use privileged commands, enter the **SET SERVER PRIVILEGED PASSWORD** command. The password can be up to 16 characters long. Here is an example changing the password to **PLANET**:

```
Local> SET SERVER PRIVILEGED PASSWORD
Password> PLANET (not echoed)
Verification> PLANET (not echoed)
Local>
```

3. Set a new value for the log-in password from the default, **ACCESS**, and enable the log-in password, as desired. The password is disabled for all ports by default. The log-in password can be up to 16 characters long. The following example changes the password to **CHICKADEE**:

```
Local> SET SERVER LOGIN PASSWORD
Password> CHICKADEE (not echoed)
Verification> CHICKADEE (not echoed)
Local>
```

4. Enable the log-in password either for all ports or for selected ports as needed (the default is **PORTS ALL DISABLED**):

```
Local> SET PORTS ALL PASSWORD ENABLED
```

or

```
Local> SET PORT n PASSWORD ENABLED
```

5. Save the **PASSWORD ENABLED** setting in the log-in database:

```
Local> SAVE PORTS ALL
```

or

```
Local> SAVE PORT n
```

6. Inform the appropriate users of the new log-in password.

You have now changed these passwords only in the operational database. When you customize the permanent database, repeat these changes (see Section 6.1.1.1). If a down-line load occurs before you repeat these modifications in the permanent database with TSC DEFINE commands, the default passwords overwrite the ones you just specified.

7. Make a record of your passwords.

Note

If you forget the passwords you defined, you can change them again on the server, as long as you remember the privileged password for the SET PRIVILEGED command to make your terminal privileged. You are not prompted for an old password when you specify a new one.

If you do not remember the privileged password you defined, you can always change passwords or reset the defaults in the permanent database (see Section 6.1.1.1).

3.3 Determining Your Server's Load Hosts

The network manager assigns load hosts when a server is delivered and its distribution software is installed. It is usually the manager of the load host system who performs the software installation. The following procedure starts where the software installer's ends:

1. Ask the network manager for the names (and operating systems) of the systems that he or she assigned to be load hosts for your server. You can identify at least one load host with this server command:

```
Local> SHOW SERVER STATUS
```

2. Ask the network manager for the names of the system managers of these load hosts.
3. Contact the system managers to find out if they, indeed, are the software installers and if the complete software installation procedures, as described in the *DECserver 500 Software Installation* manual, are finished.

After these procedures, each server has its software image residing on the load host. In addition, servers have received an initial down-line load of their image and are fully operational.

4. Ask the load host system managers for a copy of the *DECserver 500 Release Notes*, if they printed the release notes file during the software installation, as described in the *DECserver 500 Software Installation* manual.
5. Get the name of the server directory and all the files related to the server that are now in that directory. If the load hosts are different operating systems, the directory names and the names of some of the files are different.

This information is in the *DECserver 500 Software Installation* manual for the operating system of the load host. You can also ask the load host system managers.

Note

If they still have the *DECserver 500 Software Installation* manual, ask them for it and return it to the documentation binder.

6. If the software installer did not print the release notes file, print the file now and read the *DECserver 500 Release Notes*. When you are finished with them, it is a good idea to store these release notes in the documentation binder.
7. Discuss getting the appropriate privileges with the load host system managers. For most load hosts, you need privileges to perform server management tasks on these systems. The programs, procedures, and commands that you use on load hosts to manage your server are:
 - TSC
 - NCP LOAD and NCP TRIGGER commands
 - RCF
 - DSVCONFIG
 - TSM (optional software for VMS load hosts)

3.4 Customizing the Server Image on a Load Host Using TSC

After setting new passwords for your running server and after getting the necessary privileges, customize the server image on the load host if you want to change any default values and have them remain in effect after down-line loads. You can modify the server image extensively or keep most of the default values for the port, server, and service characteristics. These values make up the permanent database.

Note

For the CXM04 line card to run, you must use TSC to predefine the CXM04 line card type (see Section 5.13.6).

See Section 1.2.2.4 for a discussion of the differences between changing values in the operational database and changing values in the permanent database.

3.4.1 Operating with All Default Values

This is the default situation immediately after system installation and verification are complete:

- Your server is operational:
 - It is set up for up to 128 interactive users, depending on the number and type of line cards it has.
 - It can communicate with up to 100 nodes.
 - Each port can maintain up to four sessions.
 - It can operate with any combination of valid line cards.
- The values in the operational and log-in databases are the same as those in the permanent database.
- All server, port, and service characteristics have default values. Your server has not yet been customized for your particular environment.
- Server passwords also have default values.

- The security status for all ports is nonprivileged.
- The log-in and privileged passwords are available to anyone who has a copy of the *Terminal Server Commands and Messages* manual. In addition, all the privileged commands are described in that manual.

Although your server is fully operational, its ports are limited to one function — supporting interactive terminals. The server needs to be customized and fine-tuned if you want to use many of its features.

3.4.2 Changing the Defaults to Customize Your Server

Customizing the server image consists of:

1. Determining the use of each port on the server. The server supports these types of devices:
 - Terminals
 - Printers
 - Computers that do not have an Ethernet controller module (non-LAT hosts)
 - Personal computers (in terminal-emulation or in file-transfer mode)
 - Modems (dial-in and dial-out)

All DECserver 500 series hardware installation manuals discuss connecting devices to the server ports.

You can configure any server port, except for port 0, for terminals, printers, or personal computers. Port 0 is reserved for use as a management port. See Chapter 7 for descriptions and examples of the port configurations you can choose.

2. Deciding what characteristics to modify.

After the hardware and software installations, when you take over as server manager, you should know what line cards are in the server and what cables are in the various ports. This information helps you determine the characteristics to modify.

The hardware installer can tell you what line cards and cables have been installed.

Make a list of the port, server, and service characteristics you want to change from the defaults and what new values you will define. All DEFINE commands change the permanent database. The Preface can help you identify the chapters with the information you need.

3. Logging in to a load host, entering TSC, and opening a server image file. Section 6.1.2 of this manual explains how to use TSC. The *DECserver 500 Software Installation* manual for each load host operating system tells you how to start TSC on that operating system.
4. Defining the passwords in the server image to match those you set on the server (see Section 6.1.1.1).
5. Defining any other characteristics to suit your particular network environment. Identifying and performing initial management tasks.
6. Exiting TSC.

3.5 Ensuring That All Load Hosts Have the Same Server Image

All of your server's load hosts, both primary and backup, should have the latest version of the server image. The name of each server image is stored in the load host's server configuration database and is known there as the server's "load file."

The server can initialize and request a down-line load in several ways. Unless you use the NCP LOAD command method, you have no way of knowing beforehand which load host will actually load your server. Therefore, to ensure that the server is always loaded with the latest values that you defined in the permanent database, all the load hosts need the same version of the load file.

To ensure that all your server's load hosts have the newest image file, put all your TSC DEFINE commands into a TSC command file. Copy the command file to the various load hosts and then run it again at each load host to update the server image.

Digital recommends this command file method of ensuring that all load hosts have the same version of the server image because:

- It makes customizing easier to repeat.
- It makes upgrading to a new version easier.

- It protects your efforts in case the software image becomes corrupted or is deleted by mistake, and you need to reissue the same TSC commands.

See Section 6.1.2.6 for information about TSC command files.

3.6 Down-Line Loading the Customized Server Image

After you ensure that all the load hosts also have the server image file that you customized with TSC, down-line load the customized server image to the server. The new values are loaded into the operational and log-in databases.

You can initiate a down-line load from three locations: your server's hardware, a terminal connected to one of the server's ports, or a load host. Section 5.2 discusses all the ways to down-line load and shows how to initiate a down-line load from the server. Section 6.2 describes how to load your server from a load host.

To request a down-line load from your server, you can do either of the following:

- Reset by pressing the boot switch on the server hardware.
- At a privileged port, issue:

```
Local> INITIALIZE DELAY 7  
Local -199- WARNING - Server shutdown in 7 minutes
```

The server displays the warning at each logged in port.

See Section 6.1.2.7 for information about upgrading the customized server image.

Introducing Day-to-Day Management Tasks

This chapter outlines your routine tasks as manager of a server. The main purpose of Chapter 4 is to help you understand the scope of your responsibilities and the type of information you need to make the appropriate decisions.

Use this chapter as an orientation, and then see Chapter 5, “Performing Day-To-Day Management Tasks,” for details on both concepts and procedures. In addition, see Chapter 6, “Performing Server Management Tasks on the Load Host,” for instructions on server management tasks that you do at a load host.

Here is a list of your day-to-day tasks as a server manager:

- Coordinating your tasks with the network manager and your tasks on the load host with the load host system manager
- Customizing the operational database as needed
- Customizing the log-in database as needed
- Recustomizing the server image on a load host as needed, ensuring that all the other assigned load hosts for your server have the new image, and down-line loading the new image
- Verifying that all the ports are operational
- Maintaining server security with passwords
- Reconfiguring the load hosts’ node databases as needed

- Monitoring the status and utilization of the server, the port devices, some service nodes, and the Ethernet
- Helping users with questions or problems
- Troubleshooting the server unit and its port devices as needed

4.1 Coordinating Your Tasks with the Load Host System Manager and Others

As discussed in Section 3.3, on most load hosts you need an account with special privileges to perform your server management tasks. Discuss getting the appropriate privileges with the load host system managers.

Because you are managing a network node, you also need to coordinate some of your tasks with the network manager. Your server's users can connect to many other service nodes on the network. In addition, your server also acts as a service node when you set up local services. See Section 5.12 for considerations that concern your management of a server as part of the LAT network.

4.2 Customizing the Operational Database

The operational database contains temporary values you define with SET commands. These changes are called "temporary" because they are lost whenever the server is reloaded. When a down-line load occurs, the values in the permanent database — both the ones you defined with DEFINE commands and any existing default values that you did not change — replace the temporary values in the operational database.

See Section 1.2.2.4 for a discussion of the differences between changing values in the operational database and changing values in the permanent database.

The task of customizing the operational database consists of:

- Deciding if, when, and how to reconfigure the ports and what characteristics to modify
- Changing temporary port characteristics

- Changing temporary server characteristics
- Changing temporary local service characteristics

Actually, you have already changed the server's operational database with the initial management task of setting new passwords. All SET commands change the operational database. These chapters can help you when you are changing values in the operational database:

- See Chapter 5 for detailed information about using server commands to modify the server's characteristics and use its features efficiently.
- See Chapter 7 for examples of the characteristics to modify, depending on how a port is to be used.
- See Chapter 8 for a description of all the characteristics.
- See Chapter 9 for an illustration and description of all the information displays.

In addition, see the *Terminal Server Commands and Messages* manual for this information:

- For each characteristic, the default and valid range of values
- Complete syntax information about the SET command
- The privilege level of each command option

4.3 Customizing the Log-In Database

Customize the log-in database with the SET PORT command and save your customized database with the SAVE PORT command. The log-in database stores the operational port values in effect when the port logs in (or a remote-access session is established) and any new port values changed with SET PORT commands and then saved with SAVE PORT commands. See Section 1.2.2.3 for a definition of the log-in database.

While new port values in the log-in database do not persist through reloading, the server can retain them after the port logs out. For local-access ports, these new port values are copied to the operational database when a user logs out, and they become the operational port characteristics. For remote-access ports, they are copied to the operational database whenever a remote-access session terminates.

Nonprivileged users cannot change values in the log-in database. They can use SET PORT commands to modify some of their port characteristics, or they might ask you to do it for them. However, they lose their changes as soon as they log out (or hang up) without the SAVE PORT command.

To change values in the log-in database:

1. You or nonprivileged users can make changes with SET PORT commands.
2. You must issue the SAVE PORT command to store the new port values in the log-in database.

You can save most port changes in the log-in database. However, SAVE PORT does not save privileged status or locked status. See the *Terminal Server Commands and Messages* manual for the syntax of the SAVE PORT command.

4.4 Customizing the Server Image

Change the server image on a load host as needed, and then ensure that all the other assigned load hosts for your server have the new image (see Section 6.1.2.9). All DEFINE commands change the permanent database. Section 6.2 can help you when you are changing values in the permanent database.

To have these changes take effect, you must reload the server with the updated image.

4.5 Down-Line Loading the Customized Server Image

Whenever you customize the server's image using TSC, you need to down-line load the new image to the server. After you down-line load, the server immediately copies the new values to its operational and log-in databases. Server users, both at locally connected devices and on remote systems and servers, can then use the server in the environment you have provided.

Section 5.2 discusses and compares all the methods you can use to initiate a down-line load. The same section also gives you procedural information about initiating a down-line load from the server. Section 6.2 explains the procedures that you can use to initiate a down-line load from a load host.

4.6 Verifying That the Ports Are Operational

Immediately after a down-line load, it is a good idea to issue the `SHOW DEVICES ALL` command to verify that the ports are operational, especially if you made a change to the server's image with the `DEFINE DEVICE` command (see Section 8.4).

If you made an error defining a device, the server checks, recognizes the error, renders nonoperational all the ports associated with that device, but does not automatically inform you of the problem. However, checking with the `SHOW DEVICES ALL` command (see Section 9.2.1) gives you status information for all the ports.

Look at the "Status" field of the `SHOW DEVICES ALL` display. If a port's status is "Wrg Typ," the port is not operating because the type of line card you specified with `DEFINE DEVICE` is not the actual type of line card in that slot. If a port's status is "Failed," there is a hardware problem (see the *DEC server 500 Problem Solving manual*).

Issuing `SHOW DEVICES` after a down-line load is a good idea even if you did not make changes with the `DEFINE DEVICE` command.

4.7 Maintaining Server Security with Passwords

Setting passwords to establish server security is one of the first server management tasks. In addition, you can change and clear passwords routinely to maintain server security. The commands that set passwords are all privileged commands, except for the one that specifies a lock password, a general user command.

Section 5.1 shows how to set and clear passwords on the running server. Section 6.1.1.1 provides the procedures for making these changes in the permanent database. For information about the reasons for using the server's passwords, see Section 2.7.2. In addition, Section 5.8.5 discusses unsuccessful attempts at entering service passwords.

4.8 Reconfiguring the Load Host's Node Database

Reconfigure the load host's node database for servers as needed. You modify the database by running an automated command procedure called DSVCONFIG.

Section 2.3 discusses the various reasons for reconfiguring the load host's node database. Section 6.5 explains how to use DSVCONFIG and defines the load host's node database.

4.9 Monitoring the Server

Day-to-day server management includes your monitoring of the status and use of the server, its port devices, the service nodes, and the Ethernet.

You can request many displays that help you monitor server operations. The server commands that generate these displays are SHOW and MONITOR. In addition, the TSC LIST command generates several displays that show you information about the server's permanent database.

See Chapter 9 for illustrations of the displays that give you status information and for the commands you use to generate these displays. See Chapters 5, 6, and 7 for guidelines on how to use the server.

4.10 Helping Server Users

The other server users might ask you for help with server commands and might call you when they have problems. In addition, you are the only user who can save new values for port characteristics through logins and logouts with the SAVE PORT command (see Section 4.3). For more information about helping users, see Section 5.4.

4.11 Troubleshooting the Server

When necessary, you will have to troubleshoot the server and its port devices. See the *DECserver 500 Problem Solving* manual for complete troubleshooting information and for a discussion of up-line dumping.

4.12 Keyboard Mapping Commands

The Terminal Server Configurator (TSC) general command `USE TABLE` establishes a particular keyboard mapping table as the TSC context and allows you to operate on the specified table.

For example:

```
$ RUN DS5CFG
```

```
Terminal Server Configurator - V3.0  
Copyright (c) Digital Equipment Corporation. 1989. All Rights Reserved.
```

```
Server image:
```

```
TSC> USE TABLE TEST:CXM$NORTH_AMERICAN.KEYS VARIANT A  
Version 1.0 keyboard table file last modified on 12-JUN-1989 14:58:08  
TSC> LIST USAGE
```

```
Current image is file: COREY.SYS  
DECserver 500, V2.0 (Database V9).  
Server image last changed on 29-MAY-1989 11:34:29 on PETS
```

```
Current table is file: TEST:CXM$NORTH_AMERICAN.KEYS  
122-KEY Keyboard  
Multinational Character Set  
Variant A
```

After you open the keyboard table with the `USE TABLE` command, you can execute TSC commands to view and customize keyboard mapping.

The 3270 Terminal Option software is shipped with standard keyboard tables for the most common languages. These tables contain translations of 3270 key scan codes to VT220 standard keys and escape sequences for different 3270 keyboard types.

Individual keys on the 87-key, 102-key, and 122-key 3270 keyboards are mapped to individual Digital VT220 keys. Mapping means that pressing a specific key on the 3270 keyboard generates a specific VT220 keyboard ASCII or escape sequence character.

Each 3270 key has a unique scan code. Scan codes may differ for the 87-key, 102-key, and 122-key keyboards. The keyboard table currently in use determines how the scan code for a specific 3270 key translates to a VT220 key.

Occasionally you may want to change the translation of certain keys to suit users' requirements. For this reason TSC enables you to modify keyboard mapping tables. Digital supplies two copies (variants) of each table. The STANDARD variant table contains the Digital-supplied default mappings for the table. You cannot modify this table. The VARIANT A tables are copies of the STANDARD tables, and are custom-modifiable. You can append this table to a server's image file using the PURGE LANGUAGE and DEFINE LANGUAGE commands. The next time the server is initialized, the modified table is available to all 3270 users connected to the server.

Table 4-1 lists and briefly describes the TSC keyboard mapping commands. For a detailed description of each command see Chapter 2 of the *Terminal Server Commands and Messages*.

Table 4-1: Summary of TSC Keyboard Mapping Commands

Command	Description
CLOSE TABLE	Closes the currently open mapping table,
DEFINE MAPPING	Changes the mapping of individual 3270 keys to VT220 keys.
LIST MAPPING	Displays keyboard mapping of all or individual keys in the current table.
LIST TABLES	Lists the keyboard tables in the current table file.
USE TABLE	Establishes that subsequent commands will use the specified keyboard table file and table within the file for keyboard mapping.

Note

Keyboard mapping tables are provided for use only with those systems that have CXM04 line cards installed.

Performing Day-to-Day Management Tasks

This chapter tells you how to carry out many of the day-to-day management tasks outlined in Chapter 4. Chapter 5 has details about specific tasks such as managing the server connection queue, managing host-initiated requests, and assigning groups. In addition, this chapter presents considerable background material on modem control, flow control, managing 3270 terminals on the CXM04 line card, and defining a standby line card. See Chapter 6 for details on the routine server management tasks that you perform on a load host.

Chapter 5 covers these server management tasks in detail:

- Maintaining server security
- Down-line loading the server image
- Making use of groups
- Managing local-access ports
- Managing sessions
- Setting up and managing modem control
- Managing flow control
- Managing your server as a service node (establishing local services)
- Managing ports used for host-initiated requests
- Managing the connection queue

- Managing file transfers
- Managing your server as part of the LAT network
- Managing 3270-class terminals on the CXM04 line card
- Defining a standby line card for swap capability

5.1 Maintaining Server Security with Passwords, Password-Related Characteristics, and Security-Related Characteristics

Routinely changing passwords helps maintain server security. This section shows how to set and clear passwords on the running server. For information about using the server's various passwords for server security, see Section 2.7.2.

The commands that set passwords are all privileged commands except for the one that specifies a lock password, a general user feature.

5.1.1 Setting the Privileged Password

To set the privileged password on the running server, use the **SET SERVER PRIVILEGED PASSWORD** command. For example, to change the privileged password to **PLANET**, enter:

```
Local> SET SERVER PRIVILEGED PASSWORD "PLANET"
```

OR

```
Local> SET SERVER PRIVILEGED PASSWORD
Password> PLANET (not echoed)
Verification> PLANET (not echoed)
Local>
```

You cannot clear the privileged password

- By specifying **NONE** or by typing a null string ("") on the command line. You get an error message.
- By specifying **NONE** or by typing a null string ("") at the **Password>** prompt. The password remains unchanged.

To reset the default **SYSTEM**, specify "**SYSTEM**" on the command line or **SYSTEM** at the **Password>** prompt.

5.1.2 Setting the Log-In Password

To set the log-in password on the running server, use the `SET SERVER LOGIN PASSWORD` command. For example, to change the log-in password to `CHICKADEE`, enter:

```
Local> SET SERVER LOGIN PASSWORD "CHICKADEE"  
Local>
```

or

```
Local> SET SERVER LOGIN PASSWORD  
Password> CHICKADEE          (not echoed)  
Verification> CHICKADEE     (not echoed)  
Local>
```

You cannot clear the log-in password

- By specifying `NONE` or by typing a null string ("") on the command line. You get an error message.
- By specifying `NONE` or by typing a null string ("") at the `Password>` prompt. The password remains unchanged.

To reset the default `ACCESS`, specify "`ACCESS`" on the command line or `ACCESS` at the `Password>` prompt.

Digital has two suggestions for keeping this security feature effective:

- Use discretion in deciding to whom you reveal the password.
- Change the password on a regular basis and inform the selected users of the new password.

5.1.3 Setting the Maintenance Password

The maintenance password cannot be set on the running server. You can define this password only in the permanent database on a load host, using `TSC` (see Section 6.1.1.1).

5.1.4 Setting and Clearing Service Passwords

To set a service password on the running server, issue the SET SERVICE command and specify the local service and its password. The following examples set the service password GUTENBERG for the local service LASER:

```
Local> SET SERVICE LASER PASSWORD "GUTENBERG"  
Local>
```

or

```
Local> SET SERVICE LASER PASSWORD  
Password> GUTENBERG (not echoed)  
Verification> GUTENBERG (not echoed)  
Local>
```

Unlike the privileged and log-in passwords, you can clear service passwords. To clear the password on the running server, you must enter the keywords PASSWORD NONE or PASSWORD "" on the command line, for example:

```
Local> SET SERVICE LASER PASSWORD NONE
```

or

```
Local> SET SERVICE LASER PASSWORD ""
```

Note that when you clear a service password, you remove it as a restriction for users who wish to connect to that local service.

5.1.5 Setting and Clearing a Lock Password

Any user can specify a lock password. The *DECserver 500 Use* manual explains how to set this password.

However, one routine management task exists for the lock password. If a user locks his or her terminal and then forgets the password to unlock it, the only way to return the terminal to normal is to issue the privileged LOGOUT PORT *n* command at another terminal, specifying that user's port as the target. If the user has any active sessions, they are all disconnected.

5.1.6 Setting Other Password-Related Characteristics

Some other password-related characteristics you might want to set are as follows:

- If you want to make the log-in password required at any port, enable it with the `SET PORT PASSWORD ENABLED` command. You can enable the password on one, all, or selected ports. The following example enables the log-in password for all ports:

```
Local> SET PORT ALL PASSWORD ENABLED
```

With the log-in password disabled for a port, the log-in sequence does not include a log-in password. However, if you enable this feature, the log-in sequence prompts users for the log-in password by displaying the pound sign (#) and sounding a beep signal. The user must then enter the correct log-in password to continue.

Save the `PASSWORD ENABLED` setting in the log-in database, for example:

```
Local> SAVE PORT ALL
```

- By default, the server limits a potential user to three attempts to specify correctly the log-in password, a service password, and the privileged password.

You can change the number of times that the server allows a person to specify incorrectly these passwords. Issue the `SET SERVER PASSWORD LIMIT` command and specify the number of tries permitted, for example:

```
Local> SET SERVER PASSWORD LIMIT 5
```

5.1.7 Setting Other Security-Related Characteristics

Part of maintaining server security is deciding what ports you need to make secure and then setting the secure privilege level for those ports. You can enable security on one, all, or selected ports. The following example enables security for ports 17 through 32, ports 49 through 64, and port 128:

```
Local> SET PORT 17-32,49-64,128 SECURITY ENABLED
```

In addition, you can restrict the `SHOW` command information available to the secure port. By enabling the port characteristic `LIMITED VIEW`, you prohibit a port from executing `SHOW NODES` and `SHOW SERVICES`. For example:

```
Local> SET PORT 17,18 LIMITED VIEW ENABLED
```

5.2 Down-Line Loading the Customized Server Image

This section explains down-line loading, compares the different ways you can do it, and discusses the procedures for initiating a down-line load from the server. Section 6.2 explains the procedures that you can use to initiate a down-line load from a load host or maintain a customized server image after you've installed new software.

Whenever you customize the server's image using TSC, you need to down-line load the new image to the server to make your changes operational. After the down-line load, the server immediately copies the new values to its operational and log-in databases. Server users, both at locally connected devices and on remote systems and servers, can then use the server in the environment you have provided.

5.2.1 The Initialization Process

Initialization is usually a two-part process. What happens in the first step determines if there is a second step. These two steps are:

1. The server runs its diagnostic self-test.
2. The server requests that its image be down-line loaded to it from a load host.

Powering up and resetting with the boot switch force the server to run its self-test before asking for a down-line load. In contrast, the following methods do not invoke the self-test: the INITIALIZE command, the NCP LOAD command, and the NCP TRIGGER command. For detailed information on resetting with the boot switch, see the *DECserver 500 Problem Solving* manual.

The initialization process is this sequence of events:

1. The server disconnects sessions to its remote-access ports 1 minute before shutdown. Those users receive the following disconnect message:

```
Local -222- Connection to service-name not established
Server shutdown in progress
```
2. The server runs its diagnostic self-test, if this is a power up or you pressed the boot switch.
3. The server requests a load of its image.

4. A load host down-line loads the server image to the server.
5. Control of the server is passed to the server software and the newly loaded image.

The server's LEDs give you the status of each of these steps as they occur.

5.2.2 The Different Ways to Initiate a Down-Line Load

You can initiate a down-line load in a number of ways:

- Issue the INITIALIZE command from the server.
- Reset the server by pressing the boot switch.
- Issue the NCP LOAD command from a load host.
- Issue the NCP TRIGGER command from a load host.

Each way works somewhat differently. The best method to use depends on your location, whether you want to ensure that a particular load host loads the server, and how many initialize options you want.

The following table lists the four methods and summarizes the advantages and disadvantages of each.

Table 5–1: Methods of Initiating a Down-Line Load

	Location	Delay Option	Automatic Warning	Cancel Option	Diagnostics Option
INITIALIZE	Local mode prompt	Yes	Yes	Yes	Yes
Reset with the boot switch	Hardware unit	No	No	No	No
LOAD*	Load host	No	No	No	No
TRIGGER	Load host	No	No	No	No

* You can specify the load host you want to down-line load.

5.2.2.1 How INITIALIZE Works

If you are at a terminal connected to the server or if you are connected to the server's management port with either RCF or TSM, the server's INITIALIZE command is a convenient way to load the server. This method has several options that give you the most control over the loading process, compared with the other down-line loading methods. With the INITIALIZE command, you can specify the elapsed time until the start of the down-line load, warn users, use special diagnostics, and cancel the request if necessary.

Note

You can use the DELAY and DIAGNOSE options of the INITIALIZE command at the same time. INITIALIZE CANCEL is described in the *Terminal Server Commands and Messages* manual as a separate command.

Here are the advantages of using the INITIALIZE command over resetting with the boot switch, issuing the NCP LOAD command, and issuing the NCP TRIGGER command:

- The INITIALIZE command with the DELAY option lets you delay down-line loading. The delay feature is important if your server currently has active sessions and offers local services. You can specify the time period of delay before the actual initialization so that users can properly disconnect their sessions and log out.

Even if you omit the DELAY option of INITIALIZE, the server delays the down-line load request for 1 minute by default.

- The INITIALIZE command automatically displays a shut-down warning at every logged-in port (see Note in Section 5.2.4.2).
- The INITIALIZE command with the DIAGNOSE option transfers control of the server to the Console Commands Interface (CCI) so that you can run additional diagnostic programs.

You can issue **INITIALIZE DIAGNOSE** at any port, but it is most convenient to use port 0. The command starts the power-up self-test and if the self-test completes successfully, the **Console >** prompt appears at port 0. At this prompt you can use special diagnostic commands to test the server hardware. The diagnostic tests reside in and execute from ROM. When you invoke these diagnostics, the server software is not running.

To terminate the diagnostics and reinitialize, issue:

```
Console > BOOT
```

For detailed information about CCI, see the *DECserver 500 Problem Solving manual*.

- The **INITIALIZE CANCEL** command lets you cancel a delayed initialization.
- Since **INITIALIZE** is a server command, you can conveniently issue it on the server at the local mode prompt. You do not have to go to a load host or start a session with one that is offered as a service.

This is how the server's **INITIALIZE** command works. It instructs the server to send a **MOP REQUEST PROGRAM** message to the primary host. The server waits about 90 seconds for a response. If the primary host does not respond, the server repeats this process with each load host in the backup host list. If none responds, the server finally multicasts the message to all DECnet load hosts on the same Ethernet.

The primary host is normally equivalent to the load host from which the server was last loaded. This is also usually the first load host in the backup list.

The backup load hosts are the DECnet node names of up to five backup load hosts if the primary load host fails to respond. The server tries the backup load hosts in the order you specified with the **DEFINE SERVER BACKUP HOSTS** command.

INITIALIZE does not ensure that a particular load host performs the down-line load, if there is more than one load host, as Digital recommends. With this method, you do not know beforehand which load host will actually down-line load the server image.

5.2.2.2 Resetting the Server by Pressing the Boot Switch

If you are at the server, pressing the boot switch is convenient, but this method is limited. It has no options and allows you no control of the initialization process, which starts immediately. Digital suggests that you press the boot switch only if you are sure that there are no current active users.

Note

There are two switches on the server hardware that you can use to initialize the server. You can use the power switch, which heavily taxes the power supply, or you can use the boot switch, which is not as demanding on the power supply. Digital strongly recommends that you use only the boot switch to initialize the server.

Pressing the boot switch has one advantage. Since you are at the server, you can observe the LED display on the CPU module. Several codes show the status of the loading process. The LEDs are helpful for troubleshooting. See the *DECserver 500 Problem Solving* manual for the meaning of each code.

This method of initiating a down-line load does not work the way the server's INITIALIZE command works. Pressing the boot switch instructs the server to multicast a MOP REQUEST PROGRAM message to all DECnet hosts on the server's Ethernet. This message requests a down-line load from any assigned load host.

This method does not ensure that a particular load host performs the down-line load, if there is more than one load host, as Digital recommends. With this method, you do not know beforehand which load host will actually down-line load the server image.

5.2.2.3 How NCP LOAD Works

You must issue the NCP LOAD and TRIGGER commands at a load host. These commands work differently. The advantage of the NCP LOAD command is that it ensures that the load host at which you issue the command is the node that performs the down-line load. Note that the down-line load, however, might be slower than with the TRIGGER command.

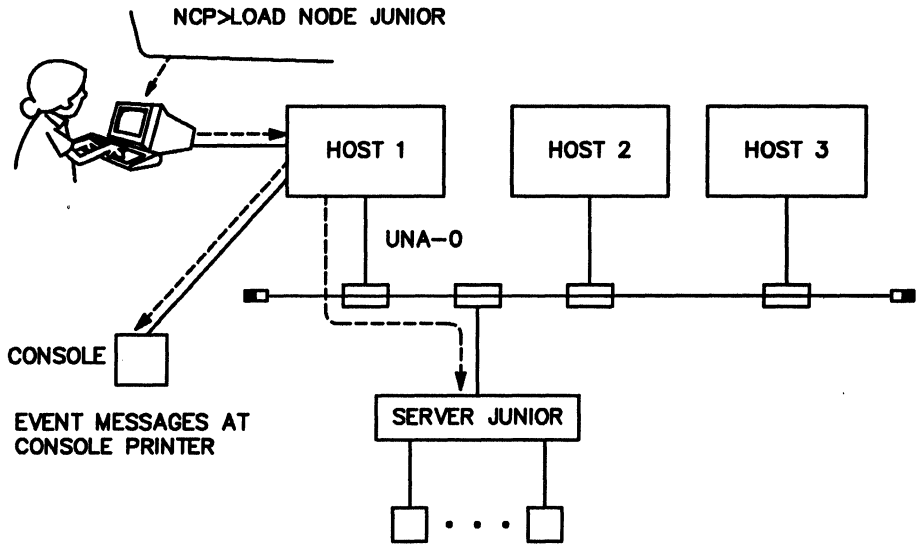
This method offers no automatic warning or delay options. However, you can still warn current users of the down-line load that is about to occur with the server's **BROADCAST** command. You can issue the warning either directly connected to the server or at the load host using either RCF or TSM to connect to the server's management port.

This is how the **LOAD** command works:

1. You issue the **LOAD** command on one of your server's load hosts.
2. The load host sends a **MOP REMOTE CONSOLE BOOT** message with a direct load option specified.
3. When the server receives this message, the server sends a **MOP REQUEST PROGRAM** message directly to that load host.
4. The load host and the server use additional **MOP** messages to transfer the server image, one block at a time, into the server's memory.

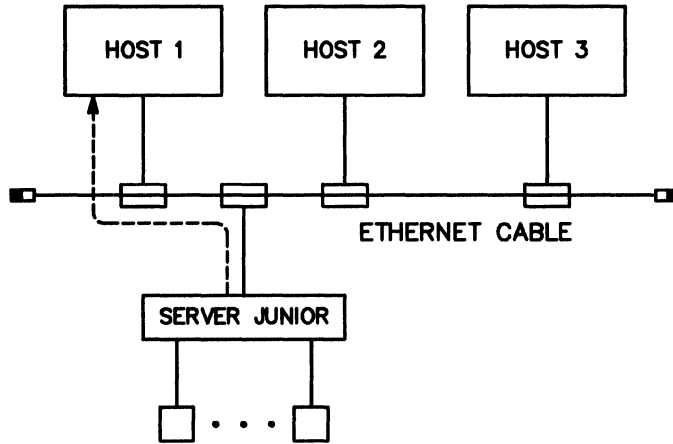
Figure 5–1 shows a server manager on load host **HOST1** issuing **LOAD** to load server **JUNIOR**, over service circuit **UNA–0**. Figure 5–2 shows **JUNIOR** asking **HOST1** for a down-line load. Figure 5–3 shows **HOST1** down-line loading **JUNIOR**'s image to **JUNIOR**. The arrows show the message path that **LOAD** generates.

Figure 5-1: Server Manager Enters LOAD Command at HOST1



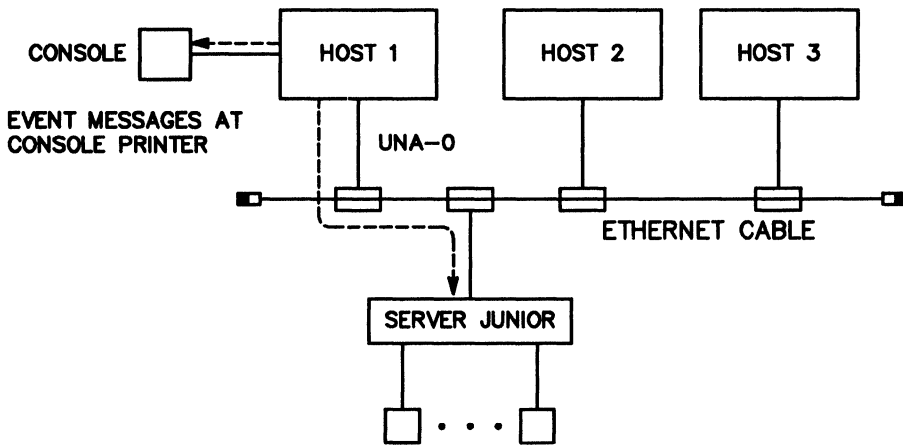
LKG-0043-88
REV. 1

Figure 5-2: Server JUNIOR Asks HOST1 for a Down-Line Load



LKG-1020-87
REV. 1

Figure 5-3: HOST1 Loads Server JUNIOR



LKG-1021-88
REV. 1

5.2.2.4 How NCP TRIGGER Works

If you are at a load host, the advantage of the NCP TRIGGER command is that, depending on the load host, the down-line load is faster than with the LOAD command. TRIGGER is usually faster than LOAD because the server does not have to wait for a particular load host to respond to its request.

The TRIGGER command does not ensure that a particular load host performs the down-line load. With this method, you do not know beforehand which load host will actually down-line load the server image.

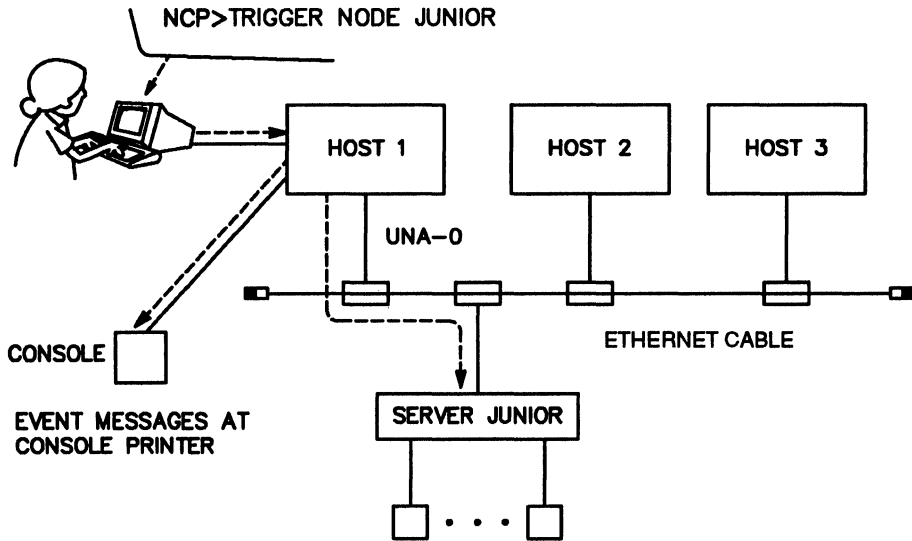
As with the LOAD command, with this method there are no automatic warning or delay options. You can still warn current users of the down-line load that is about to occur, however, with the server's BROADCAST command. You can issue the warning either directly connected to the server or at the load host using either RCF or TSM to connect to the server's management port.

This is how the TRIGGER command works:

1. You issue the TRIGGER command on one of your server's load hosts.
2. The load host sends a MOP REMOTE CONSOLE BOOT message with the TRIGGER option specified.
3. When the server receives this message, the server multicasts a MOP REQUEST PROGRAM message.
4. The first load host that responds and the server both use additional MOP messages to transfer the server image, one block at a time, into the server's memory. The server ignores other responders once the load is in progress.

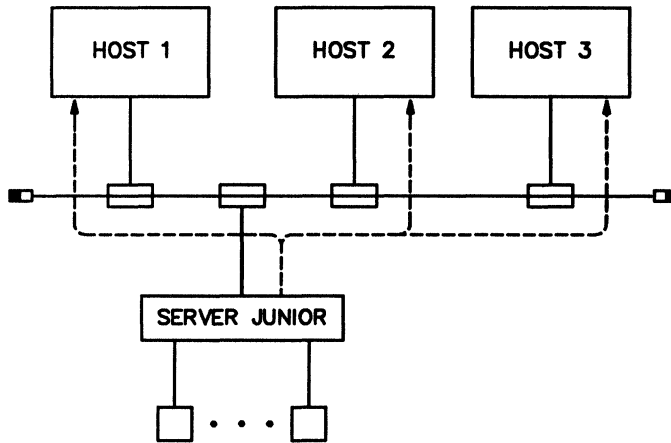
Figure 5-4 shows a server manager on load host HOST1 issuing TRIGGER to load server JUNIOR. Figure 5-5 shows JUNIOR multicasting a request for a down-line load. Figure 5-6 shows load host HOST3 responding by down-line loading the server image to JUNIOR.

Figure 5-4: Server Manager Enters TRIGGER Command at HOST 1



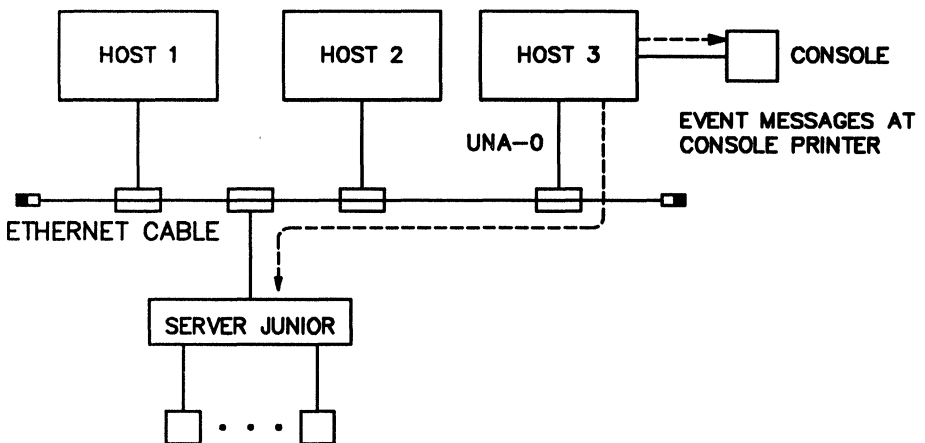
LKG-1103-87
REV. 1

Figure 5-5: Server JUNIOR Sends Multicast Message



LKG-0045-88
REV. 1

Figure 5-6: First Load Host to Respond, HOST 3, Loads Server JUNIOR



LKG-0046-88
REV. 1

5.2.3 The Different Ways To Monitor a Down-Line Load

Regardless of how you initiate it, you can monitor a down-line load in several ways:

- Read the 900-series messages. These messages report the down-line loading status to the terminal connected to the console port (port 0).
- Observe the LED display on the CPU module. Several codes show the status of the loading process. See the *DECserver 500 Problem Solving* manual, or see either the *DECserver 500 Troubleshooting Quick Reference Card* or the *DECserver 550 Troubleshooting Quick Reference Card* for the meaning of each code.
- Set up DECnet event logging for load hosts and review the messages that are logged during the down-line load.

5.2.4 Preparing for Down-Line Loading

To prepare for down-line loading:

1. Enable DECnet event logging.
2. Warn current server users of the upcoming down-line load.
3. Shut down local services.

Note

The server automatically does steps 2 and 3 if you are using the INITIALIZE command.

All the preparatory NCP commands needed for down-line loading, such as the ones that set the Ethernet line and identify the service circuit, are done by the DSVCONFIG command procedure and are executed when you or the software installer runs that procedure, as discussed in Section 6.5. In addition, SERVICE must be ENABLED on the service circuit, which is also performed by DSVCONFIG.

5.2.4.1 Setting Up DECnet Event Logging

DECnet event-logging messages can confirm that a down-line load was successful. Event logging is a service provided by DECnet nodes.

You can use privileged NCP commands to enable event logging at any of your server's load hosts. With event logging enabled, a DECnet node usually generates a short series of event messages when a load or dump sequence starts and completes. These messages clearly indicate that the server has been correctly loaded from the load host's point of view.

When event logging is set up on a DECnet node, you can specify the destination, called the sink, of the messages. Digital suggests that you set up one DECnet sink node to receive all the logging events associated with loading your server or servers. In this way, all load request status information is available at one node. See Section 6.2.1 for an example of the commands that set up event logging on a VMS load host. For similar instructions on other load host systems, see the *DECserver 500 Software Installation* manual for that operating system.

5.2.4.2 Warning Users

The least disruptive time to perform a down-line load is during off hours. If it is possible, Digital suggests that you reload your server when there are few or no current users.

You can conveniently down-line load during off hours by:

- Specifying the DELAY option of the server's INITIALIZE command, if you are using INITIALIZE
- Putting the NCP LOAD or TRIGGER command in a batch job on the load host to run at night, if you are using LOAD or TRIGGER

When you issue INITIALIZE DELAY, the server first takes these preparatory steps to warn users:

1. The server sets an initialize timer to control the number of minutes until the server shuts down and reboots. You can postpone the initialization process for a specified number of minutes. (If you do not use the DELAY option, INITIALIZE is delayed by 1 minute by default.)

You can check the current number of minutes on the initialize timer by viewing one of the status displays. Issue SHOW SERVER STATUS and look at the "Minutes to Shutdown" field (see Section 9.6.3).

2. The server sends a warning message to all logged-in ports, which indicates that shutdown will occur in n minutes. The number in the message is the number of minutes until shutdown.

With the `DELAY` option, the server transmits the warning message to port users when you issue the command. Then, the server sends the message again when 5 minutes are left. Thereafter, a message is sent every minute until the initialize timer is at 1 minute. No notice is sent when the shutdown actually begins.

Note

The `SET/DEFINE SERVER BROADCAST DISABLED` command has no effect on initialization messages. However, the `SET/DEFINE PORT n BROADCAST DISABLED` command does inhibit the reception of the messages at port n . In addition, a nonprivileged user who issues a `SET PORT BROADCAST DISABLED` command inhibits the reception of shutdown messages at his or her port.

3. Users connected to remote-access ports receive a session disconnect message, “system shutdown in progress,” when the initialize timer reaches 1 minute.

The server’s `BROADCAST` command is another way of warning users of a shutdown. If you plan to reload your server with either `LOAD` or `TRIGGER`, you can first issue the privileged `BROADCAST ALL` command on the server to warn current users of the shutdown. `BROADCAST ALL` sends a message to each port if:

- You issued `SET/DEFINE SERVER BROADCAST ENABLED` (the default).
- The port user did not issue a `SET PORT BROADCAST DISABLED` command (the default is `ENABLED`) for his or her port.

Your message can be up to 72 characters long. The following command sends the following message to all the ports:

```
Local> BROADCAST ALL "The server will be shut down today at 18:00."
```

5.2.4.3 Managing Local Services Before Shutdown

Regardless of the method you use to reload the server, before shutting it down during work hours, you can take these precautions to protect users from any extra inconvenience:

1. Disable further queuing on the server.
2. Disable future connections to local services.

Strict guidelines do not exist, but the following considerations may help you decide whether to take either precaution:

- For servers that receive host-initiated requests, disable queuing far enough in advance of shutdown to avoid having a large number of entries queued at shutdown.

The actual amount of time before disabling the server queue depends on the number of existing entries: the more entries in the queue, the farther in advance it should be disabled. Usually 30 minutes is enough time.

You can learn the size of the queue with:

```
Local> SHOW QUEUE ALL
```

To disable queuing on the server, issue:

```
Local> SET SERVER QUEUE LIMIT 0
```

- If the average session is fairly short-lived for a local service, disabling connections for a period before initialization reduces the likelihood of disrupting active sessions. For example, for a printer, 10 minutes is likely to be sufficient for a session to begin and for a print job to finish. Therefore, 10 minutes before shutdown is a reasonable time for disabling future connections.

To disable connections for a local service, issue the `SET SERVICE` command and specify the local service. For example, to disable connections for local service `LASER`, type:

```
Local> SET SERVICE LASER CONNECTIONS DISABLED
```

5.2.5 Initiating a Down-Line Load

Initiate a down-line load by issuing the `INITIALIZE` command, pressing the boot switch, issuing the `NCP LOAD` command, or issuing the `NCP TRIGGER` command.

5.2.5.1 Issuing the INITIALIZE Command

To initiate a down-line load from your server, at a privileged port issue the INITIALIZE DELAY command. Here is an example, specifying a delay of 10 minutes:

```
Local> INITIALIZE DELAY 10  
Local -199- WARNING - Server shutdown in 10 minute(s)
```

The server displays the warning at each logged-in port (see Note in Section 5.2.4.2). The full syntax of this command is described in the *Terminal Server Commands and Messages* manual.

5.2.5.2 Resetting by Pressing the Boot Switch

See the appropriate DECserver 500 series hardware installation manual for information about initiating a down-line load by pressing the boot switch on the server hardware. For an explanation of the accompanying LED displays, see the *DECserver 500 Problem Solving* manual.

5.2.5.3 Issuing the NCP LOAD and TRIGGER Commands

See Section 6.2 for examples of initiating a down-line load from a load host.

5.2.6 Monitoring a Down-Line Load

You can monitor a down-line load by reading the 900-series messages, noting the server's LED displays, and reading the DECnet event-logging messages.

5.2.6.1 Reading the 900-Series Messages After the Down-Line Load

See the *DECserver 500 Problem Solving* manual for information about the 900-series messages. For the meanings of these messages, see the *Terminal Server Commands and Messages* manual.

5.2.6.2 Reading the Server's LED Displays During the Down-Line Load

To interpret the LED displays, see either the *DECserver 500 Troubleshooting Quick Reference Card* or the *DECserver 550 Troubleshooting Quick Reference Card* located on the front of the server. This card lists the server status and error codes and gives their meanings. For more information, see the *DECserver 500 Problem Solving* manual.

5.2.6.3 Reading Event-Logging Messages After the Down-Line Load

These messages appear on the system console terminal of one or all of the server's load hosts. Event messages identify the system that loaded the server. These messages reporting down-line loads have two parts, one that logs the server's request for the load and the second that confirms the successful down-line load.

Assuming that logging is enabled for all load hosts, the location of these messages depends on how you initiate the down-line load:

- With the **LOAD** command, both parts of the message appear only at the load host from which you issue the command.
- With the **TRIGGER** command and with system power-up, the first part of the message is logged at all the server's load hosts because the server multicasts the request. However, the second part of the message that confirms the load appears only at the load host that answers the request and actually performs the load.

Also check for any errors reported by NCP, if you used either the **LOAD** or **TRIGGER** command to start the load. If no errors are reported, you can assume that the load was successful. See the *DECserver 500 Software Installation* manual for an example of event-logging messages after a successful down-line load.

If you do see errors in the event-logging messages, follow these steps:

1. Check the meaning of the errors in the NCP documentation of the operating system that performed the down-line load.
2. Check that your server hardware is working satisfactorily. If there is an error indicating a problem, see either the *DECserver 500 Troubleshooting Quick Reference Card* or the *DECserver 550 Troubleshooting Quick Reference Card*, or see the *DECserver 500 Problem Solving* manual. If the hardware unit is fine, the problem is probably with the load host.
3. Check the **DSVCONFIG.DAT** file, especially the Ethernet address of your server. At the same load host, run **DSVCONFIG** and select the **List** option.
4. Check that the server image is in the appropriate directory.

5. Check that DECnet software is running.
6. Try again to down-line load. If it is unsuccessful, see the *DECserver 500 Problem Solving* manual for troubleshooting procedures.

If no DECnet events have been logged, check that **SERVICE** is **ENABLED** for the DECnet service circuit over which the server software is supposed to be down-line loaded.

5.3 Making Use of Groups

This section discusses groups you set up for your users, groups you set up for all network users, comparable groups set up by other server managers, and groups set up by the network manager. This section explains how all these groups are related and gives you procedures for establishing and making use of groups. In addition, this section mentions the nonprivileged user's limited ability to control groups.

This section covers:

- The **SERVICE GROUPS** server characteristic
- The **AUTHORIZED GROUPS** port characteristic
- The **GROUPS** port characteristic
- The "Server Groups" field of the **SHOW/MONITOR/LIST SERVER SUMMARY** display

Every service node on the network is assigned at least one **service group**, either by the network manager or by the service node managers in cooperation with one another. Often, a service node is assigned several groups. The **LAT** network manager coordinates the division of service groups among the service nodes.

If you want a port user to have access to a service node, assign the same group list, or at least one of the node's groups, to the port. Make these assignments with the **AUTHORIZED GROUPS** port characteristic. **Authorized groups** for a port determine the ability of a port to access services.

5.3.1 Network Service Groups: Overview

Each service node has its own set of service groups for the services it offers. Assigning service groups requires coordination among the managers of all the servers and service nodes on your LAT network.

Digital recommends a service-specific approach to assigning service groups. The network manager selects a unique service group for each service (or set of related services) offered on the LAN and assigns that service group to all service nodes offering that service. Assigning groups to sets of services rather than to individual services is suggested if the network has a very large number of services.

A service-specific approach is also helpful when several nodes offer the same service, such as a VAXcluster offered as a single service, or several servers offering modems as part of a single service. This method is also helpful when you have several ports that are configured for host-initiated requests and that are offered in common to service nodes.

The service-specific approach to assigning service groups has advantages to both service nodes and servers. These advantages are:

- To service nodes

Service-specific service groups operate independently of what service nodes currently offer services. Therefore, a system manager can add an existing service to a new service node without involving server managers.

- To servers

Since most users are oriented to services rather than to service nodes, this approach helps you assign a single authorized group for a service offered by multiple service nodes.

Another benefit is that the number of authorized groups remains small for each port. Furthermore, if the relationship between a service and the service nodes offering it changes, you do not have to update the **AUTHORIZED GROUPS** of every port that requires that service.

The following simple example shows a LAT network manager's assignment of all the services, service nodes, and service groups in the network:

LAT Groups

Service Node Names	Groups	Service Names
AEGEAN	6	AQUA
ARTSY	5	CADD
BAILEY	1-3,6	BIGTOP
BARNUM	1-3,6	BIGTOP
BIGFIN	3,6	RSX
BONBON	2,6	ULTRIX
LYNX	4,6	FASTPRINT,MODEM2
TIGER	1-6	A_DEVICE,LASER,LN01,MODEM1
TOPCAT	1,4,6	VAX_VMS

LAT Group Access

Group 0	Unavailable
Group 1	Software Development A A_DEVICE,BIGTOP,LASER,LN01,MODEM1,VAX_VMS
Group 2	Software Development B A_DEVICE,BIGTOP,LASER,LN01,MODEM1,ULTRIX
Group 3	Software Development C A_DEVICE,BIGTOP,LASER,LN01,MODEM1,RSX
Group 4	Publications A_DEVICE,FASTPRINT,LASER,LN01,MODEM1, MODEM2,VAX_VMS
Group 5	Design Services A_DEVICE,CADD,LASER,LN01,MODEM1
Group 6	Project X A_DEVICE,AQUA,BIGTOP,FASTPRINT,LASER,LN01, MODEM1,MODEM2,RSX,ULTRIX,VAX_VMS

A variation of the service-specific approach helps you assign authorized groups to ports that you configured for host-initiated requests. These ports must share an authorized group with each service node making requests. Be sure to tell the system managers of these service nodes what group to enable as a service group being configured for making host-initiated requests to your server.

5.3.2 Assigning Service Groups for Your Server

When you establish your server as a service node, you must assign service groups, just as the manager of the LAT network (or other system managers) assigns service groups for each service node. Communicate with the network manager when you assign service groups. Assign service groups for your server with the **SERVICE GROUPS** server characteristic.

Before setting up the first local service, assign service groups. By default, the server has service group 0 enabled and other service groups disabled as soon as you establish the first local service.

It is important to discuss the nature of the local services you plan to offer with the network manager. He or she will probably then tell you what service groups to assign.

Next, ensure that all server managers know the service groups that you have enabled on your server. They can then determine the ports of their users who need these services and assign the same groups to those ports.

Service groups on the server are used when people issue **CONNECT** commands at other nodes. At these times, the server checks that the requester has at least one authorized group that matches the server's service groups.

The following example assigns service groups 1 through 6 to your server and then sets up the local service named **LASER** (note that **TSC** requires that you specify at least one characteristic on the **DEFINE** command line):

```
Local> SET SERVER SERVICE GROUPS 1-6
Local> SET SERVICE LASER PORTS 113,114
```

OR

```
TSC> DEFINE SERVER SERVICE GROUPS 1-6
TSC> DEFINE SERVICE LASER PORTS 113,114
```

All users on the network, both on your server and on other servers, can access the service LASER, if the users' ports have at least one authorized group from among groups 1 through 6.

To see the service groups you assigned, issue the `SHOW/LIST SERVER CHARACTERISTICS` command, which displays a Service Groups field (see Section 9.6.1).

5.3.3 Assigning Authorized Groups for Your Ports

Authorized groups determine the access to network services from each port and control the display of these services from each local-access port with the `SHOW SERVICES` command. In addition, by specifying authorized groups, you limit the number of service nodes stored in server memory.

Note

When a port is privileged it has access to all the services that every other port is authorized to access.

As a whole, the authorized groups you assign for all your server's ports are known as the **server groups**. The server uses the total authorized groups for these functions:

- Storing known service nodes in the database
- Checking authorization for host-initiated requests

To assign authorized groups effectively, you need information about LAT services on the LAN and about each port user.

5.3.3.1 Service information

You need the following service information:

- The service groups of each service node
- The intended users for each service

If the network manager maintains an up-to-date record of service groups and intended users for each service, you can use it to plan your authorized groups.

You also can display the service groups for each node with the **SHOW NODE STATUS** display, if at least one port already has at least one authorized group in common with at least one service group of that node. The **Node Groups** field gives you the groups assigned to that service node. If you want a particular port to have access to the service, assign at least one of the groups to that port.

In the following example, service node **TOPCAT** is assigned service groups 1, 4, and 6 and offers a service called **VAX_VMS**. The example assigns authorized groups 1, 4, and 6 to ports 65–112 so that users on these ports can connect to this VMS system.

```
Local> SET PORTS 65-112 AUTHORIZED GROUPS 1,4,6 ENABLED  
Local> SAVE PORTS 65-112
```

OR

```
TSC> DEFINE PORTS 65-112 AUTHORIZED GROUPS 1,4,6 ENABLED
```

5.3.3.2 User Information

For each port, you need to know the requirements of the user or users. In some cases, you might anticipate that a specific user will use a terminal on a particular port, such as a person with a terminal located in a private office. In other cases, there may be an identifiable set of users for a port, such as a dial-in modem port. In both cases, you should be able to gather information from the users about what services they need. Then, you can authorize groups for ports accordingly.

In other cases, you might have a terminal that is available to many heterogeneous users. In this case, memory usage or security issues might be the best way to decide on the number and selection of groups to authorize for the port.

To see the authorized groups you assigned for one port, issue the **SHOW/LIST PORT CHARACTERISTICS** command, which displays an “Authorized Groups” field (see Section 9.4.1). To see the sum of all the authorized groups for all ports, issue the **SHOW/LIST SERVER SUMMARY** command, which displays a **Server Groups** field (see Section 9.6.4). Note that **Server Groups** is not a characteristic, it is simply the total of all the ports’ authorized groups.

5.3.3.3 Adding and Replacing Authorized Groups

Once you assign a set of authorized groups for a port, you can add groups to the list. Issue the **SET/DEFINE PORT AUTHORIZED GROUPS ENABLED** command again and specify the new group or groups. For example, the following command adds group 2 to the existing group list for ports 65 through 112, so that the users can now also connect to **ULTRIX**, a service offered on service node **BONBON**:

```
Local> SET PORTS 65-112 AUTHORIZED GROUPS 2 ENABLED
Local> SAVE PORTS 65-112
```

or

```
TSC> DEFINE PORTS 65-112 AUTHORIZED GROUPS 2 ENABLED
```

You can also replace an existing group list with a new one. Issue the **SET/DEFINE PORT AUTHORIZED GROUPS** command without the keywords **ENABLED** or **DISABLED**. The following example replaces the old group list (groups 1, 2, 4, and 6) for ports 65 through 112 with a new list that contains groups 3 through 5:

```
Local> SET PORTS 65-112 AUTHORIZED GROUPS 3-5
Local> SAVE PORTS 65-112
```

or

```
TSC> DEFINE PORTS 65-112 AUTHORIZED GROUPS 3-5
```

5.3.3.4 Reducing Authorized Groups to Current Groups

Nonprivileged users can issue the **SET PORT GROUPS** command to further restrict, from among their ports' authorized groups, their own access to services. This nonprivileged command also shortens their node and service displays.

These groups are shown on the displays as (Current) Groups. They are ignored for remote-access ports. A nonprivileged user can enable only the groups that you authorized with the **AUTHORIZED GROUPS** characteristic. **GROUPS** are always equal to, or a subset of, the **AUTHORIZED GROUPS**. If a user specifies **GROUPS ALL**, the groups become the same as the enabled **AUTHORIZED GROUPS**. If users want to save their changes, however, they must ask you to do it with the privileged **SAVE PORT** command.

The server uses the current groups for these functions:

- Checking authorization when the user issues a **CONNECT** command on the server
- Displaying information with the **SHOW NODES** and **SHOW SERVICES** commands

The following example shows the command for nonprivileged users to assign groups from among their authorized groups. The example reduces the port's access to the service **CADD**. In addition, when the user issues **SHOW SERVICES**, he or she sees only this service.

```
Local> SET PORT GROUPS 5
```

To see the groups that a nonprivileged user assigned for his or her port, issue the **SHOW PORT CHARACTERISTICS** command, which displays a (Current) Groups field (see Section 9.4.1).

Just as you can add authorized groups or replace an authorized group list, the nonprivileged user can add to, or replace, his or her current groups.

To add groups, the user issues the **SET PORT GROUPS ENABLED** command again and specifies the new group or groups. To replace an existing group list with a new one, the user issues the **SET PORT GROUPS** command without the keywords **ENABLED** or **DISABLED**.

5.4 Managing Local-Access Ports

Your routine tasks include managing the environment of interactive devices such as terminals, keyboard printers, and personal computers connected either directly to the server or remotely with dial-in modems. See Chapter 7 for a discussion of the basic port configurations for these interactive devices; Table 5-2 lists the relevant sections.

Table 5–2: Local-Access Applications Discussed in Chapter 7

Section	Application
7.4	A Terminal Capable of Connecting to Many Services
7.5	A Terminal Using a Dedicated Service
7.6	A Personal Computer Used As a Terminal and As a Service*
7.8	A Printer Used with a Dedicated Service*
7.11	A Dial-In Modem*
7.15	A Terminal Using DSR/DTR Flow Control
7.16	A 3270-Class Terminal Emulating a VT220 Terminal
7.17	A TD/SMP Session Management Terminal

* These devices can also be used on remote-access ports.

The port configuration information in Chapter 7 explains only the port characteristics that are essential to the proper functioning of each interactive device. However, there are additional characteristics, called user-oriented characteristics, of the server and its ports. You can use these user-oriented characteristics to control a port's environment.

Some user-oriented port characteristics — for example, switch characters and a preferred service — can be defined by nonprivileged users for the duration of a log-in period. To keep these port characteristics for users after they log out, you can help them in two ways:

- Execute **SAVE PORT**, a privileged command. **SAVE PORT** retains the new values until the next down-line load.
- Define their port values in the permanent database. **TSC** and **TSM DEFINE PORT** commands retain the values regardless of down-line loads.

There are other user-oriented characteristics — the log-in password, for example — that only you can change with privileged commands. Use the privileged user-oriented characteristics to regulate the user environment. The rest of this section focuses on the privileged port characteristics and related server characteristics.

5.4.1 Identifying Who Uses the Local-Access Ports

To configure each local-access port effectively, you need to learn about your server's users. The following considerations might be significant:

- The experience of the users of the device
- The usefulness of multiple sessions to the users
- The essential services required by the users
- The services never required by the users
- The need of users to know about both the server and the network as a whole
- Your need as server manager to broadcast notices to logged-in users

5.4.2 Session Management Terminal (TD/SMP)

Any suitably configured interactive terminal at a server port can have a single terminal session with multiple service sessions. Most terminals display the output of the current service session only and suspend any data exchange of the other active sessions.

In contrast, a **TD/SMP session management terminal** is an interactive terminal that supports the TD/SMP protocol and can process multiple terminal sessions, each with a single LAT service session. In this way, the session management terminal can process multiple service sessions simultaneously without suspending the data exchange for the noncurrent sessions. The terminal keeps the “context” of each service session. So, when the user switches terminal sessions, the most recent output of the associated service session appears without the user having to press any keys at the keyboard. The user can input data to only one of the service sessions, but output continues from all sessions. Also, some session management terminals display output of all service sessions on a divided display screen.

For each terminal session, the user enters server commands in local mode or service commands in service mode. However, the terminal user manages each terminal session at the terminal itself using terminal commands. For example, for some terminals, the user can execute terminal commands to divide the display screen to show the output for more than one terminal session.

You can visualize a session management terminal as two or more standard terminals using the same physical server port. However, this method of operation produces some restrictions in the use of local mode commands. Table 5–3 summarizes these restrictions.

Table 5–3: Local Mode Command Restrictions During Session Management

Command	Description
BACKWARDS	This command does not work during session management.
CONNECT	Establishes a service session for any terminal session. However, you are restricted to one service session for each terminal session.
DISCONNECT DISCONNECT ALL DISCONNECT SESSION <i>session-number</i>	The DISCONNECT command disconnects the current service session and returns you to local mode for the terminal session. The DISCONNECT ALL command disconnects all service sessions on your port. All terminal sessions return to local mode. Neither command disconnects terminal sessions. You can use the DISCONNECT SESSION <i>session-number</i> command to disconnect a service session of another terminal session. When you switch to the affected terminal session, your terminal will be in local mode with no service session.
FORWARDS	This command does not work during session management.
LOGOUT LOGOUT PORT	LOGOUT closes your current terminal session only and disconnects the service session associated with it (if there is one). You are not logged out of the server. You can open or switch to another terminal session. LOGOUT PORT does a full logout, logging you out of the server, closing all terminal sessions and service sessions.
RESUME	Returns you to your current service session from local mode. You cannot use the RESUME SESSION <i>session-number</i> command to resume a specific session.
SET PORT	Changes the current characteristics for a server port.

Table 5–3 (Cont.): Local Mode Command Restrictions During Session Management

Command	Description
DEFINE PORT	Changes apply to all terminal sessions for that port. The PREFERRED characteristic behaves differently for terminal sessions. The preferred service is supported while you are in a terminal session if you use a CONNECT command without specifying a service. The preferred service also takes effect when you establish a terminal session if you do not specify a service name when the terminal prompts you for one. If you do not want to connect to the preferred service from your terminal session, enter the name LOCAL when your terminal prompts you for a service name.
PRIVILEGED	Applies to the port and to all terminal sessions on the port.

5.4.3 Educating Users

For users to gain full benefit from the server, tell them about the many features the server offers that can improve their productivity.

Digital suggests that you inform server users about the features of local-access ports such as multiple sessions and related commands/switches, the types of services available on your LAT network, load balancing among VAXcluster nodes, automatic failover, and file transfer capabilities.

In addition, encourage users to use the server's tutorial and reference on-line Help. Inform them of the *DECserver 500 Use* manual. Finally, tell them to contact you if they have a problem.

5.4.4 User-Oriented Server Characteristics

You can control some user-oriented features, for example, broadcast and lock, for the server as a whole. The **BROADCAST** and **LOCK** server characteristics are enabled by default. This section explains them to help you determine whether to leave them enabled. Passwords and other security-related characteristics are also user-oriented features and are discussed in Section 5.1.

5.4.4.1 The Broadcast Feature

The broadcast feature sends messages between logged-in local-access ports. With the privileged **BROADCAST ALL** command, you can notify interactive users of impending changes in server status, such as the removal of a local service. By using the nonprivileged **BROADCAST PORT *n*** command, nonprivileged users can send a message to one port. Secure users cannot use **BROADCAST**.

You control whether the broadcast feature is enabled server-wide. Digital suggests that you leave the **BROADCAST** server characteristic **ENABLED** to allow both yourself and other users to use the **BROADCAST** command. If you do, nonprivileged users can leave the **BROADCAST** port characteristic **ENABLED** or they can disable it for their own port, disabling the reception of any messages.

The **BROADCAST** command creates a one-line message of up to 72 characters and sends it to the designated ports that are logged in and set to **BROADCAST ENABLED**. You do not have to enclose your text in quotation marks; the server processes them as characters.

Here is an example of a nonprivileged **BROADCAST** command that sends a message to port 3:

```
Local> BROADCAST PORT 3 "I'd like to transfer files to you."
```

The following two privileged **BROADCAST ALL** commands send messages to all the ports and to selected ports, respectively:

```
Local> BROADCAST ALL Server shut down at 12:15; back up at 1:00.  
Local> BRO POR 17-32 Please log out for hardware maintenance until 14:00.
```

Since broadcast messages overwrite displays on port devices, excessive use of the **BROADCAST** command can be inconvenient to users. Therefore, some users might prefer to disable the reception of messages at their ports.

Digital suggests that you urge users to leave **BROADCAST ENABLED** on their ports, but to inform you if they receive excessive or annoying broadcasts. If you receive complaints, you can set the sender's port to secure status, which disables the use of the **BROADCAST** command from that port.

Note

When a user disables the reception of broadcasting with the BROADCAST port characteristic, his or her port ignores all messages (that is, messages from nonprivileged users, your BROADCAST messages regarding events on the server., and so forth).

However, the server's automatic reinitialize warnings are unaffected by the BROADCAST server characteristic.

5.4.4.2 The Lock Feature

With both the server characteristic LOCK and the port characteristic LOCK enabled, which are the defaults, any user can lock a terminal with the nonprivileged LOCK command.

The lock feature lets a user specify a password that must be re-entered before the terminal can be used again. Locking a terminal permits users to leave a terminal with active sessions without the risk of another user tampering with them. However, since anyone can lock any terminal, the lock feature could cause inconvenience.

If a lock password is forgotten by a user, you have to log out his or her port before it can be used again. Having to help users unlock their terminals frequently is also inconvenient. Therefore, you might find that it is better to disable lock and encourage users always to disconnect their sessions when they leave their terminals.

5.4.5 User-Oriented Port Characteristics

Many port characteristics let you control the use of the ports. This section considers only the privileged user-oriented port characteristics. There are also some unrestricted port characteristics that nonprivileged users can set for their own ports.

Your management decisions about the privileged user-oriented port characteristics are shown in Table 5-4.

Table 5–4: Management Decisions Affecting Local-Access Ports

Decision	Port Characteristic
Assigning a dedicated service	DEDICATED*
Enabling the log-in password	PASSWORD
Enabling security	SECURITY
Assigning group access to services	AUTHORIZED GROUPS
Specifying the session limit	SESSION LIMIT
Enabling interrupts on dynamic-access ports	INTERRUPTS
Prohibiting display information about service nodes and services	LIMITED VIEW
Enabling logout of inactive ports	INACTIVITY LOGOUT
Deciding whether to define a permanent username	USERNAME (used with DEFINE)

* If you assign a dedicated service, all user-oriented characteristics, except for PASSWORD, are ignored by the port.

For a port with a session management terminal, when you change port characteristics with the SET PORT command, the new values apply to all terminal sessions.

5.4.5.1 Assigning a Dedicated Service

If you wish to restrict a terminal to a single session with only one service, specify a dedicated service for the port. Use a dedicated service whenever you wish to simulate a hard-wired connection between a terminal and a service node. Users of a dedicated service need not know that they are using a server, unless you enable the log-in password on the port or specify a password-protected service. Assign unsophisticated users, who require access to only one service, to a port that is dedicated to that service.

Note that you cannot assign a dedicated service to a port that has the MULTISESSIONS port characteristic enabled. For session management to operate at a port, the terminal must communicate with the server. With a dedicated service for a port, the terminal communicates directly with the service node. For a dedicated port, set MULTISESSIONS to DISABLED.

5.4.5.2 Enabling the Log-In Password

A single log-in password is used for the whole server, although you enable it on a port-by-port basis. This password is most likely to be useful when you wish to reserve access to a server from a terminal that is in a public place. Enabling the log-in password ensures that your general user population is unable to use that terminal. A log-in password is also highly recommended on ports connected to dial-in modems.

If you plan to enable the log-in password, Digital suggests that you follow this procedure:

1. Take care in selecting with whom you share the password.
2. Change the password on a regular basis.
3. Whenever you change the password, inform those selected users of the new password.

5.4.5.3 Assigning Security Status

Security status applies to local-access ports. See Section 2.7.1 for a discussion of security status and privilege levels. By default, all ports are nonprivileged.

Digital suggests that you do not give the privileged password to any other user except to a backup server manager, if you have one. At any port, a user who knows the privileged password can issue the `SET PRIVILEGED` command and then enter privileged commands.

Set ports to secure status as you feel is needed. A secure port is quite limited. It isolates users from the activities of the server and from other users. Users on a secure port can issue only these server commands:

- `CONNECT` and `DISCONNECT`
- `BACKWARDS` and `FORWARDS`
- `HELP`
- `LOCK`
- `LOGOUT`
- `RESUME`

- SET PORT AUTOPROMPT
- SET PORT BACKWARD SWITCH
- SET PORT FORWARD SWITCH
- SET PORT LOCAL SWITCH
- SET PORT MULTISESSIONS
- SET PORT TYPE
- SET PORT VERIFICATION
- SET SESSION
- SHOW NODES
- SHOW PORT (only for their port)
- SHOW SERVICES
- SHOW SESSIONS
- TEST PORT (only for their port)

Enable secure status with the SET/DEFINE PORT SECURITY command. For example, to change ports 14, 15, and 16 to secure ports, issue:

```
Local> SET PORTS 14-16 SECURITY ENABLED
Local> SAVE PORTS 14-16
```

or

```
TSC> DEFINE PORTS 14-16 SECURITY ENABLED
```

5.4.5.4 Assigning Authorized Groups

Authorized groups control the access to network services from each local-access port and control the display of these services for each local-access port user. To assign authorized groups effectively, you need information about LAT services on the LAN and about each user. See Section 5.3 for a complete discussion of groups.

5.4.5.5 Specifying a Session Limit

You can limit the permitted number of LAT sessions on each local-access port to a number from 0 to 8 by specifying the desired number for the **SESSION LIMIT** characteristic. You can use the session limit of the server to help control how much server memory is used for managing sessions.

Use the session limit of the port to control the level of activity on the specific port. If you set a session limit to 0, the affected users cannot connect to any services (current sessions are not affected). If you specify **NONE**, the port user can have up to 8 sessions, for example:

```
Local> SET PORTS 17-80 SESSION LIMIT NONE
Local> SAVE PORTS 17-80
```

or

```
TSC> DEFINE PORTS 17-80 SESSION LIMIT NONE
```

5.4.5.6 Enabling Interrupts on Dynamic-Access Ports

For dynamic-access ports, you can enable interrupts if you want the owner of the main user of the device to have full control over it (a hardcopy terminal used as a printer, for example).

Set the port to **INTERRUPTS ENABLED** and **BREAK LOCAL**. Use caution when enabling interrupts, however, because they might inconvenience people using the device for remote-access applications; that is, it might not be offered as a service.

5.4.5.7 Enabling Inactivity Logout

When you have dial-in modems on local-access ports or use devices other than printers on dynamic-access ports, you should generally set **INACTIVITY LOGOUT** to **ENABLED**. Enabling this feature prevents users from monopolizing devices by remaining logged in when they are not actually using a service.

On a port set to **INACTIVITY LOGOUT ENABLED**, the server logs out the port if no sessions are active on the port for the number of minutes you specified for the server's inactivity timer.

The inactivity timer of another service node might also apply to a user with service sessions on that node. In this case, use the server characteristic **INACTIVITY TIMER** in conjunction with the other service node's inactivity timer. If the service node automatically logs out sessions, you might not need to enable **INACTIVITY LOG-OUT** on the ports that can access services on that node.

5.4.5.8 Assigning Permanent User Names

The **DEFINE PORT USERNAME** command allows you (or the port user) to assign a permanent username for the port. Upon server login, the Enter Username prompt is not issued, and the permanent username is used as the dynamic username. This function is designed to accommodate interactive terminals that have one permanent user. Terminals that are usually shared among users should not have a permanent username assigned.

5.4.5.9 Controlling Access to All Services on the LAN

The following commands reduce access for your server users to services offered by any service node, including the local service node:

- To isolate all ports from all services (after the next initialization), define the server **SESSION LIMIT** to be 0 and then reboot the server. Use the following command:

```
DEFINE SERVER SESSION LIMIT 0
```

- To isolate a specific port from a specific service, disable any authorized group shared by the service node(s) offering the service. Use the following command:

```
DEFINE PORT n AUTHORIZED GROUPS group-list DISABLED
```

See Section 5.3 for information about selecting authorized groups.

- To isolate a local-access port from all services, set its port session limit to 0. Use the following command:

```
SET PORT SESSION LIMIT 0
```

To isolate all local-access ports from all services, set the server session limit to 0. Use the following command:

```
SET SERVER SESSION LIMIT 0
```

5.5 Managing Sessions

This section briefly discusses the display of information about sessions and then tells you how to terminate them. For information about controlling the data transparency of a session, see Section 5.7.3.

5.5.1 Displaying Session Information

You can display one line of information about the current status of a port with the `SHOW PORT n SUMMARY` command. You can also display a list of the current sessions at one port, selected ports, or all ports with the `SHOW SESSIONS` command, for example:

```
Local> SHOW SESSIONS PORT 8
```

or

```
Local> SHOW SESSIONS PORTS 8,9,10
```

or

```
Local> SHOW SESSIONS ALL
```

For remote-access ports and dynamic-access ports with a current remote-access session, the user name is given as one of the following:

- (remote access)
- (host initiated)

For remote-access ports responding to a `TEST SERVICE` command, the user name shows as:

(test responder)

For an example of a typical display and an explanation of the display fields, see Section 9.8.

5.5.2 Terminating Sessions

You can terminate any session. The guidelines for terminating sessions are generic, in that they apply to all ports. You can use these methods:

- With the privileged `LOGOUT PORT n` command, which allows you manually to log out any port, all sessions terminate at the port you specify. If the port device supports session management, `LOGOUT PORT` disconnects all of the terminal sessions (and associated LAT service sessions) and then logs out the port.

For example, to disconnect port 4 from all its sessions, enter the following:

```
Local> LOGOUT PORT 4
```

The port that you specify can have local, remote, or dynamic access. Use caution when logging out a user's port. When you log out a port, you abruptly stop all sessions and data might be lost. The port characteristics are also reset to the permanent values unless you saved them with `SAVE PORT`.

- Disconnect session *x* port *y*.
- For CXY08 ports with `MODEM CONTROL ENABLED`, the server routinely logs out a port whenever the attached device drops the Data Set Ready (DSR) modem signal, which can happen because the user ends a session by logging out at the device or the device is powered off. In addition, if the attached device drops the Carrier Detect (CD) modem signal for more than two seconds, the server drops all modem signals at that port.

When the server drops the DTR signal on a modem-controlled port used with a non-LAT host, the non-LAT host is assumed to use this as an indication to log out any user processes associated with that port.

- With `MODEM CONTROL DISABLED`, you can enable a power-off logout for the server by setting the port to `DSRLOGOUT ENABLED`. This feature causes the server to log out the port if the attached device loses power.

For ports on CXY08 line cards, power-off logout operates when the server responds to the dropping of DSR by the attached device by logging out the affected port. However, without modem control, a non-LAT host cannot respond to the dropping of DSR by the server, and the host continues to maintain its sessions to that server. Therefore, use `MODEMENABLED` rather than `DSRLOGOUT ENABLED` when a port is connected to a non-LAT host.

5.6 Setting Up and Managing Modem Control

This section discusses the concepts you need to implement modem control, the appropriate procedures, and the topic of how the server monitors modem control.

5.6.1 Introduction to Modem Control

Modem control at a port means that the server and the port device use EIA-232-D modem signaling to control communications between port and device. Modem control facilitates the use of dial-in and dial-out modems with the server. It also enhances the security of sessions at both local-access and remote-access ports.

The server supports only full-duplex asynchronous modems such as the Digital DF03, DF112, DF124, and DF224 modems or modems that are compatible with one of these modems. See the server SPD for a list of modems you can use with your server.

Modem control requires the use of suitable hardware. For modem control to work at a port, you need:

- A CXY08 line card for the port
- A device cable that conducts modem signals between port and device in the manner required for the particular device

The CXY08 line card lets you implement modem control for up to eight associated ports. If you attempt to enable modem control for a port that is not on a CXY08 line card, you get an error:

- From the server, if you try to enable modem control on the running server
- From TSC, if you try to enable modem control with TSC
- From TSM, if you try to enable modem control with TSM

If you enable the MODEM CONTROL port characteristic for a port, you can use the port in one of three ways:

- With a leased, private, or hard-wired line (including short-haul modems or line drivers) on remote- or local-access ports

- With a dial-in modem on local-access or dynamic-access ports
- With a dial-out modem on remote-access ports or dynamic-access ports

The server automatically determines which of these modem applications is being used with the port when the connection is made.

The cable you choose lets the port and port device act as either DCE or DTE equipment. DCE and DTE roles are determined by the port access characteristic (LOCAL, REMOTE, or DYNAMIC) and the kind of device you are using, for example, interactive terminal, non-LAT host, or modem.

Section 7.1 tells you what cable to use for each kind of port device. All of the DEC-server 500 series hardware installation manuals have the physical pin-out diagram for each cable. The server's role in the communication is determined by the configuration of the port and by the port device:

- If the port is a local-access port, the server appears as a data terminal equipment (DTE) device to a dial-in modem, and looks like a data communication equipment (DCE) device to personal computers and terminals.
- If the port is a remote-access port, the server looks like a DCE device to the port device (computer system interface).
- If the port is a remote-access port with a dial-out modem, the server operates as a DTE device.

Modem control provides security for a non-LAT host that is offered as a service by the server. Therefore, when a server port is used with a non-LAT host, Digital highly recommends that you set the port to **MODEM CONTROL ENABLED**.

This security results from the way in which the server and a non-LAT host handle the loss of DSR signals. Using the appropriate null-modem cable between the server port and the host, each device regularly receives DSR signals as the result of the assertion of DTR signals by the other device. Each device monitors the reception of DSR signals and responds to the loss of those signals by terminating the affected sessions:

- When a session is terminated at the host (for example, because a user logs out of the host) the host drops DTR. The server detects this as a loss of DSR and terminates the session.

- When a session is terminated at the server (for example, because a user issues a DISCONNECT command or you power down the server that is offering the service to the host port) the server drops DTR. The host detects this as a loss of DSR and logs out the user.

Without modem control, the host would not detect the loss of DSR. It would continue the session, leaving it open to another user.

Note that the server software assumes that the non-LAT host will log out its session when the server drops DTR. That is, the cable connecting the non-LAT host and the server appears to the host as a dial-in line.

5.6.2 Modem Control Standards

The server conforms to the following communications standards:

- EIA-232-D refers to an “Interface Between Data Terminal Equipment and Data Communication Equipment Employing Serial Binary Exchange”
- CCITT V.24 refers to a “List of Definitions for Interchange Circuits Between Data Terminal Equipment and Data Circuit Terminating Equipment”
- CCITT V.28 refers to “Electrical Characteristics for Unbalanced Double-Current Interchange Circuits”
- CCITT V.25 refers to “Automatic Calling and/or Answering Equipment on the GSTN Using the 100-Series Interchange Circuits”

5.6.3 Restrictions

There are certain features for modems that the server cannot simulate. For example, it cannot force the Ring Indicator (RI) signal on remote-access ports at the time of session establishment to cycle ON and OFF as most modems do when an incoming call is received. This restriction might limit the use of the server with certain types of data switches or computer terminal interfaces.

If a user connects to a modem-controlled remote-access port with DTRWAIT enabled, the server turns on DTR at the line-card interface. If the line card interface does not detect DSR to be on within two seconds after DTR was turned on, the server assumes that the port is attached to a dial-out modem and maintains the session. The server does not prevent a session from being established due to the lack of received modem signals.

Also, Digital does not supply a cable that allows a non-LAT host to have CTS/RTS flow control and the ability to see the modem RI signal. See Section 7.9 for recommended cables on a non-LAT host application.

5.6.4 Modem Control Signals

The line signals supported by the server are shown in Table 5-5. For each EIA-232-D pin being used in modem support, this table lists the signals by pin number, EIA circuit name (along with the usual abbreviation), and EIA and CCITT circuit designations (separated by a slash [/]). The table also gives a short description of the server's use of each signal.

The server hardware always acts as a DTE device, but when another DTE is at a port, the server's signals are received at the other DTE as DCE signals. In these configurations, a null-modem cable is used to transmit the server's signals so that they are received as DCE signals by the device.

Table 5-5: Line Signals Supported by the Server

EIA Pin Number	EIA Circuit Name	EIA/CCITT Circuit Designation	Use By Server
1	Protective Ground (G)	AA/101	Used for cable shield.
2	Transmitted Data (TD)	BA/103	Asserted by server when transmitting data to the port device.
3	Received Data (RD)	BB/104	Monitored by server when receiving data from the port device.
4	Request To Send (RTS)	CA/105	Asserted by the server with Data Terminal Ready. RTS indicates to the port device that the server is ready to exchange further control signals with the port device to initiate the exchange of data.

Table 5-5 (Cont.): Line Signals Supported by the Server

EIA Pin Number	EIA Circuit Name	EIA/CCITT Circuit Designation	Use By Server
5	Clear To Send (CTS)	CB/106	Monitored by the server to receive an indication from the port device that the port device is ready to receive data.
6	Data Set Ready (DSR)	CC/107	Monitored by the server to receive an indication from the port device that the port device is ready to exchange further control signals with the server to initiate the exchange of data.
7	Signal Ground (SG)	AB/102	Establishes the signal common ground for all leads except the Protective Ground.
8	Received Line Signal Detect (CD)	CF/109	Monitored by the server to receive an indication from the port device that the received line signal is within acceptable limits (commonly called Carrier Detect).
20	Data Terminal Ready (DTR)	CD/108	Asserted by the server to indicate that the server is ready to exchange further control signals with the port device to initiate the exchange of data. (DTR is accompanied by RTS.)
22	Ring Indicator (RI)	CE/125	Monitored by the server to receive an indication that a calling signal is being received by the port device.

5.6.5 Modem Control Signaling Sequences

This section describes the modem control sequences for the following situations:

- Establishing a connection
- Momentary CTS signal loss
- Disconnection due to signal loss
- Disconnection due to LOGOUT command

Establishing a connection

1. The server uses one of these:
 - Local-access ports with dial-in modems
 - Local-access ports with leased lines
 - Local-access ports with null-modem connections
 - Remote-access ports with leased lines
2. The server checks for DSR. If DSR is not present on a remote-access port, the server assumes the port is a dial-out line. If DSR is not present on a local-access port, the server assumes the port is a dial-in line and proceeds to Step 3. If DSR is present, the server assumes the port is a leased line or null-modem connection and proceeds to Step 3.
3. The server asserts Data Terminal Ready (DTR) and Request To Send (RTS), if DTRWAIT is DISABLED, and proceeds to Step 4. If DTRWAIT is ENABLED, DTR and RTS are not asserted until the modem has indicated an incoming phone call by asserting a Ring Indicator (RI) signal to the server. The server proceeds to Step 5.
4. For dial-in lines, the server waits for DSR to be asserted by the modem before Step 5.
5. The server samples CTS and CD. If CTS and CD are detected within 30 seconds of Data Set Ready (DSR) detection, the server considers the connection successful and enables data flow on the line. The dial-in user must log in to the server successfully within 60 seconds, or the server automatically disconnects the call.

On dial-in lines, if CTS and CD are not detected within this 30-second interval, the server disconnects the line.

Using remote-access ports with dial-out modems

1. The server asserts DTR and RTS only after a connection is made to the port, unless DTRWAIT is DISABLED. After asserting these signals, the server proceeds to Step 2.
2. The server waits 2 seconds for the modem to assert CTS. If CTS is not asserted within the 2-second interval, the server assumes that the modem does not assert CTS for dial-out command entry and proceeds to the next step. This step is done for compatibility with CCITT V.25 bis modems.
3. The user can now enter dial-out commands to the modem, as if the modem were physically attached to the user's terminal.
4. When the destination answers, the modem asserts DSR.
5. If CTS and CD are detected within 30 seconds of DSR detection, the server considers the connection successful and enables data flow on the line.

If CTS and CD are not detected within 30 seconds or DSR is dropped, the failed call count is incremented. The total number of failed calls allowed per session is determined by the server's password limit. If the password limit has not been reached, the user remains connected to the port and can dial out again. Otherwise, the session is disconnected.

Momentary CTS signal loss

If the modem drops CTS (but not CD), the server suspends data transmission on the line until the modem reasserts CTS.

Disconnection due to signal loss

1. If the modem drops CD for more than 2 seconds or ever drops DSR, the server automatically disconnects all sessions on the port and waits for the stop bit of the last transmitted character to be given to the modem.
2. The server drops DTR and RTS.
3. After 5 seconds, the server attempts to establish a connection.

Disconnection due to LOGOUT command

1. The server waits for the stop bit of the last transmitted character to be given to the modem.
2. The server drops DTR and RTS.
3. After 5 seconds, the server attempts to establish a connection.

5.6.6 Implementing Modem Control

This section explains the port characteristics that relate to modem control and provides procedures for establishing modem control.

5.6.6.1 Port Characteristics Related to Modem Control

Several port characteristics define, or are otherwise related to, modem control. The values of these characteristics often affect each other. If you disable `MODEM CONTROL`, then `DTRWAIT` is inoperative. If you enable `MODEM CONTROL`, then `DTRWAIT` can be either `ENABLED` or `DISABLED`. With `MODEM CONTROL DISABLED`, you can use `DSRLOGOUT`. `SIGNAL CHECK` can only be `ENABLED` for a port that also has either `MODEM CONTROL` or `DSRLOGOUT` set to `ENABLED`. Here are the port characteristics that affect modem control:

- **MODEM CONTROL**

This is the principal port characteristic related to modem control. You can set up `MODEM CONTROL` as `ENABLED` or `DISABLED` with the `SET/DEFINE PORT` command. The presence or absence of modem control determines whether or not the port communicates with the port device using modem signals before allowing data to pass through the port.

- **DTRWAIT**

With modems, the server normally asserts the DTR and RTS signals at all times except during a disconnect sequence. However, there are instances when the assertion of DTR and RTS is undesirable. For example, with some autoanswering dial-in modems, the port should not assert DTR and RTS until the port receives an indication of an incoming call from the modem.

If you set up **DTRWAIT ENABLED**, the server does not assert DTR until it detects an incoming signal from the modem. The default is **DTRWAIT DISABLED**, which means that the server asserts the DTR and RTS signals on an idle port.

You should also use **DTRWAIT ENABLED** on remote-access ports. **DTRWAIT ENABLED** forces the server to assert DTR and RTS signals only when a user actually connects to the port. This makes for more efficient use, for example, of a non-LAT host's resources used in detecting when a new user is trying to log in to the host.

The only time to use **DTRWAIT DISABLED** is for dial-in lines to local-access ports.

- **DSRLOGOUT**

This characteristic functions only on ports with **MODEM CONTROL DISABLED**. The port device can have local access (for a terminal or PC) or can have remote access (for host-initiated requests to a printer or sessions to a non-LAT host).

For local-access ports, **DSRLOGOUT ENABLED** lets the server detect the power off of a terminal or other device. When the server detects a power off, it logs out the port involved in the power off. For remote-access ports, **DSRLOGOUT ENABLED** lets the server log out the port when a remote access session terminates. Note that a port using DSR/DTR flow control must be set to **DSRLOGOUT DISABLED**.

Enabling **DSRLOGOUT** is an effective way of logging out a port when a terminal powers off if the following conditions exist:

- The terminal asserts the DTR signal when powered up.
- The terminal is connected to the server with the appropriate null-modem cable.

If DSRLOGOUT is DISABLED, the port without modem control is not logged out if the port device is powered off.

- **SIGNAL CHECK**

This characteristic allows the server to determine whether a modem controlled device is physically attached to a port *before* making the connection. The server rejects an attempted connection to a port if no signal is seen within five seconds.

Specify SIGNAL CHECK ENABLED for a port only if that port is also set to either MODEM CONTROL ENABLED or DSRLOGOUT ENABLED and is either ACCESS REMOTE or ACCESS DYNAMIC.

- **DIALUP**

During a user's attempted connection to some service nodes, the DIALUP port characteristic can provide additional security for the node. This characteristic protects service nodes from accounts that allow dial-up lines.

If you enable DIALUP, the server passes the value of the DIALUP characteristic to the service node during the connection-request sequence. When the service node detects that DIALUP is enabled, it has the option of rejecting the connection request.

On the server, you enable the DIALUP characteristic for a particular port; the service node manager enables it for a particular account on his or her system.

5.6.6.2 Procedure

To set up a port for modem control, follow these steps:

1. Check that a CXY08 line card is inserted into the slot associated with the port. Issue the SHOW DEVICES command to display the actual kind of line card currently used with each port. Check the field Device Type (Section 9.2.1 illustrates and explains the display).
2. Digital suggests that you set up modem control in the permanent database rather than in the operational database. If you do, for each CXY08 line card in the server, use the DEFINE DEVICE command to map a port logically to a CXY08. For example, this command defines device LC1 as a CXY08, which allows ports 1 through 8, the ports on LC1, to be set up for modem control:

```
TSC> DEFINE DEVICE LC1 TYPE CXY08
```

3. Issue the `LIST DEVICES` command to verify your `DEFINE DEVICE` commands. `LIST DEVICES` displays the kind of line card used with each port, as specified with `DEFINE DEVICE` commands. Check the Device Type field.
4. Issue `DEFINE PORT` to enable modem control. The following example enables modem control for ports 1 through 8:

```
TSC> DEFINE PORTS 1-8 MODEM ENABLED
```

5. Issue additional commands to specify values for other port characteristics related to modem control that you want to set up for particular applications. The following example sets up port 5 for a dial-in/dial-out modem offered as a local service with a service password:

```
TSC> DEFINE PORT 5 ACCESS DYNAMIC AUTOB DIS DTRWAIT ENA
TSC> DEFINE SERVICE DIALOUT PORT 5 PASSWORD "PIERRE"
```

In this example, users can dial in to port 5 to connect to services. If you connect a terminal to port 5, users can connect to local service `DIALOUT`.

6. Down-line load the updated server image to make the new port characteristics operational. For example, you can press the unit's boot switch to initiate a down-line load.
7. At the server, issue the `SHOW DEVICES` command again to display the status of the ports associated with the device you defined as `CXY08`. The Status column for each port should say "Running." If, on the other hand, you see `Wrg Typ` (wrong type) in this field, it means that the actual device in the slot is not a `CXY08` line card.

5.6.7 The Monitoring of Modem Control by the Server and TSC

The server monitors the modem control hardware. The server also monitors your input when you issue the `SET PORT` command with modem-related characteristics. TSC monitors the equivalent input when you issue the `DEFINE PORT` command with modem-related characteristics.

If the server encounters difficulties, it sends you an error message. The information that the server gives you and the appropriate corrective actions depend on the line card type for the port:

- `CXA16`, `CXB16`, or `CXM04` line card

If you enter a command related to modem control, the server displays the following error message:

```
Local -761- Port hardware does not support modem signals
```

- CXY08 line card

The TSC and TSM DEFINE DEVICE commands specify line-card types for each line-card slot on the server hardware unit. After a down-line load, the server checks the line-card type actually installed in each slot. If you issued DEFINE DEVICE and specified a CXY08 line card, but the down-line loaded software finds that this type is not actually installed in the appropriate slot, the status Wrg Typ appears for that CXY08 in the SHOW DEVICES display (see Section 8.4).

5.7 Managing Flow Control

Flow control is a mechanism for a receiving device or port to start and stop the transmission of data from a transmitting device or port. Using flow control ensures that no data is lost due to lack of buffering space. You can handle flow control in two ways, only one of which can be active at a time.

5.7.1 In-Band Flow Control

By default, two special characters — XON/XOFF (DC1/DC3) — start and stop data flow on a server port. Because these characters are transmitted and received, respectively, as normal data, this is a form of in-band flow control. XON/XOFF flow control is the normal type of flow control used with all Digital terminals, personal computers, and printers.

Use XON/XOFF flow control when MODEM CONTROL is enabled.

5.7.2 Out-Of-Band Flow Control

CTS/RTS and DSR/DTR flow control are forms of out-of-band flow control used with DTE devices that are connected to the server with null-modem cables. You must use the CXY08 line card for ports with out-of-band flow control. Only the CXY08 supports the CTS/RTS and DSR/DTR signals.

With CTS/RTS flow control, a device transmits data only when it detects that CTS has been asserted, which occurs only after RTS is asserted by the communicating device. With DSR/DTR flow control, a device transmits data only when it detects DSR, which occurs only after DTR is asserted by the communicating device.

When a port is set with `MODEM DISABLED`, the server can use either pair of modem signals for flow control between the port and the attached device. To configure a port for CTS/RTS flow control (see Section 7.14), issue `SET/DEFINE PORT FLOW CONTROL CTS`. To configure a port for DSR/DTR flow control (see Section 7.15), issue `SET/DEFINE PORT FLOW CONTROL DSR`.

Note

You cannot use `DSRLOGOUT` with DSR/DTR flow control.

5.7.3 Data Transparency Modes for a Local-Access Session

By changing the data transparency mode of a local-access session, a user can prevent the server from recognizing and intercepting XON/XOFF characters for a specific session. The data transparency mode determines how the server handles special characters, including any user-specified switch character and XON and XOFF flow control characters.

By default, if any special character is defined on the port, it is recognized and intercepted by the server during each session. However, any user can change the data transparency mode of a specific session by using the `SET SESSION` command. The data transparency mode of a session operates only while that session is active. For a complete command description of `SET SESSION`, see the *Terminal Server Commands and Messages* manual.

Note

CTS/RTS and DSR/DTR flow control, which use out-of-band modem signals, are unaffected by this command.

Controlling data transparency for a session makes it easier to use the session for applications such as file transfers. This control is useful when data transparency is not automatically controlled by the service node software or the file transfer software utilities. However, service nodes frequently do control the data transparency of sessions.

5.8 Managing Your Server As a Service Node

This section discusses the server as a service node. It provides detailed information on setting up, modifying, managing, and clearing local services.

5.8.1 Introduction to Local Services

When properly configured, the server can offer devices, such as non-LAT hosts, printers, personal computers, and modems, as services on the LAN. A service that the server offers is called a **local service**. If you establish local services, a user can connect to the port of an applications device by specifying the service name in a connection request. Local services are available to users on any server on the LAT network, if the users' ports share at least one common group with the server.

Before the server can offer a local service, you must first configure the port for the attached device.

By default, as soon as you establish one local service, the server functions as a service node by issuing multicast service announcements. These announcements describe the server's available services and contain identification information, such as the server's name and identification string.

5.8.2 Commands That Affect Local Services

Several commands affect local services. The following few sections discuss the server characteristics and service characteristics that affect local services, and the commands you use to modify them. Following this discussion, the next sections provide step-by-step procedures for setting up local services. Table 5-6 lists the commands that you use for creating and managing local services.

Table 5–6: Server and TSC Commands That Affect Local Services

Command	Defaults of Characteristics
CLEAR/PURGE SERVICE <i>service-name</i> or LOCAL	
REMOVE QUEUE <i>option</i>	
SET/DEFINE SERVER	
<i>characteristics</i>	
ANNOUNCEMENTS <i>state</i>	ENABLED
IDENTIFICATION " <i>text</i> "	no text
MULTICAST TIMER <i>seconds</i>	60
NAME <i>name decnet-node-name</i>	
NUMBER <i>number</i>	0
QUEUE LIMIT <i>depth</i>	8
SERVICE GROUPS <i>group-list state</i>	0 ENABLED and 1–255 DISABLED
SET/DEFINE SERVICE	
<i>service-name characteristics</i>	
CONNECTIONS <i>state</i>	ENABLED
IDENTIFICATION " <i>text</i> "	no text
PASSWORD " <i>password</i> "	no password
PORTS <i>port-list state</i>	ALL DISABLED
QUEUE <i>state</i>	ENABLED
SHOW/MONITOR NODE <i>server-name</i> [<i>option</i>]	
SHOW/LIST/MONITOR PORTS ACCESS {DYNAMIC/REMOTE} [<i>option</i>]	
SHOW/MONITOR QUEUE	
SHOW/LIST/MONITOR SERVICE { <i>service-name</i> /LOCAL} [<i>option</i>]	

5.8.3 Server Characteristics That Affect Local Services

This section summarizes the server characteristics that affect the local services your server offers. For more information about these characteristics, see Sections 8.2.4 and 8.2.5.

- **NAME**

Specifies the server's name, which identifies it as a service node on the LAT network. The server includes its name in multicast announcements in order to identify itself as a service node.

Service nodes making host-initiated requests also use the server name to identify a target server. This name must be unique on the network. Digital recommends that you keep the default name, which is your server's DECnet node name.

- **IDENTIFICATION**

Specifies the server identification string, which is included in multicast announcements to describe the local service node to users.

- **ANNOUNCEMENTS**

Specifies whether the server transmits LAT multicast messages for the services it offers. Issuing multicast announcements is enabled by default. To stop the server from issuing announcements, disable them.

A single multicast service announcement is issued at the interval indicated by the multicast timer.

- **MULTICAST TIMER**

Specifies the value of the multicast timer. This timer determines the interval for issuing multicast announcements. By default, multicast announcements are issued every 60 seconds.

- **SERVICE GROUPS**

Specifies the service groups that are enabled for local services. Use service groups to control whether ports — both on your server and on other servers — can access a local service. For information about specifying service groups, see Section 5.3.

- **QUEUE LIMIT**

Specifies the value of the queue limit. The default limit is 8. For information about managing the connection queue, see Section 5.10.

5.8.3.1 The Name of Your Server As a Service Node

The server uses its server name as its service node name. The default server name is the server's DECnet node name. If you modify the server NAME characteristic, that name is used as the name of the server as a service node. The name must be unique on the network.

You can change the server's NAME characteristic (and thereby the service-node name) only if no current sessions and no queued requests exist.

5.8.3.2 Controlling the Announcement of Local Services

The server must have ANNOUNCEMENTS ENABLED (the default) to multicast its announcements. With announcements enabled, when you set up the first local service, the server starts multicasting announcements.

The server continues to do so until you either clear the last local service or disable announcements. The multicast timer controls the frequency of multicasting these announcements.

5.8.3.3 Managing the Multicast Timer

Normally, a 60-second timer provides timely service notification to users with minimal overhead. However, if your network has a very large number of service nodes, you can increase the value of the multicast timer to reduce network traffic. Note that this increases the time before you can detect that a service node is no longer offering services.

5.8.3.4 Specifying Service Groups

Before establishing the first local service, specify service groups (see Section 5.3).

5.8.4 Service Characteristics

Use the service characteristics to establish, modify, and manage local services. A summary of the service characteristics follows. These characteristics are described in more detail in Section 8.3.

Each service requires a unique service name, which you specify when you create the service. If two or more service nodes offer the same service name, servers assume that all the services with that name are identical to each other and are interchangeable. The following example creates and names service LASER (note that TSC requires that you specify at least one characteristic on the DEFINE command line):

```
Local> SET SERVICE LASER
```

OR

```
TSC> DEFINE SERVICE LASER PORT 7
```

You can use the same command to specify service characteristics for the new service, or to modify characteristics for an existing service, for example:

```
Local> SET SERVICE LASER PORT 7 ENABLED PASSWORD "GUTENBERG"
```

or

```
TSC> DEFINE SERVICE LASER PORT 7 ENABLED PASSWORD "GUTENBERG"
```

- **CONNECTIONS**

Specifies whether future connections to the service are allowed. Current connections are not affected. The default is **ENABLED**.

- **IDENTIFICATION**

Identifies the service to users. Try to specify meaningful text to help people understand the nature of the service.

- **PASSWORD**

Specifies a password that the user must enter when requesting a connection to the service. During the connection-request sequence, the server prompts the requesting user for the password.

- **PORTS**

Assigns one or more ports to the service. Each port must have either remote or dynamic access and be configured for a specific applications device.

- **QUEUE**

Specifies whether host-initiated requests for the service can be held on the connection queue. Managing the queue is discussed in Section 5.10.

5.8.5 Using Service Passwords

A service password controls access to a service offered by the server. You can define a service password for some or all local services.

Caution

Do not set up passwords for services that will be accessed by host-initiated requests using the service name.

A service password is particularly useful for unprotected devices such as modems used for dial out. However, note that attempts to connect to password-protected services fail in these two situations:

- Host-initiated connections to services on a server bypass password checking. Therefore, service passwords have no effect on host-initiated connections.
- Older versions of distribution software might not support connections to password-protected services and will always fail.

In these two cases, any request for a connection is denied. The user is not prompted for a password, but the server notifies the user that the connection failed because of an invalid password.

When the server receives a request for a connection to one of its local services that is protected by a password, the server sends a message to the user's server, which might be the same server, and requests the service password from the user. If the user's server supports service passwords, it prompts the user for a password. When the user types the correct password, the user's server retries the connection using the supplied password.

If the password is incorrect, the server offering the service rejects the connection. The user's server reprompts for the password each time the user enters an incorrect password and again attempts the connection. This process continues until the user either correctly types the password or reaches the password limit of the user's server. When the limit is reached, the server stops this process and issues an error message.

If a user requesting a connection to this service is unaware that a password is required or does not know the password, he or she can regain the local mode prompt by entering `CTRL/Z` at the password prompt.

5.8.6 Establishing a Local Service

This section tells you how to set up a local service.

5.8.6.1 Prerequisites

This section considers these prerequisites for offering a local service:

- Recommended line card
- Ports
- Service groups
- Guidelines for naming a local service

Recommended Line Card

Digital strongly recommends that you set up services for non-LAT computers only at ports on a CXY08 line card. CXA16, CXB16, and CXM04 line cards do not support modem control, which is essential for maintaining secure sessions with the services offered. Therefore, with a CXA16 or CXB16 line card, take extreme caution when using the server as a service node.

If the device is a nonsecure printer, this situation might not be of concern. However, connections to non-LAT host systems using a CXA16 or CXB16 line card might result in a user accessing another user's data. When the user logs out of a session with the non-LAT service, the server cannot turn off the modem signals that cause the host to stop the user's process. When another user starts a session with the service, the non-LAT host might connect the new user to the former user's process.

Ports

You need to choose what ports you will assign to a local service and how you want users to access the service. These decisions depend mostly on the type of line card that the port is on and the device attached to the port.

Either you or the hardware installer must attach an application device to a properly configured port. The values for port characteristics are specific to each device. Note that in some cases, such as printers, an application device can accept remote-access connections without being assigned to a service. Chapter 7 discusses the port configurations for service-related applications; Table 5–7 lists the relevant sections.

Table 5-7: Service-Related Applications Discussed in Chapter 7

Section	Application
7.6	A Personal Computer Used As a Terminal and As a Service
7.7	A Printer Configured for Host-Initiated Requests
7.9	A Non-LAT Host
7.10	A Dial-Out Modem
7.12	A Dial-In/Dial-Out Modem
7.13	A Terminal Switch
7.14	A Printer Using CTS/RTS Flow Control

Assigning a port to a service does not automatically make the service available. For each port, you must specify either remote or dynamic access. A service without accessible ports is given a service rating of 0 by the server, which means that no one can connect to this service. You must also disable autobaud for each assigned port.

Service Groups

Before you set up the first local service, assign service groups. The same groups apply to all the services offered by your server; **SERVICE GROUPS**, therefore, is a server characteristic. Assigning service groups prevents local services from being advertised with the wrong groups, if **ANNOUNCEMENTS** is **ENABLED**. Section 5.3.3 shows you how to specify service groups.

Naming a Local Service

The following guidelines apply to naming a local service:

- The service name can be from 1 to 16 characters.
- These are not valid service names: **LOC**, **LOCA**, **LOCAL**.
- You can duplicate names for services, or you can define unique names. Sometimes duplicating service names is desirable. If two or more nodes offer the same service, that service is more available to users on the LAN.

Procedure

The default values for the service characteristics become effective when you define a service. Once you set up a local service, connection and queuing are enabled by default.

The following procedure shows you, step-by-step, how to set up a service and define local service characteristics. If you wish, you can establish a new local service, assign ports to it, and specify all its characteristics in one command. However, TSC requires that you specify at least one characteristic on the DEFINE command line. To establish a local service, follow these steps:

1. Specify a name for the service and the port or ports that will offer the service. Here is an example, which assigns ports 1, 3, 6, 7, and 8 to local service DIALOUT and enables connections to them:

```
Local> SET SERVICE DIALOUT  
Local> SET SERVICE DIALOUT PORTS 1,3,6-8 ENABLED
```

OR

```
Local> SET SERVICE DIALOUT PORTS 1,3,6-8 ENABLED
```

OR

```
TSC> DEFINE SERVICE DIALOUT PORTS 1,3,6-8 ENABLED
```

2. Provide a service identification string that helps users recognize the service. Enclose the string in quotation marks (""). The string can be up to 40 characters long. The following example supplies an identification string for a local service named A_DEVICE:

```
Local> SET SERVICE A_DEVICE IDENTIFICATION "Useful information"
```

OR

```
TSC> DEFINE SERVICE A_DEVICE IDENTIFICATION "Useful information"
```

3. If appropriate, assign a service password for the service. The following example assigns the password PHONE_HOME to the service DIALIN:

```
Local> SET SERVICE DIALIN PASSWORD "PHONE_HOME"
```

OR

```
TSC> DEFINE SERVICE DIALIN PASSWORD "PHONE_HOME"
```

4. Specify values for other characteristics that affect the local service. Here is an example, which disables the queuing of host-initiated requests to local service DIALOUT:

```
Local> SET SERVICE DIALOUT QUEUE DISABLED
```

OR

```
TSC> DEFINE SERVICE DIALOUT QUEUE DISABLED
```

5. Verify that the new local service is functioning. Try connecting to it. For example, for the local service A_DEVICE and its port 5, whose default port name is LC-1-5, issue:

```
Local> CONNECT A_DEVICE DESTINATION LC-1-5
```

When the connection is established, you can see if the device responds appropriately. The appropriate response depends on what device is attached to the port. When you have adequate information, return to local mode and disconnect the service.

For a non-LAT host or a dial-out modem, you might want to repeat this procedure to verify that your first session was disconnected by the host. You should receive the standard log-in prompts each time you connect to any service offering a non-LAT host.

If you have any problem with connecting to the service or with using the device, you can use the following series of commands to review the service and port characteristics:

- Issue the `SHOW SERVICE service-name CHARACTERISTICS` command to see if the service is set up correctly. For example, with the service A_DEVICE, issue:

```
Local> SHOW SERVICE A_DEVICE CHARACTERISTICS
```

The display shows all the ports assigned to A_DEVICE, as well as the other service characteristics. For an example of the service characteristics display, see Section 9.7.1.

- Issue the `SHOW PORT CHARACTERISTICS` command for the assigned port to see if the port is properly configured. For example, for port 5, issue:

```
Local> SHOW PORT 5
```

For an example of the port characteristics display, see Section 9.4.1. The port values that should appear are shown in the tables in the related application sections of Chapter 7.

- Issue the **SHOW SERVER CHARACTERISTICS** command to check the server's service groups. Then check the port's authorized groups with the **SHOW PORT CHARACTERISTICS** command. The service groups should match the authorized groups, for example:

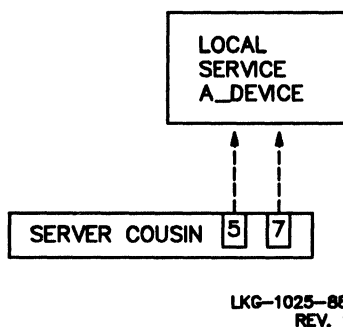
```
Local> SHOW SERVER CHARACTERISTICS
Local> SHOW PORT 5 CHARACTERISTICS
```

See Section 9.6.1 for an example of a server characteristics display, with its "Service Groups" field and Section 9.4.1 for an example of a port characteristics display, with its "Authorized Groups" field.

If you cannot connect to the service, there are several possible reasons for the connection failure; for example, the server is lacking necessary memory. See the *DECserver 500 Problem Solving* manual for a discussion of these problems.

Figure 5-7 illustrates the relationship between a local service and its assigned ports.

Figure 5-7: Ports Offering a Local Service



5.8.7 Preventing Remote Access to a Port That Offers a Local Service

There are various methods you can use to prevent remote access to a port that offers a local service. For a discussion of controlling access to services, see Section 5.3.

As for any session, you can always terminate a remote-access session by using the privileged **LOGOUT PORT *n*** command, where *n* specifies the remote-access port.

5.8.8 Displaying Information About Local Services

To check the existence of a local service, use the `SHOW/LIST SERVICE` command. Use the `SHOW SERVICES LOCAL` command to display one line about all local services known to the running server. To learn which ports are assigned to a particular service and whether connections and/or queuing are enabled for that service, use the `SHOW/LIST SERVICE service-name CHARACTERISTICS` command. These commands and the displays that they produce are described in Section 9.7.

5.8.9 Controlling Access to Local Services

At any time you can reduce, change, or prevent access to a local service. For the methods that use a `DISABLE` option, restore access by entering the complementary `ENABLE` form of the command.

5.8.9.1 Controlling Access to All Local Services

The following commands control access to all existing local services:

- To prevent your server from announcing its services, disable announcements:

```
Local> SET SERVER ANNOUNCEMENTS DISABLED
```

- To prevent all or part of the network from gaining access to your local services, disable your server's service groups that are shared by the servers or service nodes you wish to exclude. Use the following command:

```
Local> SET SERVER SERVICE GROUPS group-list DISABLED
```

5.8.9.2 Controlling Access to a Specific Local Service

Use the following commands to reduce or to prevent access to one local service:

- To prevent connections to a local service, disable connections. If you disable connections on the running server and there are existing sessions, they are not affected. With connections disabled, the server rejects all future connection requests, including host-initiated requests. The following example disables connections to local service `DIALOUT`:

```
Local> SET SERVICE DIALOUT CONNECTIONS DISABLED
```

or

```
TSC> DEFINE SERVICE DIALOUT CONNECTIONS DISABLED
```

- To limit access to selected users, specify a service password for the local service, for example:

```
Local> SET SERVICE LASER PASSWORD "GUTENBERG"
```

OR

```
TSC> DEFINE SERVICE LASER PASSWORD "GUTENBERG"
```

- To prevent connections to specific devices, remove the assigned ports from the local service. Use the `SET/DEFINE SERVICE PORTS DISABLED` command. Here is an example that disables printers on ports 7, 8, and 9; these printers are offered by local service LASER:

```
Local> SET SERVICE LASER PORTS 7,8,9 DISABLED
```

OR

```
TSC> DEFINE SERVICE LASER PORTS 7,8,9 DISABLED
```

- To change the access to a specific local service, specify a new list of ports for the service to replace the existing list, for example:

```
Local> SET SERVICE LASER PORTS 15-21
```

OR

```
TSC> DEFINE SERVICE LASER PORTS 15-21
```

- To reduce host-initiated requests to a service, disable queuing. Use the `SET SERVICE service-name QUEUE DISABLED` command. The following example disables queuing to local service LN01:

```
Local> SET SERVICE LN01 QUEUE DISABLED
```

OR

```
TSC> DEFINE SERVICE LN01 QUEUE DISABLED
```

- To stop connections to a service on a port-by-port basis, change the access of the port to NONE. If a port currently has a session, that session is disconnected when you log out the port. The following example prevents all connections on port 55:

```
Local> SET PORT 55 ACCESS NONE
```

```
Local> SAVE PORT 55
```

```
Local> LOGOUT PORT 55
```

OR

```
TSC> DEFINE PORT 55 ACCESS NONE
```

5.8.10 Clearing Local Services

You can delete any existing local service. When you clear a local service, all ports associated with that service are released, and the service is no longer advertised in the service announcement. When you clear the last existing service, the server stops issuing multicast announcements and ceases to function as a service node.

On the running server, you cannot clear a local service that has an established or pending connection. However, if you must clear a local service immediately, you can disable connections for that service and log out the ports with sessions in progress; then, you can clear the local service. Here is an example that clears all local services:

```
Local> CLEAR SERVICES LOCAL
```

OR

```
TSC> PURGE SERVICES LOCAL
```

The following example deletes the local service LABWORK:

```
Local> CLEAR SERVICE LABWORK
```

OR

```
TSC> PURGE SERVICE LABWORK
```

5.9 Managing Ports Used for Host-Initiated Requests

This section discusses the management of a port used for receiving host-initiated requests. Section 7.7 gives the basic port configuration for host-initiated requests.

5.9.1 Deciding Whether to Assign a Port Name or Service Name

For host-initiated requests, a device on a remote-access port need not have a service name assigned. A server configured for host-initiated requests can have devices accessed by a port name without the use of a service name. Frequently, however, assigning and using a service name offers advantages.

One advantage is that a service name can be associated with equivalent devices on more than one remote-access port. Assuming that queuing is enabled for the service, these ports respond collectively to host-initiated requests on a first-come-first-served basis as they become free. With two or more ports, the delay for users of the service is minimized.

At the same time, the possibility of disabling queuing for any service permits you to control the queuing of host-initiated requests for the service, if necessary. Furthermore, a request for named services can be controlled by disabling connections and/or disabling one or more groups for the port at which the device is attached. These features do not affect host-initiated requests that specify a port without a service name.

5.9.2 Naming the Port or Service

Sometimes you might prefer not to offer a printer as a service, for example, to prevent users with personal computers from using the `CONNECT` command to access the printer.

If you do not use a service name, defining a descriptive port name makes it easier to configure service nodes and other servers for requesting a specific port. For example, you might match the port name to the name being used for the corresponding applications port on service nodes, such as `LA310`, or to a name that describes the device, such as `LASER_PORT`.

Note that the name of each port must be unique on the server. Port names follow the naming conventions of the server described in the *Terminal Server Commands and Messages* manual.

Using descriptive names for ports used with printers is also useful if a port specified by host-initiated requests fails. In this case, you can reassign the port name to another port and use the new port in place of the failed one, without involving any service node.

5.9.3 Reassigning a Port

Reassigning ports involves the following steps:

- Select a new port and attach the printer to it.
- Configure the new port for host-initiated requests as described in Section 7.7.

```
DECLIT AA CROSS HUBOD  
DECserver 500 management
```


- Return the failed port to its default name (*LC-n-n*) and transfer the name you used for host-initiated requests (such as *LA310* or *LASER_PORT*) to the new port.
- Determine whether any service node manager uses a service name as well as a port name when configuring a service node for host-initiated requests. If both are used, when you substitute a new port for a failed port, also disable the service for the failed port with this command:

```
SET/DEFINE SERVICE service-name PORTS n DISABLED
```

Then enable the service for the new port with this command:

```
SET/DEFINE SERVICE service-name PORTS n ENABLED
```

This process lets you manage a failed port without forcing a system manager to re-configure service nodes.

5.10 Managing the Connection Queue

This section discusses the connection queue and the commands and characteristics that allow you to manage it.

The connection queue of the server is a first-in-first-out (FIFO) queue. The queue has entries for two kinds of requests:

- Host-initiated requests from a service nodes
- Connection requests for services from local-access users on the local server or on other terminal servers

The basic operation of the queue is explained in Section 1.5. When the server queues a connection request, the server sends LAT protocol messages to the service node. The messages indicate the status of the connection request in relation to other requests in the queue. The messages also state the queue entry identifier. These messages do not appear as a display on a user terminal at the service node. When the server queues a connection request from a local-access port, the port user's server sends him or her messages about the queue status. The messages show the position of the user's entry in the queue. They appear at the port device each time the queue position changes.

5.10.1 Displaying Server Queue Entries

Use the `SHOW/MONITOR QUEUE` command to selectively observe the status of remotely initiated requests that have been queued by the server. With this command you can obtain information about queue entries, as follows:

- The entries from a specific requesting node by using the `SHOW QUEUE NODE node-name` command.
- The entries for a specific requested service by using the `SHOW QUEUE SERVICE service-name` command.
- All queue entries by using the `SHOW QUEUE ALL` command.

For example, you can obtain information about the entries for the service `LASER` by using the following command:

```
Local> SHOW QUEUE SERVICE LASER
```

The entry identification numbers can range from 1 to 65535. They are not related to the queue depth or to the queue limit. For a description of the queue display, see Section 9.5.

5.10.2 Managing the Queue Limit

Use the `SET/DEFINE SERVER QUEUE LIMIT` command to specify the queue depth, that is, the maximum number of entries allowed into the queue. The server can queue up to 32 requests; the default is 8.

If you reduce the queue limit, existing queue entries are not deleted from the queue. However, no new requests are added until the number of queue entries falls below the new limit. For example, if you reduce the queue limit from 16 to 10, an entry in position 12 remains in the queue, but the server does not accept any new requests for connections that require queuing until fewer than 10 entries remain.

`QUEUE LIMIT 0` disables the queue, and new connection requests are refused unless ports are immediately able to accept connections. Local-access port users with the port characteristic `QUEUING` set to `ENABLED` receive a message informing them that queuing is not available.

5.10.3 Disabling Further Queuing

Disabling queuing prevents new entries for a specified service from being added to the queue, but does not affect existing queue entries. You can disable further queuing for any local service by issuing:

```
Local> SET SERVICE service-name QUEUE DISABLED
```

With queuing disabled, when all ports offering the service are busy, the server rejects all further connection requests for that service. However, queuing is not disabled for host-initiated requests that specify a port name rather than a service name. Since these requests are not associated with a service, the server continues to place them in the queue.

When you disable connections for a service but queued requests for that service exist, the server dequeues them at the appropriate time and then rejects them.

You can also disable further queuing on the server as a whole by issuing the SET SERVER QUEUE LIMIT 0 command.

5.10.4 Removing Entries from the Queue

Use the REMOVE QUEUE command to modify the connection queue by selectively removing entries from the queue. When you remove an entry from the server queue, the server notifies either the requesting service node (for a host-initiated request) or the terminal user (for a local-access request) that the request is being rejected.

No default entry exists for the REMOVE QUEUE command, and failure to specify entries to be removed results in an error. You can remove:

- A specific entry by using the REMOVE QUEUE ENTRY *entry-number* command for each entry
- The entries from a specific requesting node by using the REMOVE QUEUE NODE *node-name* command
- The entries for a specific service by using the REMOVE QUEUE SERVICE *service-name* command
- All the queue entries by using the REMOVE QUEUE ALL command

The `REMOVE QUEUE ALL` command deletes all queue entries, but it does not disable the queue; the next entry takes position 1 in the queue.

For example, you can remove entry number 10 by using the following command:

```
Local> REMOVE QUEUE ENTRY 10
```

5.11 Managing File Transfers

The server supports the file transfer capability of a personal computer on a server port. This allows a user of a personal computer to send and to receive files over the LAN. The personal computer is attached to a server port. For a particular session, the server permits a user to control data transparency — that is, whether flow control and other special characters are intercepted by the server. Note that service nodes frequently control data transparency for you.

For users to transfer files, you must set up the server port and the personal computer to function as the initiator of a session with another computer, which is the partner in the transfer. The degree of data transparency needed for binary file transfers typically requires setting the current session to `PASSALL` mode, either by `Local> SET SESSION PASSALL` or `$ SET TERM/PASSALL`, if the host node is running VMS. The partner computer can be a service node, or it can be a non-LAT host or a personal computer that is offered as a LAT service. Once the initiator establishes a session to a partner, you can transfer files in either direction between the initiator and the partner if the partner has the necessary software.

When the partner in a file transfer is a personal computer or a non-LAT host, see the *DECserver 500 Use* manual for information about setting up the partner.

When the partner is a service node, it is already capable of acting as a file transfer partner. However, you might have to disable flow control on some service nodes prior to initiating file transfers. For information about using a particular service node as a partner in transferring personal computer files, see the documentation of the service node.

The computer serving as the file transfer partner on a remote-access port might require some modifications before a file transfer. To learn what modifications are required, see the documentation for the computer and for the file transfer program.

A personal computer or a non-LAT host that is to be a file transfer partner must be on a port that is properly configured and is offered as a service on the LAT network. The port configuration for personal computers is described in Section 7.6; the port configuration for a non-LAT host is explained in Section 7.7.

5.12 Managing Your Server As Part of the LAT Network

The network manager coordinates the activities of service nodes and servers. This section provides some guidelines to help the network manager achieve maximum performance from the LAT network. These guidelines are optional, but failure to follow them might result in unnecessary performance degradation. Cooperate with the network manager when you specify values for characteristics that affect the entire network.

5.12.1 Distributing Devices on Servers

With the LAT protocol, the network manager can optimize the network bandwidth. The method is to place many terminals (or other devices) on a fewer number of large servers, rather than distributing the same number of terminals on more, but smaller, servers.

Bandwidth is optimized in this way because each server can process sessions from a greater number of ports over a single virtual circuit. With the server, the large number of ports and devices generally optimizes the use of the bandwidth.

5.12.2 Controlling the Number of Known Service Nodes

Minimize, as much as is practical, the number of service nodes that your users access from your server. Every user connected to a different node utilizes more of the network bandwidth than many users connected to fewer nodes.

To reduce the number of service nodes accessed from a particular server, the network manager can assign users to a particular server based on their need for common services. After your server's users are assigned, you should then assign the appropriate authorized groups for each port (see Section 5.3.3 on assigning authorized groups).

5.12.3 Selecting the Value of the Circuit Timer

The value of the circuit timer, which defines the interval at which virtual circuit messages are sent from the server to the service node, is important for balancing fast response time and network utilization against optimal service node performance.

As you increase the value for the CIRCUIT TIMER server characteristic, the LAT protocol overhead decreases on the service node and on the network. However, any gain achieved by setting the circuit timer higher must be weighed against the increase in response time at terminals.

The circuit timer value also affects file transfers. As the circuit timer is reduced, there is less likelihood that the port buffers will be filled between virtual circuit messages. If you have a PASSALL file transfer (with no flow control between port and device), a lower circuit timer value can mean fewer data overrun errors at the port. The file transfers might also be more likely to run successfully at increased speeds.

For normal interactive functions, set the circuit timer at the default value of 80 milliseconds, which provides a good balance between terminal response time and service node performance.

5.12.4 Selecting the Value of the Retransmit Limit

Retransmission of messages ensures reliable communications on the LAN. The RETRANSMIT LIMIT server characteristic defines the number of times a message is retransmitted before the virtual circuit is declared “down” and any current attempt to establish a session is timed out. (Failover to another service node occurs only after a circuit times out.)

If traffic load is heavy or if the network is experiencing “noise” problems, set the value higher than the default, which is 8. On the other hand, if rapid error detection is important, you might need to specify a lower value.

5.12.5 Selecting the Value of the Keepalive Timer

The keepalive timer defines the interval between idle run messages. Idle run messages are sent by the server to service nodes on inactive virtual circuits. Acknowledgment of these messages by the service nodes lets the server continually monitor the status of all circuits. The server treats a lack of acknowledgment as a suspected “circuit down” event.

The value you set for the **KEEPALIVE TIMER** server characteristic is a trade-off between fast “circuit down” detection and unnecessary traffic flow on the network. The default value of 20 seconds represents a good compromise value. Increase the value for heavily loaded networks.

5.12.6 Controlling Access to Network Services

There are several commands that control user access to network services:

- **SET/DEFINE PORT AUTHORIZED GROUPS**
- **SET/DEFINE PORT SESSION LIMIT**
- **SET/DEFINE SERVER SESSION LIMIT**

You can use the following commands to control the display of services and user access to those services:

- To isolate a specific user from displaying and connecting to specific services, disable any authorized group for the user’s port that is also a service group of the service nodes offering these services. Current sessions are unaffected if you use the **SET** command.

Here is an example that prevents the user of port 5, who could previously connect to the services offered by service nodes with groups 1, 2, 6 through 19, and 25, from gaining access to any of those services:

```
Local> SET PORT 5 AUTHORIZED GROUPS 1,2,6-19,25 DISABLED
Local> SAVE PORT 5
Local> LOGOUT PORT 5
```

or

```
TSC> DEFINE PORT 5 AUTHORIZED GROUPS 1,2,6-19,25 DISABLED
```

- To prevent any new connections and, in addition, prevent users from seeing any services, disable all the authorized groups. You can disable groups for one port, selected ports, or all ports. If you use **SET SERVER**, current sessions are unaffected.

The following examples prevent any future connections and inhibit the display of services. The **ALL** keyword completely prevents connections server-wide.

```
Local> SET PORTS 18-42 AUTHORIZED GROUPS ALL DISABLED
```

OR

```
Local> SET PORTS ALL AUTHORIZED GROUPS ALL DISABLED
```

OR

```
TSC> DEFINE PORTS 18-42 AUTHORIZED GROUPS ALL DISABLED
```

OR

```
TSC> DEFINE PORTS ALL AUTHORIZED GROUPS ALL DISABLED
```

- To prohibit users on a particular port from determining the nodes and sessions on the network (but allow the users to connect to services about which they already know), enable **LIMITED VIEW** on the port:

```
Local> SET PORT 5 LIMITED VIEW ENABLED
```

```
Local> SAVE PORT 5
```

- To prevent a particular port from allowing further connections, set its port session limit to 0. Any current sessions (if you use **SET PORT**) are still intact, and the user can still display all current authorized services. Here is an example that prevents future connections at port 6:

```
Local> SET PORT 6 SESSION LIMIT 0
```

OR

```
TSC> DEFINE PORT 6 SESSION LIMIT 0
```

- To prevent all the ports from allowing further connections, set the server session limit to 0. Any current sessions (if you use **SET PORT**) are still intact, and users can still display all current authorized services. The following example prevents all future sessions server-wide:

```
Local> SET SERVER SESSION LIMIT 0
```

OR

```
TSC> DEFINE SERVER SESSION LIMIT 0
```

Note

To limit access with the **SET/DEFINE PORT SESSION LIMIT** command and the **SET/DEFINE SERVER SESSION LIMIT** command, do not use the value **NONE**. **NONE** means “no limit,” so that the server thus allows the maximum number of sessions.

5.12.7 The Use of Groups on the Network

Groups are vital to the functioning of the LAT network. Section 5.3 presents a detailed discussion of groups. One topic is the effect of your group assignments for your ports and for your local services on the network.

5.13 Setting Up and Managing Ports for 3270 Terminals

This section discusses the concepts you need to set up and manage ports on the 3270 Terminal Option Card. This discussion includes a list of supported IBM 3270 Information Display System terminals, terminal behavior at server power up and power down, configuring the line card and its associated ports, and defining the card for up-line dumping.

5.13.1 Introduction to the 3270 Terminal Option Card

The 3270 Terminal Option Card (CXM04 line card) is a Q-bus option card for the DECserver 510 and 550 terminal servers. The card provides a means for 3270 terminals, or PCs that emulate 3270 terminals, to connect to systems on an Ethernet through an Ethernet controller in the DECserver 510 or 550 server hardware. This is known as VT mode of operation.

The 3270 Terminal Option Card is available for 3270 terminal users who need to access applications on Digital systems. To applications on an Ethernet system, the 3270 terminal appears to be a VT220 terminal. In 3270 mode, the 3270 terminal can access applications on an IBM Cluster Control Unit (CCU) connected to the line card.

You can use this line card in environments where the IBM cluster controller is within the vicinity of the Digital system with which the 3270 terminals need to communicate. The DECserver 510 or 550 terminal server must be on the same extended LAN as the target Digital systems.

For the DECserver 500 distribution software to support the CXM04 line card, you must also install 3270 Terminal Option software, which is in a separate installation kit. The 3270 Terminal Option software contains files that the install procedure appends to the base server image. These files are of two classes: (1) firmware for the different components of the CXM04, and (2) translation tables that map 3270 terminal keystrokes into VT220 terminal character sequences.

For the DECserver 500 distribution software to recognize the CXM04 line card, you must carry out the following sequence of steps in the order shown:

1. Ensure that you are running DECserver 500 V2.0 software on a DECserver 510 or 550 server hardware.
2. Identify a DECserver 510 or 550 device slot that will contain the CXM04 line card.
3. Decide upon the line card CONFIGURATION (4 or 8). Refer to the appropriate hardware installation manual for the steps to configure the line card hardware.
4. Insert the CXM04 line card in the DECserver 510 or 550 device slot. Note that the DECserver 510 hardware has two factory-installed CXM04 line cards.
5. If this is the first installation of a CXM04, install the 3270 Terminal Option software on the load host. (This software contains CXM04 firmware and keyboard mapping tables.)
6. Use TSC or TSM to DEFINE DEVICE LC n TYPE CXM04 for the specified device slot LC n . (Defining the CXM04 in this manner automatically appends the CXM04 firmware and keyboard mapping tables to the server image if it is not already present.) If a port's MODE characteristic requires a value other than the default, you can use DEFINE PORT MODE to configure the port.
7. Down-line load the server. (The server software loads the CXM04 firmware and keyboard mapping tables onto the CXM04 line card.)
8. The 3270 terminals associated with the CXM04 ports are now ready to operate in one of two modes, depending upon your configuration.

The 3270 terminal can operate in VT mode or 3270 mode. You can configure the CXM04 and its associated ports so that the terminal has the capability to switch back and forth between the two modes. However, you can also configure a port to restrict a terminal to one mode of operation. In the two mode configuration, the user switches between the two modes by pressing the ALT, then SHIFT keys, or, in some cases, such as PCs, an alternate hot-key sequence. You can use the alternate hot-key sequences by either pressing ALT, then BACKSPACE, or by pressing SYSREQ twice. Consult your PC owner's manual for key sequences that may be used for other functions.

In VT mode, the firmware on the CXM04 emulates a VT220 terminal. To the terminal server, the 3270 terminal appears to be a VT220 terminal. The server's local mode prompt is displayed. From the local mode prompt, the 3270 terminal user can connect to LAT services as a user would from a VT220 terminal.

In 3270 mode, the terminal and the CCU are "hard-wired" together and communicate directly through the CXM04. With this "hard-wired" configuration, no other terminal can access this particular channel of the CCU. The 3270 terminal behaves exactly as if it were connected directly to the IBM CCU.

5.13.2 Supported Terminals and Keyboard Mapping

The 3270 Terminal Option software includes keyboard mapping tables for different types of 3270 keyboards. When you configure this line card, these tables are appended to the server image.

The card's operational firmware determines what terminal and keyboard type are present and what language is specified on the terminal Set-Up screen. The firmware then selects the appropriate keyboard map from those tables that were down-line loaded for the port. Refer to the *3270 Terminal Option Use* manual for information about the mapping of keys on 3270 terminals to keys on the VT220 terminal.

The 3270 Terminal Option Card supports the 3270, coax A type, CUT mode terminals. For a list of supported terminals, refer to the *Software Product Description (SPD)* for this product.

5.13.3 The Effect of Server Power Up on 3270 Terminals

When the server is powered up, all 3270 terminal ports stay in 3270 mode to their corresponding CCU ports if their mode is set to DYNAMIC. However, after the server software loads the operational firmware onto each CXM04 line card, the card's diagnostic firmware transfers control to the operational firmware. Thus, if the server manager sets the terminal's mode to either VT or 3270, the terminal assumes that mode when the server powers up.

5.13.4 The Effect of 3270 Terminal Power Up

When a 3270 terminal is powered down and then up, if the terminal is in VT mode, the CXM04 firmware interrogates the terminal for its type in order to load the correct keyboard mapping table from the library of tables that was down-line loaded with the server image. However, if the terminal was powered down and then up in 3270 mode, it performs normal 3270 operations. The firmware places the terminal either in VT mode or in 3270 mode, depending on how you configured the card and port prior to down-line loading the server image. In DYNAMIC mode, the terminal powers up in the mode that was in effect when the terminal powered down.

5.13.5 The Effect of Power Loss or Line Card Failure

If power is removed from the CXM04 card, the 3270 terminal ports go into 3270 mode to the CCU, provided that the card was defined as CONFIGURATION 4. This is also true if there is an unrecoverable firmware or hardware error. Failure of the server or the CXM04 card does not affect the connection between the terminal and the CCU. Under these conditions, the CXM04 reverts to a logical piece of wire.

5.13.6 Image Configuration

For the CXM04 to run, you must use TSC or TSM to predefine the CXM04 line card type. That is, you must execute the TSC/TSM DEFINE DEVICE TYPE command for the CXM04 in order to append the CXM04 firmware and keyboard mapping tables to the server image. This must be done prior to down-line loading the server image. If not, the server software cannot load the firmware onto the card and thus will not accept the CXM04 line card (causing ports associated with the card to become disabled).

Note

The Terminal Server Configurator (TSC) is included in the DECserver 500 distribution software and is used specifically for configuring the server image. The Terminal Server Manager (TSM) is an optional software product that has the capability of managing the entire DECserver family, which includes the TSC configuration capability.

When you define the CXM04 line card, you choose one of two configurations either explicitly or by default. CONFIGURATION 4 (the default) specifies that four ports, each with an associated 3270 terminal, are configured to operate in both modes (VT and 3270). CONFIGURATION 8 specifies that eight ports are configured for terminals to operate in VT mode only. For example:

```
TSC> DEFINE DEVICE LC1 TYPE CXM04 CONFIGURATION 4
TSC> DEFINE DEVICE LC2 TYPE CXM04 CONFIGURATION 8
```

If you choose CONFIGURATION 4, a 3270-class terminal can switch between VT mode and 3270 mode. In this configuration, a 3270-class terminal can either emulate a VT220 terminal or be connected to the IBM controller.

In CONFIGURATION 4, each port's MODE characteristic defaults to MODE DYNAMIC (both modes). However, you can restrict a port to either VT mode or 3270 mode by configuring the port's MODE characteristic accordingly. The following example defines a line card for both modes of operation but restricts two of its ports to a single operating mode:

```
TSC> DEFINE DEVICE LC1 TYPE CXM04 CONFIGURATION 4
TSC> DEFINE PORT 3 MODE VT220
TSC> DEFINE PORT 4 MODE 3270
```

If you choose CONFIGURATION 8, the firmware configures the card for VT mode only. All eight ports are connected to 3270 terminals, and all terminals are in VT mode. In this line card configuration, the TSC automatically sets the port MODE characteristic to VT220.

When you define the first CXM04 line card in a hardware configuration, the TSC automatically appends to the server image the keyboard tables of four VT languages shipped with the CXM04 product. These languages are North American, British, French, and German. The 3270 terminal user can choose one of these languages through the use of the terminal's VT Set-Up screen.

The server image is limited to four language entries. If the user needs a language other than those four defined in the image, you can add a customized language to the server image by using the DEFINE LANGUAGE command. First, however, you have to remove (PURGE) an unused language from the server image. For example:

```
TSC> PURGE LANGUAGE GERMAN
TSC> DEFINE LANGUAGE FRENCH FILE FOO::SYS$COMMON:[DECSERVER]CXM$FRENCH.KEY
```

Use the `TSC LIST LANGUAGES` command to see what languages are currently defined in the server image. For more information about defining a language, see Section 8.5.

Note

Ensure that the hardware configuration (setting of jumpers on the line card) matches the software configuration as described in the hardware installation procedure.

5.13.7 Up-Line Dumping CXM04 Information

The CXM04 line card provides an up-line dump capability to help with diagnosing CXM04 firmware problems. You can use the `SET/DEFINE DEVICE DUMP` command to cause a specified line card to dump CXM04 information as part of a server up-line dump.

There are two `DUMP` options you can specify: `DISABLED` (the default) or `ENABLED`. With `DUMP` disabled, the CXM04 is not part of a server up-line dump. With `DUMP` enabled, the CXM04 dumps registers, data, and instruction space. The following commands set a CXM04 for up-line dumping:

```
Local> SET DEVICE LC2 DUMP ENABLED
```

or

```
TSC> DEFINE DEVICE LC2 DUMP ENABLED
```

Note

Use the `DUMP` command with the `ENABLED` option only where Digital advises it. Otherwise, be sure that the `DUMP` command is `DISABLED`.

5.14 Line Card Redundancy

Line card redundancy is a software feature that allows you to redirect line card operation from an active line card to a standby line card. This “swap” capability means port users on a faulty line card can be switched to an inactive standby line card that is then activated by a command from the running server.

Use the TSC command `DEFINE DEVICE LC n STATE STANDBY` to define a standby line card. Use the server commands `SET DEVICE STATE OFFLINE` and `MOVE DEVICE` in order to switch operation later from the source (failed) line card to the target standby line card.

Note

Line cards must be defined as standby prior to down-line loading the server image. Otherwise, the server image will have to be reconfigured and reloaded when a line card fails.

To define and activate a standby line card, follow these steps:

1. Identify a device slot that will contain the standby line card.
2. Insert the standby line card into the device slot.
3. Use TSC or TSM to define the specified slot as a standby line card. For example:

```
TSC> DEFINE DEVICE LC7 STATE STANDBY
```

Note

While only eight line cards can be on-line at a time (two in the DECserver 510), line cards in any of the server's ten slots can be designated as standby cards. If LC9 and LC10 are used, then the line cards in those slots must be standby cards. DECserver 510 does not have any additional slots for standby cards.

4. Down-line load the server. Note that the standby line card will not be on-line yet.
5. When an active line card fails, execute the `SET DEVICE LC n STATE OFFLINE` command (where n is the slot number of the failed line card) on the running server (but notify server users prior to doing so). For example:

```
Local> SET DEVICE LC4 STATE OFFLINE
```

This command logs out all ports on LC4 and disables all interrupts from that line card.

6. Execute the `MOVE DEVICE LC n to LC x` command (where x is the slot number of the standby line card) on the running server. For example:

```
Local> MOVE DEVICE LC4 TO LC7
```

This command performs a series of checks: (1) that the source line card is off-line, (2) that the target line card is in a standby state, and (3) that both line cards are the same type. If the checks succeed, the logical move occurs. The source line card's state becomes "MOV LCx," and it is no longer available to the server users. The target line card's state changes from "standby" to "running."

7. Switch associated cabling from the source line card to the target line card. Note that swapping a cable on CXM04 line cards ends any IBM sessions on the source line card. Also note that when CXM04 line card user are switched, all user established port parameters are lost as well as the contents of all counters.

For reasons of security, line card redundancy does not attempt to preserve any sessions that users on the source line card may have had prior to the line card swap.

On the DECserver 500 and 550 only, LC9 and LC10 are reserved for automatic standby line cards only. It is possible to have standby line cards in the normal device slots LC1 through LC8.

To implement line card redundancy, the following restrictions apply:

- The standby line card must first be defined using the TSC or TSM.
- The standby line card must be physically present in the server at the time of initialization.
- The source and standby line cards must be the same type.
- Once the standby line card becomes active as a result of the MOVE DEVICE command, it cannot return to standby status without reloading the server.

Performing Server Management Tasks on the Load Host

This chapter discusses server management on the load host. You need to perform some of these tasks on only one of your server's load hosts, while you must repeat some of the other procedures on all load hosts. Chapter 6 also explains how to use the applicable utilities and commands on the load host.

Here is a list of your tasks on the load host and the management tools you use:

- Customizing the server image file
Load host utility: The Terminal Server Configurator (TSC) or Terminal Server Manager (TSM, optional software package)
- Down-line loading the server's image file
Load host utility: DECnet Network Control Program (NCP),
LOAD and TRIGGER commands
DECnet event logging
- Up-line dumping

- Performing remote management

Load host utility: The Remote Console Facility (RCF) or TSM

- Reconfiguring the load host's node database

Load host utility: DSVCONFIG or TSM

Note

TSM is an optional software product that helps you remotely monitor and control multiple servers on an extended LAN. TSM runs on suitably configured DECnet VMS Phase IV load hosts.

TSM performs all the functions of TSC, RCF, and DSVCONFIG, and provides additional features. The following sections on TSC, RCF, and DSVCONFIG also apply to TSM. See the *Terminal Server Manager Software Product Description* for details.

6.1 Customizing the Server Image: Using the Terminal Server Configurator (TSC)

Perhaps your most important management task on the load host is customizing your server's image according to the uses and configurations you want for your server. Customizing might also help to achieve optimal network performance.

Except for the CXM04 line card, customizing is not required for the server to operate successfully, but it is necessary if you want to use many of the server's features. For each CXM04 line card, you must **DEFINE DEVICE TYPE** prior to down-line loading the server image. See Section 3.4.1 for a description of the running server with all default values.

Your server's system image contains executable code and the permanent database. Whenever you want to change values in this database, you issue **TSC DEFINE** commands. This procedure is known as **customizing the server's image**. TSC acts directly on the image file when you enter these commands. However, for your changes to affect the server, you must down-line load the values in the changed image file to your server. These changes are called "permanent" because they do not change when the server is reloaded.

The server image always resides on the server's load hosts. Both TSC and the image file reside in the same server directory. See the *DECserver 500 Software Installation* manual for the name of this directory. See Section 6.1.2 on how to run TSC.

6.1.1 Defining Port, Server, and Service Characteristics

When you customize the image, the characteristics you define depend on the way you decide to use the server and, especially, its ports. Digital suggests that before you go to a load host and start TSC, you list all the characteristics you plan to modify, along with the new values you will specify. This might help if you plan to make many changes.

In addition, some of the values you choose depend on the network manager. These are values for the server's characteristics that affect network performance (see Section 5.12).

Use these chapters in this guide and these additional documents to help you make your list:

- Chapter 7 contains examples of various port configurations. It shows the particular characteristics and their values you must define for each configuration.
- Chapter 8 is a complete reference on all the characteristics. It defines them and describes how to choose values for each.
- The *Terminal Server Commands and Messages* manual describes the usage and syntax of the `DEFINE PORT`, `DEFINE SERVER`, `DEFINE SERVICE`, and `DEFINE DEVICE` commands. It lists every possible keyword and value you can specify on the command line.

Even if you want to use default values for all other characteristics, you should customize the server's image to at least duplicate the new passwords you set on the server with `SET` commands.

6.1.1.1 Defining Passwords, Password-Related Characteristics, and Security-Related Characteristics

To define passwords in the permanent database, issue the following TSC commands:

- To define the privileged password, execute the **DEFINE SERVER PRIVILEGED PASSWORD** command. The privileged password is from 1 to 16 characters long. Enclose the password in quotation marks. Here is an example changing the password to **PLANET**:

```
TSC> DEFINE SERVER PRIVILEGED PASSWORD "PLANET"
```

You cannot clear the privileged password. If you omit a password in the command line, specify **NONE**, or type a null string (""), you get an error message. To reset the default **SYSTEM**, specify it on the command line.

- To define the log-in password, use the **DEFINE SERVER LOGIN PASSWORD** command. The log-in password is from 1 to 16 characters long. Enclose the password in quotation marks. For example, to change the password to **CHICKADEE**, type:

```
TSC> DEFINE SERVER LOGIN PASSWORD "CHICKADEE"
```

You cannot clear the log-in password. If you omit a password in the command line, specify **NONE**, or type a null string (""), you get an error message. To reset the default **ACCESS**, specify it on the command line.

- To define the maintenance password, use the **DEFINE SERVER MAINTENANCE PASSWORD** command. Unlike other server passwords, the maintenance password contains from 1 to 16 hexadecimal digits (the characters 0 to 9 and A to F). (A value of 0 means that the server never checks the DECnet service password with remote operation requests.) Enclose the password in quotation marks. Here is an example, using the password **FF23**:

```
TSC> DEFINE SERVER MAINTENANCE PASSWORD "FF23"
```

To clear a previously set maintenance password to the default value 0, specify 0, or "", or **NONE** (without the quotation marks) as the password, for example:

```
TSC> DEFINE SERVER MAINTENANCE PASSWORD NONE
```

- To define a service password for a local service, issue the **DEFINE SERVICE** command and specify the service and its password. A service password is from 1 to 16 characters long. Enclose the password in quotation marks. Here is an example using the password **GUTENBERG**:

```
TSC> DEFINE SERVICE LASER PASSWORD "GUTENBERG"
```

Note

Do not set up passwords for services that will be accessed using the service name by host-initiated requests.

To clear a previously set service password to the default value 0, specify 0, or "", or **NONE** (without the quotation marks) as the password, for example:

```
TSC> DEFINE SERVICE LASER PASSWORD NONE
```

There are some other password-related characteristics you might want to define:

- If you want to make the log-in password required at any port, enable it with the **DEFINE PORT PASSWORD ENABLED** command. You can enable the password on one, all, or selected ports. The following example enables the log-in password for all ports:

```
TSC> DEFINE PORTS ALL PASSWORD ENABLED
```

- To change the password limit, issue the **DEFINE SERVER PASSWORD LIMIT** command and specify the number of incorrect tries permitted, for example:

```
TSC> DEFINE SERVER PASSWORD LIMIT 5
```

- You can enable security on one, all, or selected ports. The following example enables security for ports 17 through 32, ports 49 through 64, and port 128:

```
TSC> DEFINE PORTS 17-32,49-64,128 SECURITY ENABLED
```

- You can prohibit any selected port from displaying information about nodes and services by enabling the **LIMITED VIEW** characteristic:

```
TSC> DEFINE PORTS 17-21,29-30 LIMITED VIEW ENABLED
```

6.1.1.2 Defining Other Characteristics

In addition to changing passwords and defining password-related characteristics, you can further customize the server image by changing values for other port, server, and service characteristics. Use the **DEFINE PORT**, **DEFINE SERVER**, and **DEFINE SERVICE** commands to set up the server for your particular network environment.

There is an additional **DEFINE** command, **DEFINE DEVICE**, that you can use to specify the line-card type of a device on the server. TSC uses this information to test the validity of the values you specify with **DEFINE PORT** commands that relate to modem control (for example, **DSRLOGOUT**, **DTRWAIT**, **MODEM CONTROL**, **SIGNAL CHECK**, and **CTS/DSR FLOW CONTROL**) or to other line-card-specific features. In particular, you must use this command and specify the line-card type as **CXY08** for ports on that card to have modem control features enabled.

6.1.2 Using TSC

TSC is one of the server management tools that reside on the load host. Almost every server **SET** command has an equivalent TSC **DEFINE** command. As with server commands, you use TSC commands to specify values for server characteristics that determine how the server operates. When you want to change these values in the server's permanent database, use TSC. In addition, TSC display commands provide information about the permanent database.

To execute TSC commands, first invoke the TSC program. TSC asks you to name an image file. Specify the name of the image file to open. You then get the TSC prompt (TSC>), at which you issue TSC commands.

The host on which you run TSC can be any one of your server's load hosts. However, after you define new values, you must ensure that every load host has the latest changes. Coordinate using TSC with the load host system manager because, for most load host operating systems, you need certain privileges to run this utility.

TSC is part of the DECserver 500 distribution software. After the software installer performs the entire installation procedure described in the *DECserver 500 Software Installation* manual, TSC is in the server directory of each assigned load host for your server.

TSC runs on load hosts, which must have DECnet installed. However, DECnet does not have to be running while you are making changes with TSC commands except for one command. This is the `DEFINE SERVER BACKUP HOSTS` command. TSC uses DECnet to convert between the DECnet node name you specify on the `DEFINE` command line and the DECnet node number required in the server image.

Note that TSC commands do not affect the server's operational database. (You change a loaded image with the server `SET` command.) However, the TSC commands and the server commands have a common command syntax described fully in the *Terminal Server Commands and Messages* manual. See Section 2.1 for a discussion of the server commands.

One of the files in the load host's server directory is a TSC command file that contains `DEFINE` commands to reset every default value (see Section 6.1.2.7).

6.1.2.1 Overview of TSC Commands

This section outlines the TSC commands. While many examples in this manual illustrate the exact command syntax, use the *Terminal Server Commands and Messages* manual for complete syntax information on all the TSC commands, keywords, valid ranges of values, and defaults.

TSC commands are for the server manager to customize the server's image. They are all "privileged" commands.

Each TSC command begins with a descriptive verb. These verbs and their meanings are as follows:

- `CLOSE` — Closes a previously open keyboard mapping table
- `DEFINE` — Modifies values in the server's permanent database
- `EXIT` — Exits you from TSC
- `HELP` — Displays the TSC on-line documentation

- **LIST** — Displays information in or about the permanent database
- **PURGE** — Deletes specified local **SERVICES** or a 3270-terminal **LANGUAGE** from the permanent database
- **USE** — Opens a keyboard mapping table

Note

If coaxial terminals with 102-key keyboards are attached to the CXM04, do not purge the North American language from the DECserver 500 image. The 102-key keyboard's only mapping table is North American.

The **DEFINE** command syntax consists of the following parts:

- The verb **DEFINE**
- A keyword that names the component to modify, for example, **PORT**, **SERVER**, **SERVICE**, **DEVICE**, or **LANGUAGE**
- Parameters, known as **characteristics**, associated with the component, for example, **AUTHORIZED GROUPS**, **PASSWORD**, or **IDENTIFICATION** (Section 7 describes in detail all the characteristics.)
- Values for the characteristics, for example, **6-19**, **PLANET**, **ENABLED**

The following example illustrates a typical **DEFINE** command:

```
TSC> DEFINE PORT 8 AUTHORIZED GROUPS 1,2,6-19,25 ENABLED SESSION LIMIT 3
```

The example above contains these parts:

- The verb is **DEFINE**.
- The component is **PORT 8**.
- The characteristics are **AUTHORIZED GROUPS** and **SESSION LIMIT**.
- The values for **AUTHORIZED GROUPS** are **1,2,6-19,25** and **ENABLED**. The value for **SESSION LIMIT** is **3**.

The keywords for the components you can modify are as follows:

- **DEVICE** — Specifies the **TYPE**, **STATE**, and **DUMP** characteristics of line card for a particular hardware slot
- **LANGUAGE** — Specifies that a new language be added to the server image
- **PORT** — Modifies port characteristics, for example, data-signaling speed and character size
- **SERVER** — Modifies operating characteristics, for example, the server's identification and node limit
- **SERVICE** — Creates or modifies services offered by the server

The **LIST** command syntax consists of the verb **LIST**, a keyword that specifies the component about which you want information, and a display type, for example:

```
TSC> LIST PORTS ALL SUMMARY
```

The keywords for the components about which you can request information are as follows:

- **DEVICES** — Displays the server's hardware configuration as you specified with **DEFINE DEVICE** commands
- **LANGUAGES** — Displays those languages currently defined in the server image
- **NODES** — Displays information about the server as a local service node including services offered by the server
- **PORTS** — Displays information about ports as defined with **DEFINE PORT** commands
- **SERVER** — Displays information about the server's operating characteristics as defined with **DEFINE SERVER** commands

- **SERVICES** — Displays information about local services offered by the server as defined with **DEFINE SERVICE** commands
- **USAGE** — Displays information about when and where the permanent database was last customized, as well as the name of the image file being processed

See Chapter 9 of this manual and the *Terminal Server Commands and Messages* manual for more information about the **LIST** command.

6.1.2.2 Starting TSC

The server image and the TSC program are in the server directory. For all load hosts, the image file is named *DS5node-name.SYS*. Run TSC and specify this file.

To start TSC, see the *DECserver 500 Software Installation* manual for the operating system of the load host you are on. The command to run the procedure varies for each supported operating system, but once you begin it, TSC is identical on all load hosts. Here is an example for a VMS load host:

1. Log in to the system account and set the default directory:

```
$ SET DEFAULT SYS$COMMON: [DECSEVER] 
```

2. Execute TSC:

```
$ RUN DS5CFG.EXE 
```

3. TSC displays:

```
Terminal Server Configurator - V3.0
```

```
Copyright (c) Digital Equipment Corporation. 1989. All Rights Reserved.
```

```
Server image:
```

Type the name of the server image file, *DS5node-name.SYS*.

Here, *node-name* is the DECnet node name of the server. For example, a DECserver 500 server with the DECnet node name TIGER has the image file name *DS5TIGER.SYS*. Note that when you type the image name, you can omit *.SYS*, for example:

```
Server image: DS5TIGER 
```

4. TSC opens the file and displays:

```
DECserver 500, V2.0.0 (Database V9).  
Server image last changed on 6-Nov-1988 at 16:28:50 on TOPCAT  
TSC>
```

6.1.2.3 TSC Problems with Opening Files

If TSC cannot open a server image file, one of several problems might exist. If so, TSC might display an error such as:

```
%TSC-E-RMSERR, Record Management Services error  
%TSC-I-UNOPEN, Unable to open image file for writing, image-file-name  
%TSC-I-RMSSTS, Status code(s): nnnn
```

See the file system documentation of the load host for the exact meanings of the status codes.

Possible problems are as follows:

- The image file is not in the correct directory.
- The image file is invalidly formatted.
- The image file is not write-accessible.
- The image file is currently being accessed.
- The image file you specified does not exist on this load host. Perhaps you mistyped its name or perhaps this system is not a load host for your server.

To check for installed servers and image file names, exit TSC, run DSVCONFIG, and select the List option from the DSVCONFIG Menu (see Section 6.5.5.1).

There is another situation that prevents TSC from proceeding. If the image file you specify is an unsupported version of terminal server software, TSC displays the following warning message, which includes the image file you specified, and then returns you to the system prompt:

```
%TSC-F-VERNSP, File has an unsupported database version, image-file-name
```

6.1.2.4 Entering TSC Commands

Here are some guidelines for entering TSC commands. See the documentation of the load host's operating system for additional information.

- Issue DEFINE, LIST, and PURGE commands at the TSC> prompt.
- You can enter TSC commands in either uppercase or lowercase characters or a combination of both.
- You can separate the words in a command line by one or more spaces. For DEFINE commands, you can separate two characteristics by a comma.
- Depending on the load host, you can enter up to 132 characters on a command line, which can be continued onto a second terminal display line if you do not press the RETURN key at the end of the first line.
- If you make an error in a command line, TSC rejects the entire command line and gives you an error message. (This convention is different from the way the running server handles errors in command lines.) With some error messages, a pointer tells you the exact place in the command line with the invalid input.
- Depending on the load host, you can use the keyboard keys to recall and edit previously executed TSC commands.
- You can exit TSC in one of two possible ways: either issue the EXIT command or press **CTRL/Z**:

```
TSC> EXIT RET
```

or

```
TSC> CTRL/Z
```

See the *Terminal Server Commands and Messages* manual for complete information about TSC command syntax.

6.1.2.5 TSC On-Line Help

TSC has on-line reference help for all TSC commands. With TSC help, you can request a brief description for any TSC command. To invoke help, type:

```
TSC> HELP
```

TSC responds with a list of command keywords for which information is available and prompts you again:

```
Topic?
```

When you enter a command keyword from the list, for example, LIST or DEFINE, TSC gives you a brief description of the function performed by that command and lists any subtopics associated with it. TSC then prompts you for a subtopic. For example,

```
Topic? DEFINE 
DEFINE
```

```
Use DEFINE commands to change characteristics and options in the server's permanent database.
```

```
DEFINE {
  SERVER
  SERVICE
  PORT
  DEVICE
  LANGUAGE
  MAPPING
}
```

```
Additional HELP available for:
```

```
SERVER    SERVICE    PORT    DEVICE    LANGUAGE    MAPPING
```

```
DEFINE Subtopic? PORT 
```

The server lists all DEFINE PORT options and prompts you again for a subtopic.

If you already know the option you want, you can skip these intermediate steps by typing it immediately. For example, to get information about specifying flow control, enter the following command:

```
TSC> HELP DEFINE PORT FLOW CONTROL
```

To redisplay the options you can enter in response to Topic?, enter:

Topic? ?

Note

Help information employs the graphic conventions [] and { } to indicate command usage. Do not enter these graphic characters in your command lines. All graphic conventions are described in the Preface of this manual.

6.1.2.6 Executing TSC Commands from a TSC Command File

You can execute TSC commands from a command file. In fact, Digital suggests that instead of customizing the server image command-by-command, you create a command file with all the TSC DEFINE commands you want to execute, and then run the command file. This approach has the following advantages:

- If you manage more than one server, customizing is easier because you can apply, using one step, the same set of commands to multiple images.
- If your server has more than one load host (as Digital recommends), customizing is easier because, again, you can apply the same set of commands to multiple images by copying the command file.
- It protects your efforts in case the software image becomes corrupted or deleted by mistake, and you need to reissue the same TSC commands.
- It protects your efforts in case you mistakenly run the TSC defaults command file, which resets all the defaults (see the next section).
- The command file is a record of all the current values you defined. If you forget a value that does not show up on any server display, for example, a password you changed, you can type or print the command file for ready reference.
- If you submit a Software Performance Report (SPR), send along this command file to help Digital analyze the problem (see the *DECserver 500 Problem Solving* manual).
- It makes upgrading the DECserver 500 software easier.

To create a TSC command file, follow these steps:

1. Create a file in the [DECSEVER] directory. You can use the format *node_name.com* to identify the file more readily.
2. Edit the file, using the following information to invoke TSC.

```
$ TSC:== RUN SYS$COMMON:[DECSEVER]DS5CFG.EXE
$ TSC
DS5TSV
```

3. Copy the default command file, DS5_020_DEFAULTS.COM (in the DEC-SEVER directory) and edit it to your needs.

At this point you can type in a list of customized TSC commands or continue to create another command file and call the file from the *node-name.com* file. For example:

```
$ TSC:== RUN SYS$COMMON:[DECSEVER]DS5CFG.EXE
$ TSC
DS5TSV
@DS5TIGER.COM
```

In this example we have renamed the DS5_020_DEFAULTS.COM file DS5TIGER.COM.

To run the TSC command file, type the at symbol (@) followed by the *node_name* file name at the \$ prompt. Just as you can do at the operating system level, you can omit the file type if it is the default command file type. For example, to run a TSC command file named DS5TIGER.COM on VMS to customize an image file named DS5TIGER.SYS, type:

```
$ @TIGER 
```

```
Terminal Server Configurator - V3.0
```

```
DECserver 500, V2.0.0 (Database V9).
```

```
Server image last changed on 21-May-1989 at 16:28:50 on TOPCAT
```

```
(TSC commands and displays follow)
```

```
.
.
.
```


6.1.2.7 Updating the Server Image File

Each time you run DSVCONFIG.COM to upgrade with new software or to reinstall the existing software, the new server image replaces the existing server image file on your host. Thus, any customization that you made to your server image is overwritten by the new server image. The result is a new image with default parameters.

To maintain the customized server image, Digital recommends that you create a command file for each server image. There are two ways to do this. One way is to create a command file in the [DECSEVER] directory and name the file *node-name.com*. This file contains all the customized TSC commands. See Section 6.1.2.6 for information on how to create this file.

The other way is to update the customized server image file by invoking the DCL command, @TSC\$DS5_V20_GET_CHAR.COM. This command file automatically creates a TSC command file that you can use subsequently to reproduce the current settings. The command file created by this procedure is *imagename_SETUP.COM*.

To update the server image file with this command file, follow these steps:

1. Install the DECserver 500 software, as described in the *DECserver 500 Software Installation* manual.
2. Invoke the command file @TSC\$DS5_V20_GET_CHAR.COM from the DCL prompt. This file is found in the distribution software.

```
$ @TSC$DS5_V20_GET_CHAR.COM image-name 
```

where

image-name is the name of the server image.

Once invoked, the command file displays the following information:

```
%DCL-I-SUPERSEDE, previous value of SYS$INPUT has been superseded
Creating command file: image-name_Setup.com
Processing image image-name.SYS
! Device LC1 setup
! Device LC2 setup
! Device LC3 setup
.
.
.
! Device LC10 setup
! Port 0 setup
! Port 1 setup
! Port 2 setup
.
.
.
! Port 128 setup
```

3. Run DSVCONFIG, as described in the *DECserver 500 Software Installation* manual. Use the option “Swap an existing DECserver ” (option 3) to replace the existing customized server image with the new customized image.
4. Run TSC on each server image to make any changes or additions to the new server image.

6.1.2.8 Resetting All Values to the Defaults

If you want to return server values to the original defaults, run the TSC defaults command file. This command file, in the load host’s server directory, contains DEFINE commands to reset every value for port, server, and service characteristics to the default.

For example, to change the customized image file DS5TIGER.SYS on VMS to all default values, type:

```
TSC> @DS5_020_DEFAULTS 
```

Keep in mind that resetting default values erases all your customized characteristics for the server, its services, and specialized port configurations. Digital recommends that you customize by putting all your DEFINE commands in one TSC command file and that you reset all the defaults in the server’s image only when absolutely necessary.

To see the TSC defaults command file, see Appendix B. You can also type or print it from the server directory.

6.1.2.9 After Running TSC

After you complete making changes, ensure that every load host assigned to your server has the updated image. Repeat your TSC session at the other load hosts. This procedure is especially easy if you put all the `DEFINE` commands in a TSC command file, which Digital recommends, and then copy the command file to the other load hosts.

When all the load hosts have the new image file, down-line load it to your server. You can initiate a down-line from your server or from a load host.

6.2 Down-Line Loading the Customized Server Image

Whenever you customize the server's image using TSC, you need to down-line the new image to the server. This section describes the ways to initiate a down-line load from a load host. See Section 5.2 for complete information about all the ways to initiate a down-line load, including preparatory steps beforehand and verification afterwards.

On load hosts, which are always DECnet nodes, two DECnet NCP commands can initiate a down-line load: the `LOAD` command and the `TRIGGER` command. You might need an account with certain privileges to execute these commands.

6.2.1 Setting Up DECnet Event Logging

DECnet event-logging messages can confirm that a down-line load was successful. Operating system-specific information about setting up event logging is in the *DECserver 500 Software Installation* manual for the operating system of the load host. In addition, event logging is explained in the NCP documentation of each load host operating system.

Here is an example of the commands that set up event logging on a VMS load host:

```
$ MCR NCP
NCP>SET LOGGING CONSOLE EVENT 0.3
NCP>SET LOGGING CONSOLE EVENT 0.7
NCP>SET LOGGING CONSOLE STATE ON
NCP>SET LOGGING MONITOR STATE ON
```

Event code 0.3 refers to automatic service events, including down-line loads. Event code 0.7 refers to aborted service events.

6.2.2 Warning Users

If you plan to reload your server with either **LOAD** or **TRIGGER**, you can first issue the **BROADCAST ALL** command on the server to warn current users of the shutdown. See Sections 5.2.4.2 and 5.4.3.1 for information about the **BROADCAST** command.

6.2.3 Managing Local Services Before Shutdown

Before shutting down the server during work hours, you can protect users from losing data. See Section 5.2.4 for information on the steps to take.

6.2.4 Issuing the NCP **LOAD** and **TRIGGER** Commands

Issue the **LOAD** and **TRIGGER** commands at the **NCP>** prompt (for information on entering **NCP**, see the *DECserver 500 Software Installation* manual for the operating system of the load host). On the command line, enter either the DECnet node name or the DECnet node address of the server. The **LOAD** and **TRIGGER** commands have a similar syntax:

```
LOAD NODE node-name
TRIGGER NODE node-name
```

or

```
LOAD NODE node-address
TRIGGER NODE node-address
```

The following examples use the **LOAD** command to load a server named **TIGER** with a node address of **28.1008**.

```
NCP>LOAD NODE TIGER
```

or

```
NCP>LOAD NODE 28.1008
```

If you changed your server's maintenance password from the default value of **0**, you usually must specify this password on the **LOAD** and **TRIGGER** command lines. For example, to load the same server **TIGER** with maintenance password **FF23**, type:

```
NCP>LOAD NODE TIGER SERVICE PASSWORD FF23
```

or

```
NCP>LOAD NODE 28.1008 SERVICE PASSWORD FF23
```

or

```
NCP>TRIGGER NODE TIGER SERVICE PASSWORD FF23
```

or

```
NCP>TRIGGER NODE 28.1008 SERVICE PASSWORD FF23
```

For a discussion of the relationship between the server's maintenance password and the DECnet service password, see Section 2.7.2.3.

You can exit from NCP in one of two possible ways:

```
NCP>EXIT
```

```
$
```

or

```
NCP> CTRL/Z
```

```
$
```

See the DECnet documentation of the load host for complete information about the **NCP LOAD** and **TRIGGER** commands.

6.3 Up-Line Dumping

If the server attempts to up-line dump, it always dumps to a load host. The server up-line dumps its memory, a copy of the running image, under these two conditions:

- If the server experiences an unexpected failure, it automatically up-line dumps its memory.
- If you want a copy of memory for diagnostics, issue the CRASH command, which performs an up-line dump.

When you use the Add option of DSVCONFIG, DSVCONFIG assigns a name for your server's dump file (see Section 6.5.2.6). If the server up-line dumps, the load host takes the data and creates the dump file. If the server dumps more than once, a new version of that file is created. After an up-line dump, the server automatically reinitializes.

See the *DECserver 500 Problem Solving* manual for more information on up-line dumping, the creation of the server's up-line dump file, and how Digital can use this file for problem analysis.

6.4 Using the Remote Console Facility (RCF)

From most load hosts, you can remotely connect to your server using the load host's Remote Console Facility (RCF). When you are not near a terminal that is physically attached to the server, it might be convenient to use RCF. With RCF, you can perform any management task that requires logging in to the server and issuing server commands.

RCF establishes a logical connection between your terminal on the load host and the management port on the server. The management port can receive input from (1) RCF and (2) the physical port 0, which is also called the console port. The remote terminal is called a **remote management console** and the connection is called a **remote management session**.

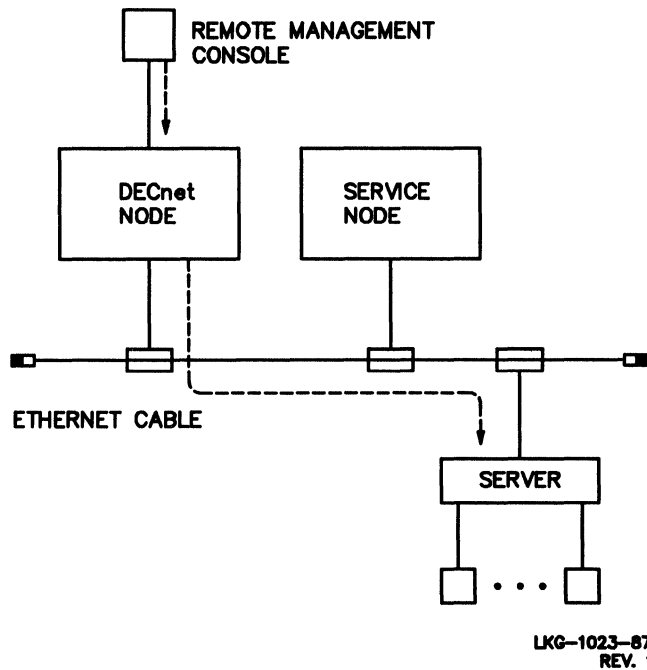
Note

TSM also uses the Remote Console Facility. See Section 2.11 for information about TSM.

For you to use a terminal for a remote management session, the terminal must be logged in to a DECnet node on the same Ethernet as the server. The node must have DECnet Phase IV software but need not be a LAT service node or a load host for your server.

Figure 6–1 shows a remote management console setup.

Figure 6–1: Remote Management Console on an Ethernet



6.4.1 RCF and Other Input to Port 0

If you have attached a terminal or a console printer to physical port 0 (see Section 2.5), port 0 could simultaneously receive input from both RCF and the physically attached device. While RCF is active, input from the physical device attached to port 0 is disabled.

In addition, when you use the remote management port, your output appears both at your remote device and on the device attached to physical port 0. You can use the data on the physically connected device to log the remote console session and for diagnostics.

6.4.2 Using Remote Management

You can enter most of the server commands with RCF. However, the remote management port has a number of features that distinguish it from the other ports:

- To enter local mode from service mode, use the tilde character (~), the default local-switch character.
- Personal computer (PC) file transfers are not supported during a remote management session.
- You cannot use the SET PORT command to change the values for the following port characteristics:
 - ACCESS
 - AUTHORIZED GROUPS
 - AUTOBAUD
 - CHARACTER SIZE
 - DEDICATED
 - DSRLOGOUT
 - DTRWAIT
 - FLOW CONTROL
 - GROUPS
 - INPUT SPEED
 - MODEM CONTROL
 - MULTISESSIONS
 - ON-DEMAND LOADING
 - OUTPUT SPEED

- PARITY
- SIGNAL CHECK
- SPEED

If you enter a restricted form of SET PORT, the server displays:

```
Local -780- Parameter inappropriate for the console port
```

Note that the same command restrictions also apply at a terminal physically attached to the console port (port 0) (see Table 8-4).

6.4.3 Starting a Remote Management Session

Only one remote management session at a time can exist for a particular server. To set up such a session, use the Network Control Program (NCP) Facility for the host system at which your terminal is logged in.

The commands to invoke RCF and then connect to your server differ slightly on each load host operating system. However, once you connect to the server, all remote sessions are the same. The *DECserver 500 Software Installation* manual for the operating system you are using has an appendix on using RCF from that particular system.

On the command line requesting the connection, you have to specify a password if you, as server manager, gave the server a maintenance password (see Section 2.7.2.3).

To disconnect the remote management session, type `CTRL/D`. The server automatically logs out port 0.

The following example shows the procedure from VMS systems. The procedure varies slightly for other operating systems (see the *DECserver 500 Software Installation* manual for these systems).

This example shows a connection to a server with DECnet node name TIGER, DECnet node address 28.1008, and Ethernet address 08-00-2B-04-AA-2B. In addition, TIGER's server manager defined FF23 as the server's maintenance password.

1. To enter NCP, type:

```
$ MCR NCP
```

2. Use the **CONNECT NODE** command if you are on one of your server's load hosts, or issue the **CONNECT VIA** command if the DECnet node is not a load host.

- On a load host:

```
NCP>CONNECT NODE TIGER SERVICE PASSWORD FF23  
Console connected (press CTRL/D when finished)
```

OR

```
NCP>CONNECT NODE 28.1008 SERVICE PASSWORD FF23  
Console connected (press CTRL/D when finished)
```

If the server requires that you specify the password and you omit it, NCP displays this error message:

```
Target does not respond
```

- On a VMS DECnet node, with service circuit ID **UNA-0**, that is not a load host:

```
NCP>CONNECT VIA UNA-0 PHYS ADD 08-00-2B-04-AA-2B SERVICE PASSWORD FF23
```

3. Press the **RETURN** key to activate the server:

```
Console connected (press CTRL/D when finished) RET
```

4. One of two possible prompts appears:

- # (accompanied by a beep)

You see this prompt if you previously enabled the log-in password for port 0 with this command: **SET/DEFINE PORT 0 LOGIN PASSWORD ENABLED**.

Enter the log-in password and press the **RETURN** key. You see:

```
DECserver 500 Terminal Server V2.n - LAT V5.n
```

```
Please type HELP if you need assistance
```

```
Enter username>
```

- Enter username>

You see this prompt if you did not enable the log-in password for port 0. The prompt follows the introductory banner and help message:

```
DECserver 500 Terminal Server V2.n - LAT V5.n  
  
Please type HELP if you need assistance  
  
Enter username>
```

Enter your user name and press the RETURN key:

```
Enter username> Manager
```

5. The server displays its prompt:

```
Local>
```

You can use most of the server commands. Enter these commands just as you would if you were using a device connected to a physical server port.

6. To terminate a remote console session, type **CTRL/D**. Control passes back to the NCP prompt on the VMS system:

```
Local> CTRL/D  
NCP>
```

7. To exit from NCP, type:

```
NCP>EXIT  
$
```

OR

```
NCP> CTRL/Z  
$
```

6.5 The Load Host Configuration Procedure: DSVCONFIG

Another management task that you perform on the load host is reconfiguring your load host's node database. Section 2.3 lists the possible reasons for reconfiguring the database. Your tool to perform this task is a configuration command procedure called DSVCONFIG or the optional software package called Terminal Server Manager (TSM).

The load host's node database contains an entry for your server. The entry provides information that DECnet needs for down-line loading and up-line dumping.

The host on which you run DSVCONFIG can be any one of your server's load hosts. However, after you modify the database, you must ensure that every assigned load host has the latest entries. Coordinate running DSVCONFIG with the load host system manager because, for most load host operating systems, you need certain privileges to run this procedure.

DSVCONFIG is part of the DECserver 500 distribution software. After the software installer performs the entire installation procedure described in the *DECserver 500 Software Installation* manual, DSVCONFIG is in the server directory of each assigned load host for your server. Except for the TSC help text library, the load host creates and maintains all server files in this directory. As part of installation, the software installer uses the Add option of DSVCONFIG to define new servers in the database.

As server manager, you can also use DSVCONFIG to delete and modify the database entry for your server. The act of adding, swapping, deleting, or restoring server entries is what is meant by **configuration of the load host's node database**.

Note

The version of DSVCONFIG that comes with your server hardware accommodates the DECserver 100 server, DECserver 200 server, DECserver 500, DECserver 510, and DECserver 550 server. In contrast, some previous releases of DSVCONFIG cannot handle your server and might corrupt existing databases. Therefore, use only the latest version of DSVCONFIG. You can check with the load host's system manager to ensure that the DSVCONFIG command file in the server directory is the version that supports the server.

6.5.1 Overview of DSVCONFIG

DSVCONFIG has four configuration options, all of which affect the **load host's node database**.

6.5.1.1 Databases Affected by DSVCONFIG

The DSVCONFIG command procedure operates on the load host's node database. This database for servers comprises the following three separate databases:

1. Server configuration database

This database is stored in the file DSVCONFIG.DAT. It has the information you see when you select Option 1, List, from the DSVCONFIG menu.

2. Operational DECnet database

3. Permanent DECnet database

When you run DSVCONFIG, server information is copied from the server configuration database to the DECnet databases. It is important that these databases remain synchronized.

The DSVCONFIG command procedure automatically keeps these databases in synchronization. Even though DSVCONFIG includes several NCP commands, do not execute these NCP commands yourself because NCP affects only the DECnet databases.

6.5.1.2 DSVCONFIG Options

With DSVCONFIG, you can:

- List all servers that are currently defined in DSVCONFIG.DAT.
- Add an entry for a new server in the load host's node database.

Adding an entry supplies information that identifies the server on the Ethernet and, thus, establishes this system as a load host for the new server.

- Swap an existing server for a new one or redefine an existing server's DECnet characteristics.

Swapping retains the DECnet node address of an existing server, replacing its Ethernet address with the Ethernet address of a new server. You can also use this option to replace other DECnet characteristics, such as the DECnet node Performing Server Management Tasks on the Load Host name, either for a new server or for an existing one.

- Delete an entry for an existing server.

Deleting an entry prevents the load host from recognizing the server. Thus, it is no longer a load host for that server.

- Restore existing servers to the load host's DECnet databases.

Restoring servers copies entries from the server configuration database to the DECnet databases.

Here is the DSVCONFIG Menu with its list of options:

```
DECserver Configuration Procedure  V n.n

Menu of Options

1 - List known DECservers
2 - Add a DECserver
3 - Swap an existing DECserver
4 - Delete an existing DECserver
5 - Restore existing DECservers
<CTRL/Z> - Exit from this procedure
```

6.5.1.3 Other DSVCONFIG Functions

DSVCONFIG also prepares the node as a load host by enabling SERVICE on the service circuits. SERVICE must be ENABLED for down-line loading.

6.5.2 Specifying DECnet Characteristics During DSVCONFIG

Several DECnet characteristics apply to servers. DECnet uses these characteristics for down-line loading and up-line dumping. For each server, you must specify, during the Add and Swap options, some of the following characteristics, while DSVCONFIG creates the others.

DECnet Characteristic	You Specify	DSVCONFIG Supplies
DECnet node address	X	
DECnet node name	X	
Server type*	X	
Service circuit ID	X	
Ethernet address	X	
Load file		X
Dump file name		X

* "Server type" is actually a DSVCONFIG.DAT characteristic, not a DECnet characteristic.

The information that you must specify is recorded on each server's *Identification Card*. The software installer should have given you this card after installation.

6.5.2.1 DECnet Node Name

Each server must have a unique DECnet node name. This name must have from 1 to 6 alphanumeric characters with at least one letter. For example, DSV5 and 77LION are valid DECnet node names.

This name becomes the default name of the running server (the server characteristic NAME). The server characteristic NAME and the server's DECnet node name should be identical. Digital suggests that you do not change the NAME characteristic (see Section 8.2.4).

The network manager assigns DECnet node names. During the hardware installation, the hardware installer records the DECnet node name on the server's *Identification Card* for each server.

6.5.2.2 DECnet Node Address

Each server has a unique DECnet node address. This number must be a decimal number from 1 to 1023.

If your DECnet network is divided into areas, each DECnet node address takes the form *aa.nnnn*. Here, *aa* is a decimal area number from 2 to 63, *nnnn* is the node address, and the period distinguishes area from address. For example, 17.1003 is a valid node address.

The network manager assigns DECnet node addresses. During the hardware installation, the hardware installer records the DECnet node address on the server's *Identification Card* for each server.

6.5.2.3 Ethernet Hardware Address

Each server is delivered with a unique Ethernet hardware address. This address is six pairs of hexadecimal digits with a hyphen (-) separating each pair. For example, 08-00-01-00-AB-CD is an address with a valid format.

The Ethernet address is on the front of your server. During the hardware installation, the hardware installer records the Ethernet address on each server's *Identification Card*.

6.5.2.4 Server Types

Your server hardware is either a DECserver 500 terminal server, a DECserver 510 terminal server, or a DECserver 550 terminal server. In any case, specify DS500 for DECserver 500 series servers. DSVCONFIG uses the information to create a unique image file for your server.

6.5.2.5 Load File (Server Image File)

Your server has a unique image file, named *DS5node-name.SYS*. In both cases, *node-name* is the DECnet node name of your server. For example, a DECserver 500 server with the DECnet node name TIGER has the image file name DS5TIGER.SYS.

In addition, each type of server in the DECserver family has its own image file name. Some examples are as follows:

Server Type	Server Image File
DECserver 100s	PS0801ENG.SYS
DECserver 200s	PR0801ENG.SYS
Each DECserver 500 series	DS5 <i>node-name</i> .SYS
ETS	<i>node-name</i> TSV.SYS

If you use the Add option to define a new server, DSVCONFIG creates the image file by copying the default server image, DS5TSV.SYS, to a new file named DS5*node-name*.SYS. This is the image that you customize, if desired, before down-line loading. The Swap option also creates DS5*node-name*.SYS if you specify a new DECnet node name.

When you customize your server's image with TSC, the system modifies the file in place. As a result, whenever you load your server, only one version of its image, with the appropriate parameters, exists and therefore gets down-line loaded.

Note that deleting a server entry from the node database with the Delete option does not delete that server's image file. The image remains in the load host's server directory even though that system is no longer a load host for your server.

Subsequently, if you add a server with the same DECnet node name or swap servers and give the new one, again, that same DECnet node name, you get a message. It tells you that an image file for a server with that DECnet node name already exists. It asks you if you want to use this image for the server or if you want to delete it and use a new image with default parameters. Decide if the parameters in the existing image file are appropriate for the new or swapped server.

Note

If you accidentally delete the entry for your server and the image file has customized values, you can use this feature to "recreate" all your modifications. Select the Add option, specify the same DECnet node name, and answer "yes" to the prompt.

6.5.2.6 Dump File Name

Each server has a unique dump file name, *DS5node-name.DMP*. Here, *node-name* is the DECnet node name of the server. For example, a server with the DECnet node name TIGER has the dump file name *DS5TIGER.DMP*. If the server dumps more than once, a new version of that file is created each time.

When you use the Add option to define a new server, DSVCONFIG assigns a name for the dump file. The Swap option also assigns *DS5new-node-name.DMP* if you specify a new DECnet node name for a server.

See Section 6.3 for information about up-line dumping.

6.5.2.7 Service Circuit

Each server has a service circuit ID identifying which adapter the load host uses to reach the server when loading and dumping occur.

Service Circuit ID	Ethernet Controller
UNA- <i>n</i>	UNIBUS Ethernet controller (DEUNA or DELUA)
QNA- <i>n</i>	Q-bus Ethernet controller (DEQNA or DELQA)
BNA- <i>n</i>	BI Ethernet controller (DEBNT or DEBNA).
SVA- <i>n</i>	VAXstation 2000/MicroVAX 2000 Ethernet controller (DESVa)

Here, *n* is an integer (typically 0 or 1).

When you run DSVCONFIG to add or swap more than one server, the procedure asks you to specify the service circuit each time. The first time you are asked, the default is the service circuit for the processor type of the load host from where you run the procedure. If you respond by specifying a different service circuit, that response becomes the default until you either specify another service circuit or you exit the procedure.

The following is a partial list of the possible default values for each load host's CPU type. Refer to the *DECserver 500 Software Product Description (SPD)* for a current listing.

CPU Type	Service Circuit ID
VAX-11/780, 785	UNA-0
VAX-11/730,750	UNA-0
VAX 8600, 8650	UNA-0
VAX 8200, 8300, 8500, 8550, 8700, 8800	UNA-0 or BNT-0
MicroVAX II	QNA-0
VAXstation II	QNA-0
MicroVAX 2000	SVA-0
VAXstation 2000	SVA-0
PDP-11 (UNIBUS)	UNA-0
PDP-11 (Q-bus)	QNA-0

If the load host's CPU supports more than one Ethernet controller, you might choose a service circuit ID number other than zero.

6.5.3 Preparing to Run DSVCONFIG

Before beginning the procedure:

1. Check the *Identification Card*. The network manager and the hardware installer recorded the following information on this card, which you need to answer prompts during DSVCONFIG.
 - DECnet node name
 - DECnet node address
 - Ethernet address
2. From the documentation binder, get the *DECserver 500 Software Installation* manual for the operating system of the load host from which you plan to run DSVCONFIG. The preparation for running DSVCONFIG and the command to start it vary slightly for each supported operating system. These are the software installation guides:
 - DECserver 500 Software Installation manual (VMS)
 - DECserver 500 Software Installation manual (RSX-11M-PLUS)
 - DECserver 500 Software Installation manual (Micro/RSX)

6.5.4 DSVCONFIG Conventions and Requirements

DSVCONFIG is an automated, interactive, menu-driven command procedure. When you start DSVCONFIG, a menu of options displays. Within the Add, Swap, and Delete options, you get a series of questions. After each question, the default response, if there is one, displays in brackets ([]). At the end of each question, either a colon (:) or a question mark (?) appears.

For the load host from which you are running DSVCONFIG, check the *DECserver 500 Software Installation* manual for that operating system. The conventions of and requirements for running DSVCONFIG vary slightly for each supported operating system.

DSVCONFIG has some additional conventions and requirements that are common to all load hosts:

- When you finish an option, DSVCONFIG automatically returns you to the DSVCONFIG Menu.
- At the end of the Add, Delete, and Swap options, you might get NCP messages (information, confirmations, and errors). In the case of error messages, the operation might not have been successful. For the meanings of these messages, see the load host documentation on messages.
- For you to run DSVCONFIG on a particular load host, the distribution software must already be installed onto that system.

6.5.5 Running DSVCONFIG

To start DSVCONFIG, see the *DECserver 500 Software Installation* manual for the operating system of the load host you are on. The command to run the procedure varies for each supported operating system, but once you begin it, DSVCONFIG is identical on all load hosts.

1. Type the command that invokes DSVCONFIG. The procedure starts with these actions:
 - It determines whether DECnet is installed. If DECnet is missing, DSVCONFIG prints a message and exits. You must have DECnet to run this procedure.

- It checks the existence and format of a data file called DSVCONFIG.DAT. It finds one of three possible situations and continues accordingly:
 - The DSVCONFIG.DAT file does not exist in the server directory. The procedure creates DSVCONFIG.DAT and tells you with a message.
 - The DSVCONFIG.DAT file exists in the server directory, but not in the correct format. The procedure reformats the file. (Some older versions of this file do not have a service circuit ID for each server.)
 - The DSVCONFIG.DAT file exists in the server directory, formatted correctly. This is the case if DSVCONFIG was previously used to add server entries. The procedure continues with its next task.
- It informs you that each server must have a unique DECnet node name and DECnet node address.
- It asks you either to continue or to exit:

Press <RET> to start, or <CTRL/Z> to exit...

Press the RETURN key if you have the information you need for each server:

- Server type for Add and Swap options
- DECnet node name for Add, Swap, and Delete options
- DECnet node address for Add option
- Ethernet address for Add and Swap options
- Service circuit ID for Add and Swap options

2. DSVCONFIG displays:

DECserver Configuration Procedure

Vn.n

Menu of Options

- 1 - List known DECservers
- 2 - Add a DECserver
- 3 - Swap an existing DECserver
- 4 - Delete an existing DECserver
- 5 - Restore existing DECservers
- <CTRL/Z> - Exit from this procedure

Your selection?

Type the number that corresponds to the option you want and press the RETURN key.

6.5.5.1 List Known DECservers (Option 1)

Select Option 1 to list the servers in the DSVCONFIG.DAT data file. The load host uses the information in this file for performing down-line loads to servers and for receiving up-line dumps from them.

Type the number 1 and press the RETURN key. The contents of DSVCONFIG.DAT displays in seven columns. Option 1 displays a listing such as this:

DECnet Address	DECnet Name	Server Type	Service Circuit	Ethernet Address	Load File	Dump File
28.1001	TUNA	DS200	UNA-0	08-00-2B-02-24-CC	PR0801ENG.SYS	DS2TUNA.DMP
28.1002	SHRIMP	DS200	UNA-0	08-00-2B-04-AA-2B	PR0801ENG.SYS	DS2SHRIMP.DMP
28.1003	CONCH	DS100	UNA-0	08-00-2B-02-24-DD	PS0801ENG.SYS	PSDMP24DD.SYS
28.1005	OYSTER	DS200	UNA-0	08-00-2B-04-AA-F1	PR0801ENG.SYS	DS2OYSTER.DMP
28.1008	TIGER	DS500	UNA-0	08-00-AA-BB-CC-DD	DS5TIGER.SYS	DS5TIGER.DMP
28.1011	LYNX	DS500	UNA-0	08-00-BB-CC-DD-EE	DS5LYNX.SYS	DS5LYNX.DMP
28.1019	LION	DS500	UNA-0	08-00-CC-DD-EE-FF	DS5LION.SYS	DS5LION.DMP
28.1022	BEAR	DS500	UNA-1	08-00-23-45-E1-F1	DS5BEAR.SYS	DS5BEAR.DMP

Total of 8 DECservers defined.

(Press RETURN for menu)

6.5.5.2 Add a DECserver (Option 2)

Select Option 2 to add an entry for a new server in the load host's node database. To create an entry, you must supply:

- The server type
- A unique DECnet node name for the server
- A unique DECnet node address for the server
- The Ethernet address of the server
- The service circuit ID

To add a server, follow these steps:

1. Type the number 2 and press the RETURN key.

2. DSVCONFIG asks:

DECserver type?

Type DS500 (for all DECserver 500 series terminal servers) and press the RETURN key.

3. DSVCONFIG asks:

DECnet node name for unit?

Specify the DECnet node name for the new server.

4. DSVCONFIG asks:

DECnet node address for unit?

Specify the DECnet node address for the new server.

5. DSVCONFIG asks:

Ethernet address of unit?

Specify the Ethernet address of the new server.

6. If you are adding a server with a DECnet node name that was previously used for a now-deleted server, DSVCONFIG asks if you want the existing image file (possibly customized for that deleted server) or a new file with default values.

On a single-system VMS load host, for example, the message looks like this:

```
File DS5node-name.SYS already exists in the SYS$SYSROOT:[DECSERVER]
directory
```

```
Do you wish to keep this file [YES]?
```

If you want the existing image file (possibly customized), press the RETURN key. On the other hand, if you want the new server's image to have all default parameters, type NO and press the RETURN key.

7. DSVCONFIG asks:

```
DECnet Service Circuit-ID [default-id]?
```

Press the RETURN key if the default service circuit is the same as the circuit that connects the load host to the same Ethernet as the server. If not, specify the service circuit ID of the desired Ethernet controller:

- UNA-*n* (for DEUNA or DELUA)
- QNA-*n* (for DEQNA or DELQA)
- BNA-*n* (for DEBNT or DEBNA, valid for VMS V5.0)
- SVA-*n* (for DESVA)

Here, *n* is an integer (typically 0 or 1). See Section 6.5.2.7 for a discussion of service circuits.

DSVCONFIG adds the entry for the new server to the databases and sets SERVICE ENABLED on the specified service circuit, both of which are necessary for down-line loading and up-line dumping.

Note

If you get an error from DECnet while you are adding a server, the entry is added to the DSVCONFIG.DAT file, even though it is not entered in the DECnet databases. To correct this synchronization problem, follow these steps:

- Use Option 4 to delete the entry.
- Fix the condition causing the DECnet error.
- Return to Option 2 to add the server again.

If you specify a node address that is already defined in DSVCONFIG.DAT, you get a DSVCONFIG error, nothing is added, and the Add option is terminated.

6.5.5.3 Swap an Existing DECserver (Option 3)

Select Option 3 to swap an existing server with a new server. Swapping is useful if you need to replace a server that malfunctions or if you are upgrading the software. When you replace servers, Swap retains the DECnet node address of the original server.

Swapping is also helpful for renaming servers and changing other DECnet characteristics. Option 3 lets you modify these DECnet characteristics for both new and existing servers:

DECnet Characteristic	Default
DECserver type	The type of server you are replacing.
DECnet node name	The name of the server you are replacing.
Ethernet address	There is no default. You must specify the Ethernet address.
DECnet service circuit ID	The service circuit ID of the load host. This should change only if you are using a different service circuit to load the new server.

If you specify a new DECnet node name, the Swap option creates a new image file, *DS5new-node-name.SYS*, while the old image file, *DS5old-node-name.SYS*, still exists in the server directory.

To swap an existing server or to modify any DECnet characteristics, follow these steps:

1. Type the number 3 and press the RETURN key.

2. DSVCONFIG asks:

What is the DECnet node name you want to swap?

Specify the DECnet node name of the existing server that you want to replace or modify.

3. DSVCONFIG displays:

DECserver at Ethernet address *nn-nn-nn-nn-nn* is being modified.

Enter the new Ethernet address and any other DECnet characteristics you want to modify.

DECserver type [*default-type*]?

Type the RETURN key if you are replacing a DECserver 100 server with another DECserver 100 server, a DECserver 200 server with another DECserver 200 server, or any DECserver 500 series terminal server with another DECserver 500 series server. If you are changing server types, specify the type of the new server and press the RETURN key. Valid responses are:

- DS100
- DS200
- DS500
- ETS

4. DSVCONFIG asks:

DECnet node name for unit [*default-name*]?

Type the RETURN key if you want the replacement server to have the same DECnet node name as the old server. If you are changing node names, specify the name of the new server and press the RETURN key.

5. DSVCONFIG asks:

Ethernet address of unit?

Specify the Ethernet address of the new server you are swapping or of the existing server you are modifying.

6. If you are not changing the DECnet node name, DSVCONFIG asks if you want the existing image file (possibly customized for the swapped or modified server) or a new file with default values.

On a single-system VMS load host, for example, the message looks like this:

```
File DS5node-name.SYS already exists in the SYS$SYSROOT:[DECSERVER]
directory
```

```
Do you wish to keep this file [YES]?
```

If you want to use the existing image, press the RETURN key. On the other hand, if you want the swapped (or modified) server's image to have all default parameters, type NO and press the RETURN key.

7. DSVCONFIG asks:

```
DECnet Service Circuit-ID [default-id]?
```

Press the RETURN key if the replacement server is loaded with the same service circuit as the old server. If the circuits are different, specify the service circuit ID of the new server and press the RETURN key. Valid service circuit IDs are:

- UNA-*n* (for DEUNA or DELUA)
- QNA-*n* (for DEQNA or DELQA)
- BNA-*n* (for DEBNT or DEBNA, valid for VMS V5.0)
- SVA-*n* (for DESVA)

Here, *n* is an integer (typically 0 or 1). See Section 6.5.2.7 for a discussion of service circuits.

DSVCONFIG swaps the DECnet characteristics you just specified with the old ones for the server with the same DECnet node address (this address cannot be swapped). DSVCONFIG also sets SERVICE ENABLED on the service circuit defined for the server.

6.5.5.4 Delete an Existing DECserver (Option 4)

Select Option 4 to remove a server from the load host's node database. Deleting a server is useful if you are reconfiguring the network or changing load hosts for a server. After you delete a server entry, the system is no longer a load host for that server.

Note that this server's image file is not deleted from the load host's server directory.

To delete servers from the database, follow these steps:

1. Type the number 4 and press the RETURN key.
2. DSVCONFIG displays:

```
(Press <CTRL/Z> to return to menu.)  
Enter the DECnet node name of the server you want to delete?
```

Specify the DECnet node name of the server you want to remove and press the RETURN key.

DSVCONFIG checks that the name you specified is an entry in DSVCONFIG.DAT. Then, it deletes this entry, reports the successful removal, and returns you to the menu. If the entry does not exist, DSVCONFIG informs you, terminates the Delete option, and returns you to the menu.

6.5.5.5 Restore Existing DECservers (Option 5)

Select Option 5 to restore the load host's DECnet databases so that they include all the servers in the server configuration database. The Restore option affects both the operational and permanent DECnet databases.

If the DECnet network contains a large number of nodes, the load host system manager might store the system's permanent DECnet database on a central, remote node and copy this database at each system startup. However, if many servers exist on the network, Digital advises against defining them in that central database.

If servers are not defined in the central database, therefore, the load host system manager must restore them whenever he or she copies the local DECnet database from the central DECnet database. Each time the system manager copies the central DECnet database, he or she can use Option 5 to restore existing server configurations.

Type the number 5 and press the RETURN key. The following messages confirm the restoration:

```
Restoring existing DECservers to host DECnet database...  
Host DECnet database successfully restored.
```

6.5.6 Restoring with the RESTORE Parameter and from the Load Host's Start-Up Procedure

There is another way, which can be automated, to restore the local DECnet database: run DSVCONFIG with the RESTORE parameter.

Using RESTORE bypasses the menu and lets the load host manager include this restoration in the system's start-up procedures. To restore servers to the DECnet database at system startup, edit the system start-up file. For instructions on how to edit this file, see the *DECserver 500 Software Installation* manual for the operating system on which you are running DSVCONFIG.

DSVCONFIG RESTORE also turns on all the specified service circuits. Note that placing @DSVCONFIG RESTORE in your start-up procedures might add time to system startup.

6.5.7 After Running DSVCONFIG

After you make any changes with the configuration procedure, repeat the same changes at all other load hosts. (This step is not required on VAXclusters.) Another way to copy entry changes to all load hosts is to copy the DSVCONFIG.DAT file to them and then run DSVCONFIG RESTORE. If you choose this method, you might have to change the service circuit IDs permanently with the Swap option.

Note

Load hosts that are VAXcluster nodes might require special considerations. See the *DECserver 500 Software Installation (VMS)* manual for details.

For step-by-step examples of running DSVCONFIG, see the *DECserver 500 Software Installation* manual for the appropriate operating system.

6.6 Keyboard Mapping

Terminal Server Configurator (TSC) enables the terminal server manager to customize keyboard tables supplied with the 3270 Terminal Option software by changing the way individual 3270 keyboard keys are mapped to Digital VT220 keys.

Keyboard tables are supplied in the distribution software for the most common languages. These tables translate 3270 key scan codes to Digital standard ASCII and escape sequence keys.

TSC commands allow you to open a keyboard table file, to list the key definitions in that table, and to change the key definitions.

You can then make the tables available to a server by using the `PURGE LANGUAGE` command to remove old table data for a particular keyboard language, and the `DEFINE LANGUAGE` command to load the modified tables into the server image. The next time the server is initialized, these tables are available to all 3270 users connected to the server.

Once tailored tables are available on a server, 3270 users can select either the `STANDARD` table or modified table variant (A) for a specified language and character set with the following terminal Set-Up options: keyboard language; national/multinational; variant.

Use the commands as follows:

- `USE TABLE` allows you to select the keyboard table file and specific keyboard table (specified by keyboard size, national or multinational character set, and table variant) within that file.
- `LIST MAPPING` displays the keyboard mapping for the specified key or all keys within the selected keyboard table.
- `LIST TABLES` lists the keyboard tables in a selected keyboard table file.
- `DEFINE MAPPING` changes the mapping of a 3270 keyboard key, specified by its scan code and the key state, to a Digital VT220 key.

- **LIST USAGE** displays information about the current keyboard table, including the keyboard table file, keyboard size, character set, and table variant when a keyboard mapping table is in use.
- **CLOSE TABLE** closes a currently open keyboard mapping table.

These commands are described in detail in Chapter 2 of the *Terminal Server Manager Commands and Messages*.

6.6.1 Example of Keyboard Mapping

The following example shows how to modify a particular keyboard table and how to make the modified table available to 3270 users on a particular server.

Use the following to open the file:

```
SYS$COMMON: [DECSERVER]CXM$FRENCH.KEYS
```

Use the 122-key keyboard (default), multinational character set (default), and Variant A table (default; may be omitted from the command).

```
TSC> USE TABLE SYS$COMMON: [DECSERVER]CXM$FRENCH.KEYS VARIANT A
Version 1.0 keyboard table file last modified on 12-JAN-1989 14:58:08
```

Next, use the **DEFINE MAPPING** command to redefine the mappings to the desired values.

The next command shows the languages currently defined in the server image.

```
TSC> LIST LANGUAGES

Language Name: North American
File:          SYS$COMMON: [DECSERVER]CXM$NORTH_AMERICAN.KEYS

Language Name: British
File:          SYS$COMMON: [DECSERVER]CXM$BRITISH.KEYS

Language Name: German
File:          SYS$COMMON: [DECSERVER]CXM$GERMAN.KEYS

Language Name: French/Belgian
File:          SYS$COMMON: [DECSERVER]CXM$FRENCH.KEYS
```

Although the `SYSS$COMMON:[DECSERVER]CXM$FRENCH.KEYS` is displayed, the tables in the server image contain the information from the old version of the file. You need to configure the server image with the modified table file as follows:

```
TSC> CLOSE TABLE
TSC> PURGE LANGUAGE FRENCH
TSC> DEFINE LANGUAGE FRENCH FILE SYSS$COMMON:[DECSERVER]CXM$FRENCH.KEYS
```

The `PURGE LANGUAGE` command removed the old French mapping tables, and the `DEFINE LANGUAGE` command loaded the French mapping tables from the updated file.

Now the modified table is in the server image file. The next time the server is initialized, the modified table(s) will be available to 3270 users connected to the server.

To use the modified tables, the user must first be using a 122-key native-mode keyboard (since the table modified was for 122-key keyboards). The user then uses the Set-Up screen to select the keyboard language (French), the character set (multinational), and the variant (A).

Configuring Ports for Common Applications

Chapter 7 provides guidelines to help you customize the server's ports for common applications. The application dictates which line card to use for the port. This chapter presents a section for each common application.

Before describing individual applications, Chapter 7 first explains cabling requirements, the next section discusses physical port characteristics, and the following section provides you with guidelines for using the application sections that follow.

This chapter discusses the following port applications:

- Terminal capable of connecting to many services
- Terminal using a dedicated service
- Personal computer used as a terminal and as a service
- Printer configured for host-initiated requests
- Printer used with a dedicated service
- Non-LAT host
- Dial-out modem
- Dial-in modem
- Dial-in/dial-out modem
- Terminal switch

- Printer using CTS/RTS flow control
- Terminal using DSR/DTR flow control
- 3270-class terminal emulating a VT220 terminal
- TD/SMP session management terminal

7.1 Cabling Requirements

This section discusses cabling requirements for each of the server line cards:

- CXY08 line card (EIA-232-D interface)
- CXA16 line card (EIA-423-A interface)
- CXB16 line card (RS-422-A interface)
- CXM04 line card

7.1.1 Cabling for the CXY08 Line Card (EIA-232-D Interfaces)

This section describes the types of cables that can be used with the CXY08 line card. The cable you choose for your port application connects to the BC19N-12 cable. The BC19N-12 connects to the CXY08 line card. See the appropriate DECserver 500 series hardware installation manual for details.

Note that although the CXY08 line card supports modem control, you can connect devices that do not use modem control. Section 7.1.1 discusses cables. For each cable, the intended applications and the permissible settings of the MODEM CONTROL port characteristic and related characteristics are specified.

7.1.1.1 Null-Modem Cables

In the following list, simpler cables are discussed before more complex cables, which can function in place of simpler ones.

1. BC22D shielded null-modem cable (data-leads-only)

The BC22D cable can be used to attach most devices that do not require modem control to a CXY08 line card. This cable permits DSR/DTR flow control and terminal power-down detection (DSRLOGOUT). It requires that the server port be set to MODEM CONTROL DISABLED.

2. BC17D shielded null-modem cable

The BC17D cable operates with ports set either to MODEM CONTROL ENABLED or to MODEM CONTROL DISABLED. It is suitable for connecting most null-modem devices that require modem control, such as non-LAT host systems, to a CXY08 line card. However, CTS/RTS flow control is not supported by the BC17D. This cable can also be used with terminals and printers that require a port without modem control.

3. BC22R shielded null-modem cable

The BC22R cable can be used for all null-modem applications except a non-LAT host that requires the modem RI signal (which the cable does not support). It is recommended for null-modem operations on ports set to MODEM CONTROL ENABLED. This cable is essential for null modem applications that require CTS/RTS flow control (which is required by some printers).

It operates with ports set either to MODEM CONTROL ENABLED or to MODEM CONTROL DISABLED.

Though it is not recommended (because of the unnecessary expense), you can use a BC17D cable in place of a BC22D cable. Except for certain restrictions mentioned above, you can use a BC22R cable in place of either the BC17D cable or the BC22D cable.

7.1.1.2 Modem Connections Using Straight-Through Cables

In the following list, the simplest cable is discussed first:

- BC22E shielded straight-through cable (full modem)

The BC22E cable, which supports 16 pins, is recommended for all normal connections to full-duplex modems on a CXY08 line card. It requires that the server port be set to MODEM CONTROL ENABLED.

- BC22F shielded straight-through cable (full modem)

The BC22F cable, which supports 25 pins, can be used for all normal connections to full-duplex modems on a CXY08 line card. Although, you can use it wherever a BC22E cable is suitable, the BC22F cable supports many unnecessary pins, which make it an expensive alternative. Like the BC22E cable, the BC22F cable requires that the server port be set to MODEM CONTROL ENABLED.

Note

See the *DECserver 500 Hardware Installation* manual for a technical description of the cables that can be used to connect devices to the CXY08 line card. Ordering information is also included in that guide.

7.1.2 Cabling for the CXA16 and CXB16 Line Card (EIA-423-A and RS-422-A Interfaces)

The CXA16 and CXB16 line cards use a 36-conductor cable (the BC16C/D) to connect to an H3104 cable concentrator for data-leads only operation. The H3104 cable concentrator contains eight ports, each of which accepts a 6-conductor terminal interconnection cable (a BC16E cable) for connecting devices. Various components can be used to extend cables. See the appropriate DECserver 500 series hardware installation manual for information about cable lengths and auxiliary components.

7.1.3 Cabling for the CXM04 Line Card

The CXM04 line card uses RG-62 coax cable or twisted-pair cable (shielded or unshielded) for connecting devices (3270-class terminals). The RG-62 coax or twisted-pair Baluns connect directly to the BNC connectors located on the module's handle. This connection requires no interface cable or interface panel. See the appropriate DECserver 500 series hardware installation manual for information about cable lengths and auxiliary components.

7.2 Configuring Physical Port Characteristics

For every device attached to the server, you must ensure that the physical characteristics of the port match the physical characteristics of the device. Table 7-1 shows the default values of these port characteristics (for more information, see Section 8.1.3).

Table 7–1: Physical Port Characteristics

Characteristic	Default
CHARACTER SIZE	8
PARITY	NONE
SPEED	9600
TYPE	SOFTCOPY
FLOW CONTROL	XON

Note

If you want to modify physical port characteristics remotely, enable REMOTE MODIFICATION.

You might experience incorrect character echoing on a terminal or be unable to communicate with an applications device. In either case, you should see whether the values of the physical characteristics on the port and the device are identical. For a port, you can use the `SHOW PORT n` command to learn these values. You must change the value of any mismatched characteristic on either the port or the device.

Note

Throughout this chapter, the examples assume that the values for physical port characteristics are identical for devices and ports. Therefore, physical port characteristics are not included in the example SET/DEFINE PORT commands.

7.2.1 Local-Access Ports

Local-access ports generally can use the autobaud facility to adjust the speed, parity, and character size of the port to the equivalent characteristics of the attached interactive device. For autobaud to function, a device must have either of the following sets of characteristic settings:

- CHARACTER SIZE 8, PARITY NONE, any autobaud-supported speed
- CHARACTER SIZE 7, PARITY EVEN, any autobaud-supported speed

The autobaud facility does not function with unusual physical characteristics, such as mark parity or split-speed operation. Some interactive devices cannot be reset so that autobaud can function. In this case, you must set the port to AUTOBAUD DISABLED and redefine the physical characteristics of the port as needed.

Always ensure that the TYPE set for a local-access port used with an interactive device is compatible with the output format used by the device (for information about the TYPE port characteristic, see Section 8.1.3).

7.2.2 Remote-Access or Dynamic-Access Ports

On a remote- or dynamic-access port, the autobaud facility cannot normally be used (unless the port device is a terminal and the application is initiated by user input). Therefore, you usually must change settings for mismatched physical characteristics in one of these ways:

- Change the character size, parity, and speed on the device itself to match the settings on the server port.
- Change the character size, parity, and speed of the port to match those of the device by using the SET/DEFINE PORT *n* command.

7.3 Guidelines for Using the Following Application Sections

The remainder of this chapter consists of application sections that describe particular uses for the server's ports. You should study these sections the first time you use any of them. Each section contains:

- A description
- A procedure that includes examples
- An illustration of the application
- A table that provides the required and recommended port values for the application
- Application notes

The port values for each application are classified as either required or recommended:

Required	Values that are essential for configuring a port for a particular application. On the tables, these values are shown in bold type.
----------	---

Recommended Values that meet the needs of the situation that you are most likely to encounter with a particular application.

7.3.1 Using Examples

The command examples are intended for you to follow when you are configuring a port that still has the default port configuration. These examples have required values and recommended nondefault values for port characteristics. The command examples reflect the following assumptions:

- The port you are configuring has all the original default values for the port characteristics.
- The port where you enter your commands has privileged status.
- You are working at a port other than the one you are configuring. Therefore, examples use the privileged “PORT *n*” form of the SET/DEFINE PORT command, in which you specify the port that you are configuring. (To reconfigure many previously configured ports, you must be working from a port other than the one to be configured.)
- The physical characteristics for devices match the default values of those characteristics on ports. Therefore, physical characteristics are not included in the example SET/DEFINE PORT commands.

7.3.2 Using Tables

Whenever you configure a port that no longer has the original default port values, use the application tables to ensure that you configure the port properly. The tables are necessary because the examples omit some of the characteristics whose recommended values are the original defaults. Table 7–2 shows the conventions used in the application tables.

Table 7–2: Using the Tables

Convention	Meaning
Bold print	Required values
Standard print	Recommended values
“Manager’s choice”	Values that you should select
“User’s choice”	Values that the port user should select

Note

User-oriented port characteristics for nonprivileged users to tailor their own environments are not discussed.

If a port is currently configured with nondefault values, you might have to specify additional values for characteristics that are omitted from the examples. There are two possible ways that you can reconfigure a port with a nondefault configuration:

- You can issue SET/DEFINE PORT commands that specify every characteristic for which an application value is suggested in the table. This method involves specifying values for about 15 port characteristics, but saves you the effort of comparing the existing configuration of the port to the application configuration.

This method might be most efficient if the applications configuration is radically different from the existing configuration.

- The alternative method has these three steps:
 - Use the SHOW/LIST PORT *n* CHARACTERISTICS command to learn the current values.
 - Compare the existing values with the application values presented in the table and identify the characteristics for which you must specify new values.
 - Issue SET/DEFINE PORT commands for only those characteristics that require new values.

This method might be most efficient if the new configuration is similar to the existing configuration.

7.4 A Terminal Capable of Connecting to Many Services

Description

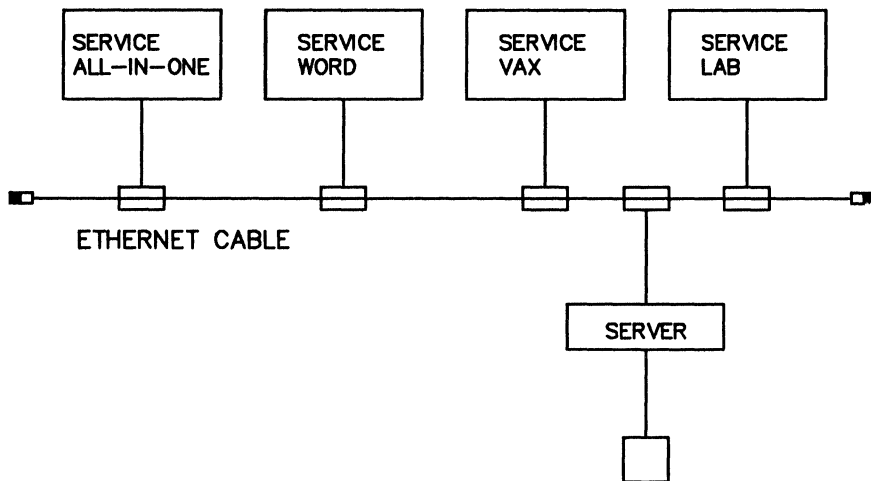
An interactive terminal is attached to a server port, which allows terminal users to access multiple services.

Procedure

This is the “default application.” All the original default values for the port characteristics are designed for this application. If all the port characteristics currently have the defaults, there is no procedure. Figure 7-1 illustrates this application.

For ports that no longer have the default configuration, see Table 7-3. It lists the values that are required and recommended for this application.

Figure 7-1: A Terminal Capable of Connecting to Many Services



LKG-1026-88
REV. 1

Table 7-3: Port Values for a Terminal Capable of Connecting to Many Services

Characteristic	Value*	Comment
ACCESS	LOCAL or DYNAMIC	
AUTOBAUD	ENABLED	See note 1
AUTOCONNECT	User's choice	
AUTOPROMPT	ENABLED	
BREAK	User's choice	See note 2
DEDICATED	NONE	
DSRLOGOUT	ENABLED	See note 3
FLOW CONTROL	XON	
INACTIVITY LOGOUT	Manager's choice	
INTERRUPTS	DISABLED	
MODEM CONTROL	DISABLED	
PASSWORD	DISABLED	See note 4

* Bold values are required for this port configuration.

Notes

1. Physical characteristics: If the autobaud facility cannot function with the terminal, set **AUTOBAUD** to **DISABLED**. For information about physical port characteristics, see Section 7.2.
2. Someone using a remote-access port might want to pass **BREAK** signals to the connected service. He or she needs **BREAK** set to **REMOTE**. On the other hand, some interactive users might want to use the **BREAK** key to return to local mode. In this case, **BREAK** must be set to **LOCAL**.
3. Cable requirements for DSR logout: DSR logout requires a null-modem cable (equivalent to a BC22D cable).
4. If the terminals attached to the server's ports are in an open area, you can set **PASSWORD ENABLED** to use log-in passwords to control user access. On the other hand, if terminals are in private offices, or you are familiar with the working area and the users, you might find no need for log-in passwords. In this case, leave the **PASSWORD** characteristic **DISABLED**.

Line Card and Cable Requirements

- CXA16 or CXB16 line card with the BC16E device cable

- CXY08 line card with the BC22D cable

Usage Notes

When logging in to a local-access port, a user encounters all or some of the following events, depending on how you configure the port:

1. If AUTOBAUD is ENABLED at a port, the server adjusts a logged out port to the speed, character size, and parity of the port device when the user presses the RETURN key several times. If AUTOBAUD is DISABLED, the server responds after the user presses the RETURN key once.
2. If PASSWORD is enabled at a port, the log-in prompt (#) appears at the port device accompanied by a beep sound. The user must enter the log-in password to gain access to the port.
3. By default, an introductory banner and help information appear as follows:

```
DECserver 500 Terminal Server V2.n - LAT V5.1  
  
Please type HELP if you need assistance
```

Note

With a dedicated service defined, the server immediately connects the port to the dedicated service and does not permit access to local mode.

4. Except when a permanent user name is defined for a port, the user name prompt (Enter username>) appears. The user enters a user name as follows:

```
Enter username> Roger
```
5. By default, the server displays the local mode prompt when the log-in procedure is completed. However, with a preferred service defined and AUTOCONNECT enabled, the server immediately connects the port to the preferred service without displaying the local mode prompt; however, the user can enter local mode at any time thereafter.

7.5 A Terminal Using a Dedicated Service

Description

An interactive terminal is attached to a server port, which is dedicated to a single service. No local mode server commands can be entered by the user.

Procedure

Use the following steps for configuring a port that has all the original default port values. Substitute the actual number of your port for the example port number 1 and the actual name of your service for the example service ALL-IN-ONE.

1. Specify these values:

```
Local> SET PORT 1 AUTOCONNECT ENA BREAK DIS DEDICATED ALL-IN-ONE
```

OR

```
TSC> DEFINE PORT 1 AUTOCONNECT ENA BREAK DIS DEDICATED ALL-IN-ONE
```

2. Ensure that the AUTHORIZED GROUPS for the port share at least one group with the service. For example, for a service belonging to group 25 on one service node and to group 99 on another service node, the following command ensures that the port can communicate with the service on both service nodes:

```
Local> SET PORT 1 AUTHORIZED GROUPS 25,99
```

OR

```
TSC> DEFINE PORT 1 AUTHORIZED GROUPS 25,99
```

3. If you make these changes on the running server, save the changes:

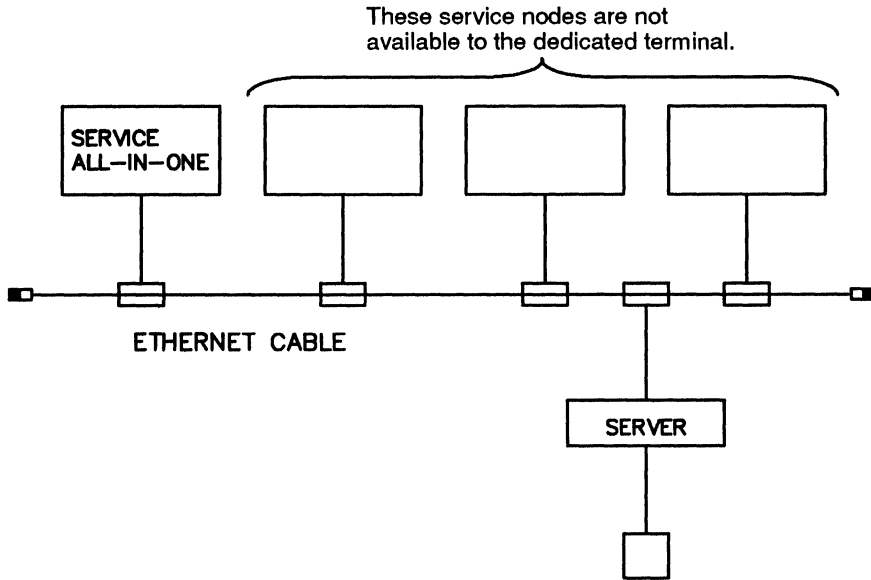
```
Local> SAVE PORT 1
```

4. If you make these changes on the running server, to begin the dedicated service, log out the port (at the next login, port 1 is automatically connected to the service ALL-IN-ONE):

```
Local> LOGOUT PORT 1
```

Figure 7-2 illustrates this application. For ports that no longer have the default configuration, see Table 7-4. The table lists the values that are required and recommended for this application.

Figure 7-2: A Terminal Using a Dedicated Service



LKG-1027-88
REV. 1

Table 7-4: Port Values for a Terminal Using a Dedicated Service

Characteristic	Value*	Comment
ACCESS	LOCAL	
AUTOBAUD	ENABLED	See note 1
AUTOCONNECT	ENABLED	See note 2
AUTOPROMPT	Manager's choice	
BREAK	DISABLED or REMOTE	See note 3
DEDICATED	<i>service-name</i>	
DSRLOGOUT	Manager's choice	See note 5
DTRWAIT	DISABLED	
FLOW CONTROL	XON	
INACTIVITY LOGOUT	Manager's choice	See note 6
INTERRUPTS	DISABLED	See note 6
MODEM CONTROL	DISABLED	
PASSWORD	DISABLED	See note 4

* Bold values are required for this port configuration.

Notes

1. **Physical characteristics:** For information about matching the physical characteristics of the port and the device, see Section 7.2.
2. **Autoconnect enabled:** The server connects the port to the dedicated service immediately at login. If the initial connection fails or a session terminates abnormally, the server attempts to reestablish the session approximately every 30 seconds until the connection is made. When the user logs out of the service, the server terminates the session and waits for a user to type input at the terminal. However, you can get dedicated functions with **AUTOCONNECT DISABLED**.
3. **BREAK:** The **BREAK** signal is ignored on a port with a dedicated service, but Digital suggests that you disable **BREAK** along with all other switch characters. Note, however, that if you need to pass the **BREAK** signal to a dedicated service for any application of that service, then set **BREAK** to **REMOTE**, so that the **BREAK** signal is passed to the service node.
4. **The log-in password:** If you want to protect a dedicated service from unauthorized users, enable the log-in password on the port. In this case, users receive the log-in prompt (#) before the service log-in sequence.
5. **Cable requirements for DSR logout:** On a **CXY08** line card, **DSR** logout requires a null-modem cable (equivalent to a **BC22D** cable).
6. The combination of both **INACTIVITY LOGOUT** and **INTERRUPTS ENABLED** is an efficient method of controlling remote access. **INACTIVITY ENABLED** by itself without modem control is not very useful. However, if a user trying to dial in cannot connect for some reason, **INACTIVITY ENABLED** logs out this user and then hangs up the line. The modem is then available for an attempted dial-in by another user.

Line Card and Cable Requirements

- **CXA16** or **CXB16** line card with the **BC16E** device cable
- **CXY08** line card with the **BC22D** cable

Usage Notes

1. Connecting without keyboard intervention

You can set up the dedicated service so that the server automatically tries to reconnect, without any keyboard intervention, a session that is abnormally disconnected. After you establish the dedicated service for the port, disable autobaud and enable autoconnect. The following example illustrates this procedure for port 1:

```
Local> SET PORT 1 DEDICATED ALL-IN-ONE
Local> SET PORT 1 AUTOBAUD DIS AUTOCONNECT ENA
Local> SAVE PORT 1
Local> LOGOUT PORT 1
```

2. Restoring a dedicated port to a multiple-service port

To restore a dedicated port to a multiple-service port, use the following commands. Begin with the port logged-in. Substitute the actual number of your port for the example port 1.

```
Local> SET PORT 1 AUTOCONNECT DIS AUTOBAUD ENA
Local> SAVE PORT 1
Local> LOGOUT PORT 1
Local> SET PORT 1 DEDICATED NONE
```

or

```
TSC> DEFINE PORT 1 DEDICATED NONE
```


7.6 A Personal Computer Used As a Terminal and As a Service

Description

A personal computer is attached to a server port that is set to `ACCESS DYNAMIC`. The degree of data transparency needed for binary file transfers typically requires setting the current session to `PASSALL` mode, either by

```
Local> SET SESSION PASSALL
```

or

```
$ SET TERM/PASSALL
```

if the host node is running `VMS`. The personal computer has the following alternative uses:

- Sometimes the computer is an interactive device (capable of functioning either in terminal emulation or in file transfer mode).
- At other times the personal computer is available as a local service (and it can be connected to as a file transfer partner by another personal computer). The port must be assigned to a local service for the personal computer to receive remote requests for connections. For information about offering a local service, see Section 5.8.

Note

All discussions of file transfers assume that the file transfer programs treat the data as binary rather than as ASCII.

Procedure

Use the following steps for configuring a port that has all the original default port values. Substitute the actual number of your port for the example port number 2 and the actual name of your service for the example service `MICRO`.

1. Specify these values:

```
Local> SET PORT 2 ACCESS DYNAMIC MODEM ENABLED DTRWAIT ENABLED
Local> SET PORT 2 AUTOBAUD DIS BREAK DIS
Local> SET PORT 2 INACTIVITY ENA LOCAL SWITCH ^\
```

or

```
TSC> DEFINE PORT 2 ACCESS DYNAMIC MODEM ENABLED DTRWAIT ENABLED
TSC> DEFINE PORT 2 AUTOBAUD DIS BREAK DIS
TSC> DEFINE PORT 2 INACTIVITY ENA LOCAL SWITCH ^\
```

- 2. Ensure that both the AUTHORIZED GROUPS and the CURRENT GROUPS for the port of the user trying to connect to the service share at least one group with the service.**
- 3. If you make these changes on the running server, save the changes and log out the port:**

```
Local> SAVE PORT 2
Local> LOGOUT PORT 2
```

- 4. Assign the port to a service and specify an identification string for the service:**

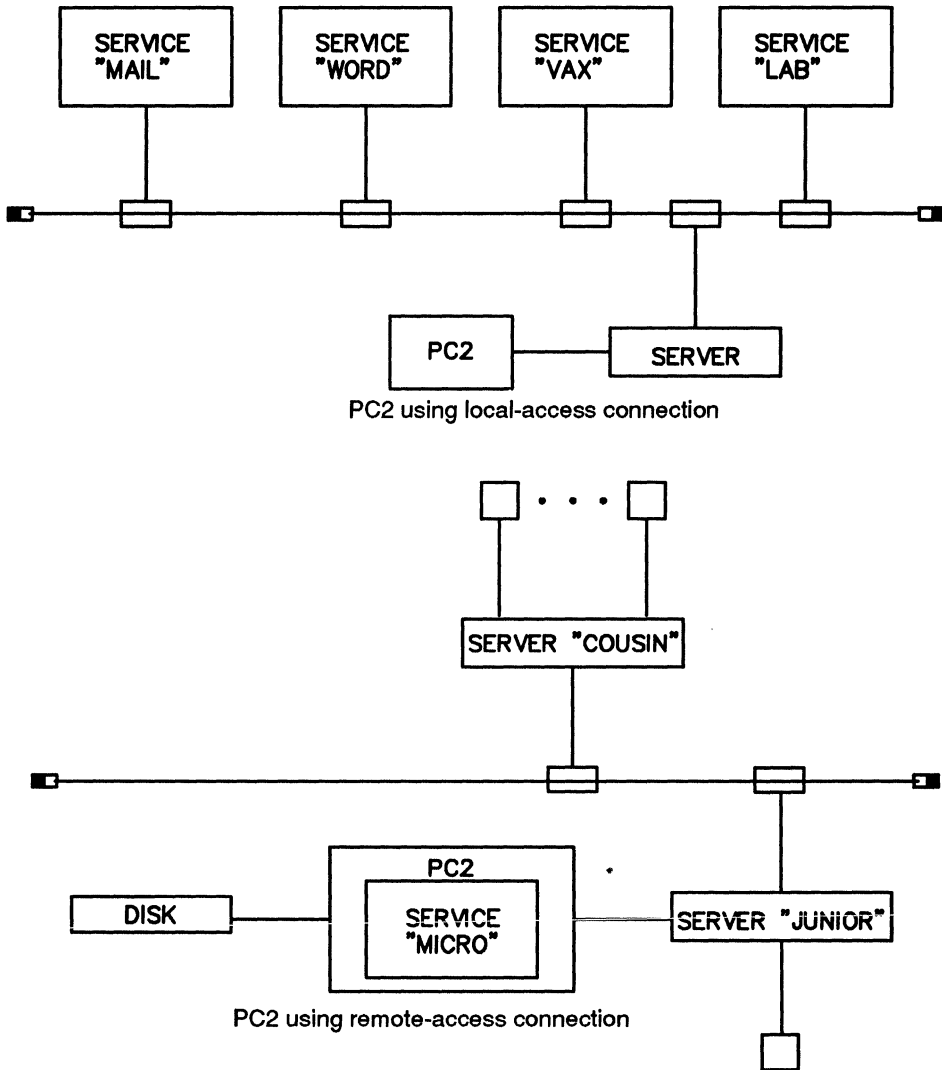
```
Local> SET SERVICE MICRO PORT 2 IDENT "Personal computer 2"
```

or

```
TSC> DEFINE SERVICE MICRO PORT 2 IDENT "Personal computer 2"
```

Figure 7–3 illustrates this application. For ports that no longer have the default configuration, see Table 7–5. The table lists the port values that are required and recommended for this application.

Figure 7-3: A Personal Computer Used As a Terminal and As a Service



LKG-1042-87

Table 7-5: Port Values for a Personal Computer Using Dynamic Access

Characteristic	Value*	Comment
ACCESS	DYNAMIC	
AUTOBAUD	DISABLED	See note 1
AUTOCONNECT	User's choice	
AUTOPROMPT	ENABLED	
BREAK	DISABLED	See note 2
DEDICATED	NONE	
DSRLOGOUT	DISABLED	
DTRWAIT	ENABLED	
FLOW CONTROL	XON	
INACTIVITY LOGOUT	ENABLED	See note 3
INTERRUPTS	DISABLED	See note 4
LOCAL SWITCH	Manager's choice	See note 5
MODEM CONTROL	ENABLED	
PASSWORD	DISABLED	See note 6

* Bold values are required for this port configuration.

Notes

1. **Physical characteristics:** Because the autobaud facility does not usually work with remote access, set **AUTOBAUD** to **DISABLED**. Ensure that the physical characteristics of the port and the personal computer are matching. For information about matching the physical characteristics of the port and the device, see Section 7.2.
2. **BREAK:** Users should not use **BREAK** while the personal computer is functioning as a service. Digital recommends that you set **BREAK** to **DISABLED**, unless you decide to enable **INTERRUPTS** (see note 4). With **BREAK DISABLED**, ensure that you also define a local switch character.
3. **Inactivity logout:** Digital recommends that you enable the inactivity logout feature since remote access cannot occur while the port remains logged in.
4. **Interrupting sessions:** If you decide to enable interrupts by setting a port to **INTERRUPTS ENABLED**, also set **BREAK** to **LOCAL**.
5. **Local switch:** When you specify **BREAK DISABLED**, also specify a local switch character. For information about selecting a switch character see the *DECserver 500 Use* manual.

6. **Log-in password:** Enabling the log-in password restricts local access to the personal computer. This is an important form of security in some environments. Give this password only to authorized users. However, if such security is unnecessary, specify **PASSWORD DISABLED**.

Note

For remote-access security, specify a service password for the local service offering the personal computer.

Line Card and Cable Requirements

Use the CXY08 line card with one of the following cables:

- BC22R shielded null-modem cable *
- BC17D shielded null-modem cable
- * Recommended

Usage Notes

With the port set to **ACCESS DYNAMIC**, the PC can switch back and forth from local access to remote access:

1. Local access

Using local access, a personal computer can alternate between the following modes:

- Terminal emulation mode, which allows the personal computer to access services on the LAT network.
- File transfer mode, which allows the personal computer to initiate file transfers with another computer as a transfer partner. The partner must have a file transfer program that is compatible with the program used by the transfer initiator. For information about managing file transfers, see Section 5.11.

Note

The PC functioning as the file transfer partner might also require some modifications to its setup before a file can be transferred. See the documentation for that personal computer and for the file transfer program that you are using.

To learn how to access and use these two modes, see the documentation of each personal computer.

Personal computers using local access can connect to a printer offered as a service when a user issues a `CONNECT` command. However, for the user to access the printer, the personal computer must have an applications program capable of sending files to the printer. The person in charge of the computer must supply the appropriate applications program. Unlike host-initiated requests, connection requests to a printer using `CONNECT` are not queued by the server.

2. Remote access

To be available for remote-access connections, a personal computer must be logged out from the server port. When a remote-access connection is made to the port, the port shifts to remote-access mode. With the port in remote-access mode, the port groups become inactive. However, because the port is assigned to a local service, the service groups that you defined for local services take effect. For an explanation of groups, see Section 5.3.

You can enable local-access interrupts of remote-access sessions but Digital does not recommend that you normally do this. With `INTERRUPTS ENABLED` on the port, a user at the personal computer can interrupt a remote-access connection by pressing the `BREAK` key on the computer keyboard, after entering terminal emulation mode.

7.7 A Printer Configured for Host-Initiated Requests

Description

A printer used with an asynchronous EIA-232-D or DECconnect interface is attached at a remote- or dynamic-access port. (Dynamic access allows a keyboard printer to alternate, according to user demand, between operating as a printer and as a terminal.)

Suitably configured service nodes containing LAT V5.1 service software can access the printer by making host-initiated requests. See Appendix C for more information on setting up remote printer queues.

Procedure

This application requires a configuration procedure for the server and for the service node.

- On the running server or with TSC

Use the following steps for configuring a port that has all the original default port values. This example uses an LN01 laser printer. Substitute the actual number of your port for the example port number 4 and select appropriate names for the port and the service:

- Specify these values:

```
Local> SET PORT 4 ACCESS REMOTE AUTOBAUD DIS BREAK DIS NAME LN01A
Local> SAVE PORT 4
Local> LOGOUT PORT 4
```

OR

```
TSC> DEFINE PORT 4 ACCESS REMOTE AUTOBAUD DIS BREAK DIS NAME LN01A
```

- Setting up a service for printers is optional but can be a useful management aid. If you decide to offer a printer as a service, choose an appropriate service name such as LASER:

```
Local> SET SERVICE LASER PORT 4 IDENT "LN01 laser printer"
```

OR

```
TSC> DEFINE SERVICE LASER PORT 4 IDENT "LN01 laser printer"
```

- Host-initiated connections are constrained by the **AUTHORIZED GROUPS** of the ports offering the printers. Ensure that the ports share at least one group with the requesting service node or nodes.

For information about offering a local service, see Section 5.8.

For ports that no longer have the original default values, see Table 7–6. The table lists the values that are required and recommended for this application.

- **On the service nodes**

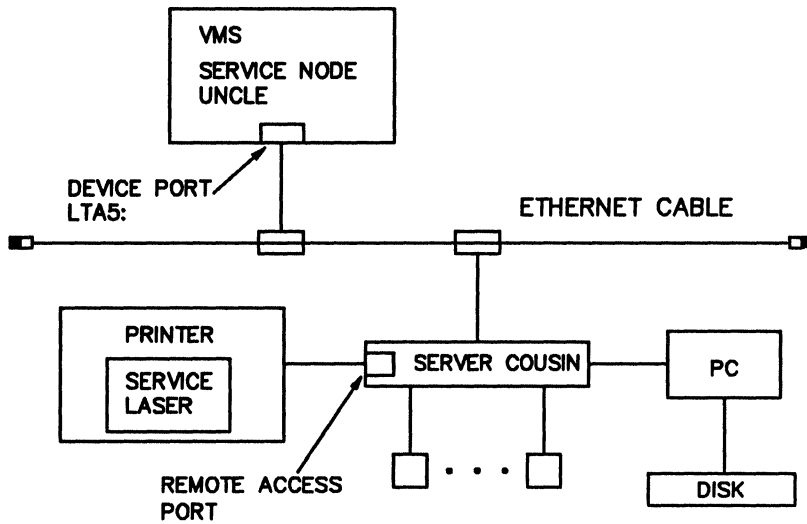
Service nodes that contain the LAT V5.1 service software must be suitably configured to access a printer on a remote- or dynamic-access port. Once configured, those service nodes can access the printer. Supply the system managers with the following information for configuring service nodes:

- The server name
- The service names and/or the port name or names
- At least one group that is enabled as an authorized group on the port

To learn whether the service software used by a particular operating system supports host-initiated requests, see the software product description (SPD) for that system. For systems supporting host-initiated requests, see the LAT documentation of the operating system for information about configuring a service node for host-initiated requests. For VMS systems V4.4 and V4.5, see the *LATplus/VMS Service Node Management Guide*. For VMS systems V5.0 to V5.2, see the basic VMS documentation set.

Figure 7–4 illustrates this application.

Figure 7-4: A Printer Offered As a Service for Host-Initiated Requests



LKG-0356-57
REV. 1

Table 7–6: Port Values for a Printer Configured for Host-Initiated Requests

Characteristic	Value*	Comment
ACCESS	REMOTE or DYNAMIC	See note 1
AUTOBAUD	DISABLED	See note 2
AUTOCONNECT	User's choice	
AUTOPROMPT	ENABLED	
BREAK	DISABLED	
DEDICATED	NONE	
DSRLOGOUT	ENABLED	See notes 3 and 6
DTRWAIT	DISABLED	
FLOW CONTROL	XON	See note 4
INACTIVITY LOGOUT	Manager's choice	See note 1
INTERRUPTS	Manager's choice	See notes 1 and 5
MODEM CONTROL	DISABLED	See notes 3 and 6
NAME	<i>port-name</i>	See note 7
PASSWORD	DISABLED	
SIGNAL CHECK	ENABLED	See note 3

* **Bold values are required for this port configuration.**

Notes

1. **Access:** For a keyboard printer, you can set the port to **ACCESS DYNAMIC** to allow the printer to function sometimes as a terminal. In this case, you might want to enable **INTERRUPTS** (see note 5) along with **INACTIVITY LOGOUT**.
2. **Physical characteristics:** For information about matching the physical characteristics of the port and the device, see Section 7.2.
3. With **MODEM CONTROL DISABLED**, you can use **DSRLOGOUT ENABLED** to detect a printer that is powered off if the printer asserts modem signals when powered up. **DSRLOGOUT ENABLED** then disconnects the current session on the port. Depending on the service node's print queuing capability, this could cause the print job to be terminated. Note that **SIGNAL CHECK** may be enabled only for a port that also has either **MODEM CONTROL** or **DSRLOGOUT** set to **ENABLED**.

You can also obtain this function by using a BC17D cable with **MODEM ENABLED**.

4. **Flow control:** CTS/RTS or DTR/DSR flow control is used by some printers instead of XON/XOFF.
5. **Interrupting sessions:** With ACCESS DYNAMIC, you can enable local-access interrupts of remote-access sessions. With INTERRUPTS ENABLED on the port, a user at a keyboard printer can interrupt a remote-access connection by pressing the BREAK key on the keyboard. BREAK must be set to LOCAL for interrupt to work.
6. **Modem control:** You cannot always specify MODEM DISABLED for a directly connected printer. A printer might be attached to the server either by data switches or by a line over which signals are amplified using line drivers or short-haul modems. In these cases, you might have to enable MODEM CONTROL on the port used with the printer. You should also enable MODEM CONTROL when using a BC17D cable.

You can use MODEM ENABLED on certain printers so that the server disconnects the session when the printer powers off. Depending on the service node's operating system, the service node then usually terminates the print job (but possibly restarts it later when the printer is powered back on).

For information about using dial-out modems on remote-access ports, see Section 7.10; for information about using dial-in/dial-out modems on dynamic-access ports, see Section 7.12.

7. **Naming remote-access ports:** You can facilitate explicit requests for ports by changing the port name to a descriptive term. For example, you might match the port name to the name being used for the corresponding applications port on service nodes (such as LA310) or to a name reflecting an associated service name (such as LASER_PORT1).

Note that the name of each port must be unique on the server. Port names follow the naming conventions of the server described in the *Terminal Server Commands and Messages Reference*. They must contain at least one alphabetic character.

Line Card and Cable Requirements

Use the CXA16 or CXB16 line card with the BC16E device cable.

Use the CXY08 line card with one of the following cables:

- For directly connected printers:
 - BC22D shielded null-modem cable (or DSRLOGOUT or DTR/DSR flow control) (data-leads-only)*
 - BC22R shielded null-modem cable**
 - BC17D shielded null-modem cable
- * Recommended (except with CTS/RTS flow control)
- ** Use with CTS/RTS flow control
- For printers used with modems:
 - BC22E shielded straight-through cable (full modem)*
 - BC22F shielded straight-through cable (full modem)
- * Recommended

7.8 A Printer Used with a Dedicated Service

Description

An asynchronous EIA-232-D or DECconnect printer is attached to a dedicated port. You connect the port to the dedicated computer service by using a series of local mode commands.

This facility allows you to connect printers to hosts that do not support host-initiated requests. For printers used with service nodes that support the LAT V5.1 protocol, use the port configuration described in Section 7.7.

Procedure

Use the following steps for configuring a port that has all the original default port values. Substitute the actual number of your port for the example port number 88 and the actual name of your service for the example service BUDDY.

1. Specify these values:

```
Local> SET PORT 88 ACCESS LOCAL
Local> SET PORT 88 AUTOBAUD DIS AUTOCONNECT ENA
Local> SET PORT 88 AUTOPROMPT DIS DEDICATED BUDDY
```

or

```
TSC> DEFINE PORT 88 ACCESS LOCAL
TSC> DEFINE PORT 88 AUTOBAUD DIS AUTOCONNECT ENA
TSC> DEFINE PORT 88 AUTOPROMPT DIS DEDICATED BUDDY
```

2. Ensure that the **AUTHORIZED GROUPS** for the port share at least one group with the service.

3. If you make these changes on the running server, save the changes:

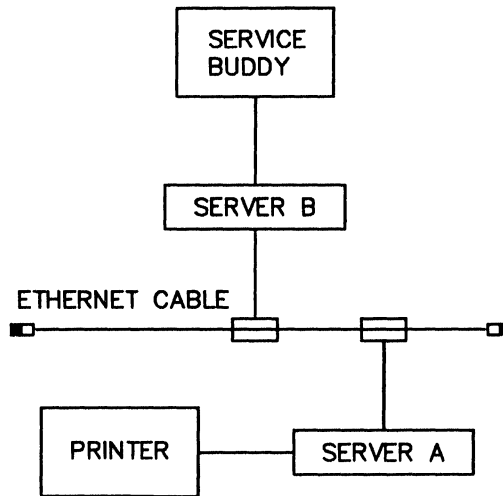
```
Local> SAVE PORT 88
```

4. If you make these changes on the running server, produce the connection to the dedicated service:

```
Local> LOGOUT PORT 88
```

Figure 7-5 illustrates this application. For ports that no longer have the default configuration, see Table 7-7. The table lists port values that are required and recommended for this application.

Figure 7–5: A Printer Used with a Dedicated Service



LKG-0195-88
REV. 1

Table 7–7: Port Values for a Printer Used with a Dedicated Service

Characteristic	Value*	Comment
ACCESS	LOCAL	
AUTOBAUD	DISABLED	See note 1
AUTOCONNECT	ENABLED	
AUTOPROMPT	DISABLED	See note 2
BREAK	LOCAL	
DEDICATED	<i>service-name</i>	
DSRLOGOUT	ENABLED	See notes 3 and 5
DTRWAIT	DISABLED	
FLOW CONTROL	XON	See note 4
INACTIVITY LOGOUT	DISABLED	
INTERRUPTS	DISABLED	
MODEM CONTROL	DISABLED	See note 5
PASSWORD	DISABLED	

* Bold values are required for this port configuration.

Notes

1. **Physical characteristics:** For information about matching the physical characteristics of the port and the device, see Section 7.2.
2. **Disabling autoprompt:** Autoprompting usually causes a service node log-in process to be attached to the port to wait for user input, such as a user name. This might make it difficult for another process on the service node to get control of the port for printing purposes. Therefore, it is essential to set the port to **AUTOPROMPT DISABLED**.
3. With **MODEM CONTROL DISABLED**, you can use **DSRLOGOUT ENABLED** to detect a printer that is powered off if the printer asserts modem signals when powered up. **DSRLOGOUT ENABLED** then disconnects the current session on the port. Depending on the service node's print queuing capability, this could cause the print job to be terminated.

You can also obtain this function by using a BC17D cable with **MODEM ENABLED**.

4. **Flow control:** **CTS/RTS** or **DTR/DSR** flow control is used by some printers.
5. **Modem control:** You cannot always specify **MODEM DISABLED** for a directly connected printer. A printer might be attached to the server either by data switches or by a line over which signals are amplified using line drivers or short-haul modems. In these cases, you might have to enable **MODEM CONTROL** on the port used with the printer. You should also enable **MODEM CONTROL** when using a BC17D cable.

You can use **MODEM ENABLED** on certain printers so that the server disconnects the session when the printer powers off. Depending on the service node's operating system, the service node then usually terminates the print job (but possibly restarts it later when the printer is powered back on).

For information about using dial-out modems on remote-access ports, see Section 7.10; for information about using dial-in/dial-out modems on dynamic-access ports, see Section 7.12.

Line Card and Cable Requirements

Use the CXA16 or CXB16 line card with the BC16E device cable.

Use the CXY08 line card with one of the following:

- BC22D shielded null-modem cable (or DSRLOGOUT or DTR/DSR flow control) (data-leads-only)*
- BC22R shielded null-modem cable**
- BC17D shielded null-modem cable

* Recommended except for printers using CTS/RTS flow control

** Required for CTS/RTS flow control

Usage Notes

1. To disconnect the printer from a dedicated service, enter the following commands:

```
Local> SET PORT 88 AUTOBAUD ENABLED
Local> SAVE PORT 88
Local> LOGOUT PORT 88
Local> SET PORT 88 DEDICATED NONE
Local> SAVE PORT 88
Local> LOGOUT PORT 88
```

or

```
TSC> DEFINE PORT 88 DEDICATED NONE
```

2. To use the printer on the service node, the terminal users need to know its device name at the service node. The device name usually changes when the system manager reboots the service node, when you initialize the server, or when you connect the printer to the service. The procedure for determining the printer device name depends on the operating system for the service node.

7.9 A Non-LAT Host

Description

A non-LAT host computer is attached to one or more ports and is offered as a service.

Digital strongly recommends that you offer a non-LAT host as a service only on a CXY08 port and that you set MODEM CONTROL to ENABLED on that port. If you define services for a port on a CXA16 or CXB16 line card, any host process running as a service session is not secure. In this case, when a user terminates a session, the host does not stop the user's process and a new user might have access to it.

Procedure

Use the following steps for configuring a port that has all the original default port values. Substitute the actual number of your port for the example port number 97 and the actual name of your service for the example service NONDEC.

1. Specify these values:

```
Local> SET PORT 97 ACCESS REMOTE AUTOBAUD DISABLED BREAK DISABLED
Local> SET PORT 97 DTRWAIT ENABLED MODEM ENABLED
```

or

```
TSC> DEFINE PORT 97 ACCESS REMOTE AUTOBAUD DISABLED BREAK DISABLED
TSC> DEFINE PORT 97 DTRWAIT ENABLED MODEM ENABLED
```

2. Digital suggests that for any remote- or dynamic-access application you change the port speed to match the device. Therefore, you might want to change the port speed to match the device with this application since AUTO-BAUD is DISABLED, for example:

```
Local> SET PORT 97 SPEED 7200
```

or

```
TSC> DEFINE PORT 97 SPEED 7200
```

3. Ensure that both the AUTHORIZED GROUPS and the CURRENT GROUPS for the port of the user trying to connect to the service share at least one group with the service.

4. If you make these changes on the running server, save the changes and log out the port:

```
Local> SAVE PORT 97
```

```
Local> LOGOUT PORT 97
```

5. Assign the port to the service:

```
Local> SET SERVICE NONDEC PORT 97 IDENT "XYZ minicomputer"
```

or

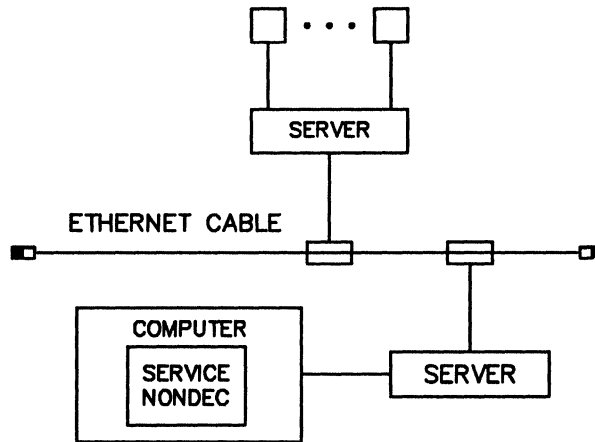
```
TSC> DEFINE SERVICE NONDEC PORT 97 IDENT "XYZ minicomputer"
```

6. Attach any of the terminal interfaces of the computer and any port that you have configured as described in this section. By using multiple terminal interfaces and ports, you can use more than one port with a single computer system. Ensure that each port is assigned to a service.

Figure 7–6 illustrates this application. For more information about offering a local service, see Section 5.8.

For ports that no longer have the original default configuration, see Table 7–8, which lists required and recommended port values.

Figure 7-6: A Non-LAT Host Offered As a Service



LKG-1083-88
REV. 1

Table 7–8: Port Values for a Non-LAT Host

Characteristic	Value*	Comment
ACCESS	REMOTE	See note 1
AUTOBAUD	DISABLED	
AUTOCONNECT	DISABLED	
BREAK	DISABLED	
DEDICATED	NONE	
DSRLOGOUT	DISABLED	
DTRWAIT	ENABLED	
FLOW CONTROL	XON	
INACTIVITY LOGOUT	DISABLED	
INTERRUPTS	DISABLED	
MODEM CONTROL	ENABLED	See notes 2 and 3
PASSWORD	DISABLED	

* Bold values are required for this port configuration.

Notes

1. **Physical characteristics:** For information about matching the physical characteristics of the port and the device, see Section 7.2.
2. **Modem control:** With modem control enabled, the server knows when the user has logged out from the computer and automatically disconnects the session, providing an important security feature.

MODEM CONTROL ENABLED also lets the host know when a user has connected the session since the server does not assert modem signals (with **DTRWAIT ENABLED**) until a user actually connects to the remote-access port.

Without modem control, sessions remain open when a user logs out of the host system, and a subsequent user connecting to the remote-access port might gain access to the previous user's data.

3. Some non-LAT hosts require the modem RI (ring indicator) signal to transition from off to on several times to respond to a connection. The server asserts a single modem signal via a null-modem cable, which the non-LAT host interprets as the RI signal, but the server cannot force multiple RI transitions when the user connects to the remote-access port. Therefore, do not attach a non-LAT host that requires the RI signal to act this way.

Line Card and Cable Requirements

Use the CXY08 line card with one of the following:

- BC22R shielded null-modem cable (required for CTS/RTS flow control; however, this cable should not be used if the host must see the modem RI signal)
- BC17D shielded null-modem cable (required if the non-LAT host must see the modem RI signal)

Digital does not supply a cable that allows a non-LAT host to have CTS/RTS flow control and the ability to see the modem RI signal.

7.10 A Dial-Out Modem

Description

A dial-out modem is attached to a port and offered as a service. A user connects to the service and then communicates with that modem to dial out to a remote modem. The modem dials out to a remote modem to complete a connection between a host and an interactive device such as a terminal. For information about how modems operate, see Section 5.6.5.

Procedure

Use the following steps for configuring a port that has all the original default port values. Substitute the actual number of your port for the example port number 3 and the actual name of your service for the example service MODEM.

1. Specify these values:

```
Local> SET PORT 3 ACCESS REMOTE AUTOBAUD DIS
Local> SET PORT 3 BREAK DIS DTRWAIT ENA MODEM ENA
```

OR

```
TSC> DEFINE PORT 3 ACCESS REMOTE AUTOBAUD DIS
TSC> DEFINE PORT 3 BREAK DIS DTRWAIT ENA MODEM ENA
```

2. You might also want to specify the speed of port 3 on the server port. For example, with a modem that supports 1200 bits per second (bps), issue:

```
Local> SET PORT 3 SPEED 1200
```

OR

```
TSC> DEFINE PORT 3 SPEED 1200
```

3. Ensure that both the **AUTHORIZED GROUPS** and the **CURRENT GROUPS** for the port of the user trying to connect to the service share at least one group with the service.
4. If you make these changes on the running server, save the changes and log out the port:

```
Local> SAVE PORT 3
Local> LOGOUT PORT 3
```

5. Assign the port to the service:

```
Local> SET SERVICE MODEM PORT 3
```

or

```
TSC> DEFINE SERVICE MODEM PORT 3
```

6. Digital recommends that you define a service password for the dial-out modem service to protect access to the modem. The following example defines the service password **CARDINAL** for the service **MODEM**:

```
Local> SET SERVICE MODEM PASSWORD "CARDINAL"
```

or

```
TSC> DEFINE SERVICE MODEM PASSWORD "CARDINAL"
```

7. Digital suggests that you specify a service identification string that helps to use the modem or to distinguish among different kinds of modems. For example, the following identification string for service **MODEM** notes the type of modem and the two basic steps for using the modem:

```
Local> SET SERVI MODEM IDENT "DF224 modem - Press <CTRL/B>; Dialing  
format: T=nn#"
```

or

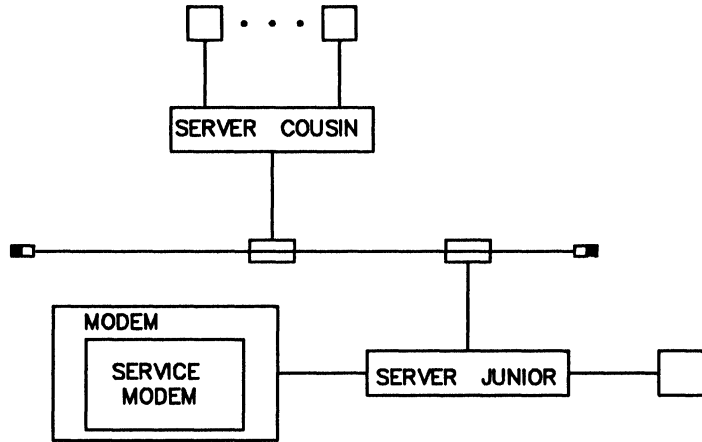
```
TSC> DEF SERVI MODEM IDENT "DF224 modem - Press <CTRL/B>; Dialing  
format: T=nn#"
```

While this information is probably insufficient for a naive user, it can help an experienced user who does not remember the particular modem's dial-out commands.

Figure 7-7 illustrates this application. For more information about offering a service, see Section 5.8.

For ports that no longer have the default port values, see Table 7-9. The table lists the port values that are required and recommended for this application.

Figure 7-7: A Dial-Out Modem Offered As a Service



LKG-1084-87

Table 7-9: Port Values for a Dial-Out Modem

Characteristic	Value*	Comment
ACCESS	REMOTE	
AUTOBAUD	DISABLED	See note 1
AUTOCONNECT	DISABLED	
BREAK	DISABLED	
DEDICATED	NONE	
DSRLOGOUT	DISABLED	
DTRWAIT	ENABLED	
FLOW CONTROL	XON	
INACTIVITY LOGOUT	ENABLED	See note 2
INTERRUPTS	DISABLED	
MODEM CONTROL	ENABLED	
PASSWORD	DISABLED	

* Bold values are required for this port configuration.

Notes

1. **Physical characteristics:** For information about matching the physical characteristics of the port and the device, see the discussion of physical port characteristics in Section 7.2.
2. **Inactivity logout:** To protect a port from being held open by an inactive user, define `INACTIVITY` as `ENABLED`.

Line Card and Cable Requirements

Use the CXY08 line card with one of the following:

- BC22E shielded straight-through cable (full modem)*
- BC22F shielded straight-through cable (full modem)

* Recommended

7.11 A Dial-In Modem

Description

Dial-in modems are used on local-access ports and are handled as a terminal by the server. Users gain access to a dial-in port from a terminal connected to a dial-out modem.

Procedure

Use the following commands for configuring a port that has all the original default port values. Substitute the actual number of your port for the example port number 6.

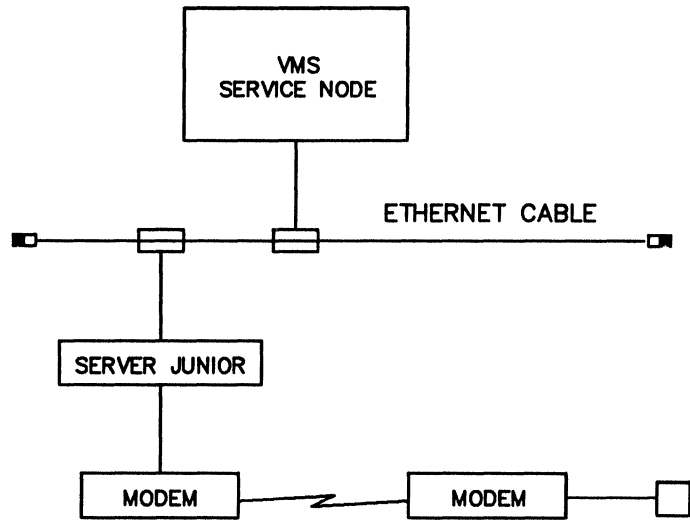
```
Local> SET PORT 6 INACTIVITY LOGOUT ENA MODEM ENA PASSWORD ENA  
Local> SAVE PORT 6  
Local> LOGOUT PORT 6
```

or

```
TSC> DEFINE PORT 6 INACTIVITY LOGOUT ENA MODEM ENA PASSWORD ENA
```

Figure 7–8 illustrates this application.

Figure 7-8: A Dial-In Modem Used with a Terminal



LKG-1085-88

For ports that no longer have the default configuration, see Table 7-10. The table lists the port values that are required and recommended for this application.

Table 7–10: Port Values for a Dial-In Modem

Characteristic	Value*	Comment
ACCESS	LOCAL	
AUTOBAUD	ENABLED	See note 1
AUTOCONNECT	DISABLED	See note 7
AUTOPROMPT	ENABLED	
BREAK	LOCAL	See note 2
DEDICATED	NONE or <i>service-name</i>	See note 7
DSRLOGOUT	DISABLED	
DTRWAIT	DISABLED	See note 3
FLOW CONTROL	XON	
INACTIVITY LOGOUT	ENABLED	See note 4
INTERRUPTS	DISABLED	
LIMITED VIEW	ENABLED	See note 6
MODEM CONTROL	ENABLED	
PASSWORD	ENABLED	See note 5

* Bold values are required for this port configuration.

Notes

1. **Physical characteristics:** For information about matching the physical characteristics of the port and the device, see Section 7.2.
2. **BREAK and a local switch:** The **BREAK** key cannot function as a local switch for some modems that disconnect the call when they receive the **BREAK** signal. For such a modem, specify a local switch character and **BREAK DISABLED**. The local switch character ensures that the user can reenter local mode after establishing a session. For information about selecting a switch character see the *DECserver 500 Use* manual.
3. **Autoanswering equipment:** The port characteristic **DTRWAIT** can be enabled to delay assertion of **DTR** and **RTS** until the server detects an **RI** signal from the dial-in modem. Normally, **DTRWAIT** should be **DISABLED** so that **DTR** and **RTS** are asserted while the port is idle. However, to support certain autoanswering equipment, you can set **DTRWAIT** to **ENABLED**.
4. **Inactivity logout:** To protect a port from being held open by an inactive user, define **INACTIVITY** as **ENABLED**.
5. **Log-in password:** Enabling the log-in password on the port is an important security measure. Digital strongly recommends this step.

6. **Limited view:** To prohibit users on dial-in ports from seeing the nodes and services available to them, enable **LIMITED VIEW**.
7. **Dedicated service:** You can set up a dedicated service for the dial-in modem. If you set **AUTOCONNECT** to **DISABLED**, the server logs out the port and disconnects the call when a session ends. If you set **AUTOCONNECT** to **ENABLED**, the server does not log out the port.

Line Card and Cable Requirements

Use the **CXY08** line card with one of the following:

- **BC22E shielded straight-through cable (full modem)***
- **BC22F shielded straight-through cable (full modem)**

* **Recommended**

Usage Notes

1. If the port is password protected, as Digital recommends, the user receives the log-in password prompt (#) and must enter the correct password before being allowed by the server to log in to the port.
2. When the user logs in to the port through the dial-in modem, the port functions like a local-access port to which the user's terminal is directly attached.

7.12 A Dial-In/Dial-Out Modem

Description

A dial-in/dial-out modem is attached to a dynamic-access port and offered as a service. Sometimes, the modem is used to receive dial-in calls from an interactive user whose terminal or terminal server is attached to a remote modem. At other times the modem is used for dial-out calls to modems attached to remote systems.

Procedure

Use the following steps for configuring a port that has all the original default port values. Substitute the actual number of your port for the example port number 4 and the actual name of your service for the example service MODEM.

1. Specify these values:

```
Local> SET PORT 4 ACCESS DYNAMIC AUTOBAUD DIS
Local> SET PORT 4 INACTIVITY ENA MODEM ENA PASSWORD ENA
```

or

```
TSC> DEFINE PORT 4 ACCESS DYNAMIC AUTOBAUD DIS
TSC> DEFINE PORT 4 INACTIVITY ENA MODEM ENA PASSWORD ENA
```

2. Digital suggests that you specify the speed of the port. For example, with a modem that supports 2400 bits per second (bps), issue:

```
Local> SET PORT 4 SPEED 2400
```

or

```
TSC> DEFINE PORT 4 SPEED 2400
```

3. Ensure that both the **AUTHORIZED GROUPS** and the **CURRENT GROUPS** for the port of the user trying to connect to the service share at least one group with the service.
4. If you make these changes on the running server, save the changes and log out the port:

```
Local> SAVE PORT 4
Local> LOGOUT PORT 4
```

5. Assign the port to the service:

```
Local> SET SERVICE MODEM PORT 4
```

or

```
TSC> DEFINE SERVICE MODEM PORT 4
```

6. Digital recommends that you define a service password for the modem service, for example:

```
Local> SET SERVICE MODEM PASSWORD "PHONE HOME"
```

or

```
TSC> DEFINE SERVICE MODEM PASSWORD "PHONE HOME"
```

7. Digital suggests that you specify a service identification:

```
Local> SET SERVICE MODEM IDENT "Combo dial-in/dial-out modem"
```

or

```
TSC> DEFINE SERVICE MODEM IDENT "Combo dial-in/dial-out modem"
```

For more information about offering a service, see Section 5.8.

For ports that no longer have the default configuration, see Table 7–11. The table lists the port values that are required and recommended for this application.

Table 7–11: Port Values for a Dial-In/Dial-Out Modem

Characteristic	Value*	Comment
ACCESS	DYNAMIC	
AUTOBAUD	DISABLED	See note 1
AUTOCONNECT	DISABLED	See note 6
AUTOPROMPT	ENABLED	
BREAK	DISABLED	See note 2
DEDICATED	NONE	See note 6
DSRLOGOUT	DISABLED	
DTRWAIT	Manager's choice	See note 3
FLOW CONTROL	XON	
INACTIVITY LOGOUT	ENABLED	See note 4
INTERRUPTS	DISABLED	
LIMITED VIEW	ENABLED	
MODEM CONTROL	ENABLED	
PASSWORD	ENABLED	See note 5

* Bold values are required for this port configuration.

Notes

1. **Physical characteristics:** For information about matching the physical characteristics of the port and the device, see Section 7.2.
2. **BREAK and a local switch:** The **BREAK** key cannot function as a local switch for some modems that disconnect the call when they receive the **BREAK** signal. For such a modem, specify a local switch character and **BREAK DISABLED**. The local switch character ensures that the user can reenter local mode after establishing a session. For information about selecting a switch character see the *DECserver 500 Use* manual.
3. **Autoanswering equipment:** The port characteristic **DTRWAIT** can be enabled to delay assertion of **DTR** and **RTS** until the server detects an **RI** signal from the dial-in modem. Normally, **DTRWAIT** should be **DISABLED** so that **DTR** and **RTS** are asserted while the port is idle. However, to support certain autoanswering equipment, you can set **DTRWAIT** to **ENABLED**.
4. **Inactivity logout:** To protect a port from being held open by an inactive user, define **INACTIVITY** as **ENABLED**.
5. **Log-in password:** Enabling the log-in password on the server port is an important security measure. Digital strongly recommends this step.

6. **Dedicated service:** You can set up a dedicated service for the dial-in modem. If you set AUTOCONNECT to DISABLED, the server logs out the port and disconnects the call when a session ends. If you set AUTOCONNECT to ENABLED, the server does not log out the port.

Line Card and Cable Requirements

Use the CXY08 line card with one of the following:

- BC22E shielded straight-through cable (full modem)*
- BC22F shielded straight-through cable (full modem)
- * Recommended

7.13 A Terminal Switch

Description (A)

A terminal switch is attached to a port and offered as a service. By connecting to that service, a user can use the terminal switch to access any host supported by the switch.

Description (B)

A terminal switch is attached to a port and acts as a front end to the terminal server. Users of the switch can select the server port if they wish to access service nodes on the Ethernet, rather than accessing non-LAT hosts that are directly attached to the switch.

Procedure

Use the following steps for configuring a port that has all the original default port values. Substitute the actual number of your port for the example port number 102 and the actual name of your service for the example service SWITCHER.

1. Specify these values:

```
Local> SET PORT 102 ACCESS REMOTE AUTOBAUD DIS
Local> SET PORT 102 BREAK DIS
Local> SET PORT 102 DTRWAIT ENA MODEM ENA SPEED 4800
```

or

```
TSC> DEFINE PORT 102 ACCESS REMOTE AUTOBAUD DIS
TSC> DEFINE PORT 102 BREAK DIS
TSC> DEFINE PORT 102 DTRWAIT ENA MODEM ENA SPEED 4800
```

2. Ensure that both the **AUTHORIZED GROUPS** and the **CURRENT GROUPS** for the port of the user trying to connect to the service share at least one group with the service.
3. If you make these changes on the running server, save the changes and log out the port:

```
Local> SAVE PORT 102
Local> LOGOUT PORT 102
```

4. Assign the port to the service:

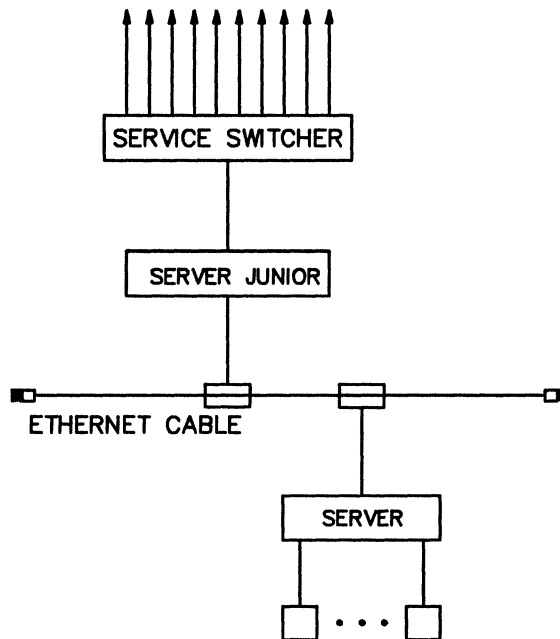
```
Local> SET SERVICE SWITCHER PORT 102 IDENT "Terminal switch"
```

or

```
TSC> DEFINE SERVICE SWITCHER PORT 102 IDENT "Terminal switch"
```

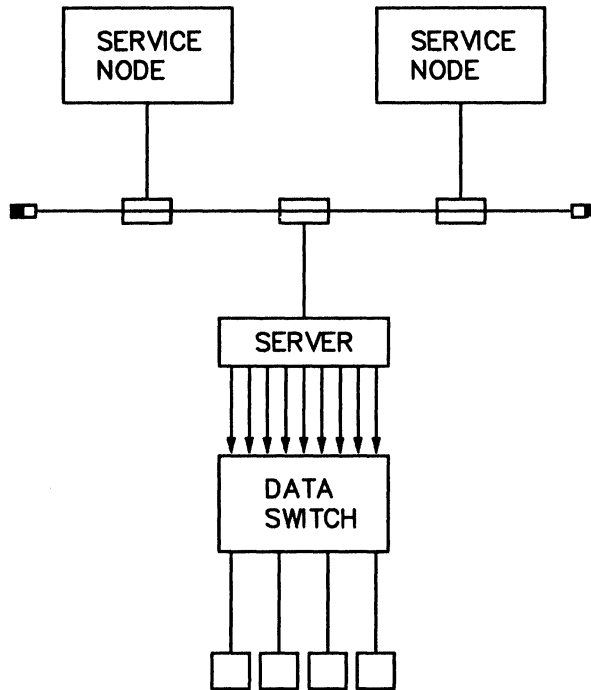
Figure 7-9 illustrates Application A, a terminal switch offered as a service. Figure 7-10 illustrates Application B, a terminal switch used as a front end to a terminal server.

Figure 7-9: A Terminal Switch Offered As a Service



LKG-0463-88
REV. 1

Figure 7–10: A Terminal Switch Offered As a Front End to a Terminal Server



LKG-1086-88

For ports that no longer have the default configuration, see Table 7–12. The table lists the port values that are required and recommended for this application.

Table 7–12: Port Values for a Terminal Switch

Characteristic	Value*	Comment
ACCESS	REMOTE	
AUTOBAUD	DISABLED	See note 1
AUTOCONNECT	DISABLED	
AUTOPROMPT	DISABLED	
BREAK	DISABLED	
DEDICATED	NONE	
DSRLOGOUT	DISABLED	
DTRWAIT	ENABLED	
FLOW CONTROL	XON	
INACTIVITY LOGOUT	DISABLED	
INTERRUPTS	DISABLED	
MODEM CONTROL	ENABLED	See notes 2 and 3
PASSWORD	DISABLED	

* Bold values are required for this port configuration.

Notes

1. Physical characteristics: For information about matching the physical characteristics of the port and the device, see Section 7.2.
2. Modem control: If a terminal switch supports modem control, modem signaling has the same significance for security with hosts that are accessed over a terminal switch as with non-LAT hosts attached directly to the server.
3. Some terminal switches require the modem RI (ring indicator) signal to transition from off to on several times to respond to a connection. The server asserts a single modem signal through a null-modem cable, which the switch interprets as the RI signal, but the server cannot force multiple RI transitions when the user connects to the remote-access port. Therefore, do not attach a terminal switch that requires the RI signal to act this way.
4. In Application B, host-initiated connections across the data switch are not supported.

Line Card and Cable Requirements

Use the CXY08 line card with one of the following:

- BC22R shielded null-modem cable
- BC17D shielded null-modem cable

7.14 A Printer Using CTS/RTS Flow Control

Description

A printer using the Clear To Send modem signal (CTS) and the Ready To Send modem signal (RTS) for flow control is attached to a server port. The printer requires a BC22R null-modem cable (or equivalent). When RTS is asserted by either the terminal or the server port, the cable causes RTS to be interpreted as CTS at the other end. When either the printer or the server stops asserting RTS, the other stops transmitting data until it again detects CTS.

Note

Although printers are described in this application section, other devices that use CTS/RTS flow control can be used on the server.

Procedure

Use the following commands for configuring a port that has all the original default port values. Substitute the actual number of your port for the example port number 2.

```
Local> SET PORT 2 ACCESS REMOTE AUTOBAUD DIS
Local> SET PORT 2 DSRLOGOUT ENA FLOW CONTROL CTS
Local> SAVE PORT 2
Local> LOGOUT PORT 2
```

OR

```
TSC> DEFINE PORT 2 ACCESS REMOTE AUTOBAUD DIS
TSC> DEFINE PORT 2 DSRLOGOUT ENA FLOW CONTROL CTS
```

For ports that no longer have the default configuration, see Table 7–13. The table lists the port values that are required and recommended for this application.

Table 7–13: Port Values for a Printer Using CTS/RTS Flow Control

Characteristic	Value*	Comment
ACCESS	REMOTE or DYNAMIC	See note 5
AUTOBAUD	DISABLED	See note 1
AUTOCONNECT	DISABLED	
AUTOPROMPT	DISABLED	
BREAK	Manager's choice	See note 3
DEDICATED	NONE	
DSRLOGOUT	ENABLED	See note 2
DTRWAIT	DISABLED	
FLOW CONTROL	CTS	See note 3
INACTIVITY LOGOUT	DISABLED	
INTERRUPTS	Manager's choice	
MODEM CONTROL	DISABLED	See note 4
PASSWORD	DISABLED	

* Bold values are required for this port configuration.

Notes

1. **Physical characteristics:** For information about matching the physical characteristics of the port and the device, see Section 7.2.
2. **DSR logout:** With **DSRLOGOUT ENABLED** on a port, the server automatically logs out the port when the device is powered off if the device asserts modem signals when powered up.
3. Most devices with out-of-band flow control do not have a **BREAK** key.
4. **Modem control:** Because the **CTS** and **RTS** modem signals are used for flow control in this application, **MODEM CONTROL** must be set to **DISABLED**.
5. The choice of **ACCESS REMOTE** or **ACCESS DYNAMIC** depends on whether you want the printer to double as a terminal. **ACCESS REMOTE** does not allow a user to issue connect commands.

Line Card and Cable Requirements

Use the CXY08 line card with the BC22R shielded null-modem cable.

7.15 A Terminal Using DSR/DTR Flow Control

Description

A terminal using the Data Set Ready modem signal (DSR) and the Data Terminal Ready modem signal (DTR) for flow control is attached to a server port. These devices require a null-modem cable. When DTR is asserted by either the terminal or the server port, the cable causes DTR to be interpreted as DSR at the other end. When either the terminal or the server stops asserting DTR, the other stops transmitting data until it again detects DSR.

Procedure

Use the following commands for configuring a port that has all the original default port values. Substitute the actual number of your port for the example port number 55.

```
Local> SET PORT 55 FLOW CONTROL DSR
Local> SAVE PORT 55
Local> LOGOUT PORT 55
```

OR

```
TSC> DEFINE PORT 55 FLOW CONTROL DSR
```

Note

For a printer using DSR/DTR flow control, follow the procedure in this section.

For ports that no longer have the default configuration, see Table 7–14. The table lists the port values that are required and recommended for this application.

Table 7–14: Port Values for a Terminal Using DSR/DTR Flow Control

Characteristic	Value*	Comment
ACCESS	LOCAL	
AUTOBAUD	ENABLED	See note 1
AUTOCONNECT	User's choice	
AUTOPROMPT	ENABLED	
BREAK	LOCAL	
DEDICATED	NONE	
DSRLOGOUT	DISABLED	See note 2
DTRWAIT	DISABLED	
FLOW CONTROL	DSR	
INACTIVITY LOGOUT	ENABLED	
INTERRUPTS	DISABLED	
MODEM CONTROL	DISABLED	See note 3
PASSWORD	DISABLED	

* Bold values are required for this port configuration.

Notes

1. Physical characteristics: For information about matching the physical characteristics of the port and the device, see Section 7.2.
2. DSR logout: This feature is incompatible with DSR/DTR flow control, and the port must be set to DSRLOGOUT DISABLED.
3. Modem control: In this application, the DSR and DTR modem signals are used for flow control; therefore, you must set MODEM CONTROL to DISABLED.

Line Card and Cable Requirements

Use the CXY08 line card with one of the following:

- BC22D shielded null-modem cable (data-leads-only)*
- BC17D shielded null-modem cable
- BC22R shielded null-modem cable

* Recommended for interactive devices using DSR/DTR flow control

These cables switch DTR signals, which are asserted at either the device or the server port, to DSR signals, which are received at the other end of the cable.

7.16 A 3270 Terminal Emulating a VT220 Terminal

Description

An interactive 3270 terminal is attached to a server port that is on a CXM04 line card. Once in VT mode, the 3270 terminal user can enter local mode server commands, allowing connection to systems on the Ethernet.

Procedure

When you DEFINE DEVICE TYPE CXM04, the TSC automatically configures all ports associated with the line card. TSC allows you to reconfigure a port's operating MODE if the default for this characteristic is inappropriate for the terminal. Use the following commands for defining a CXM04 line card and configuring its ports. Substitute the actual numbers of your devices and ports for the example devices and port numbers.

The following example configures a CXM04 line card such that four ports can operate in either VT mode or 3270 mode, but restricts port 3 to 3270 mode only.

```
TSC> DEFINE DEVICE LC1 TYPE CXM04
TSC> DEFINE PORT 3 MODE 3270
```

The following example configures a CXM04 line card for VT mode only, which means that eight ports on this line card are automatically configured to operate only in MODE VT220.

```
TSC> DEFINE DEVICE LC2 TYPE CXM04 CONFIGURATION 8
```

For ports that no longer have the default configuration, see Table 7–15. The table lists the port values that are required and recommended for this application.

Table 7–15: Port Values for a 3270-Class Terminal

Characteristic	Value*	Comment
ACCESS	LOCAL	
ALTERNATE HOTKEY	ENABLED	See note 1
AUTOBAUD	DISABLED	See note 2
AUTOCONNECT	User's choice	
AUTOPROMPT	Manager's choice	
BREAK	LOCAL	
DEDICATED	NONE	
DSRLOGOUT	DISABLED	See note 3
DTRWAIT	DISABLED	
FLOW CONTROL	XON	See note 4
INACTIVITY LOGOUT	Manager's choice	
INTERRUPTS	DISABLED	
MODE	Manager's choice	See note 5
MODEM CONTROL	DISABLED	See note 6
MULTISESSIONS	DISABLED	See note 7
PASSWORD	Manager's choice	

* Bold values are required for this port configuration.

Notes

1. **Alternate hot key:** the server manager should enable the alternate hot key sequence regardless of the terminal type. **ALTERNATE HOTKEY** is **ENABLED** (the default).
2. **Physical characteristics:** You cannot set the **SPEED**, **CHARACTER SIZE**, and **PARITY** port characteristics. When you **DEFINE** a **CXM04** line card, the TSC automatically sets **AUTOBAUD** to **DISABLED** for all ports on that card.
3. **DSR logout:** This feature is incompatible with the **CXM04** line card. Using **DSRLOGOUT** requires a **CXY08** line card.
4. **Flow control:** **XON/XOFF** characters implement flow control for the **CXM04** line card. There are no **CTS** and **DSR** signals.

5. **Mode:** If you define the line card and specify **CONFIGURATION 4**, the choices for **MODE** are **VT220**, **3270**, and **DYNAMIC** (the default). If you configure the card as **CONFIGURATION 8**, the only choice for **MODE** is **VT220** (which the TSC sets automatically for this line card configuration). Note that you can set the **MODE** characteristic only with the TSC, and not from the running server.
6. **Modem control:** This feature is incompatible with the **CXM04** line card. Using **MODEM CONTROL** requires a **CXY08** line card.
7. **Multisessions:** This feature is incompatible with the **CXM04** line card.

Line Card and Cable Requirements

Use the **CXM04** line card with one of the following:

- **RG62AU** or equivalent coaxial cable
- **Twisted-pair cable** (shielded or unshielded)

7.17 A TD/SMP Session Management Terminal

Description

A TD/SMP session management terminal is attached to a server port. You can enable a port characteristic that lets the server communicate with the session management terminal using the Terminal Device/Session Management Protocol.

Procedure

Use the following commands for configuring a port that has all the original default port values. Substitute the actual number of your port for the example port number 55.

```
Local> SET PORT 55 MULTISESSIONS ENABLED
Local> SAVE PORT 55
Local> LOGOUT PORT 55
```

or

```
TSC> DEFINE PORT 55 MULTISESSIONS ENABLED
```

For ports that no longer have the default configuration, see Table 7–16. The table lists the port values that are required and recommended for this application.

Table 7–16: Port Values for a Session Management Terminal

Characteristic	Value*	Comment
ACCESS	LOCAL	
AUTOBAUD	ENABLED	See note
AUTOCONNECT	User's choice	
AUTOPROMPT	Manager's choice	
BREAK	LOCAL	
DEDICATED	NONE	
DSRLOGOUT	Manager's choice	
DTRWAIT	DISABLED	
FLOW CONTROL	XON	
INACTIVITY LOGOUT	Manager's choice	
INTERRUPTS	DISABLED	
MODEM CONTROL	DISABLED	
MULTISESSIONS	ENABLED	
PASSWORD	Manager's choice	

* Bold values are required for this port configuration.

Application Note

Physical characteristics: For information about matching the physical characteristics of the port and the device, see Section 7.2.

Line Card and Cable Requirements

- CXA16 or CXB16 line card with the BC16E device cable
- CXY08 line card with any of the cables recommended for this line card (provided that the cable has pins 2 and 3)

Specifying Values for Server Characteristics

This chapter describes in detail the server's operating characteristics: port characteristics, server characteristics, local service characteristics, and device characteristics. This chapter also shows the commands that display these characteristics and the commands that change them.

The operating characteristics and their values make up the server's databases. Use this chapter for reference when you are deciding on values to change. For related information, see:

- Chapter 9 of this manual for complete information about the display commands, illustrations of the displays, and guidelines for interpreting the displays.
- Section 1.2.2.4 of this manual for a discussion of the differences between changing characteristics in the operational database on the running server and in the permanent database on the load host.
- *The Terminal Server Commands and Messages Reference* for:
 - Complete command syntax information about the commands that change server characteristics
 - The defaults and valid ranges of values
 - The naming conventions for LAT nodes
 - The required privilege level of each command option

The following table summarizes the commands you can use to display and change server characteristics.

Table 8–1: Server and TSC Commands Listed by Database

Permanent Database	Operational Database	Entity	Function
CLOSE		TABLE	Closes a currently open key–board mapping table.
DEFINE	SET	DEVICE LANGUAGE ** PORT SERVER SERVICE SESSION *	Modifies entries for the entity in the database
PURGE	CLEAR	LANGUAGE ** SERVICES	Deletes entry for the entity in the database
LIST	SHOW and MONITOR	DEVICES LANGUAGES ** NODES PORTS QUEUE * SERVER SERVICES SESSIONS * USAGE ** USERS	Displays information from the database
USE		TABLE	Selects a keyboard mapping table file and keyboard table for use in keyboard mapping

* Valid for the operational database only ** Valid for the permanent database only

8.1 Port Characteristics

With the port characteristics, you can configure your server's ports as required by the type of attached port devices, by the network manager, and by the server's users. In addition, nonprivileged users can change some port characteristics for their own ports. Port characteristics determine how:

- Local users connect to services

- Remote users connect to local services
- Host applications connect to remote-access ports

To view the current values for port characteristics, use the **SHOW/LIST PORT CHARACTERISTICS** commands. To change these values, issue the **SET/DEFINE PORT** commands.

Changes made with **SET PORT** remain in effect only until the next logout (or the next disconnect, in the case of a remote-access port) unless you save these changes in the log-in database (see Sections 1.2.2.2 and 1.2.2.3) by using the **SAVE PORT** command. The **SAVE PORT** command saves the current values of port characteristics until the next down-line load or until you make additional changes using **SET PORT** and **SAVE PORT** commands.

Changes to certain port characteristics do not take effect until after you log out from the port (or disconnect from a remote-access port). To preserve these changes across logins, use the combination of **SET PORT** and **SAVE PORT** commands or use **TSC DEFINE** commands and then down-line load the server image. The port characteristics that do not become effective until port logout are as follows:

- **ACCESS**
- **AUTOBAUD**
- **DEDICATED**
- **DTRWAIT**
- **MODEM CONTROL**
- **PASSWORD**

Table 8–2 groups all port characteristics by function and provides references to explanatory sections. Table 8–3 shows the default values for all but port 0, and Table 8–4 shows the default values for port 0.

Table 8-2: Port Characteristics

Access Characteristics (Section 8.1.1)

ACCESS
AUTHORIZED GROUPS
GROUPS
INTERRUPTS
LIMITED VIEW
LOCK
PASSWORD
SECURITY

Session Initiation Control Characteristics (Section 8.1.2)

AUTOCONNECT
AUTOPROMPT
DEDICATED
DIALUP
DSRLOGOUT
INACTIVITY LOGOUT
MULTISESSIONS
PREFERRED
QUEUEING
SESSION LIMIT

Physical Port Characteristics (Section 8.1.3)

AUTOBAUD
CHARACTER SIZE
PARITY
SPEED (input and output)
TYPE

Flow Control Characteristic (Section 8.1.4)

FLOW CONTROL
ON-DEMAND LOADING

Session-Switching Characteristics (Section 8.1.5)

BACKWARD SWITCH
BREAK
FORWARD SWITCH
LOCAL SWITCH

Port Display Control Characteristics (Section 8.1.6)

BROADCAST
LOSS NOTIFICATION
MESSAGE CODES
VERIFICATION

Table 8–2 (Cont.): Port Characteristics

Modem Support Characteristics (Section 8.1.7)

DTRWAIT
MODEM CONTROL
SIGNAL CHECK

Port Identification Characteristics (Section 8.1.8)

NAME
USERNAME

Remote Modification Control Characteristic (Section 8.1.9)

REMOTE MODIFICATION

3270 Terminal Characteristics (Section 8.1.10)

ALTERNATE HOTKEY
MODE

Table 8–3: Default Values for Port Characteristics

Characteristic	Default
ACCESS	LOCAL
ALTERNATE HOTKEY	ENABLED
AUTHORIZED GROUPS	Group 0 ENABLED
AUTOBAUD	ENABLED
AUTOCONNECT	DISABLED
AUTOPROMPT	ENABLED
BACKWARD SWITCH	NONE
BREAK	LOCAL
BROADCAST	ENABLED
CHARACTER SIZE	8
DEDICATED	NONE
DIALUP	DISABLED
DSRLOGOUT	DISABLED
DTRWAIT	DISABLED
FLOW CONTROL	XON
FORWARD SWITCH	NONE
GROUPS	Group 0 ENABLED
INACTIVITY LOGOUT	DISABLED
INTERRUPTS	DISABLED
LIMITED VIEW	DISABLED
LOCK	ENABLED
LOCAL SWITCH	NONE
LOSS NOTIFICATION	ENABLED
MESSAGE CODES	ENABLED
MODE	DYNAMIC *
MODEM CONTROL	DISABLED

Table 8–3 (Cont.): Default Values for Port Characteristics

Characteristic	Default
MULTISESSIONS	DISABLED
NAME	LC- <i>n-n</i>
PARITY	NONE
PASSWORD	DISABLED
ON-DEMAND LOADING	DISABLED
PREFERRED	NONE
QUEUING	DISABLED
REMOTE MODIFICATION	DISABLED
SECURITY	DISABLED
SESSION LIMIT	4
SIGNAL CHECK	DISABLED
SPEED	9600
TYPE	SOFTCOPY
USERNAME	<i>port-name</i>
VERIFICATION	ENABLED

* DYNAMIC only when the CXM04 device is defined as CONFIGURATION 4. The default is VT220 when the device is defined as CONFIGURATION 8.

Table 8–4 lists the default values for the physical console port, which is port 0, and also known as the management port. This table flags characteristics that you cannot change for port 0 and characteristics that have defaults different from those for other ports.

Table 8–4: Default Values for Port 0 Characteristics

Characteristic	Default
ACCESS *	LOCAL
ALTERNATE HOTKEY	Not applicable
AUTHORIZED GROUPS *	All server groups **
AUTOBAUD *	DISABLED **
AUTOCONNECT	DISABLED
AUTOPROMPT	ENABLED
BACKWARD SWITCH	NONE
BREAK	DISABLED **
BROADCAST	ENABLED
CHARACTER SIZE *	8
DEDICATED *	NONE
DIALUP	DISABLED
DSRLOGOUT *	DISABLED
DTRWAIT *	DISABLED

Table 8–4 (Cont.): Default Values for Port 0 Characteristics

Characteristic	Default
FLOW CONTROL *	XON
FORWARD SWITCH	NONE
GROUPS *	Not applicable
INACTIVITY LOGOUT	DISABLED
INTERRUPTS	DISABLED
LIMITED VIEW	DISABLED
LOCAL SWITCH	~ **
LOCK	ENABLED
LOSS NOTIFICATION	ENABLED
MESSAGE CODES	ENABLED
MODE	Not applicable
MODEM CONTROL *	DISABLED
MULTISESSIONS *	DISABLED
NAME	CONSOLE **
PARITY *	NONE
PASSWORD	DISABLED
ON-DEMAND LOADING	DISABLED
PREFERRED	NONE
QUEUING	DISABLED
REMOTE MODIFICATION	DISABLED
SECURITY	DISABLED
SESSION LIMIT	4
SIGNAL CHECK *	DISABLED
SPEED *	9600
TYPE	SOFTCOPY
USERNAME	<i>port-name</i>
VERIFICATION	ENABLED

* Flagged characteristics cannot be modified for port 0.

** Flagged defaults differ from the defaults for other ports.

8.1.1 Access Characteristics

These characteristics control access to ports and services by users and service nodes.

- **ACCESS**

Specifies the type of access allowed to the port. There are four types of port access:

- **LOCAL** — Supports interactive users on terminals or PCs connected to a port either directly or through a dial-in modem.

- **REMOTE** — Supports connections to printers, other applications devices, non-LAT host systems, and dial-out modems. The connected devices can be offered as LAT services by the server.
- **DYNAMIC** — Allows access to the port to alternate between **LOCAL** and **REMOTE**.
- **NONE** — Indicates that no access is possible on the port.

With **ACCESS LOCAL**, a port user can usually communicate with the server in local mode or communicate with a service in service mode. **LOCAL** is the default option for the **ACCESS** characteristic.

With **ACCESS REMOTE**, a port can offer a device as a service or provide printers or other applications devices for host-initiated requests.

You can use a remote-access port in either one or both of the following ways:

- The port can offer a local service.
- The port can be accessed by LAT V5.1 service nodes that allow host-initiated requests.

If you assign a remote-access port with a printer to a service, it is accessible by both LAT V5.1 service nodes and server users.

A remote-access port permits only one session at a time, which ensures that the remote device is used sequentially. Some features used on local-access ports, such as switch characters, are automatically ignored on a port being used for remote access. A **BREAK** signal, however, can be passed to a remote-access port. The **BREAK** signal is received from a user's terminal and asserted to the device, for example a non-LAT host, on the remote port by the server.

With **ACCESS DYNAMIC**, the server allows access to the port to switch between local and remote, according to user demand. A port with **DYNAMIC** access can either accept local mode commands (and function as a local-access port), or it can receive connection requests (and function as a remote-access port).

This access type is usually used for dial-in/dial-out modems. When the port is being used for local access, the user must log out before any requests for a remote-access connection are accepted. As with a remote-access port, if you want server users to be able to connect to a dynamic-access port, you must assign the port to at least one local service.

With ACCESS NONE, the port is disabled. Any attempts to access the port fail.

Note

The ACCESS characteristic does not take effect until the current port user logs out, or, in the case of remote-access ports, terminates the connection.

The value you specify for ACCESS in a SET PORT command never becomes effective unless you save it with a SAVE PORT command.

- **INTERRUPTS**

Specifies whether a local user can press the BREAK key to disconnect a remote session at an ACCESS DYNAMIC port in order to log in to the server. INTERRUPTS and DYNAMIC ACCESS are governed by the following rules:

- With INTERRUPTS DISABLED, a potential local user cannot disconnect a session to a remote-access port at an ACCESS DYNAMIC port to log in to the server.
- With INTERRUPTS ENABLED, a potential local user can press the BREAK key to interrupt a session at a remote-access port and start a local session. Any queued host-initiated requests remain queued and are processed when the local-access user logs out of the port. **Specifying Values for Server Characteristics**
- A request for remote access can never interrupt an ongoing local session.
- A dynamic-access port is a remote-access port by default. However, if there is no ongoing session, a session using either type of access can be started, and the above rules apply.

The default is INTERRUPTS DISABLED.

- **AUTHORIZED GROUPS**

Determines the availability of services to each port.

You can assign an authorized group list to each port. If any group in the authorized lists applies to both a port and a service node, then the port user can connect to that node's services. In addition, with the **SHOW** command, the user gets information about only these services and service nodes. The network manager normally coordinates the assignment of group lists for the service nodes and servers.

AUTHORIZED GROUPS ENABLED gives the port access to the group list; **DISABLED** denies access. By default, all ports have access to all services offered with group 0. Groups are discussed in Section 5.3.

- **GROUPS**

Lets nonprivileged users further restrict their own access to services and shorten their node and service displays. These groups are ignored for remote-access ports. A user can enable only the groups that you authorized with the **AUTHORIZED GROUPS** characteristic.

These groups are always equal to, or a subset of, the **AUTHORIZED GROUPS**. If a user specifies **GROUPS ALL**, the groups become the same as the enabled **AUTHORIZED GROUPS**.

- **LIMITED VIEW**

Restricts the **SHOW** command information available to the port. By enabling **LIMITED [VIEW]**, you prohibit the user from executing **SHOW NODES** and **SHOW SERVICES**. The default is **DISABLED**.

- **LOCK**

Enables or disables the effect of the **LOCK** command, issued by port users. When **LOCK** is enabled on the server and enabled on a port, the port user can issue the **LOCK** command to prevent access to the terminal at which the command is entered. The command prevents any input until a user enters the unlock password at that terminal.

If a user forgets his or her unlock password, you can log out the port by using the **LOGOUT PORT *n*** command.

Depending on the user environment, you might want to disable the **LOCK** command at a particular port. The default is **LOCK ENABLED**.

- **PASSWORD**

Enables or disables the log-in password for ports with access to local mode. (The log-in password is ignored on ports with remote access.) See Sections 5.1.2 and 5.4.4.2.

Note

The value you specify for **PASSWORD** in a **SET PORT** command never becomes effective unless you save it with a **SAVE PORT** command.

- **SECURITY**

Enables or disables secure port status for a port with access to local mode.

The server lets nonprivileged users issue some commands that affect other users (such as the **BROADCAST** command) or that provide one user with information about other users (such as the **SHOW SESSIONS ALL** command). If this situation is undesirable, and you want to restrict a user still further (see Section 5.4.4.3), you can give the port secure status with **SECURITY ENABLED** for that port. The default is **SECURITY DISABLED**.

8.1.2 Session Initiation Control Characteristics

These port characteristics can help you manage users' local sessions.

- **AUTOCONNECT**

How the server functions with **AUTOCONNECT ENABLED** depends on whether you or the user sets a preferred service, a dedicated service, or neither.

Attempts automatic reconnection when a connection terminates abnormally and allows automatic connections to dedicated and preferred services at login (see the port characteristics **DEDICATED** and **PREFERRED**). The default is **AUTOCONNECT DISABLED**. However, **AUTOCONNECT ENABLED** is recommended for most port users.

Note

You need not enable AUTOCONNECT to connect to a dedicated service, but you must save AUTOCONNECT ENABLED in the log-in database if you want to connect automatically a port to a preferred service whenever that port logs in to the server.

The server attempts reconnection at approximately 30-second intervals and continues trying until the connection is made or until the user enters local mode. For example, AUTOCONNECT enters a stale node purging cycle (at about 30-second intervals) if it cannot find a requested server. It remains in this cycle until the user enters the local mode. Unless a dedicated service is in effect, a status message appears at the port device indicating that the server is trying to restart a session. The new connection can be made to any service node that supplies the same service, unless the user specified a particular node with the CONNECT command.

The autoconnect facility is especially helpful when a user wants the server to repeat connection attempts to a currently nonoperational service node.

Note

The automatic failover feature, which allows the server to reconnect a session to an alternative service node when an abnormal session termination occurs, is not dependent on the AUTOCONNECT characteristic. With AUTOCONNECT ENABLED, the server attempts reconnections to the same service node if failover is not successful.

- **AUTOPROMPT**

Controls the initiation of a log-in process. The server sends the status of the autoprompt characteristic to the service node whenever a user establishes a session.

If you enable AUTOPROMPT and the service node supports this facility, the service node might perform a system-specific log-in sequence (such as displaying a service announcement or displaying a log-in prompt). If you disable autoprompt and the service node can recognize AUTOPROMPT DISABLED, the service node does not perform any log-in sequence. However, pressing the RETURN key afterwards might trigger the sequence.

Ports with nonkeyboard devices cannot respond to the log-in sequence; therefore, disable autoprompt for these ports.

- **DEDICATED**

Identifies a service to which a local-access port is permanently assigned. When assigning a dedicated service, you can include a node and a destination port name in addition to a service name. However, if you specify a node or port, automatic failover does not take place. A dedicated port simulates a direct, hard-wired connection between the port device and the service.

Note

If the dedicated service is not available, the dedicated port is nonoperational.

You cannot set this characteristic for a logged-in port. For a logged-out port, you can use the `SET PORT n DEDICATED` command from another port, where *n* is the number of the port to be dedicated. Next, save the changes in the log-in database with the `SAVE PORT n` command. Then, log in port *n* to connect to the dedicated service.

When you define a dedicated service, any existing preferred service for the port is deleted. Digital recommends that you change this characteristic in the permanent database.

- **DIALUP**

Specifies to the service node on a `CONNECT` request that the port is to be considered as attached to a dial-up line. Service nodes can use this information as a security check (see Section 5.6.6.1). The default is `DISABLED`.

- **DSRLOGOUT**

Specifies whether the server should log out a port on a CXY08 line card if the DSR signal drops on that port. The port must have hardware that supports modem control signals and `MODEM CONTROL` must be set to `DISABLED`.

Note

You can duplicate the DSR log-out function by using a BC17D cable with `MODEM CONTROL ENABLED`.

Enable DSRLOGOUT for ports in local access (for terminal or PC usage) when you want the server to automatically log out a port when the attached terminal is powered off. (Note that the terminal must assert a DTR signal when it is powered on.) Ports using DSR/DTR flow control must be set to DSRLOGOUT DISABLED.

Note

With MODEM CONTROL ENABLED, the DSRLOGOUT function is performed as part of the normal modem interaction.

If DSRLOGOUT is DISABLED, the server port without modem control signals is not logged out if the port device is powered off.

- **INACTIVITY LOGOUT**

Lets you enable or disable automatic logout for remote or local access ports. The default is INACTIVITY LOGOUT DISABLED.

If INACTIVITY LOGOUT is enabled, the server automatically logs out the port if no sessions are active (local access) or no activity (input or output) has occurred (remote access) for a specified period of time.

INACTIVITY LOGOUT helps you prevent a port from being monopolized in situations where more than one user requires access to the port, such as port with a dial-in modem. It can also prevent a dial-out modem from incurring large phone bills on inactive sessions.

If you use INACTIVITY LOGOUT for ports that have the port characteristic ACCESS set up as DYNAMIC, host-initiated requests for the port are not honored until a local-access user logs out. If the local-access user does not use the port, the server logs out the port automatically after the time-out period.

- **MULTISESSIONS**

The port user can enable MULTISESSIONS when using a session management terminal that supports the TD/SMP protocol. This allows the user to have multiple terminal sessions, each with a single LAT service session. TD/SMP maintains the context of the service session when the user switches to another service session. Session data continues even though the service session is currently inactive.

MULTISESSIONS permits the terminal user to have the server start and stop terminal session management. If **ENABLED**, the attached device initiates a terminal session and prompts the user to begin a service session. If the user subsequently enters **DISABLED** (the default value), all terminal sessions and their associated service sessions are terminated.

If a port has any active service sessions, the user cannot enable **MULTISESSIONS**. The server displays an error message.

- **PREFERRED**

Specifies a “default” service when a port user issues the **CONNECT** command without specifying a service name. This characteristic is useful for a port user who accesses a particular service often but still requires occasional connections to other services.

When you define a preferred service and define **AUTOCONNECT ENABLED** in the permanent database, the server connects the port directly to the preferred service at port login. The user can switch to local mode at any time and can make connections to other services.

When specifying a preferred service, you can include a node and a destination port name in addition to the service name. However, if you specify a node or port, automatic failover does not take place.

- **QUEUING**

QUEUING lets the server initiate queuing of connection requests that the port user makes (using the **CONNECT** command). When a requested service is busy, and **QUEUING** is set up as **ENABLED**, the connection request can be placed in the connection queue of the server that offers the requested service. If more than one server offers the service, the user’s server can attempt to make a connection to the target server that has the highest rating. For servers that offer queuing, ratings are higher for servers that have the greater number of open positions in their connection queues. If **QUEUING** is **DISABLED** (the default), and the requested service is busy, the target server does not queue the connection request. The user receives a message that indicates that the service is not currently available.

- **SESSION LIMIT**

Determines the maximum number of sessions allowed at a local-access port. The combined number of sessions for all ports on the server cannot exceed the number specified by the server characteristic **SESSION LIMIT**.

The default port session limit is 4. If you specify 0 for a port with sessions currently active, the user cannot establish any new sessions, but existing sessions are not affected.

8.1.3 Physical Port Characteristics

These characteristics control the transmission of data over a port's asynchronous line. They must be compatible with the device attached to the port.

- **AUTOBAUD**

Controls whether the autobaud facility is engaged on a port. The autobaud facility permits the server, at port login, to automatically sense the speed, parity, and character size of an interactive device. The server then adjusts the corresponding port characteristics accordingly.

For **AUTOBAUD** to function correctly, the internal characteristics of the port device must be set as follows:

- The device's input speed and output speed must be the same. Autobaud works with any speed supported by the server. The supported speed values are: 50, 75, 110, 134, 150, 300, 600, 1200, 1800, 2000, 2400, 4800, 7200, 9600, 19200, and 38400 bps.
- The port device must have one of the following character size and parity combinations: **CHARACTER SIZE 8** and **PARITY NONE**, or **CHARACTER SIZE 7** and **PARITY EVEN**.

Note

If **AUTOBAUD** is **ENABLED**, you cannot change these other port characteristics prior to port login: **SPEED**, **CHARACTER SIZE**, **PARITY**.

All terminals in the Digital VT-series operate under these conditions. Consult the terminal operator's guide if necessary.

If you want to operate the port device with different input and output speeds or with other combinations of character size and parity, set AUTOBAUD to DISABLED. Then define speed, character size, and parity as discussed in the following sections.

Note that under most circumstances, AUTOBAUD should be disabled for remote-access and dynamic-access ports.

Note

The value you specify for AUTOBAUD in a SET PORT command never becomes effective unless you save it with a SAVE PORT command.

- **CHARACTER SIZE**

Determines the number of bits in a character. Each character that is transmitted between the port device and the server is made up of 7 or 8 data bits.

The server automatically formats the characters for transmission from the server to the service node. Define CHARACTER SIZE as 7 if a device supports only 7-bit operation; otherwise define it as 8. The operator's guide for the port device you are using can assist you in determining character size. The default value is 8.

If you have AUTOBAUD enabled, the server automatically adjusts the character size.

Note

If AUTOBAUD is ENABLED, you cannot change the CHARACTER SIZE characteristic.

- **PARITY**

Provides a means for the server to check received port device characters for transmission errors. The parity can be ODD, EVEN, or NONE. If parity is not supported on a port device, enter the default, NONE. With AUTOBAUD enabled, the server sets port parity automatically.

Note

If AUTOBAUD is ENABLED, you cannot change the PARITY characteristic.

- **SPEED**

Can be defined as **SPEED**, **INPUT SPEED**, or **OUTPUT SPEED**. When you use the keyword **SPEED** alone, both input and output speeds are set to the same value.

If you do not enable **AUTOBAUD**, you must define a port speed characteristic. The input and output speeds for a port are expressed in bits per second (bps). The permissible speed values are: 50, 75, 110, 134, 150, 300, 600, 1200, 1800, 2000, 2400, 4800, 7200, 9600, 19200, and 38400 bps. Normally, all you need to specify is a value for **SPEED**.

Note

If **AUTOBAUD** is **ENABLED**, you cannot change the **SPEED** characteristic.

The optional keywords **INPUT** and **OUTPUT** allow you to set up split-speed operations. The input speed is the speed from the device to the server; the output speed is the speed from the server to the device.

Enter values for **INPUT SPEED** and **OUTPUT SPEED** only if the two are different. The **SET SPEED** command without one of these keywords affects both the input and the output speeds.

- **TYPE**

Controls certain device-specific functions, such as scrolling techniques and character deletions, when the port is in local mode. Here is a list of the **TYPE** options that you can specify:

- Use the **ANSI** option for ANSI standard video terminals (for example, VT100-series and VT200-series terminals). **TYPE ANSI** causes the server to clear the screen before each **SHOW** display and to display **MONITOR** updates in place (as opposed to scrolling them).
- Use the **SOFTCOPY** option for non-ANSI video terminals (for example, VT52 terminals). Both **ANSI** and **SOFTCOPY** erase characters when the **DELETE** key is pressed.

- Use the **HARDCOPY** option for all hard-copy devices (for example, LA120 printer/terminals). The **HARDCOPY** option echoes any deleted characters between backslashes when the **DELETE** key is pressed.

The default is **TYPE SOFTCOPY**.

Note

The **TYPE** characteristic is effective only when the port is in local mode. When a port is in service mode, all characters are passed directly to the service, and any screen manipulation is performed by the service.

8.1.4 Flow Control Characteristics

If port data is exchanged at high speeds, server memory buffers for storing messages prior to processing can become temporarily full. Data is lost if it arrives when this memory is full. The port device might support similar buffering. Flow control inhibits transmissions between the port device and the server to prevent this loss.

- **FLOW CONTROL**

Specifies the type of flow control enabled on the port. Flow control is the ability of the server or the port device to start and stop data transfer between them, as necessary to prevent buffer overflow.

These are the values you can specify for **FLOW CONTROL**:

- **CTS** — Specifies Request To Send/Clear To Send (**RTS/CTS**) modem signal flow control (valid for modem-controlled ports only).
- **DSR** — Specifies Data Terminal Ready/Data Set Ready (**DTR/DSR**) modem signal flow control (valid for modem-controlled ports only).
- **XON** — Specifies Transmit On/Transmit Off (**XON/XOFF**) character flow control. **XON** is the default flow control.
- **DISABLED** — Specifies no flow control.

The **CTS** and **DSR** flow control options operate independently of data characters moving between the service and a port device. If you use these options, the port uses the **RTS/CTS** or **DTR/DSR** modem signals to perform flow control. If the server is receiving data too quickly from the port device, it turns off **RTS** or **DTR** until it is able to accept more data.

Similarly, the server suspends output to the port if the server sees CTS or DSR turn off. This could happen if the port device receives data too quickly. The server resumes output when the CTS or DSR signal comes back on. CTS or DSR flow control affects data flow only between the port device and the server; the flow control status is not passed through LAT sessions.

Note

When using CTS or DSR flow control, you must set MODEM CONTROL to DISABLED.

- **ON-DEMAND LOADING**

Specifies on-demand loading of fonts for those foreign terminals whose fonts are composed of an unusually large number of characters. ON-DEMAND LOADING ENABLED affects XON/XOFF flow control processing only during the processing of these fonts. At this time it causes the server to ignore XOFF, thus assuring the continuous flow of characters. The default is DISABLED.

8.1.5 Session-Switching Characteristics

Session-switching characteristics let terminal users move between sessions (the forward and backward switch characters) or from a session to local mode (the local switch character). The characteristics described in this section are not used for ports currently in remote access. The session-switching characteristics are:

- **FORWARD SWITCH, BACKWARD SWITCH**

Move a user between two of his or her sessions without having to go to local mode. When the user presses the BACKWARD SWITCH character at a terminal, the server activates the user's "previous" session. Pressing the FORWARD SWITCH character activates the "next" session. If the user has only two sessions, both of these switch characters restart the inactive session.

Any nonprivileged user can set up any keyboard character as the FORWARD or BACKWARD SWITCH. Digital recommends choosing undefined control characters.

The user should not select characters that he or she ever enters while using a service because pressing a switch character interrupts the current session. Users should also avoid the tilde (~) character if they type function keys on VT200-series terminals or PCs.

Users can temporarily disable their defined switch characters for a particular session by using the **SET SESSION** command (see the *DECserver 500 Use manual*). However, the characters remain in effect outside that session.

- **BREAK**

Switches from service mode to local mode. In this case, **BREAK** signals must be interpreted by the server, and you must set the **BREAK** characteristic to **LOCAL**. If you want to send **BREAK** signals to the service when you are in a session, set **BREAK** to **REMOTE**; the **BREAK** signal is ignored by the server and passed to the service node. **DISABLED** means that the server disregards **BREAK** signals in both service and local modes.

Note

The **BREAK** key might not be acceptable for ports with the **MODEM CONTROL** and **REMOTE** characteristics enabled because using this key might cause some modems to disconnect the call.

If a user does not set up a local switch character and **BREAK** has been disabled or is not acceptable, the user might not be able to execute any server commands after establishing a session because he or she has no way to return to local mode without logging out of the service.

- **LOCAL SWITCH**

Identifies a character that, when entered by the user, switches the port to local mode from service mode. This character, like the forward and backward switch character, is intercepted by the server and is never transmitted to a service node. The **BREAK** key is also available for this function unless the **BREAK REMOTE** or the **BREAK DISABLED** option has been chosen.

When you define a local switch character, the character you choose can be used in place of the **BREAK** key, or you can continue to use the **BREAK** key. Use the **NONE** option to clear the local switch character after previously setting it. The default is **LOCAL SWITCH NONE**, which means that only the **BREAK** key can be used as the local switch.

The information on selecting switch characters in the description of the forward and backward switch (the preceding characteristic), applies equally to the local switch.

8.1.6 Port Display Control Characteristics

The port display control characteristics establish the manner in which the server passes local mode output to local-access port devices. These are the port display control characteristics:

- **BROADCAST**

Enables or disables the reception of broadcast messages at a port if the **BROADCAST** server characteristic is **ENABLED**.

If the **BROADCAST** port characteristic is **DISABLED**, the port does not receive announcements from the server or the server manager and does not receive any broadcast messages from other logged-in, local-access ports. However, a non-privileged port with **BROADCAST DISABLED** can still use the **BROADCAST PORT** command to send messages. **BROADCAST ENABLED** is the default value.

- **LOSS NOTIFICATION**

Enables or disables the sending of a beep warning when characters are lost.

The server transmits the beep to the port for each character that is lost. **LOSS NOTIFICATION** functions when a character is lost because of parity errors, framing errors, data overruns, or other reasons. In addition, there is no type-ahead facility in local mode. With **LOSS NOTIFICATION ENABLED**, users get the beep if they try to type before receiving the `Local>` prompt. The default is **ENABLED**.

- **MESSAGE CODES**

Specifies whether message codes appear with status and error messages.

Each server message has a message code. For example, in the following error message, the number 742 is a message code.

```
Local -742- Password verification failed
```

If you define **MESSAGE CODES** as **DISABLED**, message codes do not appear. The default is **ENABLED**. The *Terminal Server Commands and Messages Reference* lists all status and error messages in numerical message code order.

- **VERIFICATION**

Controls the display of session information when an existing session is started, stopped, or resumed. If you enable verification, the server displays the session number and the service name of the service. If you disable verification, no session information is displayed when a session is started, stopped, or resumed.

8.1.7 Modem Support Characteristics

These characteristics control the use of modem signals between the server and a connected device.

You can set **MODEM ENABLED** and **DTRWAIT ENABLED** only for ports connected to the one line-card type that utilizes modem signals — **CXY08**. Before enabling these characteristics, first define the port's line card as **CXY08** (see Section 8.4 for complete information).

These are the modem support characteristics:

- **DTRWAIT**

Determines if the server asserts certain modem signals when a port is inactive. Normally, **DTRWAIT** should be **ENABLED** for remote-access ports.

DTRWAIT delays the assertion of **DTR** and **RTS** signals. When communicating with modems and some system interfaces, it is normal for the server port to assert the **DTR** (and **RTS**) signals at all times except in the disconnect sequence.

However, there are situations where this is not desirable. **DTRWAIT** works only on **MODEM ENABLED** ports. When **DTRWAIT** is enabled, the server can delay the assertion of **DTR** and **RTS**, until an **RI** signal is detected from a modem or when a remote-access session begins. The default is **DTRWAIT DISABLED**.

Note

The value you specify for **DTRWAIT** in a **SET PORT** command never becomes effective unless you save it with a **SAVE PORT** command.

- **MODEM CONTROL**

Enables or disables the use of a modem control signal protocol on a port that is on a CXY08 line card. If you do not enable modem control, you cannot use that port with a modem. The default is **MODEM CONTROL DISABLED**.

With modem control enabled, the server uses sequences of modem signals to establish, maintain, and disconnect physical links between the port and the attached modem or computer interface. In addition, a user must log in to the server successfully within 60 seconds, or the server automatically disconnects the call.

For computer interface connections such as a non-LAT host, set the port to **MODEM CONTROL ENABLED** to ensure that session status is passed between the server and the host system. If you fail to enable modem control on ports connected to non-LAT time-sharing systems, security to a session on that system is compromised because a user could access another user's data. Therefore, Digital recommends that you do not connect non-LAT host systems to ports that are on CXA16 or CXB16 line cards because they do not support modem control.

Note

The **MODEM CONTROL** characteristic does not take effect with a **SET** command when a port is already logged in or has a remote-access session. If you do set this characteristic with a **SET** command, the changes are not effective unless you save them with the **SAVE PORT** command.

For more information about setting up and managing modem control, see Section 5.6.

- **SIGNAL CHECK**

Enables or disables a check for incoming modem signals to allow the server to determine if a modem controlled device is physically attached to a port. Use **SIGNAL CHECK** to control whether at least one of the following four signals must be detected at a port to allow completion of a connection attempt: Data Set Ready (DSR), Clear to Send (CTS), Ring (RI), and Carrier Detect (CD).

You can specify **SIGNAL CHECK ENABLED** for a port only if that port is also set to either **MODEM CONTROL ENABLED** or **DSRLOGOUT ENABLED** and is either **ACCESS REMOTE** or **ACCESS DYNAMIC**.

When SIGNAL CHECK is ENABLED on a port with MODEM CONTROL ENABLED, the server rejects an attempted connection to a port if no signal is seen within five seconds. If DSRLOGOUT is ENABLED, the server attempts to make the connection to another port if there is another port that offers the same service. If there are no incoming signals on a port offering the service, the port goes into the “Signal Wait” state until one of the following events puts the port back into the “Idle” state:

- The port receives an incoming signal.
- The server manager sets the port to SIGNAL CHECK DISABLED.
- The port is logged out.

If MODEM CONTROL and SIGNAL CHECK are both enabled on a port connected to a dial-out modem and no signal is detected, the user must reattempt the connection to the service if it is offered by more than one port.

8.1.8 Port Identification Characteristics

These port characteristics identify the port in the display of the SHOW PORTS CHARACTERISTICS, COUNTERS, and STATUS, and SHOW USERS commands. Use the port identification characteristics when you want a port name, a user name, or both for a port:

- NAME

Identifies a name for a port. Port names follow the LAT naming conventions, which are described in the *Terminal Server Commands and Messages Reference*. Assign a unique name for each port. The default port name is LC-*n-n*, where “*n-n*” is the line card number and the number of the port associated with that line card.

Port names are useful for remote-access ports. Section 5.9 discusses the benefits of using port names when you configure a port for use with host-initiated requests.

- USERNAME

Identifies a user-name string for a port with access to local mode. Normally, the server uses the string the user enters in response to the Enter username> prompt as the user name unless the user enters `CTRL/Z`, in which case the server uses the port’s name as the user name.

Users should specify a unique user name because the server does not prevent duplicate user names. User names appear in the SHOW USERS display.

You can use the TSC DEFINE PORT command to establish a permanent user name for a port. In this case, the Enter username> prompt is not displayed when a user logs in to the server.

Note

The SAVE PORT command does not save USERNAME, but you can permanently define it in the permanent database with TSC.

8.1.9 Remote Modification Control Characteristic

This port characteristic allows a LAT service node to modify port characteristics to match the port characteristics of a remote device, such as SPEED, CHARACTER SIZE, PARITY, and LOSS NOTIFICATION.

Remote modification enabled on a secure port allows the port user to modify the physical port characteristics from the host end. To prevent this, REMOTE MODIFICATION and SECURITY should not be enabled on the same port.

- **REMOTE MODIFICATION**

Enabling REMOTE MODIFICATION allows a LAT service node to modify port characteristics. The default is DISABLED.

8.1.10 3270 Terminal Characteristics

These port characteristics exist solely for configuring ports on the 3270 Terminal Option Card (CXM04). You define these characteristics with TSC, not on the running server. Before defining port characteristics, first define the line card TYPE (see Section 8.4 for information about defining devices).

- **ALTERNATE HOTKEY**

Using the TSC command `DEFINE PORT ALTERNATE HOTKEY DISABLED` disables the alternate hot-key sequence for a port on a CXM04 line card. A port connected to a PC that emulates a 3270 terminal needs to have `ALTERNATE HOTKEY` enabled (which is the default). PC users cannot use the normal hot-key sequence to switch between 3270 mode and VT mode.

- **MODE**

Using the TSC command `DEFINE PORT MODE` specifies the mode for a port that is on a CXM04 line card. Use `MODE` to force specified ports to operate exclusively in VT mode or in 3270 mode, provided that the CXM04 device was configured `DEFINE DEVICE LCn TYPE CXM04 CONFIGURATION 4`.

Define the CXM04 device prior to defining a port's `MODE` characteristic. If the device `CONFIGURATION` is 4, `MODE` defaults to `DYNAMIC` (either mode of operation). If the device `CONFIGURATION` is 8 (VT mode only), `MODE` defaults to `VT220`.

Specifying `PORT MODE DYNAMIC` enables a 3270 terminal user to switch between VT mode and 3270 mode. Specifying `PORT MODE VT220` causes a terminal associated with the specified port to operate exclusively in VT mode. Specifying `PORT MODE 3270` restricts a terminal to 3270 mode.

8.2 Server Characteristics

Server characteristics control the server's operations that are server-wide. That is, they affect all server users and the server's network interface. These characteristics also identify the server.

To see the current values for the server characteristics, use the `SHOW/MONITOR/LIST SERVER CHARACTERISTICS` commands. To change server characteristics, issue the `SET/DEFINE SERVER` commands.

Note

Some server characteristics cannot be changed if there are active sessions on the server. See the *Terminal Server Commands and Messages* for details.

Table 8–5 lists each server characteristic according to function and gives the section number that explains the characteristic. Table 8–6 shows the default values and ranges for each server characteristic.

Table 8–5: Server Characteristics

Network Communications Characteristics (Section 8.2.1)

CIRCUIT TIMER
HEARTBEAT
KEEPALIVE TIMER
NODE LIMIT
RETRANSMIT LIMIT

Local-Access Characteristics (Section 8.2.2)

BROADCAST
INACTIVITY TIMER
LIMITED HELP
LOCK
LOGIN PASSWORD
PASSWORD LIMIT
PRIVILEGED PASSWORD
SESSION LIMIT

Server Maintenance Characteristics (Section 8.2.3)

BACKUP HOSTS
LINE FREQUENCY
MAINTENANCE PASSWORD

Server Identification Characteristics (Section 8.2.4)

IDENTIFICATION
NAME
NUMBER
PROMPT

Service Node Characteristics (Section 8.2.5)

ANNOUNCEMENTS
MULTICAST TIMER
QUEUE LIMIT
SERVICE GROUPS

Table 8–6: Default Values for Server Characteristics

Characteristic	Default	Range
ANNOUNCEMENTS	ENABLED	
BACKUP HOSTS	No backup host	
BROADCAST	ENABLED	
CIRCUIT TIMER	80 milliseconds	10–200
HEARTBEAT	DISABLED	
IDENTIFICATION	None	
INACTIVITY TIMER	30 minutes	1–120
KEEPALIVE TIMER	20 seconds	10–180
LIMITED HELP	DISABLED	
LINE FREQUENCY	60 Hz	
LOCK	ENABLED	
LOGIN PASSWORD	ACCESS	
MAINTENANCE PASSWORD	NONE	
MULTICAST TIMER	60 seconds	10–180
NAME	<i>DECnet-node-name</i>	
NODE LIMIT	100	1–200
NUMBER	0	0–255
PASSWORD LIMIT	3	1–32
PRIVILEGED PASSWORD	SYSTEM	
PROMPT	Local>	
QUEUE LIMIT	8	1–32
RETRANSMIT LIMIT	8	5–120
SERVICE GROUPS	Group 0 ENABLED	0–255
SESSION LIMIT	256	0–512

8.2.1 Network Communications Characteristics

Some server characteristics control the exchange of messages on the network to which the server is attached. See Section 5.12 for a discussion of network communications. Digital suggests that you discuss the values of these characteristics with your network manager. These are the server characteristics that affect Ethernet communications:

- **CIRCUIT TIMER**

Controls the interval in milliseconds between messages sent by the server to service nodes.

If you choose a low value for CIRCUIT TIMER, the response time for the port is decreased, but the demand on service nodes increases. A long interval minimizes node loading but extends user response time.

Set the circuit timer in the range of 10 to 200 milliseconds. The default value of 80 milliseconds gives a generally acceptable response time while creating a moderately low overhead on the service node. The value for **CIRCUIT TIMER** is effective only as a multiple of the line clock:

- 16 2/3 ms per clock tick for 60 Hz
- 20 ms per clock tick for 50 Hz

- **HEARTBEAT**

Ensures that the status of the collision-detect check circuitry at the server transceiver is indicated. The collision-detect circuitry is used with some transceivers to ensure that the transceiver is correctly able to sense collisions of messages transmitted on the Ethernet.

HEARTBEAT is generally required for normal network operation but is disabled by default. Enable **HEARTBEAT** if the transceiver supports it. It helps isolate transceiver problems on the network.

- **KEEPALIVE TIMER**

Specifies the interval between messages — the time during which no data is being transmitted on a virtual circuit. The interval value is in seconds. The server sends status messages on the Ethernet at these intervals.

The default value is 20 seconds. Digital recommends this value for normal Ethernet environments. For a heavily loaded Ethernet, consider using a value of from 60 to 180. For applications that require quick notification and possible fail-over of a service node failure, use 10 seconds.

- **NODE LIMIT**

Specifies the number of service nodes that the server can simultaneously store in the database.

When the node limit is reached, service announcement messages from additional nodes are discarded. With the port characteristic **AUTHORIZED GROUPS**, you can usually ensure that the node limit is not reached. However, if you do not assign authorized groups (see Section 5.3), service nodes are stored in the database that users probably will never need to access and the node limit might be exceeded unnecessarily.

- **LIMITED HELP**

Specifies an abbreviated on-line command summary of DECserver 500 commands. If you enable **LIMITED HELP**, all help requests display a summary of all server commands. **LIMITED HELP** is disabled by default.

- **RETRANSMIT LIMIT**

Specifies the number of times a message is repeated if a transmission between the server and a service node fails. If the transmission is still unsuccessful after these attempts, the circuit between the server and the service node is terminated, along with all sessions associated with the circuit.

Specify a value in the range of 5 to 120. The default is 8 attempts. The value you choose depends on the type of physical link used for your network, as well as the amount of traffic on the network. See your network manager.

8.2.2 Local-Access Characteristics

Some server characteristics affect ports with local access whose users enter server commands in local mode. These ports have their **ACCESS** port characteristic set to either **LOCAL** or **DYNAMIC**. These are the server characteristics that affect ports:

- **BROADCAST**

Determines whether the **BROADCAST** command can be used.

The default is **ENABLED**, which lets you and nonprivileged users send messages to other users and receive service announcement messages in local mode when new services become available. A port must have the **BROADCAST** port characteristic enabled to receive these messages.

- **INACTIVITY TIMER**

Specifies the time-out period for remote- or local-access ports currently having no sessions and no activity (input or output), if the **INACTIVITY LOGOUT** port characteristic is **ENABLED**.

If you use the **INACTIVITY TIMER** and the **INACTIVITY LOGOUT** characteristics for ports that have the port characteristic **ACCESS** set to **DYNAMIC**, host-initiated requests for the port are honored when a local-access user logs out. If a local-access user does not use the **DYNAMIC** access port within the time-out period, the server automatically logs out the port and can then honor a host-initiated request for that port.

- **LOCK**

Enables or disables the effect of the **LOCK** command, issued by general users. When **LOCK** is enabled on the server, any user with the port characteristic enabled can issue the **LOCK** command to prevent access to the terminal at which the command is entered. The command prevents any input until a user enters the unlock password at that terminal.

If a user forgets his or her unlock password, you can log out the port by using the **LOGOUT PORT *n*** command.

Depending on the user environment, you might want to disable the **LOCK** command. The default is **LOCK ENABLED**.

- **LOGIN PASSWORD**

Defines a password that users must enter when they log in. The server has one, server-wide log-in password. It is required only for password-protected, local-access ports.

This characteristic works in conjunction with:

- The **PASSWORD** port characteristic, which you can **ENABLE** for either all or selected ports.
- The **PASSWORD LIMIT** server characteristic, which sets the number of incorrect log-in attempts that the server allows a potential user.

- **PASSWORD LIMIT**

Specifies all of the following:

- The number of times that users of local-access ports with the **PASSWORD** port characteristic **ENABLED** can incorrectly enter the log-in password before the server terminates the log-in sequence.

- The number of times that users can incorrectly enter the privileged password before the server automatically logs out their port.
- For password-protected local services, the number of times that users can incorrectly enter the service password before the server denies the connection request and displays:

```
Local -231- Connection to service-name not established
          Invalid password
Local>
```

- **PRIVILEGED PASSWORD**

Defines a password that users must enter before they can issue privileged server commands. The server has one, server-wide privileged password.

Note

The privileged server commands are exclusively for server management.

This characteristic works in conjunction with the **PASSWORD LIMIT** server characteristic, which sets the number of incorrect attempts at setting privileged status that the server allows a potential user.

- **SESSION LIMIT**

Specifies the maximum number of simultaneous sessions across all local-access ports:

- A high limit allows server users to have more sessions but results in increased memory utilization.
- A low limit decreases server memory utilization but decreases the number of allowed sessions.

If the server **SESSION LIMIT** is reached by some of the port users, the remaining port users cannot connect to sessions. In this case, you need to increase the server **SESSION LIMIT** or to decrease the individual port sessions allowed.

Set the **SESSION LIMIT** for the server either to a value of from 0 to 512 or to **NONE**. With **NONE**, the server permits up to 512 sessions to be set up, a maximum of 4 per port. The default is 256 sessions. Specifying 0 prevents any new sessions from being established.

You can also limit the number of sessions on any particular port by using the **SET/DEFINE PORT SESSION LIMIT** commands.

8.2.3 Server Maintenance Characteristics

There are three server characteristics that you can specify only with TSC: the server's backup load hosts, its line frequency, and its maintenance password. These are the server maintenance characteristics:

- **BACKUP HOSTS**

Specifies up to five backup load hosts for down-line loading with the server **INITIALIZE** command and for up-line dumping. The primary load host is usually the last load host that loaded the server. If the primary load host fails to respond to the server's down-line load or up-line dump request, the server tries the backup load hosts in the order you specified with the **DEFINE SERVER BACKUP HOSTS** command.

If the server crashes, it makes three attempts, 30 seconds apart, to up-line dump its image to the primary load host. If the primary load host does not respond, the server makes three attempts to up-line dump to each of the specified backup load hosts, in the order you entered them with the **DEFINE SERVER BACKUP HOSTS** command. If none responds, the server multicasts its **REQUEST DUMP SERVICE** message.

TSC needs access to DECnet when you specify the **BACKUP HOSTS** characteristic. You cannot change this characteristic on the running server because it does not use DECnet protocols.

For information about up-line dumping, see Section 6.3 of this manual and the *DECserver 500 Problem Solving* manual.

- **LINE FREQUENCY**

Specifies the line frequency of the server. The line frequency affects the server's timers, such as the circuit timer, and the "Uptime" value in the **SHOW SERVER** displays.

The value for this characteristic is actually a hardware parameter that the running server does not determine from the hardware configuration. The server software relies on TSC to provide this information so that the various timers on the running server are correctly calibrated.

Set the line frequency to either 50 or 60 Hz to match the line frequency of the power supply being used. The default is 60 Hz.

- **MAINTENANCE PASSWORD**

Defines the MOP maintenance password. If you specify this password, the server uses it to check the DECnet service password when the server receives one of these maintenance activity requests from a DECnet node: an NCP LOAD command, an NCP TRIGGER command, a remote console connection, or an NCP LOOP CIRCUIT command.

You must specify the maintenance password with TSC. Changing this password on the running server could make remote maintenance activities impossible if the remote person attempting the procedure does not know of the password change.

See Section 2.7.2.3 for a discussion of the maintenance password and its relationship to the DECnet service password.

8.2.4 Server Identification Characteristics

The server has three characteristics that identify it on the network: identification, name, and number.

If the server functions as a LAT service node, the server IDENTIFICATION and NAME characteristics described below are also included in the service identification messages, which are periodically announced over the LAN.

- **IDENTIFICATION**

Specifies an identification string that is associated with the server when it multicasts the availability of its local services. The server includes this identification string in the service node announcement message, along with the server name. The identification string is included in the server's SHOW NODE and SHOW SERVER displays and is also displayed when a user logs in to the server.

The IDENTIFICATION characteristic also lets you specify identification strings for local services using the SET/DEFINE SERVICE commands.

Note

You cannot change IDENTIFICATION while any sessions are active.

- **NAME**

Specifies the server's name, either as the default (the DECnet node name) or as you define it with the **SET/DEFINE SERVER NAME** command. **NAME** is used to identify the server in the following ways:

- It appears in the **SHOW/LIST SERVER** displays. Note that the **LIST SERVER** displays do not include the server's **NAME** unless you explicitly issue a **DEFINE SERVER NAME** command.
- If the server is set up as a service node, the server **NAME**, along with its services, is multicast over the **LAN**.
- Depending on the type of the service node, if there are local-access sessions between your server and a service node, the server **NAME** can be displayed on the service node.
- The server name is also displayed when a local-access port logs out of the server.

When it accepts host-initiated requests from service nodes, the server does not function as a service node, but you must give the server **NAME** to the system manager of the service nodes in order for these requests to work.

A unique server **NAME** is necessary both for a server that is used for host-initiated requests and for a server to act as a service node.

In addition, the server **NAME** must be unique on the **LAT** network. It should be identical to the server's DECnet node name, the default for this characteristic. When a new unit is installed, the network manager first assigns the server's DECnet node name and the software installer then specifies it on the server's load hosts (see Section 6.5.2.1).

You can change the server **NAME** but Digital strongly recommends that you keep the default.

- **NUMBER**

A value from 0 to 255, which you can also use to identify a server. This value appears in the **SHOW SERVER CHARACTERISTICS** display.

- **PROMPT**

Specifies a 1- to 16-character prompt for the server. The default prompt is Local>. This value appears in the SHOW SERVER CHARACTERISTICS display.

The server identification characteristics are also periodically advertised over the LAN through MOP in System ID messages (see Appendix A). Some nodes have control programs that let the node manager display the servers currently on the network. This display might use the name and the identification strings to identify your server. These strings also appear in the display produced by the SHOW/LIST SERVER commands.

8.2.5 Service Node Characteristics

The values of these server characteristics determine how your server functions as a service node. (The server NAME and IDENTIFICATION characteristics, described in the previous section, are also useful when the server acts as a service node.) The server characteristics that affect local services are as follows:

- **ANNOUNCEMENTS**

Determines whether the server multicasts service identification messages on the Ethernet to announce the availability of its services. The default is ANNOUNCEMENTS ENABLED. However, no announcements are multicast if the server does not offer any services.

- **MULTICAST TIMER**

Determines the interval, in seconds, between the server's multicast messages. If ANNOUNCEMENTS is ENABLED, these messages announce the services currently provided by the server. The timer must be in the range of 10 to 180 seconds. The default is 60 seconds.

This timer is used only if one or more local services are being offered and the server characteristic ANNOUNCEMENTS is ENABLED. Adjusting the timer affects how often other servers will be informed of changes in the server's service node information.

- **QUEUE LIMIT**

Controls the depth of the queue for host-initiated requests for the server and defines the maximum number of entries permitted at one time. The server can queue as many as 32 host-initiated requests, but you can set the queue depth to any number from 0 to 32. A value of 0 disables the queue.

The default queue depth is 8. Entering NONE implies the maximum limit of 32 queue entries. When the queue reaches its limit, no additional host-initiated requests are accepted until the queue depth falls below the limit.

- **SERVICE GROUPS**

Identifies the groups that are associated with local services, when the server offers local services and functions as a service node.

The groups enabled for the server can be different from the authorized groups enabled for a port. However, if you enable mutually exclusive groups for a port and the server, the users of the port cannot connect to any local services. For a complete discussion on groups, see Section 5.3.

8.3 Service Characteristics

The server can function as a service node and offer LAT services to users on both itself and other servers. These services are called **local services**. Local services can offer connections to devices such as non-Digital computers without LAT software, dial-out modems, and applications devices such as printers.

By default, the server is a disabled service node with no services set up and no service announcements. When you set up a local service, you can also customize the service characteristics, or you can use the defaults.

Logically, the maximum number of services that can be defined in TSC is 249; the maximum on the server is 255. In reality, the maximum number of services is probably less than these limits, depending on the memory constraints of the server.

To display local services, issue the **SHOW/LIST SERVICES** commands. The displays include the service rating and, with the **SHOW** commands, the current status of each service.

You can issue these commands to learn which server ports you assigned to a particular local service and whether you disabled connections, a service password, or queuing for the service. To display the list of local services assigned to each port, you can also use the **SHOW PORTS SUMMARY** command.

To create a local service or to modify the characteristics of an existing one, use the **SET/DEFINE SERVICE** commands. See Section 5.8.

Table 8–7 lists the local service characteristics with their defaults.

Table 8–7: Service Characteristics with Defaults

Characteristic	Default
CONNECTIONS	ENABLED
IDENTIFICATION	NONE
PASSWORD	NONE
PORTS	ALL DISABLED
QUEUE	ENABLED

These are the service characteristics for local services:

- **CONNECTIONS**

Specifies whether the server can accept further requests to connect to the service. With **CONNECTIONS DISABLED**, the server rejects any subsequent attempt to connect to the specified service. In addition, the server rejects any entry that is dequeued for that service.

When you try to disable connections to a service, sessions currently connected to that service are not affected. The server checks to see if connections are enabled when a request comes in or when a queued request reaches the top of the queue.

- **IDENTIFICATION**

Specifies an identification string that is associated with the service. The service identification can provide information about the service that is not implied by the name. For example, for a dial-out modem service, a service name such as **DIAL-OUT** can identify the nature of the device offered, while the identification can provide helpful information such as “Type <CTRL/B> for the modem’s attention.”

The service identification string is included in the server's multicast message. The server also includes this identification string in the service identification message.

The string appears beside the service name in the SHOW SERVICES displays of servers where the service is known.

- **PASSWORD**

Defines a password that users must enter before they can start a session with a local service. Each service has its own service password.

This characteristic works in conjunction with the PASSWORD LIMIT server characteristic and other password-related characteristics (see Sections 5.1.6 and 5.1.7).

- **PORTS**

Specifies the port or ports that offer the service.

The number of available ports associated with a service is reflected in the service rating that is sent in the service announcement message. If a service does not have an assigned port or if none of the assigned ports is available, the service rating is set to 0.

The default is to have no ports defined for a service. You must assign at least one port for a service to be accessible.

- **QUEUE**

Determines whether host-initiated requests for the service are stored in the connection queue of the server. Queuing is available only for host-initiated requests.

When a service with queuing enabled lacks an available port, the server usually places a host-initiated request for that service into the queue. When this queue is full, the server rejects any request for a service with no available port. For information on managing the connection queue, see Section 5.10.

8.4 Devices

There are other kinds of server “characteristics” that you can set or define for devices. One characteristic is the TYPE of line card that resides in a particular Q-bus slot on the server. Another is an operational STATE for a line card. For a CXM04 line card, you can also specify a value for the DUMP characteristic.

8.4.1 Defining Device TYPE

The TSC DEFINE DEVICE TYPE command specifies the line-card type for each physical slot of the server. After a down-line load, the server checks the actual device types against any types you specified with TSC. In the event of a mismatch because you mistakenly specified CXY08 and the actual type is CXA16, all the ports associated with that device are disabled by the server. This is also true if you forget to define the CXM04 device before down-line loading the server.

In addition, the SHOW DEVICES ALL display shows the device as “Wrg Typ” for “wrong type.” Digital suggests, therefore, that when you define a device type, you issue SHOW DEVICES ALL immediately after a reload. This ensures that the ports are operational.

Both TSC and the running server, however, do not always check line card validity. For example, there is no checking if you first issue one of the following commands:

```
TSC> DEFINE DEVICE ALL TYPE NONE
```

OR

```
TSC> DEFINE DEVICE LC3 TYPE NONE
```

In this case, TSC — and the server after a down-line load — equate NONE with CXA16, regardless of what line card is actually connected to the hardware. Because a CXA16 is a data-leads-only line card, TSC and the server would then reject any attempt, for example, to specify MODEM CONTROL ENABLED for the associated ports if the line card is actually a CXY08.

If you issue the DEFINE DEVICE command and specify any line card other than CXY08, TSC automatically does the following:

- Disables CTS and DSR flow control
- Disables modem control

- Disables DTRWAIT
- Enables XON flow control

8.4.1.1 The CXY08 Line Card

You can enable modem control for a port on either TSC or on the running server, but you must first issue the TSC DEFINE DEVICE command and specify the only line-card type that supports modem control — CXY08. For example:

```
TSC> DEFINE DEVICE LC3 TYPE CXY08
TSC> DEFINE PORT 33,34,35 MODEM CONTROL ENABLED
```

TSC uses device type information to test the validity of port characteristics that relate to modem control. After you issue any of the following commands, TSC checks that port *n* is on a CXY08 line card (if you issue the equivalent SET commands, the server does the same checking):

```
DEFINE PORT n DSRLOGOUT ENABLED
DEFINE PORT n DTRWAIT ENABLED
DEFINE PORT n MODEM CONTROL ENABLED
DEFINE PORT n FLOW CTS/DSR ENABLED
```

8.4.1.2 The CXM04 Line Card

The CXM04 line card contains firmware and keyboard mapping tables that make it possible for 3270-class terminals to emulate Digital VT220 terminals. The translation tables map 3270-class terminal keystrokes into VT220 character sequences.

If you add a CXM04 line card to your hardware configuration, you must install CXM04 firmware on the load host and then DEFINE this device type in order to append the CXM04 firmware and keyboard mapping tables to the server image. This must be done prior to down-line loading the server image. If not, the server software cannot load the firmware onto the card and thus will not accept the CXM04 line card (causing ports associated with the card to become disabled).

When you define the CXM04, you choose one of two operating configurations either explicitly or by default. CONFIGURATION 4 (the default) specifies that four ports on the line card can operate in both VT mode and 3270 mode. CONFIGURATION 8 specifies that eight ports can operate in VT mode only.

In CONFIGURATION 4, each port's MODE characteristic defaults to DYNAMIC (both modes). However, you can restrict a port's operation to either VT220 or 3270 by defining the port's MODE characteristic accordingly. For example, to configure a line card for both operating modes but restrict two of its ports to 3270 mode only, issue the following TSC commands:

```
TSC> DEFINE DEVICE LC1 TYPE CXM04 CONFIGURATION 4
TSC> DEFINE PORT 3,4 MODE 3270
```

If you choose CONFIGURATION 8, the firmware configures the card for VT mode only. Eight ports are connected to 3270-class terminals, and all terminals are in VT mode. In CONFIGURATION 8, a port's MODE characteristic can only be VT220.

Note

Ensure that the hardware configuration (the setting of the jumpers and a switch on the line card) match the software configuration as described in the hardware installation procedure.

8.4.2 Device STATE

You can use the SET/DEFINE DEVICE STATE command to change the value of the STATE characteristic. With TSC, you can specify what the line card state will be when the server image is down-line loaded: on-line, off-line, or standby. On the running server, you can specify only on-line or off-line. These are the possible states for the line card:

- **ONLINE**

Changes a previously-defined off-line or standby line card to an on-line state. ONLINE is the default state. Changing state to on-line is not valid on line cards LC9 and LC10. These two slots are reserved for standby line cards that can be activated only with the MOVE DEVICE command.

- **OFFLINE**

Logically removes a line card from the server without physically removing the line card. The server software then ignores that particular line card. This command logs out all ports on the card and disables all interrupts from that card. Therefore, it is important to notify server users prior to setting a line card to OFFLINE.

- **STANDBY**

Defines a device as a standby line card, allowing you to switch operation later from an active line card to a standby line card. Any line card on the server can be defined as STANDBY.

After defining the device with TSC as a standby line card, you down-line load the server image in order to place that device in a standby status. To activate the standby device on the running server, you execute the SET DEVICE STATE OFFLINE command on the source (failed) line card, execute the MOVE DEVICE command, and switch associated cabling from the source line card to the standby line card.

For more information about standby line cards, refer to Section 5.14.

8.4.3 Device DUMP

For the CXM04 line card only, use the SET/DEFINE DEVICE DUMP command to change the value of the DUMP characteristic. Enabling this characteristic causes the line card to dump CXM04 information as part of a server up-line dump. The line card cannot dump information independent of a server dump.

These are the possible choices for specifying the DUMP option:

- **DISABLED**

The card will not be part of a server up-line dump. This is the default.

- **ENABLED**

The card dumps all CXM04 information (registers, data, and instruction space).

8.5 Defining Languages

The DEFINE LANGUAGE command allows you to add a new language with customized keyboard tables to the server image. The command is valid only if you have defined at least one device as CXM04.

TSC recognizes only the fifteen VT language names listed in the VT220 set-up menu. Thus, language-name for a customized language must be the same as one of the VT languages.

The server image is limited to four language entries. Four VT languages are shipped with the CXM04 product, and their tables are automatically appended to the server image when defining the CXM04 card. These languages are North American, British, French, and German. Because the server image already contains four language entries, you must remove an unused language (PURGE LANGUAGE) before trying to define a new language. For example:

```
TSC> PURGE LANGUAGE GERMAN
TSC> DEFINE LANGUAGE DUTCH FILE FOO::SYS$COMMON:[DECSEVER]DUTCH.TBL
```

The file-spec parameter is the disk location of the keyboard mapping tables for the language being defined. To add new tables for a language currently defined in the server image, you must first remove the existing tables for that language (with PURGE LANGUAGE). That is, the procedure is similar to defining a new language.

Note

If coaxial terminals with 102-key keyboards are attached to the CXM04, do not purge the North American language from the DECserver 500 image. The 102-key keyboard's only mapping table is North American.

Displaying Server Information

Chapter 9 is a reference chapter that summarizes all the server and TSC display commands. This chapter also illustrates the displays, describes the data fields in the displays, and has guidelines to help you interpret the displays.

For detailed information about the syntax of display commands, see the *Terminal Server Commands and Messages Reference*.

9.1 Overview of Display Commands

A display command has three components: command verb, entity to be displayed, and display type. The display type defaults to a preset type if you omit it. These components are defined in Tables 9–1, 9–2, and 9–3. Table 9–1 summarizes the display command verbs.

Table 9–1: Display Command Verbs

Command Verb	Function
SHOW	Displays information from the operational database or displays a snapshot of the current status of the requested entity. SHOW is a nonprivileged server command.
MONITOR	Provides a continuously updated screen display of information from the operational database or of the current status of the requested entity. MONITOR is a privileged server command.
LIST	Displays information from the permanent database. LIST is a TSC command.

MONITOR commands produce displays that continuously update information. If the display device supports ANSI escape sequences and you have issued a **SET PORT TYPE ANSI** command for the port, the changing information is updated in its fixed position on the screen. If there is no ANSI escape sequence support, a new display is generated for each update.

MONITOR commands are privileged. Digital suggests that you use them sparingly because the continuous displays require more server resources than other commands. If there is any other privileged user, which Digital does not recommend, the server allows only one **MONITOR** display at any given time.

Press the **BREAK** key to halt a display immediately. Entering **CTRL/O** during a **MONITOR** display terminates the display after the full display is shown.

Table 9-2 lists the command verbs with the entities they can display.

Table 9–2: Display Command Verbs, Applicable Entities, Functions

Command	Entity	Function
SHOW MONITOR LIST	DEVICES	Display information about devices on the server.
LIST	MAPPING	Display the mapping of a single scan code, a scan code state, or all keys in the selected keyboard table.
LIST	LANGUAGES	Display those languages currently defined in the server image when using CXM04 line cards.
SHOW MONITOR LIST	NODES	Display information about service nodes on the network, including the server as a service node.
SHOW MONITOR LIST	PORT	Display information about the server ports.
SHOW MONITOR	QUEUE	Display information about the server queue of host-initiated connections.
SHOW MONITOR LIST	SERVER	Display information about the server from its permanent or operational database.
SHOW MONITOR LIST	SERVICES	Display information about services available on the network. LIST displays only services offered by the server.
SHOW MONITOR	SESSIONS	Display information about active service sessions on selected ports.
LIST	TABLES	Display the keyboard tables in a selected keyboard table file.

Table 9–2 (Cont.): Display Command Verbs, Applicable Entities, Functions

Command	Entity	Function
LIST	USAGE	Displays information about previous changes to the server image currently being processed by TSC.
SHOW MONITOR LIST	USERS	Display information about current users on the server.

The server generates a total of four types of screen displays, but not all types are available for every SHOW/MONITOR/LIST command. Table 9–3 summarizes the contents of each display type.

Table 9–3: Display Types

Display Type	Description
CHARACTERISTICS	Displays values for characteristics that you can change with SET/DEFINE commands or other users can change with SET commands.
COUNTERS	Displays the values of counters that show the number of times certain events have occurred since you reset the counters to zero. The server maintains counter information to aid you in analyzing its operation.
STATUS	Displays detailed information about the requested entity. This information might include values for additional counters and the current, highest, and maximum values for certain key fields.
SUMMARY	Displays a brief summary of information, usually one line, for each entry in a list of entities, for example, a list of services.

The rest of this chapter illustrates and describes each display.

9.2 Device Displays

The `SHOW/MONITOR/LIST DEVICES` commands display information about the devices on the server:

- `SHOW/MONITOR DEVICES` — You can specify these display types: `COUNTERS`, `SUMMARY`, and `CHARACTERISTICS` status. They give you a summary display. Each line of display provides both characteristics and summary information.
- `LIST DEVICES` — You can specify `SUMMARY` and `CHARACTERISTICS`. The `SUMMARY` and `CHARACTERISTICS` displays are the same; they give you a summary display. Each line of display provides both characteristics and summary information.

You can issue `SHOW DEVICE CONSOLE` to get information about the server's physical console port, port 0, but you can also display more details about port 0 with the `SHOW PORT 0` command.

9.2.1 Device Summary Display

Use the `SHOW/MONITOR DEVICE SUMMARY` commands or the `LIST DEVICE` command to get an overall picture of the server configuration, including — for the `SHOW/MONITOR` commands — the type and current status of each device. If there are errors, you can use the `SHOW/MONITOR DEVICE COUNTERS` display to determine the types of errors.

The default is to display `ALL` devices, or you can specify a device name, for example, `LC2`.

Figure 9–1 shows a typical device summary display.

Figure 9–1: Device Summary Display

Local> SHOW DEVICES ALL SUMMARY

Device Name	Device Type	Port List	Device Status	CSR Address	Vector Address	Total Errors	Slot
CONSOLE	DL	0	Running	177560	60	0	1
NETWORK	DESQA		Running	174440	120	0	2
LC1	CXA16	1-16	Running	160440	310	0	3
LC2	CXM04	17-20	Running	160460	320	0	4
LC3	CXM04	33-36	Running	160500	330	0	5
LC4	CXA16	49-64	Running	160520	340	0	6
LC5	CXA16	65-80	Running	160540	350	0	7
LC6	CXA16	81-96	Failed	160560	360	0	8
LC7	CXA16	97-112	Running	160600	370	0	9
LC8	CXA16	113-128	Running	160620	400	0	10
LC9	CXM04		Standby			0	11
LC10	CXM04		Fm Fail			0	12

Local>

Note

The DECserver 510 display is slightly different from the one shown here.

LIST DEVICES gives you the same information as SHOW DEVICES, except that the display does not have two fields: Status and Total Errors. Table 9–4 describes the fields in the device summary display.

Table 9-4: Device Summary/Characteristics Display Fields

Field	Description
Slot	The number of the physical slot on the server where the line card is physically attached.
Device Name	The name of the line card, for example, NETWORK or LC <i>n</i> , where <i>n</i> represents a number from 1-10.
Device Type	<p>The type of hardware module that is actually in that slot. If you issued the TSC DEFINE DEVICE command, the actual device type must be the same as the type you defined with that command or the associated ports cannot operate. The device types are shown as:</p> <p>DL An asynchronous single Digital console line, used exclusively for the console port.</p> <p>DEQNA A Digital Ethernet Q-bus adapter for DECserver 500.</p> <p>DESQA A Digital Ethernet Q-bus adapter for DECserver 500 series hardware</p> <p>CXY08 A CXY08, modem control, EIA-232 line card.</p> <p>CXA16 A CXA16, data-leads-only, EIA-423-A line card.</p> <p>CXB16 A CXB16, data-leads-only, RS-422-A line card.</p> <p>CXM04 A 3270 terminal option line card.</p> <p>None Specified Either you did not issue a DEFINE DEVICE command, or you issued it with the keyword NONE.</p> <p>Unkwn There is no line card in the slot.</p>
Port List	The ports that are attached to the line card.
Device Status	<p>The present condition of the line card and its associated ports.</p> <p>Running Functioning normally.</p> <p>Testing Self-test is in progress.</p> <p>Starting Passed the self-test and is now being configured with port parameters.</p> <p>Failed Failed the self-test and is now off-line.</p>

Table 9–4 (Cont.): Device Summary/Characteristics/Status Display Fields

Field	Description
	Wrng Typ Wrong type of device in slot. The line card you specified in TSC with DEFINE DEVICE does not match the actual line card in the physical slot. This line card and its associated ports are inoperative.
	Standby Defined as a standby line card.
	MOV LCn Moved to LCn with MOVE DEVICE and is now inoperative.
	Fm Fail Software on the CXM04 line card has reported a failure and the module is no longer operational. If the CCU connection exists, all connected terminals will automatically switch to 3270 mode.
CSR Address	The address of the first control status register of the line card.
Vector	The interrupt vector address of the line card. Address
Total Errors	The total number of combined soft and hard failures on the line card. For the CXM04 card, the total error count includes ASCII, execution, and coax errors. (See the SHOW DEVICES COUNTERS display for a breakdown of errors by type.)

9.2.2 Device Counters Display

The SHOW/MONITOR DEVICE COUNTERS commands display counters associated with the devices you specify. Different information is displayed, depending on whether you request a display for NETWORK, for a CXM04 device, or for LCn, where *n* is the line-card number of a device. If you specify ALL, you get both displays.

Figure 9–2 shows typical device counters displays.

Figure 9–2: Device Counters Display

Local> SHOW DEVICES NETWORK COUNTERS

```
Device name: NETWORK                Device Type: DESQA
Timeouts:          100              Internal Errors:    43
Local Errors:      0                Ring Errors:       5
State Errors:      0                Last TDR Reported: 5120
```

Local> SHOW DEVICES LC1 COUNTERS

```
Device name: LC1                    Device Type: CXA16
Framing Errors:    100              FIFO Overruns:     2
Parity Errors:     34              Transmit Errors:    0
Data Overruns:    0
```

Local> SHOW DEVICES LC2 COUNTERS

```
Device name: LC2                    Device Type: CXM04
Device Error Counter                3270 Mode          VT Mode
                                     CCU Coax          Terminal Coax      Terminal Coax
Receiver FIFO Overflow              0                  0                  0
Bad Receive Parity                  0                  0                  0
Invalid Ending Sequence              0                  0                  0
Loss of Mid-Bit Transition           0                  0                  0
Receiver Disabled                    0                  0                  0
No Response                          0                  0                  0
No Poll Acknowledge                 0                  --                 --
Bad Key                              --                 --                 0
Device Check                        --                 --                 0
Terminal Reconnect                  --                 0                  0
State 1                             --                 0                  0
State 2                             --                 0                  0
```

Local>

Table 9–5 describes the device counters displays.

Table 9–5: Device Counters Display Fields

Field	Description																		
Device Name	The name of the line card, for example NETWORK or LC- <i>n</i> , where <i>n</i> represents a number from 1–8.																		
Device Type	<p>The type of hardware module that is actually in that slot. If you issued the TSC DEFINE DEVICE command, the actual device type must be the same as the type you defined with that command or the associated ports cannot operate. The device types are shown as:</p> <table><tbody><tr><td>DL</td><td>An asynchronous single Digital console line, used exclusively for the console port.</td></tr><tr><td>DEQNA</td><td>A Digital Ethernet Q-bus adapter for DECserver 500.</td></tr><tr><td>DESQA</td><td>A Digital Ethernet Q-bus adapter for DECserver 500 series hardware.</td></tr><tr><td>CXY08</td><td>A CXY08, modem control, EIA–232 line card.</td></tr><tr><td>CXA16</td><td>A CXA16, data-leads-only, EIA–423–A line card.</td></tr><tr><td>CXB16</td><td>A CXB16, data-leads-only, RS–422–A line card.</td></tr><tr><td>CXM04</td><td>A 3270 terminal option line card.</td></tr><tr><td>None Specified</td><td>Either you did not issue a DEFINE DEVICE command, or you issued it with the keyword NONE.</td></tr><tr><td>Unkwn</td><td>There is no line card in the slot.</td></tr></tbody></table>	DL	An asynchronous single Digital console line, used exclusively for the console port.	DEQNA	A Digital Ethernet Q-bus adapter for DECserver 500.	DESQA	A Digital Ethernet Q-bus adapter for DECserver 500 series hardware.	CXY08	A CXY08, modem control, EIA–232 line card.	CXA16	A CXA16, data-leads-only, EIA–423–A line card.	CXB16	A CXB16, data-leads-only, RS–422–A line card.	CXM04	A 3270 terminal option line card.	None Specified	Either you did not issue a DEFINE DEVICE command, or you issued it with the keyword NONE.	Unkwn	There is no line card in the slot.
DL	An asynchronous single Digital console line, used exclusively for the console port.																		
DEQNA	A Digital Ethernet Q-bus adapter for DECserver 500.																		
DESQA	A Digital Ethernet Q-bus adapter for DECserver 500 series hardware.																		
CXY08	A CXY08, modem control, EIA–232 line card.																		
CXA16	A CXA16, data-leads-only, EIA–423–A line card.																		
CXB16	A CXB16, data-leads-only, RS–422–A line card.																		
CXM04	A 3270 terminal option line card.																		
None Specified	Either you did not issue a DEFINE DEVICE command, or you issued it with the keyword NONE.																		
Unkwn	There is no line card in the slot.																		
Time Outs	<p>The number of times that the server’s NETWORK device, for example, DEQNA, did not respond and had to be restarted by the server software. Appears only if you specify NETWORK as the device or ALL.</p> <p>A nonzero value might indicate a defective NETWORK device.</p>																		
Internal Errors	<p>The number of times the network device could not handle certain illegal Ethernet events. Appears only if you specify NETWORK as the device or ALL.</p> <p>A nonzero value might indicate a defective device elsewhere on the Ethernet, and this device is violating the Ethernet data link protocol specifications.</p>																		
State 1 and 2	These counters are for use by Digital Equipment Corporation personnel.																		

Table 9–5 (Cont.): Device Counters Display Fields

Field	Description
Local Errors	<p>The number of times the server software did not have a system buffer available for the network device to copy an Ethernet message into. Appears only if you specify NETWORK as the device or ALL.</p> <p>A nonzero value might indicate that the server software has too many system buffers dedicated to maintaining a large number of virtual circuits, sessions, or queued connections and not enough for heavy network traffic situations.</p>
Ring Errors	<p>The number of times the network device on the server lost messages because the server could not keep up with the rate at which the network device was receiving messages from the Ethernet. Appears only if you specify NETWORK as the device or ALL.</p> <p>Nonzero values might indicate that there is excessive Ethernet traffic or that the server is overloaded due to excessive input from its asynchronous lines — to the point that it cannot adequately handle network events.</p>
State Errors	<p>The number of times the network device was in a state that the software did not expect it to be in. Appears only if you specify NETWORK as the device or ALL.</p> <p>Nonzero values might indicate a software problem or a network device hardware problem.</p>
Last TDR Reported	<p>TDR means Time Domain Reflectometry. Identifies the relative location of an Ethernet error, which can be on either side of the server's connection to the Ethernet. The value here depends on the kind of network device you have.</p> <p>An example of the kind of error that can produce a nonzero TDR value is an Ethernet short circuit.</p>
Framing Errors	<p>The number of bytes received at the line card with illegally formatted frames. Appears only if you specify LCn as the device or ALL.</p> <p>Nonzero values increasing very slowly over a long period of time indicates that at least one port (and perhaps more) is operating at a speed that does not match the speed of its port device. Nonzero values increasing rapidly might indicate cabling problems, for example, noisy lines.</p>

Table 9–5 (Cont.): Device Counters Display Fields

Field	Description
Parity Errors	<p>The number of bytes received on the line card with parity errors. Appears only if you specify LC-<i>n</i> as the device or ALL.</p> <p>Nonzero values increasing very slowly over a long period of time indicates that at least one port (and perhaps more) has a parity value that does not match the parity value of its port device. Nonzero values increasing rapidly might indicate noisy lines.</p>
Data Overruns	<p>The number of bytes lost on the line card because the server software input buffers were full. Appears only if you specify LC<i>n</i> as the device or ALL.</p> <p>A nonzero value might indicate one of these conditions: noisy lines, too many ports on the line card running at high speed with FLOW CONTROL DISABLED, or at least one port device (perhaps more) is ignoring the server's attempts to perform flow control.</p>
FIFO Overruns	<p>The number of times a line card's hardware input buffers overflowed because the server software did not process the input data fast enough. Appears only if you specify LC<i>n</i> as the device.</p> <p>A nonzero value might indicate one of these conditions: noisy lines, too many ports on the line card running at high speed with FLOW CONTROL DISABLED, or at least one port device (perhaps more) is ignoring the server's attempts to perform flow control.</p>
Transmit Errors	<p>The number of times a line card attempted to transmit data and encountered an error while trying to access the part of server memory that contains the data. Appears only if you specify LC<i>n</i> as the device. A nonzero value might indicate either a hardware or a software problem.</p>

Table 9–6 lists the device (and port) counter information that is displayed only for a CXM04 line card. See the discussion of troubleshooting in the *DECserver 500 Problem Solving* manual for details regarding the specific diagnostic information CXM04 counters can provide.

Table 9–6: CXM04 Counters Display Fields

Counter Name	CCU Coax Counters	3270 Mode Terminal Coax Counters	VT Mode Terminal Coax Counters
Receiver FIFO Overflow	xx	xx	xx
Bad Receive Parity	xx	xx	xx
Invalid Ending Sequence	xx	xx	xx
Loss of Mid-Bit Transition	xx	xx	xx
Receiver Disabled	xx	xx	xx
No Response	xx	xx	xx
No Poll Acknowledge	xx	—	—
Bad Key	—	—	xx
Device Check	—	—	xx
Terminal Reconnect	—	xx	xx
State 1	—	xx	xx
State 2	—	xx	xx

The CXM04 counters are divided into three groups:

1. **CCU Coax Counters:** Provides information on the operation of the CCU Coax in both 3270 Mode and VT Mode.
2. **3270 Mode Terminal Coax Counters:** Provides information on the operation of the Terminal Coax in 3270 Mode.
3. **VT Mode Terminal Coax Counters:** Provides information on the operation of the Terminal Coax in VT Mode.

Table 9–7 provides the specific information about each of the CXM04 counter names.

Table 9–7: CXM04 Counters Display Fields

Field	Description
Receive FIFO Overflow	Increments each time a receive FIFO data overflow occurs.
Bad Receive Parity	Increments each time bad parity is detected in a received frame.
Invalid Ending Sequence	Increments each time an invalid ending sequence is detected in a received frame.
Loss of Mid-Bit Transition	Increments each time a Manchester Code mid-bit transitions is not detected while receiving
No Response	(For CCU Coax) Indicates that the CCU has not polled for 7 seconds. (For Terminal Coax) Indicates that the terminal has not responded.
No Poll Acknowledge	Increments each time the CCU fails to respond to a non-zero poll response.
Bad Key	Increments each time a 3270 terminal responds with an invalid scan code.
Device Check	Increments each time a 3270 terminal sends a Device Check status in response to a poll (Valid in VT Mode only).
Terminal Reconnect	Increments each time a 3270 terminal is disconnected and reconnected. Also increments if a terminal is powered down and up or if a terminal test switch is activated.
Invalid ASCII Sequence	Increments each time an invalid ASCII control sequence occurs (Valid in VT Mode only).
State 1	This error counter is reserved for use by Digital field service personnel.
State 2	This error counter is reserved for use by Digital field service personnel.

9.3 Node Displays

The SHOW/MONITOR NODES commands display information about the service nodes on the network. You can request NODE COUNTERS, NODE STATUS, and NODE SUMMARY displays. SUMMARY is the default display type for NODES and NODES ALL.

LIST NODE has no options and shows only the server as a service node. It displays the local services you defined with the DEFINE SERVICE command. Figure 9–3 illustrates an example showing the local services offered by server TIGER.

Figure 9–3: Node Display of Local Services

```
TSC> LIST NODE

Node: TIGER

Node id: DS500 Terminal Server

Node Groups: 2,3,5,10-35,100-115

Service Name      Identification
NONDEC            XYZ minicomputer
LASER             High-quality Laser Printing
MICRO             Personal computer 2
MODEM             Dial-out modem
SWITCHER         Terminal switch

TSC>
```

On the running server, you have to specify the server's node name when you issue the SHOW NODE command to see information about the server as a service node, for example:

```
Local> SHOW NODE TIGER
```

displays the local services offered by server TIGER.

To see information about any service node, specify a service node name with the SHOW/MONITOR/LIST NODE commands. For example, to display counters for service node PEACH, type:

```
Local> SHOW NODE PEACH COUNTERS
```

The keyword ALL is the default. For example, to see counter values for all service nodes, issue:

```
Local> SHOW NODE COUNTERS
```

9.3.1 Node Counters Display

The SHOW/MONITOR NODE COUNTERS commands display the counters for messages transmitted between the server and the LAT service nodes you specify. Some of these counters are also maintained for all the service nodes that the server recognizes. Table 9–6 describes the NODE COUNTERS display.

Counters can help you estimate server traffic on the network for specific time periods. For example, if you zero the counters at the start of each day, you can gain information about daily server use. You can also tell if the server has detected problems with any service nodes by monitoring the error counters.

The network manager can use counters data to calculate the average use of the Ethernet and the service nodes. He or she can also combine this data from your server with the counters data from other servers to calculate the network's capacity to handle more traffic.

Figure 9–4 shows a typical node counters display, illustrating the counters for LAT messages between the server and PEACH.

Figure 9–4: Node Counters Display

```
Local> SHOW NODE PEACH COUNTERS
```

```
Node: PEACH
```

Seconds Since Zeroed:	961608	Multiple Node Addresses:	0
Messages Received:	687568	Duplicates Received:	21
Messages Transmitted:	558793	Messages Re-transmitted:	35
Slots Received:	509763	Illegal Messages Received:	0
Slots Transmitted:	532932	Illegal Slots Received:	0
Bytes Received:	13876620	Solicited Msgs Accepted:	0
Bytes Transmitted:	475427	Solicited Msgs Rejected:	0

```
Local>
```

Table 9–8 describes the information displayed. All these counters have a maximum value of 4,294,967,295. If a counter reaches that value, it remains there until either you set the counters to zero or the server is initialized. The maximum values are typically not reached for several months after you set them to zero.

Table 9–8: Node Counters Display Fields

Field	Description
Node	The name of the node.
Seconds Since	The number of seconds since the counters were last set to zero.
Zeroed	(The maximum time exceeds 134 years.)
Messages Received	The number of virtual circuit messages the server received from this node.
Messages Transmitted	The number of virtual circuit messages the server transmitted to this node.
Slots Received	The number of slots the server received from this node. A slot represents a message segment for a particular session.
Slots Transmitted	The number of slots the server transmitted to this node.
Bytes Received	The number of data bytes the server received from this node.
Bytes Transmitted	The number of data bytes the server transmitted to this node.
Multiple Node Addresses	The number of times that a node advertised itself with a physical address different from that in a previous advertisement. This might indicate, for example, that two LAT service nodes are running DECnet with the same DECnet node address.
Duplicates Received	The number of virtual circuit messages the server received from this node that were not in the correct sequence.
Messages Retransmitted	The number of virtual circuit messages the server retransmitted to this node.
Illegal Messages Received	The number of invalidly formatted messages the server received from this node.
Illegal Slots Received	The number of invalidly formatted slots the server received from this node.

Table 9–8 (Cont.): Node Counters Display Fields

Field	Description
Solicited Msgs Accepted	The number of host-initiated requests the server has accepted. This number includes requests that are queued and requests that were immediately satisfied.
Solicited Msgs Rejected	The number of host-initiated requests the server has rejected.

The following guidelines apply to the node counters display:

- **Duplicates Received**

This value should be less than 1/1000 of the value for Messages Received. This count usually indicates that the service node is retransmitting a message. If this value is higher than the guideline, the server might be failing to handle the message traffic from the service node, causing the service node to retransmit messages.

- **Messages Retransmitted**

This value should be less than 1/1000 of the value for Messages Transmitted. If this value is higher than the guideline, the service node might be failing to handle the server message load.

- **Illegal Messages Received**

This value should be zero. Any other value indicates a possible software problem in either the server or the service node. A nonzero value might also indicate a hardware problem in the service node.

- **Illegal Slots Received**

This value should be zero. Any other value indicates a possible software problem in either the server or the service node. A nonzero value might also indicate a hardware problem in the service node.

- **Solicited Msgs Accepted and Solicited Msgs Rejected**

The sum of the number of solicited messages accepted and the number of the solicited messages rejected equals the number of host-initiated requests that were received by the server.

You can monitor these counters when an application program attempts a host-initiated connection. The counters indicate if the server is receiving the connection request messages from the service node.

9.3.2 Node Status Display

The SHOW/MONITOR NODE STATUS commands display information about the status of nodes, including a list of services offered by the server. STATUS is the default display type. This display can help you and the network manager track the availability and use of services.

Figure 9–5 shows a typical node status display.

Figure 9–5: Node Status Display

```
Local> SHOW NODE PEACH STATUS

Node: PEACH                               Address: 08-00-2B-00-2B-02
LAT Protocol: V5.1                         Data Link Frame Size: 1500

Identification: Terminal Server Development

Node Groups: 20-50,100-200

Service Name      Status      Rating  Identification
DEVELOP          2 Connected  255    Terminal Server Development System
TEST             Available   150    High-powered Performance Testing
TIMESHARING      Available   27     RSX-11M-PLUS Development System

Local>
```

Table 9–9 describes the node status display.

Table 9–9: Node Status Display Fields

Field	Description
Node	The name of the service node.
LAT Protocol Vx.y	The version number <i>x</i> and the update level <i>y</i> of the LAT protocol of the service node software.
Address	The Ethernet address of the service node.
Data Link Frame Size	The maximum Ethernet data link frame size used by the service node to receive messages.
Identification	The node identification string, which might contain a useful description of the service node and its application.
Node Groups	The groups enabled for this service node. They determine the ports that can connect to its services.
In the remainder of the display, one line of information appears for each service.	
Service Name	A name of a service offered on the node.
Status	The status of the node: Available The service is currently available to server users. The server is regularly receiving multicast messages and ports can be connected to it. <i>n</i> Connected The service is available and <i>n</i> currently active sessions were requested with this service name. Unreachable The node is not currently up and running. The server cannot connect to the services that this node usually offers. Bad message The server received an invalid multicast message from the node. This is a sign of a possible hardware or software problem of the service node. Unknown The node was available but now might be unavailable. The server has not recently received a multicast service announcement message from this node. An attempted connection might fail.
Rating	The rating value assigned to the service by the service node, indicating relative capacity to accept new connections.
Identification	A brief description of the service and/or its application as defined by the service node's manager.

The following guidelines apply to the node status display:

- **LAT Protocol Version**

LAT V5.1 protocol permits host-initiated requests for printers connected to terminal servers. LAT V5.0 protocol does not permit host-initiated requests.

- **Node Groups**

The values in this field tell which groups a port must have enabled to access the selected service node. For a port to access the service node, at least one of these groups must be enabled on the port. Ranges of groups are displayed as *n-m*, as shown in Figure 9–5.

- **Service Name**

The display shows the name of each service that is offered by the selected service node. The same service might be offered on other service nodes. Use `SHOW SERVICE service-name STATUS` to find the names of all the nodes offering a particular service.

- **Status**

Services with the Available and Connected status are available for connection requests. If the service is in the Connected state, the server has one or more sessions with the service; the number of connections is shown.

Note that when the local server is the service node about which information is being displayed, sessions between two of the server ports count as two sessions — one on the initiating port and one on the target port.

If a service is in the Unknown state, the server has not recently received a multi-cast message from the service node and does not know whether the service is available; therefore, attempted connections might fail.

If the service is in the Unavailable state, the server has tried connecting to the service and has either received no response or had an active session timeout. In this case, the state of the service node is “Unreachable.”

- **Rating**

This value is the current load balancing rating associated with the service. The rating varies from 0 to 255, where 255 indicates the greatest capacity of the service node to accept a new connection.

- **“Unknown” Node Status**

The value of its multicast timer is part of a node’s service announcement message. The server waits five times the period specified by the node’s multicast timer without receiving a multicast message from the node before changing that node’s status from “Reachable” to “Unknown.” For example, if a node is advertising a 60-second multicast timer, the server waits 5 minutes.

- **Reachable Nodes Shown as “Unknown”**

Sometimes nodes that are actually reachable have a status of “Unknown.” This happens if the server’s CPU becomes more than 75% utilized.

If the server’s CPU does become more than 75% utilized, which you can check by looking at the “Cur” column of the “% CPU Used” field of the SHOW SERVER STATUS display, the server temporarily stops processing service announcement multicast messages. Eventually some of the nodes have a status of “Unknown,” instead of “Reachable.” You can still connect to these nodes, however, and when the CPU becomes less than 75% utilized, the server starts listening to multicast service announcements again and updates each node’s status to “Reachable” as its announcements come in.

9.3.3 Node Summary Display

The SHOW/MONITOR NODES SUMMARY commands display one line of information for each service node. Use this display to help you determine the reachability status of service nodes. Summary is the default display type for NODES and NODES ALL.

The following command displays node summary information. LIST NODE has no options and displays less information than SHOW/MONITOR. Figure 9–6 shows a typical node summary display.

Figure 9–6: Node Summary Display

```
Local> SHOW NODES ALL SUMMARY

Node Name           Status           Identification
-----
BANANA              2 Connected     Documentation System
ORANGE              Reachable       RSX-11M-PLUS Development System
PEACH               Unreachable     Terminal Server Development
PEAR                Requesting      I like to print
TEST                Unknown         High-powered Performance Testing

Local>
```

Table 9–10 describes the nodes summary display.

Table 9–10: Node Summary Display Fields

Field	Description
Node Name	The name of the service node as defined in the server's node database.
Status	The current reachability status of the service node: <i>n</i> Connected The node is reachable and <i>n</i> sessions are currently active with services offered by the service node. Reachable No sessions are active, but the service node is accessible. Requesting A node that does not presently offer services has made remote connection requests to the server (for printer access or for local services offered). Unknown No sessions are active, and the node has not been heard from recently. Unreachable An active virtual circuit to the service node has timed out and the node is no longer multicasting service announcements. This status might indicate one of these conditions: the node is no longer attached to the Ethernet, the LAT software on the node has been stopped, or the node is no longer operational.
Identification	A brief description of the service and/or its application as defined by the service node's manager.

The following guideline applies to the node status and node summary displays:

- **Node Name**

Every service node name and server node name should be unique to allow other service nodes and users to distinguish among servers. A unique server node name is necessary for a server that is used for host-initiated requests or for a server to act as a service node.

Even though it is possible, Digital recommends against duplicating names for two service nodes. Because a server knows the Ethernet address of service nodes, it can accept connections from one service node with a name that is identical to the name of another known service node.

To distinguish two service nodes with identical names, the server replaces the second instance of a given name with the following name format:

`LAT_XXXXXXXXXXXX`

The value `XXXXXXXXXXXX` is the unhyphenated 12-digit Ethernet address of the second service node. The node summary displays use this replacement name.

9.4 Port Displays

The `SHOW/MONITOR PORT` commands display information about one, some, or all ports on the server. You can request characteristics, counter, status, and summary displays. With `LIST PORT`, you can specify characteristics and summary displays.

The `SHOW/MONITOR/LIST PORT CHARACTERISTICS` display shows the defined access type. The `SHOW/MONITOR PORT STATUS` display shows how the port is currently being used. The `SHOW/MONITOR PORT COUNTERS` display show the counters associated with each port you specify.

You can use the `SHOW PORT 0` commands to display information about port 0, the server's physical console port.

9.4.1 Port Characteristics Display

For each port you specify, the `SHOW/MONITOR/LIST PORT CHARACTERISTICS` commands display the values of its characteristics. Use the characteristics display before and after you change port values. This is the default display when you specify a single port.

Note that `LC-n-n` is the default port name. Figure 9–7 shows typical port characteristics displays.

Figure 9-7: Port Characteristics Display

```
Local> SHOW PORT 3 CHARACTERISTICS

Port 3:  Joe Smith                               Server:  PLANET

Character Size:      8                          Input Speed:      9600
Flow Control:       XON                         Output Speed:     9600
Parity:             None                       Modem Control:    Enabled

Access:             Local                       Local Switch:     None
Backward Switch:    None                       Name:            LC-1-3
Break:             Local                       Session Limit:    4
Forward Switch:     None                       Type:            ANSI

Preferred Service:  MODEM Node: OSLO  Destination: LTA15

Authorized Groups: 0-10, 20-50, 200-255
(Current) Groups:  0-10, 20-50, 200-255

Enabled Characteristics:

Autobaud, Broadcast, Lock, Multisessions, Verification

Local> SHOW PORT 19 CHARACTERISTICS

Port 19:  Nancy Ryan                             Server:  PLANET

Flow Control:       XON

Access:             Local                       Local Switch:     None
Backward Switch:    None                       Name:            LC-2-3
Break:             Local                       Session Limit:    4
Forward Switch:     None                       Type:            ANSI
Mode:              Dynamic                     Language:        French

Preferred Service:  PARIS Node: PARIS  Destination: LTA40

Authorized Groups: 0-10, 20-50, 200-255
(Current) Groups:  0-10, 20-50, 200-255

Enabled Characteristics:

Broadcast, Lock, Verification

Local>
```

The PORT 19 display is for a CXM04 port. The displayed information includes emulation mode and language, which are relevant only to the CXM04. This display excludes character size, parity, speed, and modem control because these characteristics are not applicable to the CXM04 port.

If you request a port characteristics display for PORT 0, the display does not include Authorized Groups and (Current) Groups. Port 0 is the console, or management, port and this information is not applicable. Port 0 effectively has the sum of all the groups of all the other ports, as displayed with the SHOW SERVER SUMMARY command.

The ALL option gives you a display of characteristics for all ports except the console. Table 9–11 describes the information displayed.

Table 9–11: Port Characteristics Display Fields

Field	Description
Port <i>n</i>	The number of the port.
User Name	In the server SHOW PORT display, this is the user name that the user entered at port login or the name of the port established for the port characteristic NAME, if no user name was supplied. In the TSC LIST PORT display, user name is the permanent user name you defined with the DEFINE PORT <i>n</i> USERNAME command; this user name cannot be cleared on the running server.
Character Size	The number of data bits in each character transmitted or received through the port. Possible character sizes are 7 or 8 bits.
Flow Control	The mechanism used to control data transfer on both input from the port to the server and output to the port from the server. Possible values are: <ul style="list-style-type: none"> CTS The server uses Clear To Send (CTS) and Request To Send (RTS) modem control signals. Disabled The server does not attempt or recognize any flow control mechanisms. DSR The server uses Data Terminal Ready (DTR) and Data Set Ready (DSR) modem signals. XON The server uses the ASCII characters XON (DC1) and XOFF (DC3).

Table 9–11 (Cont.): Port Characteristics Display Fields

Field	Description
Parity	<p>The mechanism by which the server checks for single-bit errors on received characters for the port. Possible values are:</p> <p>Even The server checks for an even number of bits per character.</p> <p>None The server does no checking.</p> <p>Odd The server checks for an odd number of bits per character.</p> <p>The server also includes the specified type of parity on transmitted characters.</p>
Input Speed	<p>The rate in bits per second at which the server processes characters input from the port device.</p>
Output Speed	<p>The rate in bits per second at which the server processes characters output to the port device.</p>
Modem Control	<p>Modem control is as follows:</p> <p>Disabled This setting disallows modem control. The device connected to the port uses limited EIA interface signals. Data can be exchanged between the device and the port, but no status can be exchanged. This mode is also known as data-leads-only mode.</p> <p>Enabled This setting enables modem control signal processing to establish and disable physical connections. The device connected to the port is a modem, host, or other device that manipulates the CCITT 100-series modem signals in a specific sequence.</p>
Access	<p>The current setting of the ACCESS port characteristic. Access determines how a port can access a service node or can be accessed by other interactive users and service nodes. Access is shown as one of the following:</p> <p>Local The server allows only interactive use of the port.</p> <p>Remote The server allows only remote connections to the port.</p> <p>Dynamic The server allows access to the port to alternate between local and remote.</p>

Table 9–11 (Cont.): Port Characteristics Display Fields

Field	Description
	None The server prevents any use of the port. You specify port access with the SET/DEFINE PORT ACCESS commands.
Backward Switch	The character defined to switch to the previous service session. Control characters are displayed with the ^ symbol preceding the key.
Break	The manner in which the server responds to the BREAK signal is shown as one of the following: Disabled The server ignores the BREAK signal. Local The server switches the port to local mode. Remote The server passes the BREAK signal to the connected service.
Forward Switch	The character defined to switch to the next service session. Control characters are displayed with the ^ symbol preceding the key.
Local Switch	The character defined to switch from a service session to local mode. Control characters are displayed with the _^ symbol preceding the key.
Name	The name of the port.
Session Limit	The maximum number of simultaneous sessions the port is allowed. If you issued SET/DEFINE PORT SESSION LIMIT NONE, the maximum value "8" is displayed.
Emulation Mode	The CXM04 port is defined for DYNAMIC operation. That is, a 3270 terminal on the port can operate in VT mode or 3270 mode. If the display indicates VT220 or 3270, the terminal is restricted to that mode.
Language	The language currently in use by a 3270 terminal user on a CXM04 port. The CXM04 firmware determines the language for each port when the server is initialized. The firmware also notifies the server each time the user switches to a new language.

Table 9–11 (Cont.): Port Characteristics Display Fields

Field	Description
Type	<p>The port type. This value determines the manner in which the server performs certain device-specific functions when the port is in local mode. Type is shown as one of the following:</p> <p>ANSI The attached device produces output on a video display and supports ANSI escape sequences (for example, a VT220).</p> <p>HARD The attached device produces output on paper (for example, an LA120 or a VT220).</p> <p>SOFT The attached device produces output on a video display that does not support ANSI escape sequences (for example, a VT52 or a VT220).</p>
Dedicated Service	<p>The port is set up to connect to this service when a user presses the RETURN key at port login. With the dedicated service, there can optionally be displayed an associated node or a node and a destination port. The port can also be configured to connect without keyboard intervention. The user cannot enter local mode commands.</p>
Preferred Service	<p>The port is set up to connect to this service when no service name is supplied with the CONNECT command. Moreover, when AUTOCONNECT is ENABLED, the server automatically connects to this service when someone logs in to the port. With the preferred service, there can optionally be displayed an associated node or a node and a destination. At any time, the user can enter local mode and issue server commands.</p>
Node	<p>The name of the node to which the server connects when there is either a preferred or dedicated service. The display provides this field if the keyword NODE was part of the SET/DEFINE PORT PREFERRED (or DEDICATED) command that defined the preferred (or dedicated) service.</p>
Destination	<p>The name of the port to which the server connects when there is either a preferred or dedicated service. The display provides this field if the keyword DESTINATION was part of the SET/DEFINE PORT PREFERRED (or DEDICATED) command that defined the preferred (or dedicated) service.</p>
Authorized Groups	<p>The list of groups that you set up to allow or restrict port access to various services on the network.</p>

Table 9–11 (Cont.): Port Characteristics Display Fields

Field	Description
(Current) Groups	This list might be identical to, or a subset of, Authorized Groups. The list of groups, from among the Authorized Groups, that the nonprivileged user has chosen to enable. Current Groups determine current access to services on the network for that user.
Enabled Characteristics	The port characteristics that are currently enabled.
Autobaud	At login, the server automatically detects speed, character size, and parity of the port device if that device's CHARACTER SIZE and PARITY characteristics are set to 8 and NONE or to 7 and EVEN.
Broadcast	The port can receive local broadcast messages.
Multisessions	A TD/SMP terminal on the port can run multiple terminal sessions.
Verification	The server displays a verification message when a session is started, terminated, or resumed on the port.

9.4.2 Port Counters Display

The `SHOW/MONITOR PORT COUNTERS` commands display the counters associated with each port you specify. Use `PORT COUNTERS` to discover the source of any problems between the port device and the port.

Figure 9–8 shows typical port counters displays. The `PORT 19` display is for a `CXM04` port. Refer to Tables 13 and 14 for a list of `CXM04` port numbers per card slots.

Figure 9–8: Port Counters Display

Local> SHOW PORT 1 COUNTERS

Port 1: Manager

Server: PLANET

Seconds Since Zeroed:	1182768	Local Accesses:	17
Framing Errors:	0	Remote Accesses:	0
Parity Errors:	0		
Overrun Errors:	0		

Local> SHOW PORTS 19 COUNTERS

Port 19: Bethany Corey

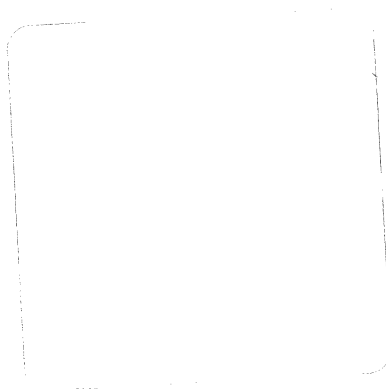
Device Counter	CCU Coax	3270 Mode Terminal Coax	VT Mode Terminal Coax
Receiver FIFO Overflow	0	0	0
Bad Receive Parity	0	0	0
Invalid Ending Sequence	0	0	0
Loss of Mid-Bit Transition	0	0	0
Receiver Disabled	0	0	0
No Response	0	0	0
No Poll Acknowledge	0	--	--
Bad Key	--	--	0
Device Check	--	--	0
Terminal Reconnect	--	0	0
State 1	--	0	0
State 2	--	0	0

Local>

Table 9–12 describes the port counters display.

Table 9–12: Port Counters Display Fields

Field	Description
Port <i>n</i>	The number of the port.
User Name	The user name the user entered at port login or, if no name was supplied, the name of the port specified by SET/DEFINE PORT NAME command.
Seconds Since Zeroed	The number of seconds since the counters for the port were last set to zero.
Framing Errors	The number of bytes received at the port with an invalid character size.
Parity Errors	The number of bytes received with parity errors at the port.
Overrun Errors	The number of characters lost because either the server software or hardware input buffers for the port were full.
Local Accesses	The number of times a server login occurred on the port.
Remote Accesses	The number of times a remote-access connection was established on the port.



For each of the counter fields, the maximum value possible is 4,294,967,295. If a counter reaches the maximum value, it remains at this value until either the counters are set to zero or the server is initialized.

The following guidelines apply to the port counters display:

- **Overflow Errors**

If this value accumulates to more than 10 daily on any one port, you might have flow control problems. The server supports three kinds of flow control:

- XON/XOFF characters
- CTS/RTS modem signals
- DSR/DTR modem signals

If the port device supports flow control, check that the server flow control and the flow control in the hardware for that device are set up in the same way.

To check the FLOW CONTROL setting, use the SHOW PORT CHARACTERISTICS command.

- **Framing Errors and Parity Errors**

If either of these values accumulates to greater than about 20 per day on any one port, you might have port line problems, such as cabling, noise, or modem errors. If the port is connected to a modem, these counters might be higher than about 200 per day due to line noise. See the discussion of troubleshooting in the *DECserver 500 Problem Solving* manual.

For port counter information that is displayed only for a CXM04 line card, refer to Tables 9–6 and 9–7. The card slot number in which the CXM04 line card is installed determines the port number of a terminal connected to the CXM04. Tables 13 and 14 list the port numbers.

Note

The following two tables are slightly different for the DECserver 510. Only columns LC1 and LC2 apply to the DECserver 510.

**Table 9–13: Port Numbering for a Server with CXM04 Line Cards
(Terminals Only) VT Mode — Configuration 8**

CXM04 Connectors	LC8	LC7	LC6	LC5	LC4	LC3	LC2	LC1
4 (Top)	116	100	84	68	52	36	20	4
8	120	104	88	72	56	40	24	8
3	115	99	83	67	51	35	19	3
7	119	103	87	71	55	39	23	7
2	114	98	82	66	50	34	18	2
6	118	102	86	70	54	38	22	6
1	113	97	81	65	49	33	17	1
5 (Bottom)	117	101	85	69	53	37	21	5

**Table 9–14: Port Numbering for a Server with CXM04 Line Cards
(CCU and Terminals) Configuration 4**

CXM04 Connectors	LC8	LC7	LC6	LC5	LC4	LC3	LC2	LC1
4 (Top) (Terminal)	116	100	84	68	52	36	20	4
8 (CCU)	116	100	84	68	52	36	20	4
3 (Terminal)	115	99	83	67	51	35	19	3
7 (CCU)	115	99	83	67	51	35	19	3
2 (Terminal)	114	98	82	66	50	34	18	2
6 (CCU)	114	98	82	66	50	34	18	2
1 (Terminal)	113	97	81	65	49	33	17	1
5 (Bottom) (CCU)	113	97	81	65	49	33	17	1

9.4.3 Port Status Display

The SHOW/MONITOR PORT STATUS commands display information about the operations of the ports you specify. The command displays additional information if you issue it at a privileged port. Figure 9–9 shows two typical port status displays. The PORT 19 display is for a CXM04 port.

Figure 9–9: Port Status Displays

```
Local> SHOW PORT 3 STATUS

Port 3: Artful dodger                Server: PLANET

Current Access: Remote                Current Service: TEST
Status: Connected                     Current Node: PEACH
Session Count: 1                      Current Port: LTA15

Input XOFFed: No                      Output Signals: DTR, RTS
Output XOFFed: No                     Input Signals: CTS, CD, DSR, RI
Controller LED: On

Local> SHOW PORT 19 STATUS

Port 19: Nancy Ryan                  Server: PLANET

Access: Local                         Current Service: TSD
Status: Connected                     Current Node: PARIS
Session Count: 1                      Current Port: LTA15

Current Emulation: VT                 Language: Default

Local>
```

Table 9–15 describes the information displayed by the SHOW/MONITOR PORT STATUS commands.

Table 9–15: Port Status Display Fields

Field	Description
Port <i>n</i>	The number of the port.
User Name	The user name the user entered at port login or, if no name was supplied, the name of the port specified by SET/DEFINE PORT NAME command.
Current Access	<p>The way the port is currently accessing a service node or is being accessed by other interactive users and service nodes. Possible values are:</p> <p>Local The server allows only interactive use of the port.</p> <p>Remote The server allows only remote connections to the port.</p> <p>Dynamic The server allows access on the port to alternate between local and remote.</p> <p>None The server prevents any use of the port.</p> <p>You specify port access with the SET/DEFINE PORT ACCESS commands.</p>
Status	<p>The current status of the port:</p> <p>Connected The port is currently connected to a service, if Current Access is Local. If Current Access is Remote, the port currently has an active remote session.</p> <p>Connecting A session is currently being established either to or from the port, depending on the current access.</p> <p>Disconnected A session was terminated while dormant.</p> <p>Disconnecting A session is currently being disconnected on the port.</p> <p>Idle The port is not in use.</p> <p>Local mode The port is logged in to the server.</p> <p>Locked A LOCK command was executed on the port.</p> <p>Logging in The Enter username> prompt is displayed and the port is waiting for the user to successfully enter his or her user name.</p>
Session Count	The number of active sessions at the port.

Table 9–15 (Cont.): Port Status Display Fields

Field	Description
Current Service	The name of the service specified when the user created the current session. On remote-access ports offering one or more services, "Current Service" indicates the particular service to which the server made the remote connection.
Current Node	The service node to which the current session is connected. If the access is remote, this is the name of the node from which the connection originated.
Current Port	The identification of the port at the other end of the current session.
Input XOFFed	The server told the port device to hold temporarily the data it is trying to send.
Output XOFFed	The port device told the server to hold temporarily the data it is trying to send.
Output Signals	If there is modem control, this is the list of modem signals that the server asserts to the port device. DTR Data Terminal Ready RTS Request to Send
Input Signals	If there is modem control, this is the list of modem signals that the server receives from the port device. CTS Clear to Send DSR Data Set Ready CD Signal Carrier Detect RI Ring Indicator
Current Emulation	The operating environment to which a CXM04 port is currently connected. The 3270 terminal can be connected to the Digital environment (VT220) or to the IBM environment (3270).

The following guidelines apply to the port status display:

- **Current Port**

If the **Current Access** field is **Local**, this field is the identification of the port on the **Current Node** that is being accessed for the **Current Service**.

If the **Current Access** field is **Remote**, this field is the identification of the requesting port on the **Current Node**. However, this identification is displayed only if the other node provides the information.

- **Current Service**

On remote-access ports offering one or more services, the **Current Service** field indicates the particular service to which the server made the remote connection. However, this identification is displayed only if the other node provides the information.

- **Current Access**

“**Current Access**” is the most useful field for you to determine the currently used mode of a dynamic-access port.

9.4.4 Port Summary Display

The **SHOW/MONITOR/LIST PORT SUMMARY** commands display one line of general information for the port you specify. Use the port summary display for information about how ports are being used. **SUMMARY** is the default display with the **ALL** option.

Figure 9–10 illustrates a typical **SHOW PORT SUMMARY** display.

Figure 9–10: Port Summary Display with Server SHOW Command

```
Local> SHOW PORTS ALL SUMMARY

Port      Access   Status      Local Services
-----
1         Local   Connected
2         Remote  Connected   LA50, PRINTER
3         Dynamic Idle        HARDCOPY
4         Local   Local mode
5         Remote  Connected   LA50, PRINTER
6         Local   Connecting
7         Local   Disconnected
8         Local   Idle
9         Local   Connected
.
.
.
128      Local   Offline

Local>
```

Figure 9–11 illustrates a typical LIST PORT SUMMARY display.

Figure 9–11: Port Summary Display with TSC LIST Command

```
TSC> LIST PORT 4 SUMMARY

Port      Access   Services offered
-----
4         Local   TIMESHARING

TSC>
```

Table 9–16 describes the port summary display.

Table 9–16: Port Summary Display Fields

Field	Description
Port	The number of the port.
Access	<p>The current setting of the ACCESS port characteristic. Access determines how a port can access a service node or can be accessed by other interactive users and service nodes. Access is shown as one of the following:</p> <p>Local The server allows only interactive use of the port.</p> <p>Remote The server allows only remote connections to the port.</p> <p>Dynamic The server allows access to the port to alternate between local and remote.</p> <p>None The server prevents any use of the port.</p> <p>You specify port access with the SET/DEFINE PORT ACCESS commands.</p>
Status	<p>The current status of the port:</p> <p>Connected The port is currently connected to a service if Current Access is Local. If Current Access is Remote, the port currently has an active remote session.</p> <p>Connecting A session is currently being established either to or from the port, depending on the current access.</p> <p>Disconnected A session was terminated while dormant.</p> <p>Disconnecting A session is currently being disconnected on the port.</p> <p>Idle The port is not in use.</p> <p>Local Mode The port is logged in to the server.</p> <p>Locked A LOCK command was executed on the port.</p> <p>Logging in A user is currently logging in to the port.</p> <p>Offline The port is on a controller that is missing or does not exist.</p>
Local Services	The local services that the server offers on the port. Remote-connection requests can be made for these services.

9.5 Queue Display

The SHOW/MONITOR QUEUE commands display the requests in the server queue. Figure 9–12 shows a typical server queue display.

Figure 9–12: Queue Display

```
Local> SHOW QUEUE ALL
```

Position	Entry	Source Node	Service	Port Name
1	128	ORANGE	TIMESHARING	4 LN03
2	130	BANANA		48 (LC3-16)
3	131	PEACH	TEST	

```
Local>
```

Table 9–17 describes the queue display.

Table 9–17: Queue Display Fields

Field	Description
Position	The current placement of each entry, indicating the relative order of the entry in the queue.
Entry	The entry number of the queued request.
Source Node	The name of the service node that made the host-initiated request.
Service	The name of the requested service, if any.
Port Name	The port number followed by the port name. If a port name was not specified in the request, this column is blank.

The following guidelines apply to the queue display:

- The server connection queue is a first-in-first-out (FIFO) queue. Each remote-connection request in the server queue has a queue position and an entry number.

The entry number is assigned by the server when the request is queued and is internal to the server. Entry numbers are from 1 to the value set as the upper limit set with SET/DEFINE SERVER QUEUE LIMIT. Although entries are processed in FIFO order, an entry can be dequeued ahead of other entries with lower position numbers, depending on port availability.

- You can monitor an entry's status relative to other queue entries with the `SHOW QUEUE` command. Queuing is allowed to one of these: the port, the service, or both. `SHOW QUEUE` lists the entries in FIFO order.
- Use the `SHOW QUEUE` display to do the following:
 - Determine the current size of the queue. You might want to adjust the queue size by altering the server characteristic `QUEUE LIMIT`.
 - Examine information about any or all of the queued host-initiated requests.
 - Estimate how deleting entries with the `REMOVE QUEUE` command will affect queue positions.
 - Monitor the frequency of requests for connections to specific printers or applications devices.
- The `MONITOR QUEUE` command generates a display that changes on your screen as remote-connection requests are queued and dequeued.

9.6 Server Displays

The `SHOW/MONITOR/LIST SERVER` commands display information about the server. `SHOW` and `MONITOR` display information from the operational database. `LIST` displays information from the permanent database.

With the `SHOW` and `MONITOR SERVER` commands, you can request characteristics, counters, status, and summary displays for the server. With `LIST SERVER`, characteristics and summary displays are available. `CHARACTERISTICS` is the default with `SHOW/MONITOR/LIST`.

9.6.1 Server Characteristics Display

The `SHOW/MONITOR/LIST SERVER CHARACTERISTICS` commands display the values of the server's characteristics. Use this display when you are defining server characteristics.

Figure 9–13 shows a typical display with the SHOW SERVER CHARACTERISTICS command. Note that the fields showing operating information do not appear on the display generated with the LIST SERVER CHARACTERISTICS command. These fields are: ROM, Uptime, and Address.

The values displayed are the current values. Either these values are the defaults, or they are values you specified with SET/DEFINE SERVER commands.

Figure 9–13: Server Characteristics Display

```
Local> SHOW SERVER CHARACTERISTICS

DECserver 500 V2.0          LAT V5.1          ROM V2.0.0      Uptime: 13 16:36:23
Address:  08-00-2B-02-F2-BB  Name: TIGER      Number: 6

Identification: Number 6 Forward and Reverse LAT Server

Circuit Timer:             80          Password Limit:   3
Inactivity Timer:          30          Prompt:          Local>
Keepalive Timer:           20          Queue Limit:     8
Multicast Timer:           60          Retransmit Limit: 10
Node Limit:                100         Session Limit:   256

Service Groups: 10-20,30-50,100-255

Backup Hosts: TOPCAT

Enabled Characteristics:

Announcements, Broadcast, Lock

Local>
```

Table 9–18 describes the server characteristics display.

Table 9–18: Server Characteristics Display Fields

Field	Description
DECserver 500 V2.0	The product designation (DECserver 500 server) and the version (2.0) of the server software now running.
LAT V5.1	The version number and update level of the LAT protocol that the server software implements.
ROM V2.0.0	The version number of the firmware (read-only memory).
Uptime	The time the server has been running since the last initialization. The time is expressed in the following format: days hours.minutes.seconds
Address	The Ethernet address of the server.
Name	The name of the server as defined with the SET/DEFINE SERVER NAME command. The default, which you normally should not change, is the server's DECnet node name. Note that the LIST SERVER display does not include the name unless you explicitly issued DEFINE SERVER NAME, even though the default is in effect.
Number	The number of the server as defined with the SET/DEFINE SERVER NUMBER command.
Identification	A character string that describes the server. The server supplies this identification when it multicasts service node announcement messages. You define this string with the SET/DEFINE SERVER IDENTIFICATION command.
Circuit Timer	The current setting for the number of milliseconds between transmissions of messages to service nodes (range: 10 to 200 milliseconds).
Inactivity Timer	The current setting for the number of minutes that a port with INACTIVITY LOGOUT ENABLED can remain logged in without any sessions (range: 1 to 120 minutes).
Keepalive Timer	The current setting for the number of seconds between transmissions of circuit verification messages when there is no data to send (range: 10 to 180 seconds).
Multicast Timer	The current setting for the number of seconds between multicast messages that announce existing local services (range: 10 to 180 seconds).
Node Limit	The current setting for the maximum number of nodes for which the server can maintain node information (range: 1 to 200). Note that you cannot decrease this value on the running server.

Table 9–18 (Cont.): Server Characteristics Display Fields

Field	Description
Password Limit	The current setting for the maximum number of times that the server allows a user to incorrectly enter the log-in, privileged, or service passwords (range: 1 to 32).
Prompt	The default setting for the local mode prompt. You can change the prompt to any ASCII text string (range: 1 to 16 characters).
Queue Limit	The current setting for the maximum number of entries allowed in the server queue of host-initiated requests (range: 0 to 32). A value of 0 disables queuing for the whole server.
Retransmit Limit	The current setting for the maximum number of times the server tries to retransmit a message that has not been acknowledged by a service node (range: 4 to 120).
Session Limit	The current setting for the maximum number of total simultaneous sessions the server allows (range: 0 to 512).
Service Groups	The set of groups assigned to all services that the server offers.
Backup Hosts	The DECnet node names of one to five backup load hosts for down-line loading with the server INITIALIZE command and for up-line dumping. If the primary load host fails to respond to the down-line load or up-line dump request, the server tries the backup load hosts in the order you specified with the DEFINE SERVER BACKUP HOSTS command.
Enabled Characteristics	<p>The server characteristics currently enabled. The following are the server characteristics that you can enable or disable and their effect when they are enabled:</p> <p>Announcements The server multicasts announcements of local services.</p> <p>Broadcast The server allows users to execute the BROADCAST command.</p> <p>Heartbeat The server reports any hardware collision-detection circuitry errors when it sends messages on the Ethernet.</p> <p>Lock The server allows users to execute the LOCK command.</p> <p>Line frequency Even though this is not a server characteristic that you enable or disable, the current value of the line frequency in the permanent database (either 50 Hz or 60 Hz) always appears in this part of the display generated by the LIST SERVER CHARACTERISTICS command.</p>

The following guideline applies to the Node Limit field of the server characteristics display:

If more service nodes appear on the network than can be held in the server database, the overflow node information is discarded. To see whether any nodes have been discarded, use the `SHOW SERVER STATUS` command and observe the “Discarded Nodes” counter.

This counter is incremented only if the server discards a node that has groups in common with the server. Therefore, you can control the amount of overflow by limiting `AUTHORIZED GROUPS` (see Section 5.3).

9.6.2 Server Counters Display

The `SHOW/MONITOR SERVER COUNTERS` commands display the current values for the global counters —Ethernet datalink and LAT protocol — maintained by the server. The counters display is useful for detecting possible network problems.

Counters can help you estimate server traffic on the network for specific time periods. For example, if you zero the counters at the start of each day, you can gain information about daily server use.

Figure 9–14 shows a typical server counters display.

Figure 9–14: Server Counters Display

```
Local> SHOW SERVER COUNTERS

DECserver 500 V2.0          LAT V5.1          ROM V2.0.0  Uptime: 13 16:50:34

Seconds Since Zeroed:      1183161  Frames Sent, 1 Collision:      8377
Bytes Received:            811416880  Frames Sent, 2+ Collisions:    16344
Bytes Sent:                141519043  Send Failures:                 1
Frames Received:          8087172   Send Failure Reasons:         000010
Frames Sent:              1572199   Receive Failures:              47
Multicast Bytes Rcv'd:    1111005   Receive Failure Reasons:       000011
Multicast Bytes Sent:     215694    Unrecognized Destination:     193760
Multicast Frames Rcv'd:   66700    Data Overrun:                  0
Multicast Frames Sent:    2179     User Buffer Unavailable:        0
Frames Sent, Deferred:    96516    System Buffer Unavailable:      0

Messages Received:        1886375  Duplicates Received:           106
Messages Transmitted:     1569667  Messages Re-transmitted:       485
Solicited Msgs Accepted:  0      Illegal Messages Received:     6
Solicited Msgs Rejected:  0      Illegal Slots Received:        0
Multiple Node Addresses:  23591  Illegal Multicasts Rcv'd:      1

Local>
```

Table 9–19 describes the server counters display. The COUNTERS data appears in two blocks:

- Ethernet data link counters

The upper block is for datagrams sent between the server and all nodes on the Ethernet network. Some of the fields displayed are bit masks, the values of which tell the reasons for certain events.

- LAT protocol counters

The lower block is for messages exchanged between the server and all LAT service nodes. You can use these counters to estimate the percentage of the server's Ethernet activity that is for LAT protocol messages.

All the counters have a maximum value of 4,294,967,295. If a counter reaches the maximum, it remains at that value until either you set the counters to zero or the server is initialized.

Table 9–19: Server Counters Display Fields

Field	Description
DECserver 500 V2.0	The product designation (DECserver 500 server) and the version (2.0) of the server software now running.
LAT V5.1	The version number and update level (5.1) of the LAT protocol that the server software implements.
ROM V2.0.0	The version number of the firmware (read-only memory).
Uptime	The time the server has been running since the last down-line load. The time is expressed in the following format: days hours.minutes.seconds
Seconds Since Zeroed	The number of seconds since the counters were last set to zero.
Bytes Received	The number of bytes contained in datagrams successfully received by the server, excluding Ethernet header and CRC data.
Bytes Sent	The number of bytes contained in datagrams successfully transmitted by the server, excluding Ethernet header and CRC data.
Frames Received	The number of datagram frames successfully received by the server, including multicast frames.
Frames Sent	The number of datagram frames successfully transmitted by the server, including multicast frames.
Multicast Bytes Rev'd	The number of bytes received by the server in multicast frames, excluding Ethernet header and CRC data.
Multicast Bytes Sent	The number of bytes transmitted by the server in multicast frames, excluding Ethernet header and CRC data.
Multicast Frames Rev'd	The number of multicast frames received by the server.
Multicast Frames Sent	The number of multicast frames sent by the server.
Frames Sent, Deferred	The number of times the server deferred a frame transmission because the data link was in use.
Frames Sent, 1 Collision	The number of times the server successfully transmitted a frame on the second attempt after a collision during the first attempt.
Frames Sent, 2+ Collisions	The number of times the server successfully sent a frame after collisions during the first two or more attempts.

Table 9–19 (Cont.): Server Counters Display Fields

Field	Description																		
Send Failures	The number of times the Ethernet interface aborted a transmission request. If this count is nonzero, see the Send Failure Reasons mask for more information.																		
Send Failure Reasons	<p>A mask providing information about the type of send failure encountered if the Send Failures counter is not zero. Note that this is a cumulative mask. The bits are numbered from right to left, with Bit 0 as the rightmost bit. The following are the bits defined in the mask:</p> <table border="1"> <thead> <tr> <th>Bit</th> <th>Definition</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>A transmission failed to complete after 16 retries, usually due to excessive collisions.</td> </tr> <tr> <td>1</td> <td>A loss of carrier on the Ethernet during a transmission.</td> </tr> <tr> <td>2</td> <td>A short circuit on the Ethernet during a transmission.</td> </tr> <tr> <td>3</td> <td>An open circuit on the Ethernet during a transmission.</td> </tr> <tr> <td>4</td> <td>A transmission aborted because the frame (packet) exceeded the maximum length allowed.</td> </tr> <tr> <td>5</td> <td>A late collision on a transmission attempt.</td> </tr> <tr> <td>8</td> <td>Heartbeat error. This error can occur only when the server heartbeat characteristic is ENABLED.</td> </tr> <tr> <td>9</td> <td>Data underflow.</td> </tr> </tbody> </table>	Bit	Definition	0	A transmission failed to complete after 16 retries, usually due to excessive collisions.	1	A loss of carrier on the Ethernet during a transmission.	2	A short circuit on the Ethernet during a transmission.	3	An open circuit on the Ethernet during a transmission.	4	A transmission aborted because the frame (packet) exceeded the maximum length allowed.	5	A late collision on a transmission attempt.	8	Heartbeat error. This error can occur only when the server heartbeat characteristic is ENABLED.	9	Data underflow.
Bit	Definition																		
0	A transmission failed to complete after 16 retries, usually due to excessive collisions.																		
1	A loss of carrier on the Ethernet during a transmission.																		
2	A short circuit on the Ethernet during a transmission.																		
3	An open circuit on the Ethernet during a transmission.																		
4	A transmission aborted because the frame (packet) exceeded the maximum length allowed.																		
5	A late collision on a transmission attempt.																		
8	Heartbeat error. This error can occur only when the server heartbeat characteristic is ENABLED.																		
9	Data underflow.																		
Receive Failures	The number of packets that were received with an error condition. For more information, see the Receive Failure Reasons field.																		

Table 9–19 (Cont.): Server Counters Display Fields

Field	Description								
Receive Failure Reasons	<p>A mask providing information about the type of receive failure encountered if the Receive Failures counter is not zero. Note that this is a cumulative mask. The bits are numbered from right to left, with Bit 0 as the rightmost bit. The following are the bits defined in the mask:</p> <table border="1"><thead><tr><th>Bit</th><th>Definition</th></tr></thead><tbody><tr><td>0</td><td>A block check error. The received packet did not pass the CRC check.</td></tr><tr><td>1</td><td>A framing error. The received packet did not contain an integral number of 8-bit bytes.</td></tr><tr><td>2</td><td>A message length error. The received packet exceeded 1518 bytes.</td></tr></tbody></table>	Bit	Definition	0	A block check error. The received packet did not pass the CRC check.	1	A framing error. The received packet did not contain an integral number of 8-bit bytes.	2	A message length error. The received packet exceeded 1518 bytes.
Bit	Definition								
0	A block check error. The received packet did not pass the CRC check.								
1	A framing error. The received packet did not contain an integral number of 8-bit bytes.								
2	A message length error. The received packet exceeded 1518 bytes.								
Unrecognized Destination	The number of times a frame was received, but the server did not recognize the multicast address or protocol type and discarded the message.								
Data Overrun	The number of times the DECserver 500 hardware lost an incoming frame because it was unable to keep up with the data rate.								
User Buffer Unavailable	The number of times the server did not have a user (or port) buffer available to copy data from a system buffer.								
System Buffer Unavailable	The number of times a system buffer was not available in the server for an incoming frame.								
Messages Received	The number of LAT circuit messages successfully received by the server.								
Messages Transmitted	The number of LAT circuit messages successfully transmitted by the server.								
Solicited Msgs Accepted	The number of host-initiated requests that the server has accepted. This number includes requests that are queued and requests that were immediately satisfied without queuing.								
Solicited Msgs Rejected	The number of host-initiated requests that the server could not process and therefore rejected.								
Multiple Node Addresses	The number of times a service node became available with different Ethernet addresses.								
Duplicates Received	The number of times that the server received consecutive messages on a LAT virtual circuit, and the messages had the same sequence number.								

Table 9–19 (Cont.): Server Counters Display Fields

Field	Description
Messages Retransmitted	The number of LAT messages that the server retransmitted because they were not acknowledged by the service nodes.
Illegal Messages Received	The number of LAT messages with an illegal format received by the server.
Illegal Slots Received	The number of LAT messages with an illegal slot format received by the server.
Illegal Multicasts Rcv'd	The number of illegally formatted multicast messages received from service nodes.

The following guidelines apply to the server counters display:

- Ethernet data link counters

- Frames Sent, Deferred

This value should be less than 20% of the value for Frames Sent. A higher value indicates excessive Ethernet traffic.

- Frames Sent, 1 Collision and Frames Sent, 2+ Collisions

These values should be less than 5% of the value for Frames Sent. A higher value indicates excessive Ethernet traffic.

- Send Failures and Receive Failures

These counters should be 0, or a very low value such as 1 or 2 daily.

If a reason for send failures is heartbeat errors and the server characteristic HEARTBEAT is enabled for a transceiver that supports heartbeat, you can usually expect up to about 200 such errors daily. This does not indicate a network problem.

If a reason for send failures is heartbeat errors and the transceiver being used does not support heartbeat, check to see whether you have HEARTBEAT ENABLED. The send failures count reflects the heartbeat errors generated from the transceiver not responding to checks of its heartbeat circuitry.

Disable the server characteristic HEARTBEAT to eliminate the reporting of heartbeat errors.

- **Unrecognized Destination**

This value reflects the amount of message traffic — both multicast and directly addressed — being received by the server that does not relate to either the LAT or MOP protocols.

A value here might indicate a software problem with one of the other nodes on the Ethernet or a hardware problem somewhere on the Ethernet. If this count is extremely high (greater than 10 for each second of uptime), the server performance might be adversely effected.

- **Data Overrun**

This value should be 0. A nonzero value might indicate a hardware problem on the Ethernet or with the server's Ethernet hardware.

- **User Buffer Unavailable and System Buffer Unavailable**

These counters should accumulate at a rate of fewer than two counts per day. It is normal to experience some errors when nodes are added to the Ethernet.

- **LAT protocol counters**

The server maintains some of these counters for each service node with which it communicates. See the node counters display descriptions and guidelines. These are totals for all nodes.

- **Solicited Msgs Accepted and Solicited Msgs Rejected**

The sum of the number of solicited messages accepted and the number of solicited messages rejected equals the number of host-initiated requests that were received by the server.

- **Duplicates Received**

This value should be less than 1/1000 of the value for Messages Received.

- **Messages Retransmitted**

This value should be less than 1/1000 of the value for Messages Transmitted.

- **Illegal Messages Received, Illegal Slots Received, and Illegal Multicasts Rcv'd**

These values should be 0. A service node transmitting such messages might have a software problem.

9.6.3 Server Status Display

The SHOW/MONITOR SERVER STATUS commands display the current status of the server. The information tells you how well the server is working under the current load. The display also warns you of network trouble or of problems with ports on the server.

Figure 9–15 shows a typical server status display.

Figure 9–15: Server Status Display

```
Local> SHOW SERVER STATUS

DECserver 500 V2.0          LAT V5.1      ROM V2.0.0   Uptime: 13 16:50:43
Address:  08-00-2B-02-F2-BB  Name: TIGER   Number: 6

                Cur   High   Max
Active Ports:   8     8     129  Minutes to Shutdown: 0
Active Users:   8     8     129  Discarded Nodes:     0
Queue Entries:  0     0     8    Resource Errors:     0

Available Services: 89   92   N/A  Port Framing Errors: 0
Local Services:    2     2   255  Port Parity Errors:  0
Reachable Nodes:  75   78   100  Port Overrun Errors: 0

Active Circuits:   4     7    64   Primary Host:        PEACH
Connected Nodes:   4     7    64   Load Address: AA-00-04-00-46-DC
Connected Sessions: 12    20   32   Dump Address: AA-00-04-00-46-DC
% CPU Used:        15    36   100
% Memory Used:     53    56   100

Local>
```

Tables 9–20 and 9–21 describe the server status display:

- Table 9–20 describes:
 - The basic server identification information on the left-hand side of the display
 - The error summaries on the right-hand side of the display

- The server maintenance information on the right-hand side of the display
- Table 9–21 describes the software and hardware resources whose current, highest, and maximum values are displayed on the left-hand side of the display.

Table 9–20: Server Status: Error Display Fields

Field	Description
DECserver 500 V2.0	The product designation (DECserver 500 server) and the version (2.0) of the server software now running.
LAT V5.1	The version number and update level (5.1) of the LAT protocol that the server software implements.
ROM V2.0.0	The version number of the firmware (read-only memory).
Uptime	The time the server has been running since the last server initialization. The time is expressed in the following format: <i>days:hours:minutes:seconds</i>
Address	The Ethernet address of the server.
Name	The name of the server as defined with the SET/DEFINE SERVER NAME command. The default, which you normally should not change, is the server's DECnet node name. Note that the LIST SERVER display does not include the server's name unless you explicitly issued DEFINE SERVER NAME, even though the default is in effect.
Number	The number of the server as defined with the SET/DEFINE SERVER NUMBER command.
Minutes to Shutdown	The number of minutes remaining on the initialize timer. If no INITIALIZE command is in effect, 0 is displayed to indicate "not applicable."
Discarded Nodes	The number of times that a node with matching groups could not be entered into the server database because of the value set for the NODE LIMIT characteristic or because of a lack of available memory.
Resource Errors	The number of times an internal data structure could not be created due to the lack of system memory.
Port Framing Errors	The sum of bytes received at the server ports with illegal character sizes.

Table 9–20 (Cont.): Server Status: Error Display Fields

Field	Description
Port Parity Errors	The sum of bytes received at the server ports with parity errors.
Port Overrun Errors	The sum of characters lost at the server ports because the server input buffers were full.
Primary Host	The name of the load host designated as the primary load host. This is the load host to which the server first sends its request for a down-line load (with the server INITIALIZE command) or for an up-line dump. The Primary Host is normally equivalent to the name of the node from which the server was last loaded.
Load Address	The Ethernet address of the node from which the server was last loaded.
Dump Address	The Ethernet address of the node that received the last up-line dump.

Table 9–21: Server Status: Resource Display Fields

Field	Description
Cur	The current running value of the resource. If the Max value is lowered because you limit the resource while the server is running with SET commands, this value can exceed the Max value for certain counters.
High	The highest value the resource attained since the server was last initialized. The length of time is shown in the Uptime field. If the Max value is lowered because you limit the resource while the server is running with SET commands, this value can exceed the Max value for certain counters.
Max	The maximum value that the resource can reach, given the physical constraints or the value you specified for a server characteristic.
Active Ports	The number of ports that have either interactive sessions or remote-access connections. Includes port 0.
Active Users	The number of users currently logged in to the server. Includes the port 0 user, who should be you.
Queue Entries	The number of host-initiated requests that are in the server queue of connection requests.

Table 9–21 (Cont.): Server Status: Resource Display Fields

Field	Description
Available Services	The number of network services that the server recognizes as being available to users on the server. (Information about these services is stored in server memory.)
Local	The number of services that the server offers locally. Services
Reachable Nodes	The number of service nodes that offer services on the network and that are reachable for service connections.
Active Circuits	The number of LAT virtual circuits that the server is currently maintaining.
Connected Nodes	The number of service nodes with which the server has established LAT virtual circuits.
Connected Sessions	The total number of LAT sessions currently being maintained by the server.
% CPU Used	The percentage of available processing time the server used. This value is calculated every time the circuit timer expires.
% Memory Used	The percentage of memory pool being used for the node and the service database, queued requests, service sessions, and virtual circuits.

The following guidelines apply to the server status display:

- All the error fields

The values for the error fields should be 0. Error fields with values other than 0 might indicate a problem. A hardware error produces nonzero values.

- Discarded Nodes

The server might be experiencing resource problems if this count is not zero.

The memory used for storing service and node information is shared with the memory used for handling multiple sessions and queued host-initiated requests.

If the server receives multicast information on a greater number of nodes than specified for the `NODE LIMIT` server characteristic, the server discards that information and increments the Discarded Nodes counter. However, if the Node Limit is not reached but the server could not find memory to store the information, the server discards the information and increments both the Resource Errors and the Discarded Nodes counter.

You can either reduce the value of the SESSION LIMIT server characteristic, adjust the value of the NODE LIMIT server characteristic, or use Authorized Groups to logically subdivide the network for use by a discrete set of users. If this count is not zero, you might want to increase the node limit.

- % CPU Used

The “% CPU Used” field shows the utilization of the server’s CPU. If the “Cur” (Current) column of this field shows that the server’s CPU is more than 75% utilized, the server stops processing service announcement multicast messages until the CPU becomes less than 75% utilized.

If the CPU is more than 75% utilized for a long time, eventually the SHOW NODES display shows that some of the nodes have a status of “Unknown,” instead of “Reachable.” You can still connect to those nodes, and when the CPU becomes less than 75% utilized, the server starts listening to multicast service announcements again and updates each node’s status to “Reachable” as its announcements come in.

- Port Errors

Values other than 0 for port errors might indicate a problem with one of the ports. If a modem is connected to the port, framing and parity errors caused by line noise are common. This does not indicate a problem with the server.

Use the port counters display to isolate the port or ports generating the errors accumulated in these counters.

9.6.4 Server Summary Display

The SHOW/MONITOR/LIST SERVER SUMMARY commands display server identification information and all the authorized groups you assigned to each port.

Use this display to determine which groups the server recognizes when it processes service announcement messages from other nodes on the network. These groups, called “Server Groups” in the display, are the sum of all the authorized groups of all the ports.

Figure 9–16 shows a typical SHOW SERVER SUMMARY display.

Figure 9–16: Server Summary Display with Server SHOW Command

```
Local> SHOW SERVER SUMMARY

DECserver 500 V2.0          LAT V5.1      ROM V2.0.0    Uptime: 13 16:53:12
Address:  08-00-2B-02-F2-BB  Name: TIGER   Number: 6
Identification: Number 6 Forward and Reverse LAT Server
Server Groups: 0,4,10-20

Local>
```

Figure 9–17 shows a typical LIST SERVER SUMMARY display.

Figure 9–17: Summary Display with TSC LIST Command

```
TSC> LIST SERVER SUMMARY

DECserver 500 V2.0          LAT V5.1
Name: TIGER                 Number: 6
Identification: Number 6 Forward and Reverse LAT Server
Server Groups: 0,4,10-20

TSC>
```

Table 9–22 describes the server summary display.

Table 9–22: Server Summary Display Fields

Field	Description
DECserver 500 V2.0	The product designation (DECserver 500 server) and the version (2.0) of the server software now running.
LAT V5.1	The version number and update level (5.1) of the LAT protocol that the server software implements.
ROM V2.0.0	The version number of the firmware (read-only memory).
Uptime	The time the server has been running since the last server initialization. The time is expressed in the following format: <i>days:hours:minutes:seconds</i>
Address	The Ethernet address of the server.
Name	The name of the server as defined with the SET/DEFINE SERVER NAME command. The default, which you normally should not change, is the server's DECnet node name. Note that the LIST SERVER display does not include the server's name unless you explicitly issued DEFINE SERVER NAME, even though the default is in effect.
Number	The number of the server as defined with the SET/DEFINE SERVER NUMBER command.
Identification	A character string that describes the server. The server supplies this identification when it multicasts service node announcement messages. You define this string with the SET/DEFINE SERVER IDENTIFICATION command.
Server Groups	A list of assigned groups on the server. The server uses this information to filter incoming multicast messages from other nodes. The list of Server Groups is the sum of all the authorized groups, except for the console port. Users can connect only to services with at least one of these groups enabled.

9.7 Service Displays

The SHOW/MONITOR/LIST SERVICES commands display information about services to which you can connect. The LIST command displays information about local services. SHOW and MONITOR display information about all the services that are currently available in the operational database.

With SHOW and MONITOR you can request characteristics, status, and summary displays. With the LIST command, there are no status displays.

9.7.1 Service Characteristics Display

The `SHOW/MONITOR/LIST SERVICE CHARACTERISTICS` commands display values that you can modify with the `SET/DEFINE SERVICE` commands. With the `LIST` command, the characteristics display is the default display for the `SERVICE` and the `SERVICE LOCAL` entity specifications.

Figure 9–18 shows two typical service characteristics displays. One shows the characteristics for the local service named `REVERSE`, and the other shows the characteristics for a service named `TEST`, offered by another service node on the network.

Figure 9–18: Service Characteristics Display for a Service Offered by the Server and for a Service Offered by Another Service Node

```
Local> SHOW SERVICE REVERSE CHARACTERISTICS

Service: REVERSE

Identification: Reverse Ports to PEACH

Ports: 1-3,5,7

Rating: 255

Enabled Characteristics:

Connections, Password, Queue

Local> SHOW SERVICE TEST CHARACTERISTICS

Service: TEST

Identification: High-powered Performance Testing

Local>
```

Table 9–23 describes the service characteristics display.

Table 9–23: Service Characteristics Display Fields

Field	Description
Service	The name that identifies the network service.
Identification	The service identification string. This string is usually a short description of the service or of how to use it.
The following fields are displayed only for services offered by the server (local services).	
Ports	The numbers of the ports at which the local service is offered.
Rating	The rating at which the server offers this service. The value is 255 minus the number of ports in use offering the service. If there are no available ports, the rating is 0.
Enabled Characteristics	The following are the characteristics that can be enabled with the SET/DEFINE SERVICE commands. See Chapter 3 or type HELP SET/DEFINE SERVICE for descriptions of these characteristics. The server displays only those characteristics that are enabled for local services.
Connections	The server allows connections to this service.
Password	The server requires the requester of the service to supply a password before access to this service is allowed.
Queue	The server places host-initiated requests for this service in a queue if the request cannot be immediately satisfied.

9.7.2 Service Status Display

The SHOW/MONITOR SERVICE STATUS commands display information about the operational condition of the network and its services, including services offered by your server. The display includes a list of the nodes that offer the selected service or services.

Use the keyword LOCAL to restrict the information displayed to locally defined services. Without the LOCAL keyword or a particular service name, you get information about all network services, including local services.

The STATUS display is the default SHOW/MONITOR/LIST SERVICE display.

Figure 9–19 shows a typical service status display.

Figure 9–19: Service Status Display

```
Local> SHOW SERVICE DEVELOP STATUS

Service: DEVELOP          -      Available

Node Name                Status   Rating  Identification
-----
ORANGE                   Reachable  27     RSX-11M-PLUS Development System
PEACH                    Unreachable 255    Terminal Server Development System
TEST                     Unknown    150    High-powered Performance Testing

Local>
```

The display's first line identifies the service. Under the column headings, a line is displayed for each node offering that service. Table 9–24 describes the display fields.

Table 9–24: Service Status Display Fields

Field	Description
Service	The name that identifies the network service and its availability, either "Available" or "Unavailable."
Node Name	The name of the service node as stored in server memory for each node that offers the service.
Status	The current accessibility of the service node: <i>n</i> Connected The service node is reachable and the server has <i>n</i> active sessions on the node. Reachable The node is accessible. Unknown No sessions are active, and the service node offering this service has not been heard from recently, that is, the server has not received a service announcement. Unreachable An active service session has timed out, or an attempt to connect has timed out. The node can also signal that it is unreachable.
Rating	The relative capability of a service node to process new sessions.
Identification	The service identification string for this service node. This string can be different from the service node identification string.

The following guidelines apply to the service status display:

- **Service Information**

The server displays information about a service or services from data stored in its memory. If none of the ports can access a particular service, the server does not retain any data about that service. Therefore, no information about that service is displayed.

- **Rating**

The service rating is assigned by a service node for each service offered by the server. The higher the rating, the greater is the capability of the service node to accept a new connection.

The server uses the rating when multiple nodes offer the same service to determine the best node — usually the least busy at that time — to attempt to connect to. The server attempts to connect to the service that advertises the highest rating for the service.

- **“Unknown” Node Status**

The value of its multicast timer is part of a node’s service announcement message. The server waits five times the period specified by the node’s multicast timer without receiving a multicast message from the node before changing that node’s status from “Reachable” to “Unknown.” For example, if a node is advertising a 60-second multicast timer, the server waits 5 minutes.

9.7.3 Service Summary Display

The `SHOW/MONITOR/LIST SERVICE SUMMARY` commands display one line of information about services.

For `SHOW` and `MONITOR`, use the keyword `LOCAL` to obtain information for all services offered by your server. Without the `LOCAL` keyword or a particular service name, you get information about all network services. The display of services varies:

- Nonprivileged users see information about services that match their current groups (whether available or unavailable).
- The privileged user sees information about services that match his or her authorized groups (whether available or unavailable).

- If you are on port 0, you see information about services that match the sum of all the authorized groups (whether available or unavailable), shown as “Server Groups” in the SHOW SERVER SUMMARY display.

LOCAL is not meaningful with LIST because LIST commands by definition display only local services.

If you specify any service names, the commands display information only for those services, provided they are included in your current groups. With SHOW and MONITOR, if you do not specify a service name or LOCAL, the server displays all services that match your current groups.

The summary display is the default display for the SERVICES, SERVICES ALL, and SERVICES LOCAL entity specifications.

Figure 9–20 shows a typical SHOW SERVICE SUMMARY display.

Figure 9–20: Service Summary Display with Server SHOW Command

```
Local> SHOW SERVICES ALL SUMMARY
```

Service Name	Status	Identification
DEVELOP	2 Connected	Hardware Timesharing Service Ident
DOCUMENT	Available	Documentation Timesharing
TEST	Unavailable	As usual

```
Local>
```

Figure 9–21 shows a typical LIST SERVICE SUMMARY display.

Figure 9–21: Service Summary Display with TSC LIST Command

```
TSC> LIST SERVICES

Service Name      Identification
DEVELOP          Hardware Timesharing Service Ident
DOCUMENT         Documentation Timesharing
TEST             As usual

TSC>
```

For each service known to the server, the display contains one line of information. Table 9–25 describes the display.

Table 9–25: Service Summary Display Fields

Field	Description
Service Name	The name that identifies the network service.
Status	The current availability of the service: Available At least one of the service nodes that offer the service has the status Reachable . <i>n</i> Connected The service is available and <i>n</i> sessions are currently active with this service. Unavailable All of the service nodes that offer the service have the status Unreachable . Unknown None of the service nodes that offer the service is Reachable , and one or more is Unknown .
Identification	The service identification string, which typically describes the service or how to use it.

The following guideline applies to the service summary display:

- **Service Information**

The server displays information about a service from data stored in its memory. If no port can access a particular service due to authorized group settings, the server does not retain any data about that service. Therefore, no information about that service is displayed.

The service information can exist in server memory but still not be displayed to a particular user. This situation occurs if the user changed his or her current groups to exclude that service.

9.8 Sessions Display

The SHOW/MONITOR SESSIONS commands display information about service sessions for one or all server ports. Figure 9–22 shows a typical sessions display.

Figure 9–22: Sessions Display

```
Local> SHOW SESSIONS PORT 1

Port 1: Manager           Service mode  Current session: 4

- Session 1: Connected   Interactive   DEVELOP (PEACH)
- Session 2: Disconnected Passall      DOCUMENT (PEAR)
- Session 3: Connected   Psthru      TEST
- Session 4: Queued at 5 MODEM (LATHE 4)
Local>
```

The first line of the sessions display shows the port number and the name of the user on the port. The user name is one of these possible displays:

- *user-name* — as you defined for the port with the DEFINE PORT USER-NAME command
- *user-name* — as the user specified after the server's Username> prompt when the user logged in to the server
- (*remote access*) — If this is a remote session and the user issued a CONNECT command
- (*host initiated*) — If this is a host-initiated connection
- (*test responder*) — If this is a remote session and the port is responding to a TEST SERVICE command

The same line displays the mode — either local mode or service mode — and the current session number, if there is an existing session.

The following lines contain active session information. One line of information appears for each active session on the port. Each line of active session information is arranged in four columns from left to right, as described in Table 9–26.

Table 9–26: Sessions Display Fields

Field	Description
Session <i>n</i>	The number <i>n</i> of the session.
Status	The status of a session appears as one of the following: <ul style="list-style-type: none"> Connected The port is currently connected to the service, if “Current Access” in the SHOW PORT STATUS display is “Local.” If “Current Access” is “Remote,” the port currently has an active remote session. Connecting The session is currently being established either to or from the port, depending on the current access. Disconnected The session was terminated while dormant. Disconnecting The session is currently being disconnected on the port.
Data Transparency	The data transparency mode for a session appears as one of the following: <ul style="list-style-type: none"> Interactive The server recognizes XON/XOFF flow control characters and these switch characters (if defined): local, forward, and backward. These five characters are called “special characters.” Passall The server passes all special characters (total data transparency). Pasthru The server recognizes only XON and XOFF characters and passes all other special characters.
<i>name (node)</i>	The name of the service associated with the session. If the name of the service differs from the name of the service node supplying the service, the display includes within parentheses the name of the service node. For a remote-access connection to the port, the service name is that of the service sought by the requesting node, and the name within parentheses is that of the requesting service node.

9.9 Users Display

The SHOW/MONITOR USERS commands display information to help you monitor port use. The displays let you:

- Determine which ports are in use
- Identify the port users
- Determine services to which active users are connected

LIST USERS displays the ports with permanent user names previously defined with the DEFINE PORT USERNAME command. Figure 9–23 shows a typical SHOW USERS display.

Figure 9–23: Users Display

```
Local> SHOW USERS
```

Port	Username	Status	Service
0	Rick	Local Mode	
1	Corey	Local Mode	
2	Bethany	Connected	TIMESHARING
3	Larry	Local Mode	
4	Bill	Connected	TEST
5	Marie Curie	Connected	RADIUM
6	Tom Edison	Connected	LIGHT
7	Ben Franklin	Connected	LIGHT
8	Issac Newton	Connected	LIGHT
9	Tim	Connected	PLANET
10	Jeff	Connected	IDLE
.			
.			
.			
128	John	Connected	DOCUMENT

```
Local>
```

The display contains one line of information for each port that is logged in to the server. The information displayed under the headings is described in Table 9–27.

Table 9–27: Users Display Fields

Field	Description														
Port	The number <i>n</i> of the port.														
Username	The user name the user entered at port login or, if no name was supplied, the name of the port as specified by SET/DEFINE PORT NAME command.														
Status	The current status of the port, which can be one of the following: <table><tr><td>Connected</td><td>The port is currently connected to a service, if Current Access is Local. If Current Access is Remote, the port currently has an active remote session.</td></tr><tr><td>Connecting</td><td>A session is currently being established either to or from the port, depending on the current access.</td></tr><tr><td>Disconnected</td><td>A session was terminated while dormant.</td></tr><tr><td>Disconnecting</td><td>A session is currently being disconnected on the port.</td></tr><tr><td>Idle</td><td>The port is not in use.</td></tr><tr><td>Local Mode</td><td>The port is logged in to the server and is in local mode.</td></tr><tr><td>Locked</td><td>A LOCK command was executed on the port.</td></tr></table>	Connected	The port is currently connected to a service, if Current Access is Local. If Current Access is Remote, the port currently has an active remote session.	Connecting	A session is currently being established either to or from the port, depending on the current access.	Disconnected	A session was terminated while dormant.	Disconnecting	A session is currently being disconnected on the port.	Idle	The port is not in use.	Local Mode	The port is logged in to the server and is in local mode.	Locked	A LOCK command was executed on the port.
Connected	The port is currently connected to a service, if Current Access is Local. If Current Access is Remote, the port currently has an active remote session.														
Connecting	A session is currently being established either to or from the port, depending on the current access.														
Disconnected	A session was terminated while dormant.														
Disconnecting	A session is currently being disconnected on the port.														
Idle	The port is not in use.														
Local Mode	The port is logged in to the server and is in local mode.														
Locked	A LOCK command was executed on the port.														
Service	The name of the current service on the port, or the name of the service interrupted when the user last entered local mode.														

9.10 Usage Display

The LIST USAGE command displays information about the server's permanent database, giving a "status" of TSC usage. After you have issued many TSC commands, this display could be useful to verify the name of the image you are modifying. The display shows you:

- The name of the image file
- The product type and version number
- The date when you last customized the server image

- The time at which you last customized the server image (TSC updates this line when you exit TSC if you make any changes.)
- The DECnet node name of the load host on which you last customized the server image

Figure 9–24 shows a typical display.

Figure 9–24: TSC Usage Display

```
TSC> LIST USAGE  
Session Display
```

```
Current image is file: DS5TIGER.SYS  
DECserver 500, V2.0.0 (Database V9) .  
Server image last changed on 6-Dec-1988 at 14:19:17 on TOPCAT
```

```
TSC>
```

MOP System ID Message Format for the DECserver 500 Server

This appendix provides some basic information to help you decode the Maintenance Operations Protocol (MOP) System ID messages that are generated by the server. Use this appendix in conjunction with the Digital Network Architecture (DNA) Maintenance Operations Functional Specification V3.0 (Order No. AA-X436A-TK).

As a Digital Ethernet node, a DECserver 500 series terminal server is required to identify itself on the Ethernet by transmitting a system identification message every 8 to 10 minutes. The server must also respond on demand to system identification requests from other nodes on the Ethernet by transmitting this system identification back to the requesting node as soon as possible.

These system identification messages are often used by the server's load hosts for down-line loading, for Ethernet-level loop tests, and for establishing Remote Console Facility (RCF) sessions. The system identification message is one of a set of messages defined by the MOP protocol. The MOP protocol and message formats used by the DECserver 500 series server are described in the DNA MOP Functional Specification.

User-written software applications running on Ethernet nodes can also read MOP System ID messages from the Ethernet to determine which terminal servers are active on the network. Complete instructions on how to write software to intercept these messages from the Ethernet are beyond the scope of this guide. However, this appendix and the MOP specification provide enough information for you to decode these messages.

The MOP System ID message transmitted by the server contains several blocks of information about that particular server. The information found in each block is identified by what the MOP specification calls the INFO TYPE field. Each INFO TYPE field is followed by a one-byte INFO LENGTH field, followed by the INFO VALUE field, which is a set of bytes that contain the actual information.

The INFO TYPEs in every MOP System ID message generated by an Ethernet node is as follows (see the MOP specification for the required encoding of the INFO VALUE fields):

INFO TYPE Value	Information	Description
1	MAINTENANCE VERSION	MOP protocol version used by server
2	FUNCTIONS	MOP functions supported by this node
7	HARDWARE ADDRESS	Server's physical Ethernet address
100	COMMUNICATION DEVICE	INFO VALUE = 35 for DECserver 500 server

Since the DECserver 500 server supports RCF, the server is also required to include these additional INFO TYPEs:

INFO TYPE Value	Information	Description
3	CONSOLE USER	Ethernet address of current RCF user
4	RESERVATION TIMER	RCF session timeout threshold in seconds
5	CONSOLE COMMAND SIZE	Server RCF command buffer size in bytes
6	CONSOLE RESPONSE SIZE	Server RCF response buffer size in bytes

A server MOP System ID message includes all the INFO TYPEs mentioned thus far when the DECserver 500 firmware is in control of the DECserver 500 hardware. The firmware controls the server when:

- Self-test is in progress
- A down-line load is in progress.
- An up-line dump is in progress.
- The Console Commands Interface is running.
- Installation testing is in progress.

After a down-line load of the server's image, the running server includes all the INFO TYPEs mentioned thus far in every MOP System ID message it transmits, plus these two optional INFO TYPEs, which are optional for all Ethernet nodes:

INFO TYPE		
Value	Information	Description
-----	-----	-----
400	DATA LINK TYPE	INFO VALUE = 1 (Ethernet)
401	DATA LINK BUFFER SIZE	INFO VALUE = 1518

MOP designates INFO TYPEs 101–199 for Ethernet nodes to communicate additional information in their MOP System ID messages. From this range, the server uses INFO TYPEs 102–106 to broadcast this device-specific information about itself:

INFO TYPE		
Value	Information	Description
-----	-----	-----
102	ROM VERSION (3) : B =	Version, ECO version, sub-ECO version
103	SOFTWARE VERSION (3) : B =	Version, update version, test version
104	SERVER NUMBER (2) : B =	Two-byte binary server number
105	SERVER NAME (I-16) : A =	ASCII string, size in INFO LENGTH field
106	SERVER ID (I-17) : A =	ASCII string, size in INFO LENGTH field

INFO TYPEs 102–106 give the same information as the first few lines of the SHOW SERVER displays (see Section 9.6).

TSC Defaults Command File

This appendix shows the TSC defaults command file, which comes with the DEC-server 500 software distribution kit. You can run this file in TSC or TSM to change all current permanent database values to their defaults. The file's name is either DS5_020_DEFAULTS.COM or DS5DEFAULTS.COM, depending on the operating system of the load host.

```
!
!           DS5 020 DEFAULTS.COM
!
!
! This file, when executed by the configurator on a DECserver 500 terminal
! server image, will restore that image to its original, unaltered state.
!
! There are two seemingly redundant statements included. The first is
! setting all device types to CXY08. This is done so that various modem
! dependent characteristics can be changed without warning error messages
! appearing. Likewise, setting autobaud disabled prior to restoring the
! default speed of 9600 is done to suppress a message warning that
! autobaud is being disabled.
!
!
!           Default DEFINE SERVER SERVICE commands:
!
DEFINE SERVER SERVICE GROUP 0
!
!           Default DEFINE SERVER commands:
!
DEFINE SERVER NAME
DEFINE SERVER NUMBER 0
DEFINE SERVER IDENTIFICATION ""
DEFINE SERVER BACKUP HOSTS
DEFINE SERVER LINE FREQUENCY 60
```

```

DEFINE SERVER LOGIN PASSWORD "ACCESS"
DEFINE SERVER PRIVILEGED PASSWORD "SYSTEM"
DEFINE SERVER MAINTENANCE PASSWORD "0000000000000000"
!
DEFINE SERVER BROADCAST ENABLED, LOCK ENABLED, ANNOUNCEMENTS ENABLED
DEFINE SERVER CIRCUIT TIMER 80, KEEPALIVE TIMER 20, PASSWORD LIMIT 3
DEFINE SERVER NODE LIMIT 100, RETRANSMIT LIMIT 10, SESSION LIMIT 256
DEFINE SERVER QUEUE LIMIT 8, INACTIVITY TIMER 30, MULTICAST TIMER 60
DEFINE SERVER HEARTBEAT DISABLE, LIMITED HELP DISABLED
!
!       Default DEFINE PORT characteristics:
!
!       Do the special case of the console first.
!
DEFINE PORT 0  SESSION LIMIT 4
DEFINE PORT 0  LOCAL SWITCH ~
DEFINE PORT 0  FORWARD SWITCH NONE
DEFINE PORT 0  BACKWARD SWITCH NONE
DEFINE PORT 0  PREFERRED NONE
DEFINE PORT 0  USERNAME ""
!
DEFINE PORT 0  AUTOCONNECT DISABLED
DEFINE PORT 0  AUTOPROMPT ENABLED, BREAK DISABLED,          BROADCAST ENABLED
DEFINE PORT 0  INACTIVITY DISABLED, INTERRUPT DISABLED,     MESSAGE ENABLED
DEFINE PORT 0  LOSS ENABLED,          PASSWORD DISABLED,     SECURITY DISABLED
DEFINE PORT 0  TYPE SOFTCOPY,         VERIFICATION ENABLED, DIALUP DISABLED
DEFINE PORT 0  LIMITED DISABLED,      LOCK ENABLED,        ON-DEMAND DISABLED
DEFINE PORT 0  QUEUING DISABLED,      REMOTE MODIFCATION DISABLED
!
!       Now, set the defaults for the remaining ports and port 0 name.
!
DEFINE PORT ALL NAME NONE
!
!       Set the console port name after all port names have been reset
!       to insure command acceptance.
!
DEFINE PORT 0  NAME CONSOLE
!
DEFINE PORT ALL  SESSION LIMIT 4
DEFINE PORT ALL  LOCAL SWITCH NONE
DEFINE PORT ALL  BACKWARD SWITCH NONE
DEFINE PORT ALL  FORWARD SWITCH NONE
DEFINE PORT ALL  AUTH GROUPS 0
DEFINE PORT ALL  GROUPS 0
DEFINE PORT ALL  DEDICATED NONE
DEFINE PORT ALL  PREFERRED NONE
DEFINE PORT ALL  USERNAME ""
!
!
!       Set the devices to CXY08 to suppress "MODEM" warning messages.
!
DEFINE DEVICE ALL TYPE CXY08
!
!       Disable AUTOBAUD to suppress "AUTOBAUD DISABLED" warning messages.

```

```

!
DEFINE PO ALL AUTOBAUD DISABLED
!
DEFINE PORT ALL ACCESS LOCAL, AUTOBAUD DISABLED
DEFINE PORT ALL AUTOCONNECT DISABLED, AUTOPROMPT ENABLED
DEFINE PORT ALL BREAK LOCAL, BROADCAST ENABLED, DIALUP DISABLED
DEFINE PORT ALL FLOW CONTROL ENABLED, INTERRUPT DISABLED, MODEM DISABLED
DEFINE PORT ALL PASSWORD DISABLED, SECURITY DISABLED, TYPE SOFTCOPY
DEFINE PORT ALL VERIFICATION ENABLED, CHARACTER SIZE 8, PARITY NONE
DEFINE PORT ALL SPEED 9600, INACTIVITY DISABLED
DEFINE PORT ALL AUTOBAUD ENABLED, MESSAGE CODES ENABLED
DEFINE PORT ALL LOSS ENABLED, DSRLOGOUT DISABLED, DTRWAIT DISABLED
DEFINE PORT ALL LIMITED DISABLED, LOCK ENABLED, ON-DEMAND DISABLED
DEFINE PORT ALL QUEING DISABLED, SIGNAL DISABLED, MULTISES DISABLED
DEFINE PORT ALL REMOTE MODIFICATION DISABLED
!
!
! Reset the devices to "NONE SPECIFIED"
!
DEFINE DEVICE ALL TYPE NONE
!
!
! Finally get rid of all predefined services
!
PURGE SERVICE LOCAL
!
! End of defaults command file
!

```

Setting Up Remote Printers for VMS Systems

This appendix describes the procedures that both the server manager and the system manager perform to set up a remote printer. These procedures, in the order in which they are performed, are as follows:

1. Setting up the remote printer on your server
2. Setting up the VMS service node for the remote printer
3. Setting up the remote printer queue on a service node

The server manager should perform the procedure in Section C.1. After the server manager has completed the procedure, the system manager should perform the procedures in Section C.2 and C.3.

Section C.4 illustrates how to create a command file that enables the system manager to invoke LATCP automatically and configure the specified remote printer upon system startup. The last section describes setting up remote printer queues on a VAX-cluster.

C.1 Setting Up the Remote Printer on Your Server

This section explains to the server manager how to set up the server to allow access to an attached remote printer through host-initiated requests from a service node.

C.1.1 Example

The following example illustrates how you might use use local mode to set up a server called TSV1 with a printer attached at a port to be named P5.

```
Local> SET SERVER NAME TSV1
Local> SET PORT 5 NAME P5
Local> SET PORT 5 ACCESS REMOTE
Local> SET PORT 5 AUTOBAUD DISABLED
Local> SET PORT 5 BREAK DISABLED
Local> SET PORT 5 SPEED 4800
Local> SET PORT 5 SIGNAL CHECK ENABLED
Local> SAVE PORT 5
Local> LOGOUT PORT 5
```

C.1.2 Procedure

In this procedure, the server manager assigns a logical name to a specific server port. You can execute this procedure on the running server (local mode), with TSC, or with TSM. If you use local mode, you must save your changes and log out to save the changes in the log-in database. If you use TSC, the values are saved in the permanent database as you execute the command. Refer to Chapter 7 for more information.

To make the changes take effect in the log-in database, the server must be rebooted. If you use TSM, refer to *Guide to Terminal Server Manager* for information on the appropriate commands.

1. If you are setting up the terminal server for the first time, set the terminal server name. Otherwise, throughout this procedure, use the server name already defined. To verify the server name (*server-name*), use the SHOW SERVER command. Note that *server-name* is not necessarily the server's DECnet node name.

```
Local> SET SERVER NAME server-name
```

or

```
TSC> DEFINE SERVER NAME server-name
```

Here, *server-name* is the name you assign to the terminal server you are configuring.

2. Specify the server port identification and assign a remote port name (*port-name*).

```
Local> SET PORT n NAME port-name
```

OR

```
TSC> DEFINE PORT n NAME port-name
```

In these commands, *n* is a port number from 1 through 128 and remote *port-name* is the name you assign to the server port. Enter the same value for *n* throughout the rest of this procedure.

3. Set the access characteristic.

```
Local> SET PORT n ACCESS REMOTE
```

OR

```
TSC> DEFINE PORT n ACCESS REMOTE
```

Specify **ACCESS REMOTE** unless your printer has a keyboard and can be used alternatively as a terminal. If your printer can also be used as a terminal, use **ACCESS DYNAMIC**. See Section 7.7 for more information.

4. Set the autobaud characteristic.

```
Local> SET PORT n AUTOBAUD DISABLED
```

OR

```
TSC> DEFINE PORT n AUTOBAUD DISABLED
```

Remote-access or dynamic-access ports do not use the autobaud facility. Refer to Section 7.2.2 for more information. For remote laser printers, also disable the **BROADCAST** characteristic.

5. Set the break disabled characteristic.

```
Local> SET PORT n BREAK DISABLED
```

OR

```
TSC> DEFINE PORT n BREAK DISABLED
```

BREAK DISABLED indicates that the server disregards break signals in both service and local modes.

6. Set the port speed characteristic to match the speed of the printer port that the system manager will configure in Section C.3. Check with the system manager for the correct printer port baud rate.

```
Local> SET PORT n SPEED rate
```

or

```
TSC> DEFINE PORT n SPEED rate
```

In these examples, *rate* is the baud rate of the printer port.

If you are using TSC, the values you entered are now stored in the server's permanent database and will be in the log-in database when the server is rebooted. If you are using Local mode, you need to execute the next two steps before the values can be saved in the log-in database.

7. Save the changes.

```
Local> SAVE PORT n
```

8. Log out.

```
Local> LOGOUT PORT n
```

The LOGOUT command ensures that the information you entered in this procedure is saved in the log-in database. These changes do not take effect until you log back in.

Once you have completed this procedure, the system manager can set up the service node to make host-initiated requests for the remote printer. The next section describes how to perform that configuration.

C.2 Setting Up the VMS Service Node for the Remote Printer

The system manager configures a VMS service node by creating a logical device on the service node. The logical device (*LTA_n*) is then mapped to the remote printer port, which was set up by the server manager as explained in Section C.1.1.

This section describes the LATCP commands that the system manager uses to configure the service node to make host-initiated requests for printers on the terminal server. Note that the system manager must get the server name and port name from the server manager. Refer to the *VMS LAT Control Program (LATCP) Manual* in the VMS documentation set for more information.

C.2.1 Example

This example illustrates setting up a VMS service node using the parameters that the server manager defined in Section C.1.2.

```
$ RUN SYS$SYSTEM:LATCP
LCP> CREATE PORT LTA1925: /NOLOG
LCP> SET PORT LTA1925: /APPLICATION /NODE=TSV1 /PORT=P5
LCP> EXIT
```

C.2.2 Procedure

1. Be sure to have CMKRNL privileges before invoking LATCP. Invoke LATCP at the DCL prompt.

```
$ RUN SYS$SYSTEM:LATCP
```

2. At the LCP prompt, create an application port on the service node.

```
LCP> CREATE PORT LTA $n$ : /NOLOG
```

The value of n is a number from 1 to 9999. The system manager should develop a scheme for assigning values to the ports. The /NOLOG command qualifier indicates that the system does not display characteristics for the application node when this command executes.

3. Set the port to logically associate (map) an applications port with a remote port on the terminal server.

```
LCP> SET PORT LTA $n$ : /APPLICATION /NODE=server-name /PORT=port-name
```

The value of n is the port number entered in Step 2.

- /APPLICATION specifies that the port on the service node functions as an applications port.
- /NODE=*server-name* specifies the name of the remote node (terminal server) to be logically associated with the applications port on the service node. The parameter *server-name* is the name of the terminal server as defined by the server manager; it is not necessarily the server's node name. Ask the server manager for the *server-name*.
- /PORT=*remote-port-name* specifies the name of the remote port on a server that is to be mapped with the applications port. The parameter *remote-port-name* is the name of the applications port as defined by the server manager. Ask the server manager for this information.

4. Exit from LATCP.

```
LCP> EXIT
```

Note that these changes are only in effect until the host is rebooted. To save these changes, enter them into the LTLOAD.COM file. The LTLOAD.COM file configures the service node and its services and maps an applications port on the service node to a remote printer on a server. Ensure that LTLOAD.COM is invoked from SYSTARTUP.COM. The call to invoke LTLOAD.COM should be after DECnet is up and running.

After completing this procedure, you should test the setup *before* continuing with the procedure in Section C.3. The next section shows you how to test the setup.

C.2.3 Checkpoint

These two test procedures check the hardware connections, port hardware, and cabling. They also ensure that the port settings match the printer settings.

- At the local prompt, type the following command and press :

```
Local> TEST PORT n COUNT count-number
```

Here, the value of *n* is the port number you want to test and *count-number* is the number of test lines to be sent (range: 1 to 65535; default 23 lines). Depending on the type of remote printer you're using, Digital suggests that you use the following values for *count-number*:

- For line printers, use a PORT COUNT of 10
- For laser printers, use a PORT COUNT of 70

- At the VMS prompt, type the following command and press :

```
$ COPY/LOG filename LTA:n:
```

Here, *filename* is the name of a test file (any printable file can be used) you want to print at the remote printer and the value of *n* is the port number you defined in step 2 of the procedure in Section C.2.2. The test file should print on the specified remote printer.

Note that once you set up the remote printer queue, you will not use the COPY/LOG command to print files. Instead, you will be able to use the PRINT/QUE command.

For more information on either of these procedures, refer to the *DECserver 500 Problem Solving* manual. The next section describes how to perform the remote printer queue.

C.3 Configuring the Remote Printer Queue on a Service Node

Before using a remote printer, the system manager uses DCL commands to set up the printer as a spooled device. This section shows how to

- set up the printer characteristics on the VMS system
- set up the remote printer as a spooled device
- initialize and start the print queue.

For complete information about any of the DCL commands presented here, see the *VMS DCL Dictionary*. Note that these commands pertain to the current version of VMS 5.0 to VMS5.2.

C.3.1 Example

The following example is a sample setup for a remote printer and a remote printer queue.

```
$ SET TERM LTA1925: /PERM /DEVICE=LN03 /WIDTH=60 /NOBROAD-  
  /SPEED=4800  
$ SET PROT=(S:RWLP,O,G,W) /DEVICE LTA1925:  
$ SET DEVICE LTA1925: /SPOOLED=(LN03_QUE,SYS$SYSDEVICE:)  
$ INIT/QUE /START /PROCESSOR=LATSYM /RETAIN=ERROR-  
  /DEFAULT=(NOBURST,FLAG=ONE) /RECORD_BLOCKING LN03_QUE-  
  /ON=LTA1925:
```

C.3.2 Procedure

1. Set up the printer characteristics on the assigned applications port.

```
$ SET TERMLTAn: /PERM /DEVICE=terminal-type /WIDTH=x /NOBROAD /SPEED=rate
```

The value of *n* is the server port identification entered in steps 2 and 3 of the procedure in Section C.2.2.

- /PERM and /NOBROAD must be specified for applications ports.
 - /DEVICE=*terminal-type* sets default characteristics for the specified printer type (such as LN03). If you use other qualifiers, such as /WIDTH, the terminal type uses the characteristics specified by the other qualifiers.
 - /WIDTH=*x* specifies the number of characters on each line of output. Width values can be in the range of 0 to 255.
 - /SPEED=*rate* specifies the rate at which the printer sends and receives data. Check the printer's manual for the correct baud rate. The speed should match the speed that the server manager set in Section C.1.1.
2. Set the protection rights for the port.

```
$ SET PROT=(S:RWLP,O,G,W) /DEVICE LTAn:
```

The value of *n* is the server port identification entered in step 1.

3. Set up the remote printer as a spooled device.

```
$ SET DEVICE LTAn: /SPOOLED=(queue-name, SYS$SYSDEVICE:)
```

The value of *n* is the server port identification entered in step 1. The system manager assigns a unique name to the parameter *queue-name*.

4. Initialize and start the print queue.

```
$ INIT/QUE /START /PROCESSOR=LATSYM /RETAIN=ERROR-  
/DEFAULT=(NOBURST, FLAG=ONE) -  
/RECORD_BLOCKING queue-name /ON=LTAn:
```

- **/START** specifies that the queue being initialized starts at the execution of this command.
- **/PROCESSOR=LATSYM** specifies the LAT print symbiont, which is required for remote printers.
- **/RETAIN=ERROR** specifies that the system generates error status message and holds in the queue only jobs that complete unsuccessfully.
- **/DEFAULT=(NOBURST,FLAG=ONE)** establishes the specified options for the PRINT command. The option NOBURST specifies that the printer will not print file burst pages. The option FLAG=ONE specifies that a flag page is placed before the first copy of the first file in the job.
- **/RECORD_BLOCKING** limits the size of the record that can be executed on a printer queue.
- ***queue-name*** The system manager assigns a unique name to the parameter *queue-name*.
- **/ON=LTAn:** specifies the applications port associated with the remote printer. The parameter *n* is the server port identification entered in step 1.

Note that these changes are only in effect until the host is rebooted. To save these changes, create (or edit) a remote printer command file (for example, REMOTE_PRINT.COM) and enter these commands into the file. This ensures automatic print queue setup for your remote printers on system startup. See Section C.4 for more information about creating a remote printer command file (REMOTE_PRINT.COM).

Using the REMOTE_PRINT.COM file allows you to maintain remote print queues separately from other queues on a node. This separation is useful because queues for local applications devices are started before the LTLOAD.COM file is executed, while remote print queues must be started afterwards. Separation also reduces the possibility that you will unintentionally interfere with the local applications devices and local queues when you are setting up applications ports and queues for remote printers. Be sure to invoke REMOTE_PRINT.COM from SYSTARTUP.COM after LTLOAD.COM is invoked and the queue manager is running.

C.4 Creating a Remote Printer Command File

This example illustrates a remote printer command file called REMOTE_PRINT.COM that sets up a remote printer and remote printer queue. The system manager may want to use this example as a template to set up subsequent remote printers. The system manager should enter the remote printer command file name in the LTLOAD.COM file. This ensures that remote printers and remote printer queue are set up automatically upon system startup.

```

$! This command procedure sets up the local characteristics of the
$! applications devices for remote printers and sets up the print
$! queues for these remote printers. These devices should have been
$! set up previously by the LTLOAD.COM command file. NOTE: The queue
$! manager must be running before executing this file.
$!
$!
$! Set up local characteristics for the applications devices.
$!
$ SET TERM LTA1925: /PERM /DEVICE=LN03 /WIDTH=60 /NOBROAD-
    /SPEED=4800
$!
$! Set the protection on the devices so that only the symbiont can
$! access them.
$!
$ SET PROT=(S:RWLP,O,G,W) /DEVICE LTA1925:
$!
$! Set the devices spooled
$!
$ SET DEVICE LTA1925: /SPOOLED=(LN03_QUE,SYSSYSDEVICE:)
$!
$ DEFINE/FORM LN_FORM 10 /WIDTH=60 /STOCK=DEFAULT /TRUNCATE
$!
$! Initialize and start the print queue
$!
$ INIT/QUE /START /PROCESSOR=LATSYM /RETAIN=ERROR-
    /DEFAULT=(NOBURST,FLAG=ONE) /RECORD_BLOCKING LN03_QUE-
    /ON=LTA1925:
$ EXIT

```

C.5 Setting Up Remote Printing on VAXclusters

On a VAXcluster, you can set up the applications ports on only the local node. However, it is recommended that you do so on at least two nodes, so that a redundant path to the device is available in the event of a failure of a cluster node. To set up a remote-printer applications port on a cluster node, include LATCP CREATE PORT and SET PORT commands for that port in the node's LTLOAD.COM file. For complete information about setting up remote printing on VAXclusters, refer to the *VMS VAXcluster Manual* in the VMS documentation set.

Index

Numbers

- 3270 mode, 1–17
- 3270 mode terminal coax counters, 9–13
- 3270 Terminal Option card
 - CXM04, 1–17
 - effect of 3270 terminal power up, 5–83
 - effect of power loss, 5–83
 - effect of server power up, 5–82
 - emulating a VT220 terminal, 7–58
 - introduction to, 5–80—5–81
 - line card failure, 5–83
 - supported terminals, 5–82
- 3270 terminals
 - characteristics of, 8–26
 - overview of, 1–17
 - setting up and managing ports, 5–80

A

- ACCESS characteristic
 - description of, 8–7
 - display field for, 9–28
 - display heading, 9–41
- Access fields, 9–41
- Active Circuits field, 9–57

- Active Ports field, 9–56
- Active Users field, 9–56
- Address field, 9–20, 9–44, 9–45, 9–54, 9–55
- ALTERNATE HOTKEY characteristic, 8–27
- Alternate load hosts, recommendation, 1–29
- ANNOUNCEMENTS characteristic, 8–37
- Application programs, 1–2
- Authorized groups, 1–12
- AUTHORIZED GROUPS characteristics, 8–10
- AUTOBAUD characteristic
 - description of, 8–16
 - speeds supported by, 8–16
 - use of, 7–5
- AUTOCONNECT characteristic, 8–11
- Automatic failover, 1–11, 8–12
- AUTOPROMPT characteristic, 8–12
- Available Services field, 9–57

B

- BACKUP HOSTS characteristic, 8–34

BACKWARD SWITCH characteristic
description of, 8–20
display field for, 9–29
recommended characters for, 8–20

Benefits
of DECserver 500, 1–1
overview of, 1–1

Boot switch, resetting the server by
pressing the, 5–10, 5–21

BREAK characteristic, 8–21
display field for, 9–29
use with modems, 7–43

BROADCAST command
description of, 5–35
port characteristic, 8–22
server characteristic, 8–31

C

Cables
null modem, 7–2
straight-through modem, 7–3

Cabling requirements, 7–2

CCU. *See* IBM Cluster Control Unit

CCU Coax Counters, 9–13

CHARACTER SIZE characteristic
description of, 8–17
display of, 9–27
specifying, 7–5

Characteristics, 2–4

CIRCUIT TIMER characteristic
description of, 8–29
display field for, 9–45
selecting the value of, 5–77

Commands of the DECserver 500, introduction to, 2–2

Communications server, 1–1

Computers, 1–19

Configuration
of load host's node database, 2–7,
6–26
options, 6–27
preparing for, 6–34

Connected Nodes field, 9–57

Connected Sessions field, 9–57

Connection queue
description of, 1–23, 8–39
managing the, 5–72

CONNECTIONS characteristic, 8–39

Console port, as a management tool,
overview of, 2–8

Control Unit Terminal (CUT) mode,
1–17

Conventions, of DSVCONFIG, 6–35

Coordinating tasks with others, 3–2

CPU, percent used, 9–57

CTS signal loss, 5–50

CTS/RTS, 1–22

Current groups, 1–12

Customized server image
customizing the server image, 6–2
down-line loading the, 3–9, 5–6—5–7,
6–18

Customizing the operational database,
4–2

CXM04, up-line dumping of information,
5–85

CXM04 line card
cabling for, 7–4
descriptions of, 1–17, 8–42

ports for, 1–17
CXY08 line card, 8–42

D

Data Overrun field
description, 9–51
guidelines, 9–53

Data transparency modes, for local-access session, 5–56

Database

changing values in the, 1–10
controlling values of, 1–7
customizing the operational, 4–2
description of, 1–7
keeping synchronized, 6–28, 6–39
log-in, 1–9
operational, 1–8
permanent, 1–8

DECnet areas, 6–30

DECnet databases, 6–28, 6–44

DECnet error messages, 6–35, 6–39

DECnet event logging, 6–18

DECnet load database, 6–28, 6–39, 6–43

DECnet node address

with areas, 6–30
description, 6–38
determining, 6–34

DECnet node name

description, 6–38
determining, 6–34

DECserver 500 commands, introduction to, 2–2

DECserver 500 commands, summary, 2–2

DECserver 500 concepts, 1–1

DECserver 500 Identification Card, 6–34

DECserver 500 product, benefits of, 1–2

DECserver 500 Terminal Server

descriptions of, 1–1, 1–2

models, 1–4

monitoring of, 4–6

troubleshooting, 4–6

DECserver 500 version field, description, 9–45, 9–49, 9–55

DEDICATED characteristic, 8–13

Dedicated port, 1–16

Dedicated service, 1–16

assigning a, 5–37

configuring port for, 7–12

definition of, 1–16

DEDICATED SERVICE characteristic, 9–30

Default values, operating with, 3–6

Device Counters Display, 9–8

Device displays, 9–5

DEVICE DUMP, 8–44

DEVICE STATE, 8–43

Device Summary Display, 9–5

Device support, 1–13

DEVICE TYPE command, defining, 8–41

Devices, 8–41

Diagnostic self-test, 1–29

Dial-out modems, configuring port for, 7–37

DIALUP characteristic, 8–13

Discarded Nodes field, description, 9–55

Display commands, overview of, 9–1

Displays, introduction to, 2–20

Distribution files, 1–29

Down-line loading

the customized server image, 5–6

- descriptions of, 1–28, 5–7, 6–37
- initiating, 5–20
- load file name, 6–31
- with NCP LOAD command, 6–19
- with NCP TRIGGER command, 6–19
- preparing for a, 5–17
- monitoring, 5–17, 5–21
- reading event–logging messages after, 5–22
- reading the 900–series messages after, 5–21
- reading the server’s LED display during, 5–21

DSR logout, 1–28

DSR/DTR, 1–22

DSRLOGOUT characteristic, 2–17, 8–13

DSVCONFIG command

- conventions, 6–35
- options
 - adding, 6–38
 - deleting, 6–43
 - listing servers, 6–37
 - restoring, 6–43
 - swapping, 6–40
- overview of, 6–28
- preparing for, 6–34
- requirements, 6–35
- restoring local database with, 6–43
- running, 6–35

DTRWAIT characteristic, 8–23

Dump Address field, 9–56

Dump file, 6–21

Dump file name, 6–33

Duplicates Received field, guidelines, 9–53

E

Error messages, 6–35, 6–39

Ethernet address

- description, 6–33
- determining, 6–34

Event logging

- description of, 6–18
- enabling, 6–19
- setting up DECnet, 5–17

F

Failover, 1–11

Failure of server

- forcing a crash, 6–21
- unexpected crash, 6–21

File transfer, managing, 5–75

Flow control

- CTS/RTS, configuring port for, 7–54
- DSR/DTR, configuring port for, 7–56

FLOW CONTROL characteristic

- description of, 8–19
- display of, 9–27
- in–band, 5–55
- out–of–band, 5–55
- specifying, 7–5
- types of, 8–19

Flow control protocols, 1–22

FORWARD SWITCH characteristic

- description of, 8–20
- display field for, 9–29
- recommended characters for, 8–20

G

Group codes, 1–12

Groups

- adding and replacing authorized, 5–29
 - assigning authorized, 5–27, 5–39
 - assigning service, 5–26
 - authorized, 5–23, 5–27
 - making use of, 5–23
 - network service, 5–24
 - overview of, 1–11
 - reducing authorized, to current, 5–29
 - server, 5–27
 - service, 5–23
 - specifying service, 5–60
- GROUPS characteristic, 8–10

H

- HEARTBEAT characteristic, 8–30
- Help, on–line
- server, 2–18–2–19
 - Terminal Server Configurator (TSC),
2–20, 6–13
 - tutorial, 2–18
- Helping server users, 4–6
- Host–initiated request
- explanation of, 1–21
 - managing ports for, 5–70
 - a printer configured for, 7–22
- Hot–key sequence, 1–17

I

- IBM 3270 Information Display System
terminals, 1–17
- IBM Cluster Control Unit (CCU), 1–17
- IDENTIFICATION characteristic, 8–35,
8–37, 8–39
- Image configuration, 5–83
- Image file, 1–28

INACTIVITY LOGOUT characteristic,
8–14

INACTIVITY TIMER characteristic,
8–31, 9–45

Initialization

- automatic after up–line dump, 6–21
- basic process of, 5–8
- warning users with BROADCAST,
6–19

Initialization process, 5–6

INITIALIZE command, 5–21

Initiating a down–line load, 5–20

INPUT SPEED characteristic, 9–28

INTERRUPTS, 8–9

K

- KEEPALIVE TIMER characteristic,
5–77, 8–30
- Keyboard mapping, 5–82, 6–45
- Keyboard mapping commands, 2–22

L

- LAN, 1–2
- Languages, defining, 8–44
- LAT, 1–3
- LAT version field, description, 9–45
- LED display, during down–line loading,
5–21
- LIMITED HELP characteristic
- descriptions of, 2–17, 8–10, 8–31
 - with on–line Help, 2–20,
 - overview of, 1–27
- LIMITED VIEW characteristic, 2–17,
8–10
- Line card redundancy, 5–85

- Line cards, 1–5
- LINE FREQUENCY, 8–34
- Load balancing
 - definition of, 1–11
 - use of service ratings in, 1–11
- LOAD command, 6–19
- Load file, 1–8, 6–31
- Load host, 1–28
- Load host
 - alternates, 1–28
 - installation, verification of, 1–30
 - node database, configuration of, 6–26
 - recommended number, 1–29
- Local Area Network (LAN), 1–2
- Local Area Transport (LAT), 1–3
- Local mode, introduction, 1–6
- Local mode prompt, 1–6
- Local modem, 1–21
- Local service
 - announcements control, 5–60
 - characteristics
 - alphabetic listing of, 8–39
 - displaying information about, 8–38
 - list of defaults, 8–39
 - clearing, 5–70
 - commands that affect, 5–57
 - controlling access, 5–68
 - description of, 1–2
 - displaying information about, 5–68, 8–38
 - establishing a, 5–62
 - introduction to, 5–57
 - managing before shutdown, 5–20
 - managing your server as a,
5–57—5–58
 - preventing remote access to a port of-
fering, 5–67
 - server characteristics that affect, 5–58

- LOCAL SWITCH characteristic
 - description of, 8–21
 - display field for, 9–29
 - recommended characters for, 8–21
- Local-access characteristics, 8–31
- LOCK characteristic, 5–36, 8–10, 8–32
- Lock password, 2–16
- Log-in password
 - description of, 5–3
 - enabling the, 5–38
- Log-in database, customizing, 4–3
- Logging in, variations in process, 7–11
- Logout, enabling inactivity, 5–40
- LOGOUT command, disconnection due
to, 5–51
- LOSS NOTIFICATION characteristic,
8–22

M

- Maintenance password
 - description of, 2–14
 - use of, 6–20
- Management tasks
 - customizing permanent database, 3–6
 - ensuring same image on hosts, 3–8
 - establishing security, 3–2
 - getting load host information, 3–4
 - initial, 3–1
 - summary of, 1–31
- Management tools
 - full description of, 2–1
 - overview of, 1–30
- Managing flow control, 5–55
- Managing sessions, 5–42
- Memory, percent used, 9–57
- MESSAGE CODES characteristic, 8–22

Messages

- reading event—logging after down—line loading, 5–22
- reading the 900—series, 5–21

MODE characteristic, 8–27

Modem

- definition of, 1–20
- description of, 7–37
- dial-in/dial-out modem
 - configuring port for, 7–45
 - definition of, 1–23
- dial-in modems, 7–41
- dial-out modems, 1–20
- local modems, 1–20
- null modem cables, 7–2
- overview of, 1–20
- remote modems, 1–20
- straight-through cables, 7–3
- use with computers, 7–35
- using remote—access ports with dial—out, 5–50
 - disconnection due to LOGOUT command, 5–51
 - disconnection due to signal loss, 5–51

Modem control

- as a DECserver 500 security feature, 2–17
- implementing, 5–51
- introduction, 5–44
- as a management tool, 2–17
- monitoring by server and TSC, 5–54
- overview of, 1–28
- port characteristics related to, 5–51
- procedure to set up a port for, 5–53
- restrictions, 5–46
- setting up and managing, 5–44
- signaling sequences, 5–49
- signals, 5–47

- standards, 5–46

MODEM CONTROL characteristic

- description of, 8–24
 - display field for, 9–28
- ## Modem support characteristics, 8–23

Monitoring a down—line load, 5–17

Monitoring the server, 4–6

MULTICAST TIMER characteristic, description of, 5–60, 8–37

Multiple sessions, 1–16

MULTISESSIONS characteristic, 8–14

N

NAME characteristic, 9–29

Names

- port NAME characteristic, 8–25
- server NAME characteristic, 8–36

NCP CONNECT command, 6–25

NCP facility, 6–25

NCP LOAD, how it works, 5–10

NCP LOAD command, 5–21

NCP TRIGGER, 5–14

Network communications characteristics, 8–29

Network services, controlling access to, 5–78

Node

- definition of, 1–1
- divided into areas, 6–30
- as load hosts, 1–28

Node database, 6–27, 6–28, 6–36, 6–37, 6–39

Node displays

- counters, 9–15
- description of, 9–16, 9–15, 9–19, 9–22

- sample of, 9–16, 9–19, 9–22
- status, 9–19
- summary, 9–22
- Node field, 9–20, 9–27
- Node groups field
 - description, 9–20
 - guidelines, 9–21
- NODE LIMIT characteristic, 8–30
- Node name heading
 - description, 9–23
 - guidelines, 9–24
- non-LAT hosts
 - configuring ports for, 7–32
 - definition of, 1–19
- NUMBER characteristic
 - description of, 8–36
 - display field for, 9–45

O

- ON-DEMAND LOADING, 8–20
- On-line help
 - display command summaries, 2–20
 - for server commands, 2–18
- Operational database, customizing, 4–2
- OUTPUT SPEED characteristic, 9–28

P

- PARITY characteristic
 - description of, 8–17
 - display of, 9–28
 - specifying, 7–5
- Password
 - conventions for specifying, 3–2
 - DECnet maintenance password, 6–24
 - DECnet service password, 6–24, 6–25

- in NCP commands, 6–20
- as a DECserver 500 security feature,
 - 2–11
- descriptions of, 2–13, 5–3
- lock password, 2–16
- log-in, 2–14
- log-in password
 - port PASSWORD characteristic,
 - 8–11
 - server PASSWORD characteristic,
 - 8–32
- log-in password prompt, 6–25
- maintaining server security with, 4–5,
 - 5–2
- MAINTENANCE PASSWORD characteristic
 - descriptions of, 2–14, 8–35
 - use of, 6–20
- overview of, 1–27
- PASSWORD LIMIT characteristic,
 - 8–32
- privileged, 2–14, 5–2
- PRIVILEGED PASSWORD characteristic, 8–33
- server maintenance, 6–25
- service, 2–16, 5–4, 5–61—5–62
- service PASSWORD characteristic,
 - 8–40
- setting and clearing a lock, 5–4
- setting the maintenance, 5–3

Password-related characteristics, setting other, 5–5

- PC
 - configuring port for, 7–16
 - overview of, 1–20
 - printers accessed by, 1–19
 - as a terminal, 1–17
- Permanent database, customizing, 3–6

Personal Computer. *See* PC

Port characteristics

- alphabetic listing of, 8-4
- displaying information about, 8-3
- list of defaults, 8-5
- modifying values of, 8-3
- on port 0, 8-6
- related to modem control, 5-51
- use of, 8-2
- user-oriented, 5-36

Port counters display, 9-31

Port devices, 1-13

Port display control characteristics, 8-22

Port displays, 9-24-9-26

Port identification characteristics, 8-25

Port name, assigning for host-initiated requests, 5-70

Port status display, 9-36

Port summary display, 9-39

Ports

- application sections, guidelines for using, 7-6
- assigning authorized groups for your, 5-27

configuring for

- CTS/RTS flow control, 7-54
- dial-in/dial-out modems, 7-45
- dial-in modems, 7-41
- dial-out modems, 7-37
- DSR/DTR flow control, 7-56
- dynamic access, 7-16
- non-LAT hosts, 7-32
- personal computers, 7-16
- physical characteristics, 7-4
- printers, 7-28
- terminal switches, 7-49
- terminal using dedicated service, 7-12

terminals using many services, 7-9

default configuration, 7-7

displaying information about, available display, 9-25

enabling interrupts on dynamic-access, 5-40

identifying who uses the local-access, 5-32

local-access, 1-9

managing local-access, 5-30

privileged, 2-10

remote-access, 1-9

service PORTS characteristic, 8-40

verifying operation of the, 4-5

PREFERRED characteristic, 8-15

Preferred service, 8-15

PREFERRED SERVICE characteristic, 9-30

Preparation

for configuring the node database, 6-34

for running the configuration procedure, 6-34

Printers

accessed by personal computers, 1-19

configuring port for

receiving queued connection requests, 7-28

using CTS/RTS flow control, 7-54

dedicated, 1-19

host-initiated requests for, 1-18

offering as a service, requirements, 1-22

offering as services, 1-21

overview of, 1-18

PROMPT characteristic, 8-37

prompt, settable, 1-6

Q

Queue

- connection and operation of, 1–23
- definition of, 1–23
- QUEUE characteristic, 8–40
- removing entries from the, 5–74

Queue display, 9–42

Queue entries, displaying, 5–73

Queue limit, managing the, 5–73

QUEUE LIMIT characteristic, 8–38

Queuing, disabling further, 5–74

QUEUING characteristic, 1–23, 8–15

R

RCF (Remote Console Facility)

- connecting to node, 6–24
- DECnet service password, 6–24
- descriptions of, 2–8, 6–21, 6–23
- prerequisites for, 6–22
- remote management console, definition of, 6–21
- remote management session, definition of, 6–21
- starting a session, 6–24

Reachable Nodes field, 9–57

Reconfiguring the load host's node database, 4–6

Remote mode, 1–21

REMOTE MODIFICATION characteristic, 8–26

Remote modification control character, 8–26

Restoring local database, with RESTORE parameter, 6–44

Restoring local databases, with DSVCONFIG, 6–43

RETRANSMIT LIMIT characteristic, 5–77, 8–31

ROM version field, description, 9–45

S

Security

- definition of, 1–26
- establishing server security, 3–2
- features of server, 2–11
- maintaining with passwords, 4–5, 5–2
- non-privileged status, definition of, 2–12
- privileged status, definition of, 2–12
- secure status, 2–13

SECURITY characteristic, 8–11

Security features, as a management tool, 2–11

Security levels of ports

- as a feature, 2–11
- as a management tool, 2–11

Security status

- assigning, 5–38
- overview of, 1–27

Security-related characteristics, setting other, 5–5

Server

- assigning service groups for your, 5–26
- definition of, 1–1
- changing the defaults to customize, 3–7
- concepts, 1–6
- distributing devices on, 5–76
- managing as part of the LAT network, 5–76
- on-line help, 2–18
- overview of, 1–1
- resetting with the boot switch, 5–10

- as a service node, 5-57—5-58
- Server characteristics, 8-27—8-28
 - alphabetical listing, 8-28
 - displaying information about, 8-27
 - factory set defaults, 8-29
 - modifying values for, 8-27
 - user-oriented, 5-34
- Server characteristics display, 9-43—9-45
- Server commands
 - access to, 1-15
 - users of, 2-2
- Server counters display, 9-47
- Server dump file, 6-21
- Server groups, 1-11, 1-12
- Server identification characteristic, 8-35, 9-45
- Server image, 1-28
 - customizing, 4-4
 - down-line load the customized, 3-9, 4-4
- Server image file, updating, 6-16
- Server installation, summary of, 1-29
- Server maintenance characteristics, 8-34
- Server manager tasks, list of, 4-1
- Server name characteristic, 9-45
- Server port, security levels of, 2-11
- Server status display, 9-54
- Server summary display, 9-58
- Server users, helping, 4-6
- Service characteristics, 5-60, 8-38
- Service characteristics display, 9-61
- Service circuit, 6-29, 6-37, 6-38, 6-42
- Service groups, 1-11, 1-12
- SERVICE GROUPS characteristic, 8-38
- Service information, 5-27
- Service mode, 1-7

- Service name, assigning for host-initiated requests, 5-70
- Service node
 - definition of, 1-2
 - name of your server as a, 5-59
- Service node characteristics, 8-37
- Service password, 2-16, 5-4
- Service ratings, use of, 1-11
- Service software, LAT, 1-3
- Service status display, 9-62
- Service summary display, 9-64
- Services
 - definition of, 1-2
 - controlling access to all, 5-41
 - local, 8-38
- Session
 - description of, 1-2
 - displaying information, 5-42
 - managing, 5-42
 - number of terminals permitted, 8-16
 - terminal, 1-16
 - terminating a, 5-43
- Session limit, specifying a, 5-40
- SESSION LIMIT characteristic
 - description of, 8-16
 - display field for, 9-29
 - port, 8-16
 - server, 8-33
- Session Management Terminal and dedicated services, 7-14
 - descriptions of, 5-32, 7-61
 - commands for, 2-6
 - port characteristics for, 3-7
 - terminate session, 1-16
- Session-switching characteristics, 8-20
- Sessions display, 9-67

SET LOGGING CONSOLE EVENT
command, 6–19

SET LOGGING CONSOLE STATE
command, 6–19

SET LOGGING MONITOR STATE
command, 6–19

Setting and clearing a lock password,
5–4

Setting the maintenance password, 5–3

Setting other password–related charac-
teristics, 5–5

Setting other security–related character-
istics, 5–5

Shutdown, managing local services be-
fore, 5–20

SIGNAL CHECK characteristic, 1–18,
8–24

Software distribution kit, 1–28

Software installation, verification of,
1–30

SPEED characteristic
description of, 8–18
specifying for, 7–5
supported by, 8–18
values of DECserver 500 server, 1–15

System manager, coordintaing tasks
with, 4–2

T

TD/SMP, 5–32, 7–61

TD/SMP protocol, 1–16

Terminal emulation. *See* 3270 terminals

Terminal server, 1–2

Terminal Server Configurator (TSC)
after running, 6–18
descriptions of 1–8, 2–6

executing commands from a command
file, 6–14

invoking, 6–10

monitoring modem control with, 5–54

on–line help, 2–20

overview of commands, 6–7

problems with opening files, 6–11

using, 6–2–6–4

Terminal Server Manager (TSM), 1–8,
2–22

Terminal session, 1–16

Terminal switches, configuring port for,
7–49

Terminals
configuring for, using many services,
7–9

configuing port for, using dedicated
services, 7–12

configuring port for, using DSR/DTR
flow control, 7–56

overview of, 1–15

session management, 1–16
and BACKWARD SWITCH, 8–20
commands for, 2–6
and FORWARD SWITCH, 8–20
port characteristics for, 8–16

TRIGGER command
definition of, 5–21
issuing, 6–19

Troubleshooting, 2–21

TSC. *See* Terminal Server Configurator
(TSC)

TSM. *See* Terminal Server Manager
(TSM)

TYPE characteristic
description of, 8–18
display field for, 9–30
specifying, 7–5

U

Up-line dumping

definition of, 6–21

received by load host, 1–29

Uptime field, 9–45

Usage display, 9–70

User information, 5–28

User name

assigning permanent, 5–41

display field for, 9–27

USERNAME characteristic, 8–25

Users

educating, 5–34

warning, 5–18

Users display, 9–69

V

VAXclusters, automatic failover in, 1–11

VERIFICATION characteristic, 8–23

VT mode, 1–17

VT mode terminal coax counters, 9–13

X

XON/XOFF, 1–22

READER'S COMMENTS

What do you think of this manual? Your comments and suggestions will help us to improve the quality and usefulness of our publications.

Please rate this manual:

	Poor			Excellent	
Accuracy	1	2	3	4	5
Readability	1	2	3	4	5
Examples	1	2	3	4	5
Organization	1	2	3	4	5
Completeness	1	2	3	4	5

Did you find errors in this manual? If so, please specify the error(s) and page number(s).

General comments:

Suggestions for improvement:

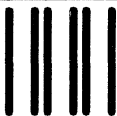
Name _____ Date _____

Title _____ Department _____

Company _____ Street _____

City _____ State/Country _____ Zip Code _____

DO NOT CUT - FOLD HERE AND TAPE



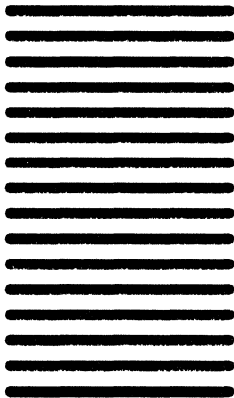
NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY LABEL
FIRST CLASS PERMIT NO. 33 MAYNARD MASS.

POSTAGE WILL BE PAID BY ADDRESSEE

digitalTM

**Networks and
Communications Publications**
550 King Street
Littleton, MA 01460-1289



DO NOT CUT - FOLD HERE