HSC V6.5 SOFTWARE USER GUIDE UPDATE

Order Number: AD–GMEAA–T6

This update to the *HSC Controller User Guide* includes replacement chapters and associated front and back matter.

HSC V6.5 SOFTWARE DOES NOT SUPPORT HSC50 CONTROLLERS

If you are using a single *HSC User Guide* for the HSC50 and the HSC40/60/70/90 controllers at your installation, retain the old user guide chapters for the HSC50 controllers running V3.90 or lower software.

Digital Equipment Corporation
Maynard, Massachusetts

CHANGE INSTRUCTIONS

The enclosed pages provide the necessary changes to update your *HSC Controller User Guide* to HSC V6.5 software. Remove the pages indicated in column 1 of the following table and replace with the pages listed in column 2. When you have completed this change, file this Change Instructions sheet as the first page after the title page in your user guide.

Remove Pages	Replace with Pages
Title/copyright	Title/copyright
Table of Contents pages iii through xv	Table of Contents pages iii through xviii
Preface pages xvii through xx	Preface pages xix through xxii
Chapter 4—entire chapter 4[1]	Chapter 4 – insert new chapter.
Chapter 5—entire chapter 5	Chapter 5 – insert new chapter.
Chapter 6—entire chapter 6[1]	Chapter 6 – insert new chapter.
Chapter 12—entire chapter 12[1]	Chapter 12 – insert new chapter.
n/a	Chapter 13—insert new chapter
Appendix A—entire appendix A [1]	Appendix A – insert new appendix.
Appendix B—entire appendix B [1]	Appendix B – insert new appendix.
Index—entire index	Index—entire index

[1]If you have only one *HSC User Guide* for the HSC50 and HSC40/60/70/90 controllers at your installation, retain the old user guide chapters for use with the HSC50 controllers running at V3.90 or V3.9A software.

HSC Controller User Guide

Order Number: AA–PFSQA–TK

This book contains overview information and operating procedures for the HSC40/70/60/90 controller, and instructions for running the HSC utilities.

Revision/Update Information: HSC Version 6.5 Software

May 1992

FCC NOTICE: The equipment described in this manual generates, uses, and may emit radio frequency energy. The equipment has been type tested and found to comply with the limits for a Class A computing device pursuant to Subpart J of Part 15 of FCC Rules, which are designed to provide reasonable protection against such radio frequency interference when operated in a commercial environment. Operation of this equipment in a residential area may cause interference, in which case the user, at his own expense, may be required to take measures to correct the interference.

Contents

PREFACE xix

CHAPTER 1 AN OVERVIEW OF THE HSC CONTROLLER 1–1

1.1 CONFIGURATION OF HSC CONTROLLER MODELS 1–3

1.2 THE HSC CONTROLLER IN A CLUSTER ENVIRONMENT 1–4
1.2.1 Host Connection 1–4
1.2.2 Storage Unit Connection 1–4
1.2.3 Initializing the HSC Controller 1–6
1.2.4 Volume Shadowing 1–6

1.3 HSC SOFTWARE 1–7
1.3.1 Utility Programs 1–8
1.3.2 Device Integrity Tests 1–9
1.3.3 Diagnostics Utilities Protocol 1–9
1.3.4 Central Error Reporting Facility 1–10
1.3.5 Error Indications 1–10
1.3.5.1 Error Message Format • 1–10

1.4 HOW TO CLEAN THE FRONT DOOR AIR FILTER 1–11

CHAPTER 2 SWITCHES AND INDICATORS 2–1

2.1 AC POWER SWITCH 2–1

2.2 DC POWER SWITCH 2–1

2.3 SECURE/ENABLE SWITCH AND INDICATOR 2–4
2.3.1 Operator Restrictions 2–4

2.4	OPERATOR CONTROL PANEL SWITCHES AND INDICATORS		2–6
	2.4.1	State Indicator	2–7
	2.4.2	Power Indicator	2–7
	2.4.3	Init Switch and Indicator	2–7
	2.4.4	Fault Switch and Indicator	2–8
	2.4.5	Online Switch and Indicator	2–8
	2.4.6	Blank Indicators	2–9
2.5	READING OCP FAULT CODES		2–9

CHAPTER 3 HOW TO BOOT THE HSC CONTROLLER 3–1

3.1	THE RX33 DISK DRIVES		3–1
3.2	A DESCRIPTION OF THE RX33 SYSTEM DISKETTE		3–3
3.3	HOW TO LOAD AN RX33 DISK DRIVE		3–4
3.4	HOW TO BOOT THE HSC CONTROLLER		3–4
3.5	AUTOMATIC REBOOT		3–6
3.6	THE SYSTEM CONFIGURATION TABLE		3–6
	3.6.1	The Template SCT	3–6
	3.6.2	The User SCT	3–7

CHAPTER 4 HOW TO OPERATE THE HSC CONTROLLER 4–1

4.1	HOW TO USE THE CONSOLE TERMINAL		4–1
	4.1.1	Using Control Characters or Special Keys at the HSC> Prompt	4–2
4.2	QUICK DISCONNECT		4–3

4.3	COMMANDS USED TO COMMUNICATE WITH THE HSC CONTROLLER		4–4
	4.3.1	RUN Command	4–5
	4.3.2	SET Command	4–5
	4.3.3	SHOW Command	4–5
	4.3.4	DIRECT Command	4–5
	4.3.5	PURGE Command	4–7
	4.3.6	CRASH Command	4–7
	4.3.7	Ctrl/Z Command	4–8

CHAPTER 5 CONFIGURING YOUR HSC CONTROLLER 5–1

5.1	OVERVIEW		5–1
	5.1.1	Data Channel Modules	5–2
	5.1.2	Device Specific Configuration Requirements	5–2
		5.1.2.1 EP–ESE Performance Considerations • 5–3	
5.2	CONFIGURING FOR PERFORMANCE		5–4
	5.2.1	DCM Priority	5–4
	5.2.2	Performance Configuration by Type of Disk or Tape Drive	5–6
		5.2.2.1 Adding Drives to Lower Priority DCMs • 5–7	
		5.2.2.2 Multiple Drives on One DCM • 5–8	
		5.2.2.3 Data Access Across Multiple Drives on the HSC Controller • 5–8	
	5.2.3	Device Placement Specifics	5–9
5.3	CONFIGURING FOR CONNECTIVITY		5–10
5.4	DYNAMIC CREDIT MANAGEMENT WITH CRMGR		5–11
5.5	HSC CONTROLLER SATURATION		5–12
	5.5.1	Request Rate	5–12
	5.5.2	Data Rate	5–13
	5.5.3	Tools for Automatic Load Balancing	5–14
5.6	TAPE CONSIDERATIONS		5–14

	5.6.1	**Pipeline Errors and Pipeline Error Reporting**	5–14
	5.6.2	**Block Size Recommendation**	5–16
		5.6.2.1 Display of Tape Configuration • 5–16	
5.7		**HOST LEVEL TOOLS**	5–17
	5.7.1	**Preferred Path Function**	5–17
	5.7.2	**One-Line HSC Commands through DUP**	5–22
5.8		**CONFIGURING THE HSC CACHE OPTION**	5–23
	5.8.1	**Global HSC Controller Cache Commands**	5–25
	5.8.2	**Disk Unit Cache Commands**	5–28
		5.8.2.1 Cache Server Write Allocation Policy • 5–28	
5.9		**CACHE NEED ANALYSIS TOOL (CNAT)**	5–29
	5.9.1	**Overview of CNAT Operation**	5–30
		5.9.1.1 Data Capture • 5–31	
		5.9.1.2 Data Analysis • 5–31	
		5.9.1.3 Interpreting the Results of a CNAT Run • 5–32	
	5.9.2	**How to Run CNAT**	5–33
		5.9.2.1 System Requirements • 5–33	
		5.9.2.2 Preparing the HSC Controller • 5–33	
		5.9.2.3 Beginning the Data Capture • 5–34	
		5.9.2.4 Ending the Data Capture • 5–37	
		5.9.2.5 Converting the Data • 5–37	
		5.9.2.6 Analyzing the Data • 5–38	
	5.9.3	**Interpreting the Results of a CNAT Run**	5–43
		5.9.3.1 Analyzing Different Applications of Cache • 5–44	
		5.9.3.2 Accuracy • 5–44	
5.10		**CACHE PERFORMANCE ANALYSIS TOOL (CPAT)**	5–48
	5.10.1	**System Requirements**	5–48
	5.10.2	**Restrictions**	5–49
	5.10.3	**Overview of CPAT Operation**	5–50
	5.10.4	**Detailed Instructions for Running CPAT**	5–51
		5.10.4.1 Initiating a DSCACHE Run • 5–51	
		5.10.4.2 Displaying the Data Output from a CPAT Run • 5–52	
		5.10.4.3 Interpreting the Results of a CPAT Run • 5–54	
		5.10.4.3.1 Scan Time • 5–55	
		5.10.4.3.2 Disk Removal • 5–56	

5.10.5 **Tuning Cache Parameters** 5–57
5.10.5.1 Overall Evaluation • 5–58
5.10.5.2 Marginal Improvement • 5–58
5.10.5.3 Read Size • 5–58
5.10.5.4 Write Size • 5–59
5.10.5.5 Purge Ratio • 5–59
5.10.6 **Rerun DSCACHE for Optimum Performance** 5–60
5.10.6.1 Order of Analysis • 5–61
5.10.6.2 Analyzing Different Applications • 5–61
5.10.7 **Performing a Deferred Analysis CPAT Run** 5–62
5.10.7.1 Limitations On Running Deferred Analysis • 5–62
5.10.7.2 Connecting to the HSC Controller • 5–63
5.10.7.3 Running DSTAT • 5–63
5.10.7.4 Terminating Data Collection • 5–64
5.10.7.5 Analyzing the Log File Data • 5–64

CHAPTER 6 SETSHO UTILITY 6–1

6.1 **HOW TO RUN SETSHO** 6–2

6.2 **HOW TO EXIT SETSHO** 6–2

6.3 **HOW TO CONCATENATE SETSHO COMMANDS** 6–2

6.4 **SETSHO COMMANDS THAT REQUIRE IMMEDIATE REBOOT** 6–3
6.4.1 **Rebooting From the SETSHO> Prompt** 6–4
6.4.2 **Rebooting From the HSC> Prompt** 6–5

6.5 **SETSHO COMMANDS THAT REQUIRE THE ENABLE REBOOT COMMAND** 6–5
6.5.1 **Using the ENABLE REBOOT Command** 6–6
6.5.2 **Suppressing Informational Messages with the ENABLE REBOOT Command** 6–6
6.5.3 **Using the ENABLE REBOOT Command Remotely** 6–7

6.6	**THE SET COMMANDS**	**6–8**
	SET ALLOCATE DISK	**6–9**
	SET ALLOCATE TAPE	**6–11**
	SET AUTOMATIC_DIT	**6–13**
	SET CI	**6–15**
	SET CREDIT_MANAGER RESET	**6–17**
	SET DATE	**6–19**
	SET DEVICE	**6–21**
	SET DUMP	**6–28**
	SET ERROR	**6–30**
	SET EXCEPTION CLEAR	**6–34**
	SET HOST	**6–36**
	SET ID	**6–38**
	SET LOAD	**6–40**
	SET MAX_FORMATTERS	**6–42**
	SET MAX_TAPES	**6–44**
	SET MEMORY	**6–46**
	SET NAME	**6–48**
	SET ODT	**6–50**
	SET PERIODIC_DIT	**6–52**
	SET POLLER	**6–54**
	SET PROMPT	**6–57**
	SET REQUESTOR	**6–59**
	SET SCOPE	**6–63**
	SET SCT CLEAR	**6–65**
	SET SERVER CACHE	**6–67**
	SET SERVER DISK	**6–69**
6.7	**THE SHOW COMMANDS**	**6–72**
	SHOW ALL	**6–73**
	SHOW CI	**6–75**
	SHOW CONNECTIONS	**6–77**
	SHOW CREDIT_MANAGER	**6–79**
	SHOW DISKS	**6–82**
	SHOW ERROR	**6–84**
	SHOW EXCEPTION	**6–87**
	SHOW HOSTS	**6–90**
	SHOW LINES	**6–92**
	SHOW LOAD	**6–94**
	SHOW MAX_FORMATTERS	**6–96**
	SHOW MAX_TAPES	**6–97**
	SHOW MEMORY	**6–98**
	SHOW ODT	**6–100**
	SHOW POLLER	**6–102**

		SHOW POOL	6–103
		SHOW REQUESTORS	6–104
		SHOW SERVER CACHE	6–106
		SHOW SERVER DISK	6–107
		SHOW SYSTEM	6–108
		SHOW TAPES	6–111
		SHOW VIRTUAL_CIRCUITS	6–113
6.8	**SETSHO MESSAGES**		**6–114**
	6.8.1	**SETSHO Inquiry Messages**	**6–114**
	6.8.2	**SETSHO Success Message**	**6–115**
	6.8.3	**SETSHO Informational Messages**	**6–115**
	6.8.4	**SETSHO Warning Messages**	**6–117**
	6.8.5	**SETSHO Error Messages**	**6–119**
	6.8.6	**SETSHO Fatal Message**	**6–123**

CHAPTER 7 BACKUP UTILITY **7–1**

7.1	**DIFFERENCES BETWEEN HSC CONTROLLER BACKUP AND HOST VMS BACKUP**		**7–1**
7.2	**HOW TO USE THE BACKUP PROGRAM**		**7–3**
	7.2.1	**Enter RUN BACKUP**	**7–3**
	7.2.2	**Enter Disk Unit Number**	**7–3**
	7.2.3	**Enter Tape Unit Numbers**	**7–3**
	7.2.4	**Enter Save-Set Name**	**7–4**
	7.2.5	**Enter Save-Set Expiration Date**	**7–6**
	7.2.6	**Change Expiration Date**	**7–6**
	7.2.7	**Enter Volume Labels**	**7–7**
	7.2.8	**Record Size Transfer**	**7–8**
	7.2.9	**Enter Tape Specifics**	**7–9**
	7.2.10	**No Operator**	**7–10**
	7.2.11	**Mount Tape**	**7–11**
	7.2.12	**Depress Return**	**7–11**
	7.2.13	**Retain Volume**	**7–11**
	7.2.14	**Change Reel**	**7–12**
7.3	**HOW TO USE RESTOR**		**7–13**

	7.3.1	Enter RUN RESTOR	7–13
	7.3.2	Enter Disk Unit Number	7–13
	7.3.3	Enter Tape Unit Numbers	7–13
	7.3.4	Enter Save-Set Name	7–14
	7.3.5	No Operator	7–14
	7.3.6	Mount Tape	7–15
	7.3.7	Press Return	7–15
	7.3.8	Save Set Expired	7–16
7.4	BACKUP/RESTOR EXAMPLES		7–17
7.5	BACKUP MESSAGES		7–20
	7.5.1	BACKUP Success Messages	7–20
	7.5.2	BACKUP Informational Messages	7–20
	7.5.3	BACKUP Warning Messages	7–22
	7.5.4	BACKUP Error Messages	7–23
	7.5.5	BACKUP Fatal Messages	7–27
7.6	RESTOR MESSAGES		7–34
	7.6.1	RESTOR Success Messages	7–34
	7.6.2	RESTOR Informational Messages	7–34
	7.6.3	RESTOR Warning Messages	7–35
	7.6.4	RESTOR Error Messages	7–35
	7.6.5	RESTOR Fatal Messages	7–41
CHAPTER 8	DKCOPY UTILITY		8–1
8.1	HOW TO USE DKCOPY		8–1
	8.1.1	Enter Run DKCOPY	8–2
	8.1.2	Enter Source Unit	8–2
	8.1.3	Enter Target Unit	8–2
	8.1.4	All Input Correct	8–2
8.2	DKCOPY EXAMPLES		8–4
8.3	DKCOPY MESSAGES		8–8

	8.3.1	DKCOPY Fatal Messages	8–8
	8.3.2	DKCOPY Error Messages	8–11
	8.3.3	DKCOPY Informational Messages	8–12
	8.3.4	DKCOPY Success Message	8–12
CHAPTER 9	**COPY UTILITY**		**9–1**
9.1	SPECIAL INFORMATION ABOUT THE SYSTEM DISKETTE		9–1
	9.1.1	Longevity of the System Diskette	9–1
	9.1.2	Write Protecting the System Diskette	9–2
9.2	HOW TO USE COPY		9–2
	9.2.1	Avoid Running COPY Under Heavy Load Conditions	9–2
	9.2.2	Format Target Diskette	9–2
	9.2.3	Enter RUN COPY	9–3
	9.2.4	Enter Source Unit	9–3
	9.2.5	Enter Target Unit	9–3
	9.2.6	Perform Verification Pass	9–4
	9.2.7	Really Perform COPY	9–4
	9.2.8	Mount Source Medium	9–4
	9.2.9	Mount Target Medium	9–5
9.3	COPY EXAMPLES		9–5
9.4	COPY MESSAGES		9–6
	9.4.1	COPY Informational Messages	9–6
	9.4.2	COPY Warning Messages	9–6
	9.4.3	COPY Error Messages	9–8
	9.4.4	COPY Fatal Message	9–9

CHAPTER 10	VERIFY UTILITY		10–1
10.1	HOW TO USE VERIFY		10–1
	10.1.1	Enter RUN VERIFY	10–2
	10.1.2	Enter Disk Unit Number	10–2
	10.1.3	Was Unit Just Formatted	10–2
	10.1.4	Print Informational Messages	10–3
	10.1.5	Report Transient Errors by Block	10–3
10.2	VERIFY EXAMPLE		10–3
10.3	VERIFY MESSAGES		10–6
	10.3.1	VERIFY Informational Messages	10–6
	10.3.2	VERIFY Warning Messages	10–12
	10.3.3	VERIFY Fatal Messages	10–16
CHAPTER 11	RXFMT UTILITY		11–1
11.1	HOW TO USE RXFMT		11–1
	11.1.1	Avoid Running RXFMT Under Heavy Load Conditions	11–2
	11.1.2	Enter Run RXFMT	11–2
	11.1.3	Enter Unit to Format	11–2
	11.1.4	Really Perform Format	11–2
	11.1.5	Mount Diskette	11–3
11.2	RXFMT EXAMPLE		11–4
11.3	RXFMT MESSAGES		11–4
	11.3.1	RXFMT Status Messages	11–5
	11.3.2	RXFMT Informational Messages	11–5
	11.3.3	RXFMT Warning Messages	11–6
	11.3.4	RXFMT Error Messages	11–7
	11.3.5	RXFMT Fatal Message	11–7

CHAPTER 12 VTDPY UTILITY 12–1

12.1 HOW TO RUN VTDPY 12–1
12.1.1 Using the VTDPY Control Keys 12–2

12.2 HOW TO INTERPRET THE VTDPY DISPLAY FIELDS 12–4

12.3 VTDPY MESSAGES 12–17
12.3.1 VTDPY Error Messages 12–17
12.3.2 VTDPY Fatal Messages 12–17

CHAPTER 13 SCTSAV UTILITY 13–1

13.1 RESTRICTIONS ON RUNNING SCTSAV 13–2

13.2 HOW TO RUN SCTSAV 13–3

13.3 SCTSAV EXAMPLE 13–4

13.4 RECOVERING FROM A FATAL SCTSAV ERROR 13–4

13.5 SCTSAV MESSAGES 13–5
13.5.1 SCTSAV Informational Messages 13–5
13.5.2 SCTSAV Inquiry Messages 13–6
13.5.3 SCTSAV Warning Messages 13–6
13.5.4 SCTSAV Fatal Messages 13–6

APPENDIX A COMMAND PROMPT AND TTDR ERRORS A–1

A.1 KMON PROMPT A–1

A.2 KMON PROMPT MESSAGES A–2

A.2.1 KMON Prompt Informational Message A–2
A.2.2 KMON Prompt Fatal Messages A–2

A.3 DIRECT ERROR MESSAGES A–7

A.4 TTDR ERROR MESSAGES A–7

APPENDIX B EXCEPTION CODES AND MESSAGES B–1

B.1 SINI-E ERROR PRINTOUT B–4

B.2 SUBMITTING A SOFTWARE PERFORMANCE REPORT B–5

B.3 EXCEPTION MESSAGES B–5

GLOSSARY Glossary–1

INDEX Index–1

EXAMPLES

5–1 Sample CNAT Run 5–46
5–2 Sample CPAT Run 5–57
6–1 SET ALLOCATE DISK Command 6–10
6–2 SET ALLOCATE TAPE Command 6–12
6–3 SET AUTOMATIC_DIT Command 6–14
6–4 SET CI Command for Node 12 6–16
6–5 SET CI Command for All Nodes 6–16
6–6 Using the SET CREDIT_MANAGER RESET Command 6–18
6–7 SET DATE command 6–20
6–8 SET DEVICE Dn NOHOST_ACCESS Command 6–25
6–9 SET DEVICE Dn W_UPDATE Command 6–27

6–10 SET DUMP Command 6–29
6–11 SET ERROR Command 6–32
6–12 SET EXCEPTION CLEAR Command 6–35
6–13 SET HOST Command 6–37
6–14 SET ID Command 6–39
6–15 SET LOAD Command 6–41
6–16 SET MAX_FORMATTERS Command 6–43
6–17 SET MAX_TAPES Command 6–45
6–18 SET MEMORY Command 6–47
6–19 SET NAME Command 6–49
6–20 SET ODT Command 6–51
6–21 SET PERIODIC_DIT Command 6–53
6–22 SET POLLER Command 6–55
6–23 SET PROMPT Command 6–58
6–24 SET REQUESTOR Command 6–61
6–25 SET SCOPE Command 6–64
6–26 SET SCT CLEAR Command 6–66
6–27 SET SERVER CACHE/CACHE_SIZE_THRESHOLD=4 6–68
6–28 SET SERVER DISK/DRIVE_TIMEOUT=4 6–70
6–29 SET SERVER DISK/VARIANT 6–71
6–30 SET SERVER DISK/CACHE 6–71
6–31 SHOW CI Screen Display 6–76
6–32 SHOW CONNECTIONS Screen Display 6–78
6–33 SHOW CREDIT_MANAGER Screen Display 6–80
6–34 SHOW DISKS Screen Display 6–83
6–35 SHOW Dn Screen Display 6–83
6–36 SHOW ERROR Screen Display 6–85
6–37 SHOW ERROR Screen Display After Entering a SET ERROR FATAL Command 6–86
6–38 SHOW ERROR After a SET ERROR ERROR/PERMANENT Command 6–86
6–39 SHOW EXCEPTION Screen Display 6–88
6–40 SHOW EXCEPTION Screen Display 6–89
6–41 SHOW HOSTS Screen Display 6–91
6–42 SHOW LINES Screen Display 6–93
6–43 SHOW LOAD Screen Display 6–95

6–44	SHOW MAX_FORMATTERS Screen Display	6–96
6–45	SHOW MAX_TAPES Screen Display	6–97
6–46	SHOW MEMORY Screen Display	6–99
6–47	SHOW ODT Screen Display	6–101
6–48	SHOW POLLER Screen Display	6–102
6–49	SHOW POOL Screen Display	6–103
6–50	SHOW REQUESTORS Screen Display	6–105
6–51	SHOW SERVER CACHE Screen Display	6–106
6–52	SHOW SERVER DISK Screen Display	6–107
6–53	SHOW SYSTEM Screen Display	6–109
6–54	SHOW TAPES Screen Display	6–112
6–55	SHOW VIRTUAL_CIRCUITS Screen Display	6–113
7–1	BACKUP with an RA80 Disk Drive	7–17
7–2	BACKUP with an RA81 Disk Drive	7–18
7–3	RESTOR with a 6250 BPI Tape to RA81 Disk Drive	7–19
8–1	Using DKCOPY to Copy From Disk 1 to Disk 2	8–4
8–2	Correcting Disk Unit Numbers in DKCOPY	8–5
8–3	Aborting DKCOPY	8–6
8–4	Copy Operation Error	8–6
9–1	COPY Session of an RX33	9–5
10–1	VERIFY Scan of an RA80	10–4
11–1	Typical RXFMT Run	11–4
13–1	Sample SCTSAV Utility Run	13–4
B–1	Crash Dump Example	B–2
B–2	SINI-E Exception Code	B–4

FIGURES

1–1	Front View of the HSC70 Controller	1–2
1–2	Basic Cluster Configuration	1–5
1–3	Filter Location	1–12
2–1	Location of AC Power Switch	2–2
2–2	Location of DC Power Switch	2–3
2–3	Secure/Enable Switch	2–5
2–4	Operator Control Panel Switches and Indicators	2–6
2–5	OCP Fault Code Displays	2–10

3–1 RX33 Disk Drive 3–2
3–2 RX33 Disk Drive Location 3–3
5–1 Front View of HSC Controller Card Cage 5–6
5–2 Cache "Hit" Eliminates Mechanical Delays in an I/O Operation 5–24
5–3 WRITE_THRESHOLD 5–27
12–1 VTDPY Display 12–5

TABLES

1 HSC Controller User Guide Conventions xx
2 Related Documentation xxi
3 Telephone and Direct Mail Orders xxii
1–1 Configuration of HSC Controller Models 1–3
1–2 Error Message Codes 1–11
4–1 Control Character and Special Key Functions 4–2
5–1 Data Channel Module Description 5–2
5–2 DCM Utilization 5–5
5–3 Configuration of Disk and Tape Drives 5–7
6–1 SETSHO Error Levels 6–31
6–2 SETSHO Error Levels 6–84
6–3 SETSHO Message Codes 6–114
7–1 Differences Between HSC Controller BACKUP and Host (VMS) BACKUP 7–2
12–1 VTDPY Control Keys 12–3
12–2 Process Description 12–11
12–3 VTDPY Disk Drive Heading Definitions 12–14
12–4 Disk Drive Status Codes 12–14
12–5 VTDPY Tape Drive Heading Definitions 12–16
12–6 Tape Drive Status Codes 12–16
B–1 Normal Operation Status Codes for K-Requestors B–3

Preface

Structure of This Document

This document contains user information for the HSC controller, including background information, how to boot the HSC, how to operate the console, and how to use the operator control panel (OCP). In addition, separate chapters describe each of the utilities you can run. A glossary and an index are at the back of this document.

Intended Audience

This document is for the system administrators who oversee operations of an HSC controller and the operators who run utilities on the HSC controller.

Conventions Used in This Document

Table 1 lists the conventions used in the text of this manual.

Table 1: HSC Controller User Guide Conventions

Convention	Meaning
DXn:	Represents the logical device name for a drive comprising the RX33 load device where *n* is 0 or 1.
Dn	Represents a host-accessible disk drive where *n* is a decimal number from 0–4094.
Tn	Represents a host-accessible tape drive where *n* is a decimal number from 0–32767.
[SIZE=2400,DENSITY=6250]	In the context of a sample prompt from a utility or device integrity test, square brackets indicate a default. In the context of a user input description, square brackets indicate the enclosed item is optional.

Ellipsis	A vertical series of periods (ellipsis) indicates partial omission of data the system could display in response to a particular command or data that a user could enter. For example:
	`SETSHO> SET NAME BULL_RUN`
	`SETSHO> SHOW HOSTS`
	.
	.
	.

T2 . . .	A horizontal ellipsis indicates additional parameters, values, or information can be entered.
Quotation mark	The term quotation mark refers to double quotation marks (").
Apostrophe	The term apostrophe (') refers to a single quotation mark.

Table 1 (Continued): HSC Controller User Guide Conventions

Convention	Meaning
Numbers	Unless otherwise noted, all numbers in the text are decimal. Nondecimal radices—binary, octal, or hexadecimal—are explicitly indicated in examples and descriptions.
HSC> prompt	Used to refer to the keyboard monitor (KMON) prompt at which commands are issued to run programs. The term "KMON prompt" is used only in Appendix A, which describes the error messages associated with this prompt.
RX33 diskette	Refers to the load medium containing HSC controller software that you load into the HSC controller.
RX33 drive(s)	Refers to the load device (consisting of two drives) from which the HSC controller software is loaded.

Related Documentation

Table 2 lists related documents that are available to users of the HSC controller:

Table 2: Related Documentation

Title of Document	Description	Order Number
HSC Controller Installation Manual	Contains installation information and procedures. After installation, this manual can be used as a general reference.	EK–HSCMN–IN–002
HSC Controller Service Manual	Information necessary for effective service and maintenance of the HSC controllers.	EK–HSCMA–SV–003
HSC Controller Pocket Reference Guide	This document summarizes important information on the HSC controller for quick reference during servicing and operation.	EK–HSCPK–RC–004

The *HSC Controller User Guide* can be ordered by telephone or direct mail order. (See Table 3 for telephone numbers and addresses.)

Table 3: Telephone and Direct Mail Orders

Your Location	Call	Contact
Continental USA, Alaska, or Hawaii	800-DIGITAL	Digital Equipment Corporation P.O. Box CS2008 Nashua, New Hampshire 03061
Puerto Rico	809-754-7575	Local DIGITAL subsidiary
Canada	800-267-6215	Digital Equipment of Canada Attn: DECdirect Operations KAO2/2 P.O. Box 13000 100 Herzberg Road Kanata, Ontario, Canada K2K 2A6
International	—	Local Digital subsidiary *or* approved distributor
Internal[1]	—	SDC Order Processing—WMO/E15 *or* Software Distribution Center Digital Equipment Corporation Westminster, Massachusetts 01473

[1]For internal orders, you must submit an Internal Software Order Form (EN–01740–07).

Chapter 4

How to Operate the HSC Controller

This chapter explains how to use the console terminal and HSC software commands to operate the HSC controller.

4.1 How to Use the Console Terminal

The HSC controller has a programmable interface to a dedicated console terminal. This terminal is shipped as part of the HSC subsystem and should remain connected to the HSC controller, except when the HSC controller is attached to a cluster console.

The HSC software sets up the appropriate communications parameters for the terminal interface. The baud rate is set to 9600 baud. Once you load the HSC software, you can run the device integrity tests and utilities from the console terminal.

CAUTION

Always operate the HSC controller with the Secure/Enable switch in the SECURE position. If you press the Break key on the terminal when the Secure/Enable switch is in the ENABLE position, the software may branch immediately to a hardware-based debugging routine.

This routine interrupts the operation of the MSCP server, halts all HSC controller activity, and requires a reboot of the HSC controller. The Break key is ignored when the Secure/Enable switch is in the SECURE position.

4.1.1 Using Control Characters or Special Keys at the HSC> Prompt

The HSC> prompt must be displayed before entering commands and running utility programs on the HSC controller. Until this prompt is displayed, the console emits a beep when you type any key on the keyboard. To get the HSC> prompt and activate the console terminal keyboard, enter Ctrl/Y.

At the HSC> prompt, you can enter commands or use the special control characters shown in Table 4–1 to communicate with the HSC controller. Control characters are generated by simultaneously entering the Control key and the letter following the slash (/).

Table 4–1: Control Character and Special Key Functions

Control Character	Special Key	Function
Ctrl/C		Aborts the HSC software utility or diagnostic program currently running.
	DEL	Deletes the last character entered. Echoes as a backslash character and a repeat of the deleted character on a hard-copy terminal. Use the SET [NO]SCOPE command to define the terminal type.
Ctrl/O		Suspends the output display until the next HSC> prompt is displayed or Ctrl/O is reentered.
Ctrl/P		Starts the maintenance diagnostic ODT program. ODT is documented in the *HSC Controller Service Manual*. If you accidentally start ODT, immediately enter ;P to resume normal operation.
Ctrl/Q		Resumes output to the terminal following the execution of a Ctrl/S. Does not echo.
Ctrl/R		Repeats the current line and its corrections. Use Ctrl/R to check the accuracy of a line containing numerous corrections.

Table 4–1 (Continued): Control Character and Special Key Functions

Control Character	Special Key	Function
Ctrl/S		Stops output to the terminal. Enter Ctrl/Q to restart.
Ctrl/U		Erases all input characters on the line and repeats the last prompt.
Ctrl/Y		Aborts the currently running HSC software utility or diagnostic program and alerts the HSC controller to accept a command. The HSC controller responds with the command prompt, HSC>.
Ctrl/Z		Erases what has been typed on the terminal. Signals the end of input, and disables further input over the console terminal until Ctrl/Y is entered.

The HSC controller does not broadcast error messages to the terminal while any prompt is being displayed. Therefore, the HSC software implements a 5-minute timeout period for every prompt. After waiting 5 minutes for input, the software executes an automatic Ctrl/C to cancel the program it is currently running. The following prompt is displayed:

```
TTDR-F Input Timeout
```

After a program completes, you may have to reenter Ctrl/Y to display the HSC> prompt.

4.2 Quick Disconnect

The HSC software includes a quick disconnect feature to disconnect the online disk drives in the event of a software failure.

If an unrecoverable error is detected and the HSC controller begins to crash, the HSC software sends commands to all disk drives to disconnect themselves from the HSC controller. In the case of dual-ported disk drives, the disconnected drives become immediately available to the alternate port. This allows very rapid failover from one HSC controller to the alternate HSC controller.

The quick disconnect feature is initiated by all IOT, NXM, and MMU HSC controller crashes.

There are other types of failure that do not cause the drives to quick disconnect. Failures that rely on the drives to timeout the HSC controller according to the drive timeout value are:

power failure
reboot with the OCP Init switch
trap through 114 memory parity error
starting Micro-ODT with the Break key

You can induce quick disconnect of the drives by entering the CRASH command as described in Section 4.3.

NOTE

> For failure types which do not invoke quick disconnect, the maximum time for the drive to become available at the alternate HSC is twice the drive timeout interval, which is set to two seconds by default.

4.3 Commands Used to Communicate with the HSC Controller

You can enter any of the following commands at the HSC> prompt:

- RUN
- SET
- SHOW
- DIRECT
- PURGE
- CRASH
- Ctrl/Z (exit)

4.3.1 RUN Command

The RUN command initiates the specified program. This program can be a utility or an inline device integrity test. The following is an example of how to run the SETSHO utility:

```
HSC> RUN SETSHO
```

4.3.2 SET Command

The SET command invokes the SETSHO utility and allows you to set a system parameter. For example:

```
HSC>  SET NAME HSC006
```

This command sets the HSC system name to *HSC006*. Refer to Chapter 6 for information on the SETSHO utility and possible error messages.

4.3.3 SHOW Command

The SHOW command invokes the SETSHO utility and allows you to show a system parameter. The following is an example of how to show system parameters:

```
HSC> SHOW SYSTEM
```

This command displays HSC system parameters such as system date and time, boot time, and system name. Refer to Chapter 6 for information on the SETSHO utility and possible error messages.

4.3.4 DIRECT Command

The DIRECT command displays the directory of the boot diskette containing HSC software. If you do not specify the disk drive containing the software diskette, the default is the drive used for the last software boot. To obtain the directory from a specified drive, specify the drive as shown in the DIRECT command example that follows.

The logical device names are:

- DX0: (RX33 on the left.) (Refer to Figure 3–1.)
- DX1: (RX33 on the right.) (Refer to Figure 3–1.)
- LB: or SY: (device used for the most recent boot—stands for "Last Boot" or "System")

The following is an example of the DIRECT command:

```
HSC> DIRECT DX0:
DIRECT-S  Directory of LB: on 31-Jan-1991 16:28:59.80
Name   .Ext      Size     Pos      Date
2NDTAP.VER         1       38     18-Jan-91
BACKUP.UTL        58       39     18-Jan-91
CACHE .SYM        25       97     18-Jan-91
CERF  .SYM        30      122     18-Jan-91
< Unused >        27      152
CIMGR .SYM        31      179     18-Jan-91
COPY  .UTL        14      210     18-Jan-91
CRASH .UTL         1      224     18-Jan-91
DEMON .SYM        16      225     18-Jan-91
DFECC .SYM         4      241     18-Jan-91
DIRECT.UTL         4      245     18-Jan-91
DKCOPY.UTL        18      249     18-Jan-91
DKRFCT.UTL        29      267     18-Jan-91
DKUTIL.UTL        43      296     18-Jan-91
DMPPAR.DAT        12      339     18-Jan-91
DMPPAR.UTL        11      351     18-Jan-91
DSTAT .UTL         9      362     18-Jan-91
DUP   .SYM        16      371     18-Jan-91
< Unused >        30      387
EXEC  .INI        59      417     18-Jan-91
FORMAT.UTL        27      476     18-Jan-91
< Unused >        12      503
HSCODT.INI        40      515     18-Jan-91
ILCACH.DIA         7      555     18-Jan-91
ILDISK.DIA        43      562     18-Jan-91
ILEXER.DIA        56      605     18-Jan-91
ILMEMY.DIA         4      661     18-Jan-91
ILMTST.DIA         1      665     18-Jan-91
ILRX33.DIA         6      666     18-Jan-91
ILTAPE.DIA        48      672     18-Jan-91
ILTCOM.DIA        20      720     18-Jan-91
.
.
.
Total of 1670 blocks in 71 files, 692 Free
```

Refer to Appendix A for the DIRECT command error messages.

4.3.5 PURGE Command

The PURGE command deletes all internally stored programs from program memory. Within program memory, a certain location is allocated to the recoverable memory list. When a program is run, the HSC software looks in the recoverable memory list to see if this program is stored. If the program is stored, it can run directly from memory. It does not require reloading from the load device, thus saving load time.

The PURGE command clears the recoverable memory list and returns that space to the free memory list. The PURGE command is rarely used. However, there are two instances when it can be used:

- When a faulty system diskette loads a bad version of the program (an extremely rare occurrence)
- After applying a patch to a utility program, to purge the unpatched copy out of memory.

A purge of the recoverable memory list is automatically executed if the free memory list is full. This makes the recoverable memory list area available to free memory.

The following is an example of the PURGE command:

```
HSC>PURGE
```

There are no error messages associated with the PURGE command.

4.3.6 CRASH Command

The CRASH command causes the HSC controller to crash, thus performing a quick disconnect of the disk drives that are online to the HSC. For dual-ported disk drives, this causes a quick failover to the alternate HSC controller. This is the most convenient way to fail over the drives when failover is desired. Refer to Section 4.2 for a description of the quick disconnect feature.

4.3.7 Ctrl/Z Command

Enter Ctrl/Z at the HSC> prompt to exit keyboard control. Ctrl/Z terminates keyboard input mode; the HSC> prompt is not printed and keyboard input causes the console to beep (see Section 4.1.1). Ctrl/Z terminates any program currently running. Enter Ctrl/Y to redisplay the HSC> prompt.

The following is an example of the EXIT command:

```
HSC> Ctrl/Z
```

There are no error messages associated with the EXIT command.

Chapter 5

Configuring Your HSC Controller

This chapter contains information about installing and configuring your HSC controller for optimum performance and/or configuration flexibility in your VAXcluster.

5.1 Overview

The physical configuration of an HSC subsystem has a significant impact on performance.

When you are choosing drives and you want optimal performance, consider the HSC subsystem workload. Each attached drive and storage array has different benefits. Depending on your primary need, a "best choice" exists for each application.

You may configure your subsystem in accordance with device speed and data channel module (DCM) priority to achieve maximum performance, or configure disk and tape devices on any DCM necessary to achieve your connectivity requirements.

5.1.1 Data Channel Modules

The HSC controller interfaces to disk/tape drives through the following DCMs:

- K.sdi (HSC5X–BA)
- K.sti (HSC5X–CA)
- K.si (HSC5X–DA)
- K.si8 (HSC9X–FA)

The K.si module may be configured to handle either disk or tape drives, but not both simultaneously. Use the SETSHO command SET REQUESTOR to load tape or disk microcode.

The HSC9X–FA module handles eight SDI disk drives and has the same performance capabilities as the other DCMs. No measurable performance difference is found between the modules.

Table 5–1 below describes the drive configuration of the modules.

Table 5–1: Data Channel Module Description

Module Type	Part Number	Description
K.sdi	HSC5X–BA	4-port disk only
K.sti	HSC5X–CA	4-port tape only
K.si	HSC5X–DA	4-port disk or tape
K.si8	HSC9X–FA	8-port disk only

The ports on an individual DCM have equal priority, but each DCM is located in the backplane in order of priority (see Section 5.2.1).

5.1.2 Device Specific Configuration Requirements

The TA90, TA90E, and TA91 tape drives require HSC5X–DA modules.

The EP–ESE (Enhanced Performance ESE) requires the use of the HSC5X–DA or HSC9X–FA modules. Configuration of the EP–ESE on an HSC5X–BA will cause the storage element to operate at the unenhanced performance level of approximately 300 I/O requests per second. Due to the high request rate of the EP–ESE, its placement on the HSC5X–DA or the HSC9X–FA with other disk drives could adversely affect its performance. However, this would be a connectivity configuration option for some customers.

To shadow Enhanced Performance ESE (EP–ESE) storage elements in Enhanced Performance mode, VMS Volume Shadowing Phase II (Host-Based Volume Shadowing) must be used. If these drives are shadowed with Shadowing Phase I (Controller-Based Volume Shadowing), they are automatically removed from Enhanced Performance mode and operated in unenhanced performance mode.

5.1.2.1 EP–ESE Performance Considerations

When transferring data to a single ESE in normal mode, the HSC controller can generate about 300 requests/second. With a single ESE in enhanced mode, this HSC I/O throughput rate can be pushed to around 1200 request/second. Since a single enhanced mode ESE can generate close to the maximum HSC I/O throughput rate, a user seeking maximum performance on a very busy system should consider the following configuration guidelines:

NOTE

These guidelines apply **only** to configurations under which enhanced mode ESEs are generating very high throughput rates. "Busy" in the following guidelines refers to an ESE that is generating over 1000 (1 to 4 block) requests per second or an equivalent amount of larger-sized requests per second.

- Configure only one "busy" enhanced mode ESE to a K.si DCM. Since an HSC DCM can transfer data on only one port at a time, performance on other disk drives connected to the same DCM as a busy enhanced mode ESE might be degraded. If the ESE is transferring near the maximum HSC I/O throughput rate, try to configure the ESE with drives that will not be accessed very frequently.
- Connect no more than two "busy" enhanced mode ESEs to a single HSC controller. Since a single ESE can generate nearly the maximum HSC I/O throughput, the number of busy enhanced mode ESEs on a single HSC controller should be limited for maximum HSC performance.

Please note that the above guidelines are specifically recommended for an HSC controller and ESE subsystem, with the HSC having very high I/O throughput rates. If an HSC is not experiencing extremely high I/O request rates, there is no need to limit the number of ESEs per DCM or per HSC controller.

5.2 Configuring for Performance

If subsystem performance is your primary concern, configure your system in accordance with device speed and data channel module (DCM) priority.

If you have an HSC40 or HSC60 controller, you should find little or no difference between configuring for performance and configuring for connectivity. That is, you can configure your HSC controller for connectivity and experience no significant change in performance.

5.2.1 DCM Priority

The data bus is a high-speed bus (13.3 megabytes per second), but it must be multiplexed between the different DCMs. If two DCMs are contending for the data bus at the same time, the lower priority DCM must wait until the higher priority DCM has finished transferring data.

DCM priority ascends from DCM number 2, with the lowest priority, through the highest DCM number on the HSC controller. For module utilization on the HSC controller, see Table 5–2 and Figure 5–1.

Table 5–2: DCM Utilization

Priority	Slot Number	Requestor Number	Ports
Highest	3	9	4
.	4	8	4
.	5	7	4
.	6	6	4 or 8 [1]
.	7	5	4 or 8 [1]
.	8	4	4 or 8 [1]
.	9	3	4 or 8 [1]
Lowest	10	2	4

[1]8-port DCMs are supported in HSC60 and HSC90

Figure 5–1 shows the relationships between module, backplane slot number, and DCM "requestor" number.

The abbreviations and descriptions of the HSC controller card cage model are explained below:

Abbreviation	Description
Mod	Module type
Bkhd	Bulkhead (where SDI/STI connections to that DCM are made)
Req	"Requestor" (DCM)
Slot	Backplane slot in the card cage that contains the DCM
4k or 4/8k	4-port or 4/8-port DCM

Figure 5–1: Front View of HSC Controller Card Cage

Mod	L0118-00 Rev: CI Port Link	L0109-YA Rev: CI Port Buffer	L0124-00 Rev: CI Port Processor	L0121-AA Rev: Memory Cache	4K	4/8K	4/8K	4/8K	4/8K	4K	4K	4K	L0123-AA Rev: Memory 4	L0111-Y Rev: J-11 I/O Cont. Proc.
Bkhd					A	B/H	C/J	D/K	E/L	F	M	N		
Req			1		2	3	4	5	6	7	8	9		0
Slot	14	13	12	11	10	9	8	7	6	5	4	3	2	1

CXO-3130A

5.2.2 Performance Configuration by Type of Disk or Tape Drive

To configure an HSC controller for maximum performance, connect the device with the higher SDI data transfer rate to the higher priority DCM, and the device with the lower data transfer rate to the lower priority DCM. Note that SDI transfer rate is an inherent device characteristic and cannot be changed by configuring the device on a different DCM. Table 5–3 shows the recommended configuration of disk and tape drives.

Table 5–3: Configuration of Disk and Tape Drives

Device	Relative Speed	Priority
Caching tape drives (TA9x, SA100/TA857)	Fastest	Highest
RA90 or RA92 disk drive	.	.
RA73 disk drive	.	.
ESE or EP–ESE storage element	.	.
RA82 disk drive	.	.
RA81 disk drive	.	.
RA71 or RA72 disk drive	.	.
RA60 disk drive	.	.
RA70 disk drive	.	.
RA80 disk drive	.	.
Non-TA90 tape drives	Slowest	Lowest

NOTE

The ESE storage element is rated lower in this list than the RA90 or RA92 disk drives. Although the spiral transfer rate of the ESE storage element is faster, the peak transfer rates of the RA90 and RA92 disk drives are actually slightly faster than the ESE storage element.

Actively utilizing fewer ports per DCM may also improve performance.

When possible, leave blank slots to allow for add-on drives without having to move existing cables.

5.2.2.1 Adding Drives to Lower Priority DCMs

If device speed/DCM priority order is not followed, the software in the HSC controller adjusts internal operating parameters to compensate. As a result, data transfer from disks may be delayed. For the recommended configuration for maximum performance, refer to Table 5–3.

Performance can be affected if drives with high transfer rates are added to lower priority DCMs. Transfers from higher priority modules may sufficiently delay the lower priority transfers so that drives on lower priority modules would have little opportunity to transfer and may eventually time out.

5.2.2.2 Multiple Drives on One DCM

Each DCM can manage up to four or eight disk drives. However, at any one time, only one of the four or eight drives may transfer data.

The possibility of channel contention increases if both of the following conditions are present:

- Transfer size is very large
- Seek and rotation time is very low

When the 8-port DCM is configured with eight active disk drives, channel contention may occur, impacting performance. For maximum performance, configure less frequently accessed disk drives or four active disk drives and four dual-port path connections on the 8-port DCMs (HSC9X–FA). (Dual porting is the ability of a disk or tape drive to be statically accessed by two controllers. Dual porting decreases the load on the HSC9X–FA module during normal operation.)

Utilization of the VMS preferred-path function will allow the maintenance of the customer's preferred configuration on reboot. See the *Release Notes for VMS V5.4*.

If frequently accessed disk drives (attached to an 8-port DCM) are also designated to be cached by the HSC controller, the concern about possible channel contention is greatly reduced. In such a configuration, frequently accessed information from those drives will reside in HSC cache, thus reducing the overall data requests to the drives.

5.2.2.3 Data Access Across Multiple Drives on the HSC Controller

You can spread data access across multiple devices, eliminating the bottleneck caused by many requests queuing to a single drive.

Examination of many systems has shown that nearly 50 percent of all I/O requests access only 1 to 3 percent of the storage capacity. Nearly 80 percent of the requests access 20 percent of the total storage capacity. (The exact values of 1 to 3 percent, 20 percent, and 80 percent may vary from one system to another, but can be used as guidelines in an initial configuration.)

For best possible performance, configure your system with 1 to 3 percent of the total capacity dedicated to ESE storage elements, 20 percent to RA70 disk drives, and 80 percent to RA90 or RA92 disk drives. Additionally, in appropriate applications, a significant improvement in response time may be achieved by utilizing HSC cache for frequently accessed blocks.

5.2.3 Device Placement Specifics

1. Disks shadowed with Controller-Based Shadowing:

   For improved controller-based shadow copy performance, configure the individual members of a controller-based shadow set on separate DCMs. This will prevent the shadow write accesses from queuing on a single DCM, which can result in degraded performance during the shadow copy process. If your I/O profile contains frequent writes with large byte counts (averaging over 8 kilobytes), configuring controller-based shadow set members on separate DCMs will also provide better performance during normal shadowing operations.

2. Paging, swapping, and image activation disk drives:

   Disk drives involved in paging, swapping, and image activation activities typically access data with large transfer sizes; therefore, they should be located on separate DCMs.

3. Applications accessing data in large transfer sizes:

   If you have an application that issues requests with a large transfer size, place the data drive on a relatively idle DCM. This will optimize the I/O performance.

5.3 Configuring for Connectivity

If device connectivity is of primary importance, you may configure disk and tape devices on any DCM necessary to achieve your connectivity requirements. You may configure without regard to the device speed and DCM priority guidelines shown in Table 5–3. This configuration flexibility may be at the expense of optimized performance.

To assure all devices have access to the data bus during transfers, devices that are NOT configured according to device speed/DCM priority are allocated more bandwidth than they would have required if they were configured according to speed/priority. Therefore, the total bandwidth is under-utilized, thus achieving less than maximum performance, but permitting a wide variety of configuration options.

For configuration flexibility, slower tape drives may be configured in the higher priority slot with a TA90 or TA91 tape drive, without causing data bus overrun error messages. A performance penalty may be apparent if the slower tape drive is utilized during heavy subsystem activity.

NOTE

> Configuring the disk and tape devices **not** in conformance to device speed and DCM priority has an adverse effect on HSC70 and HSC90 controller performance. There is no significant performance impact with HSC40 and HSC60 controllers.

5.4 Dynamic Credit Management with CRMGR

The Dynamic Credit Manager (CRMGR) automatically maximizes the availability of credits to connections based on demand rather than making initial, static allocations when connections are first established. To accomplish dynamic allocation, the CRMGR allocates fewer initial connection credits so as to keep a larger credit pool available for connections that require additional credit service. Operation of the CRMGR does not require intervention on the part of the user.

Under the CRMGR, disk connections are initially granted 12 credits and tape connections receive 6 credits. A disk connection can be granted up to 127 credits provided there are enough credits available in the credit pool. Similarly, a tape connection can be granted up to 30 credits. By default, the CRMGR is always enabled. The intent is that it should do its job invisibly, and require little or no action from the user. The CRMGR has three possible states:

- ENABLED. This is the default state. In this state the CRMGR performs its normal function of monitoring, granting, and removing credits to and from connections based on their activity.
- RESET. When the CRMGR enters RESET mode, it restores each connection to its default credits by taking credits away until the default is reached. Connection and server counters are also reset. Following completion of RESET activities, the CRMGR enters ENABLED mode. The RESET mode is designed as a tool to restore credit counts and the connection and server counters to a known state.
- SPECIAL. This mode is invoked if, when attempting to open a new connection, the CIMGR finds that there are insufficient credits to open a connection with at least default credits. In this mode, the CRMGR removes one credit from each connection in round-robin fashion until enough credits are available. SPECIAL mode is also invoked from the ENABLED mode in CRMGR in the unlikely event that it detects that the total of allocated credits has exceeded the server's maximum credits.

The CRMGR is always in the ENABLED mode. However, the SETSHO utility has commands to provide minimal control of the CRMGR modes and to display the state of the active connections. The applicable SETSHO commands are SET CREDIT_MANAGER RESET and SHOW CREDIT_MANAGER. Refer to Chapter 6 of the *HSC User Guide* for detailed information on using these commands.

5.5 HSC Controller Saturation

HSC controller saturation is an unlikely event in most user environments. Saturation depends on the byte count of the transfer requests. The HSC controller can process 1300 single-block requests per second. When the HSC controller receives a request, it spends a certain amount of time processing and setting up the appropriate data structures. The number of requests the HSC controller can perform is determined by how long it takes the HSC controller to process a request.

Large byte count transfers may limit the request rate because of the resulting data rate. For example, transfers of 50 kilobytes could not be performed at an HSC controller rate of 1000 requests per second because the resulting data rate would be 50 megabytes per second, which is far in excess of the maximum CI bus rate.

Since the majority of the requests issued by the VMS operating system are 4 kilobytes or less, data rate and fragmentation are not a concern; so the maximum rate of 1300 requests per second for an HSC controller is possible. This rate does not take into account request bursts or response time.

5.5.1 Request Rate

Request rate is the raw number of work requests per second to the HSC controller.

Request rate is not generally a bottleneck. Analysis of many workload profiles has shown that typical VMS I/O workloads generate 10 to 15 requests per second per VUP of CPU power. For example, a typical workload from a VAX 8650 with 6 VUPs would generate approximately 60 to 90 requests per second.

To monitor request rate at an individual HSC controller, use the metric "Work Requests/Sec" shown in the VTDPY display. Analysis of workload profiles has shown that the response time typically begins to increase significantly after reaching 80% of the maximum request rate. Based on the typical VMS workload mix of variable request sizes and occasional request bursts, best performance would be seen at a request rate of up to approximately 800 requests per second. If your request rate is significantly greater than 800 as shown by this VTDPY metric, you may want to reduce it by moving the busier drives to another HSC controller. (To determine which are the busier drives, use the tools described in Section 5.5.3.)

Another VTDPY metric which can be used to monitor HSC controller performance is the "% Idle" shown in the VTDPY display. To provide a reserve of CPU processing power for peaks and bursts in the I/O workload, keep this metric no less than 20% idle. To increase the percentage of idle time, move busier drives to another HSC controller.

5.5.2 Data Rate

Data rate is the amount of data transferred over the CI (computer interconnect) measured in megabytes per second.

The amount of available CI bandwidth varies depending on the arbitration scheme used in the cluster. (The arbitration scheme is a cluster communication mechanism which governs contention among host and HSC nodes for the CI bus.) There are two arbitration schemes: 16-node and 32-node. Clusters in which all CI nodes are numbered between zero and 15 may use either the 16- or 32-node arbitration scheme; clusters in which any CI nodes are numbered from 16 to 31 must use 32-node arbitration. Your Digital Services representative can determine which arbitration scheme is used in your cluster. There is a slight decrease in available bandwidth using the 32-node scheme.

For maximum performance, use the VTDPY metric disk data sectors transferred (labeled "Sectors/Sec" in the VTDPY display) to be sure the data rate is not overdriving the CI bandwidth. The number of disk data sectors transferred times the number of bytes per sector (512) yields the data rate. For best performance, leave a CI bandwidth reserve for peak I/O loads and bursts by using only 80% of the bandwidth on average.

To provide a 20% CI bandwidth reserve, you may want to limit your data rate as measured by the VTDPY metric "Sectors/Sec" as follows:

Arbitration Scheme	Disk Data Sectors Transferred
32-node	5600
16-node	6400

To reduce the data rate, move some of the busier disks to another HSC controller.

5.5.3 Tools for Automatic Load Balancing

After choosing the optimum configuration, some bottlenecks may still remain. VMS performance tools allow the assignment of files to the appropriate drives. Use VMS tools such as Monitor, VPA, and SPM, with their hotfile detection capability, to move the frequently-accessed files to the appropriate disk drive(s). Using the VMS Disk Striping Driver for VMS may further help reduce bottlenecks by implicitly providing some degree of automatic load balancing.

5.6 Tape Considerations

This section contains information on using tape drives with the HSC controller.

5.6.1 Pipeline Errors and Pipeline Error Reporting

If the configuration of your HSC controller and storage devices includes tape drives, the following message may occasionally appear:

```
ERROR-W  Data Overflow Due to Pipeline Error at dd-mmm-yyyy hh:mm:ss.s
         Command ref  #  nnnnnnnnnnnnn
         TA7x  unit    n
         Err Seq #     nnn
         Error Flags   00
         Event         FFAA
         Position      nnnn
         Retry level   12
ERROR-I End of Error
```

If a pipeline error occurs, the VMS error log displays the following message for the MSLG$EVENT field in the error log entry:

```
Data OVRFLW due to pipeline error
```

The associated formatter-detected EDC error can be recognized by a code of 0440 in the ERRN1/ERRNUM field in the error log entry. The EDC error will also have the same command reference number as the pipeline error. These errors are fully recoverable. To reduce pipeline errors, reduce your block size according to the recommendations provided.

The pipeline error message is a warning message only. It indicates the rate at which the host sent data to the HSC controller was not fast enough to keep the tape moving. This is a fully recoverable error, and if seen only occasionally with no other errors, does not indicate a hardware problem.

If you see this message on a regular basis, lower the block size of your transfers. See Section 5.6.2 to find the optimal block size for your configuration.

NOTE

> Failure to lower your block size will result in performance degradation while encountering pipeline errors. When a pipeline error occurs in the HSC controller, it restarts the entire transfer. This requires repositioning to the beginning of the record and refetching the data by the host interface (K.ci), therefore impacting performance.

When an application or operating system issues a tape command with the inhibit error recovery modifier set, the HSC controller ignores this modifier for pipeline errors and treats a pipeline error as recoverable. That is, if a pipeline error occurs when you are running the VMS BACKUP utility, the HSC controller recovers the error even though the default action is to inhibit error recovery.

5.6.2 Block Size Recommendation

The HSC CI interface can be significantly faster than the host CI adapter when performing multiple backups. Therefore, it is possible that all of the host CI bandwidth can be used by tape traffic. To prevent this, the HSC software distributes the data flow more evenly over the CI to the hosts without noticeably affecting the overall data throughput.

It is strongly recommended that you use the following operational parameters if you wish to use a block size greater than 24 kilobytes with VMS BACKUP (the default is 8 kilobytes):

- If only one DCM is configured for tape, the maximum recommended block size is 48 kilobytes.
- If two DCMs are configured for tape, the maximum recommended block size is 32 kilobytes.
- If more than two DCMs are configured for tape, the maximum recommended block size is 24 kilobytes.

NOTE

These guidelines apply to the number of tape DCMs **configured** for tape in the HSC controller (not the number of tape DCMs actively transferring data).

These guidelines **do not** apply to caching tape drives operating in the cached mode. It is still recommended that a 64 kilobytes block size be used with caching tape drives when operated in cached mode.

5.6.2.1 Display of Tape Configuration

Use the following procedure to determine how many DCMs are configured for tape in your HSC controller:

1. Enter Ctrl/Y on the HSC console or terminal.
2. Enter SHOW REQUESTOR.

Each DCM displayed as a K.sti module or as a tape K.si module is configured for tape.

CAUTION

Failure to follow these block size recommendations can result in pipeline and formatter-detected EDC errors when running multiple backup streams.

Following the recommended block size will greatly reduce the possibility of these errors occurring and will have minimal performance impact.

NOTE

Pipeline errors **do not** indicate any hardware or software fault in the HSC controller or host.

5.7 Host Level Tools

This section contains information on using special VMS tools on the host system to enhance the operation of the HSC controller.

5.7.1 Preferred Path Function

A QIO function has been added to Version 5.4 of the VMS software that performs preferred path selection. A program named PREFER.EXE and its DCL command line interface PREFER.CLD provide access to this QIO. Future versions of VMS software will contain these programs in SYS$EXAMPLES.

For convenience, these files, PREFER.EXE and PREFER.CLD, are included on the HSC software distribution medium. The programs can be uploaded from the RX33 diskette to your VMS system and used there. Instructions on uploading PREFER.EXE and PREFER.CLD from the RX33 diskette are given at the end of this section.

To set up the preferred path functionality for use:

1. Place the PREFER.EXE executable image in SYS$COMMON:[SYSEXE or some other location of your choice.

2. Define the DCL command verb PREFER using the PREFER.CLD command definition file.

If the executable image is not in SYS$COMMON:[SYSEXE], then edit PREFER.CLD to reflect the proper location.

To define PREFER as a DCL command verb in your local process command table, enter the following command:

```
$ SET COMMAND PREFER
```

To define PREFER as a DCL command verb in the system-wide DCL command table, enter the following from an account with CMKRNL privilege:

```
$ SET COMMAND /TABLE=SYS$LIBRARY:DCLTABLES -
_$ /OUTPUT=SYS$COMMON:[SYSLIB]DCLTABLES PREFER
```

To make the new command verb available to other users, use the VMS INSTALL utility. Verify that your systems have sufficient unused global pages and global sections to accommodate the modified command table. From an account with CMKRNL privilege, enter the following commands:

```
$ INSTALL
INSTALL> REPLACE SYS$LIBRARY:DCLTABLES
INSTALL> EXIT
```

NOTE

> The INSTALL utility commands must be executed from all nodes in a VAXcluster system. If your system configuration deviates from the standard usage of DCLTABLES, modify the above commands to suit your site. For further information on defining command verbs or using the INSTALL utility, consult the VMS documentation set.

Next, to use the preferred path functionality, enter the following:

```
$ PREFER device/HOST=hsc[/FORCE]
```

where:

hsc is the name of the HSC controller that is the preferred path.
/FORCE is an optional switch.

For example, device 10DUA10: has a primary path through HSC015 and a secondary path through HSC014. To select HSC014 as the primary path, enter the following:

```
$ PREFER $10$DUA10:/HOST=HSC014
```

This will set the preferred path on the local node so that the next mount will use the selected path. If the /CLUSTER qualifier is used on the MOUNT command, all nodes in the cluster will use the selected path. Note that no change is made to the SHOW DEVICE output.

The /FORCE qualifier is used to select a preferred path for mounted disks. If the disk is mounted (not /FOREIGN), then the IO$M_FORCEPATH modifier will be used to force the drive into mount verification and move it to the new HSC controller. For example:

```
$ PREFER $10$DUA10:/HOST=HSC014/FORCE
```

The path used to remount the disk will be the preferred path of the node that performs the mount verification. No other nodes in the VAXcluster system will alter their paths to the device. For proper operation, the /FORCE qualifier should be issued only from a host on which the device is mounted.

To select a preferred path for all nodes in the VAXcluster system, use the VMS SYSMAN utility to set the preferred path on all nodes in the cluster before executing the PREFER command with the /FORCE qualifier.

```
SYSMAN> SET ENVIRONMENT/CLUSTER
SYSMAN> DO PREFER $10$DUA10:/HOST=HSC014
SYSMAN> EXIT
$ PREFER $10$DUA10:/HOST=HSC014/FORCE
```

NOTE

> The PREFER command must be defined as a DCL command verb on all nodes in the VAXcluster system before using it within SYSMAN.

The SYSMAN PREFER command sets the preferred path on all nodes so that the next mount command from any node will use the selected path. The DCL PREFER command using the /FORCE qualifier causes the device to enter mount verification. After mount verification completes, the device will be remounted by all nodes through the preferred path, HSC014.

Note that for controller-based shadowed disks, preferred pathing is supported for shadow set members but not for virtual units. However, the use of the /FORCE qualifier is not supported for shadow set members or virtual units. For Host-Based Shadowed disks, preferred pathing and the /FORCE qualifier are supported for shadow set members but not for virtual units.

The procedure for uploading PREFER.EXE and PREFER.CLD from the HSC diskette to your VMS system is as follows:

1. To determine if any disk or tape devices are online to the HSC controller from which the program is to be uploaded, enter the following HSC commands:

   ```
   Ctrl/C
   HSC> RUN SETSHO Return
   SETSHO> SHOW DISKS Return
   SETSHO> SHOW TAPES Return
   ```

   Any online disk or tape drives should have both A and B port buttons set to the IN position and be cabled to another functional HSC controller with the same allocation class so that they can be failed over. Fail over or dismount all the disks and tapes connected to the HSC controller from which the program is to be uploaded. Repeat this step until no disk or tape drives are online.

2. Make the load devices visible to the HSC controller with the following HSC commands:

   ```
   SETSHO> SET SERVER DISK/LOAD Return
   SETSHO> ENABLE REBOOT Return
   SETSHO> EXIT Return
   ```

   Respond affirmatively to the SETSHO reboot query so that the HSC controller will reboot. After the HSC reboots, the load devices should be available to the operating system. Determine the drive number for the load device containing the HSC diskette by entering the following HSC command:

   ```
   Ctrl/C
   HSC> RUN SETSHO Return
   SETSHO> SHOW DISKS Return
   ```

   Enable the appropriate load device for access by VMS using the following HSC command:

   ```
   SETSHO> SET D4nnn HOST_ACCESS Return
   ```

   where *D4nnn* was derived from the SHOW DISKS printout.

Now exit SETSHO:

```
SETSHO> EXIT [Return]
```

3. From the host, use the following procedure:
   a. Enter the command:

   ```
   $ SHOW DEVICE DUA4nnn
   ```

   where *4nnn* is the device number obtained in step 2 above. Determine what device number DUA4nnn is called on your system. For example, HSC000$DUA4001: is a common name.
   b. Next, enter:

   ```
   $ MOUNT/FOREIGN xxxxxx$DUA4nnn:
   ```

   where *xxxxxx* is the prefix obtained in step 3a (for example, HSC000$DUA4001:).
   c. Now enter the commands:

```
$ EXCHANGE COPY/LOG xxxxxx$DUA4nnn:PREFER.CLD/RECORD_FORMAT=VARIABLE PREFER.CLD
$ EXCHANGE COPY/LOG xxxxxx$DUA4nnn:PREFER.EXE/RECORD_FORMAT=FIXED PREFER.EXE
```

   where *xxxxxx$DUA4nnn* represents the VMS device name as determined above.
   d. To finish the procedure, enter:

   ```
   $ DISMOUNT xxxxxx$DUA4nnn:
   ```

   The PREFER.EXE and PREFER.CLD programs are now present in your current VMS directory.
4. On the HSC console, enter the following command:

   ```
   [Ctrl/C]
   HSC> SET D4nnn NOHOST_ACCESS
   ```

   where *D4nnn* is the HSC device number determined in step 2.

   This will make the HSC load device invisible to VMS. It is important to perform this step. If this step is omitted, VMS may overwrite the HSC boot diskette.

5.7.2 One-Line HSC Commands through DUP

The program HSCCMD.MAR is included on the HSC software distribution medium. It can be uploaded from the RX33 diskette to your VMS system for use there. Instructions on uploading HSCCMD.MAR from the HSC diskette are similar to those described in Section 5.7.1. Substitute the program name HSCCMD.MAR for PATHSL.MAR in the uploading instructions.

This program will issue one command to an HSC controller through a Diagnostic Utility Protocol (DUP) connection. The command to be sent is read through the DCL foreign command line interface. This allows one-line commands to be entered from command procedures including batch jobs.

To use the command, assign a symbol that starts with a $ (to indicate a foreign command interface) which points to the image. For example:

```
$HSCCMD :== $HSCCMD
```

Enter the command:

```
$HSCCMD hsc command_string
```

where:
hsc is the name of the HSC controller that is the destination of the command
command_string is the command to be sent.

For example, to globally enable caching on HSC014, use the command:

```
$HSCCMD HSC014 SET SERVER DISK/CACHE
```

The following DCL command procedure will compile, link, and assign an appropriate symbol:

```
$ if f$search("hsccmd.mar") .nes. "" then -
    macro/list/cross'P1' hsccmd
$ if f$search("hsccmd.obj") .nes. "" then -
    link/map/cross'P1' hsccmd
$ purge/log
$ hsccmd :== $'f$logical("sys$disk")''f$directory()'hsccmd
$ exit
$
```

Note that the FY driver must be loaded and the current process must have DIAG privilege in order for this miniprogram to work.

5.8 Configuring the HSC Cache Option

The HSC cache option reduces the host-to-disk data retrieval time. In a properly configured system, the HSC cache can help system performance by eliminating some of the delay associated with seeking data on electromechanical disk devices. The HSC cache option greatly reduces the I/O response time in the case of a cache read hit (when the data for a host read request is found in cache). Notice the response time savings as diagrammed in Figure 5–2. The performance benefit of HSC cache varies based on the cache configuration and the user's application.

HSC cache is a volatile high-speed memory. For frequently accessed data, this high-speed memory can be used instead of seeking to the slower device storage. HSC's implementation of read and write update cache does not expose the user's data to loss in the event of power loss to the HSC controller. All writes to the disk are completed before they are acknowledged to the host by the HSC controller. In the event of a reboot, cache would be empty and the most frequently used data of those disks participating in cache would, through use, again become resident in the cache.

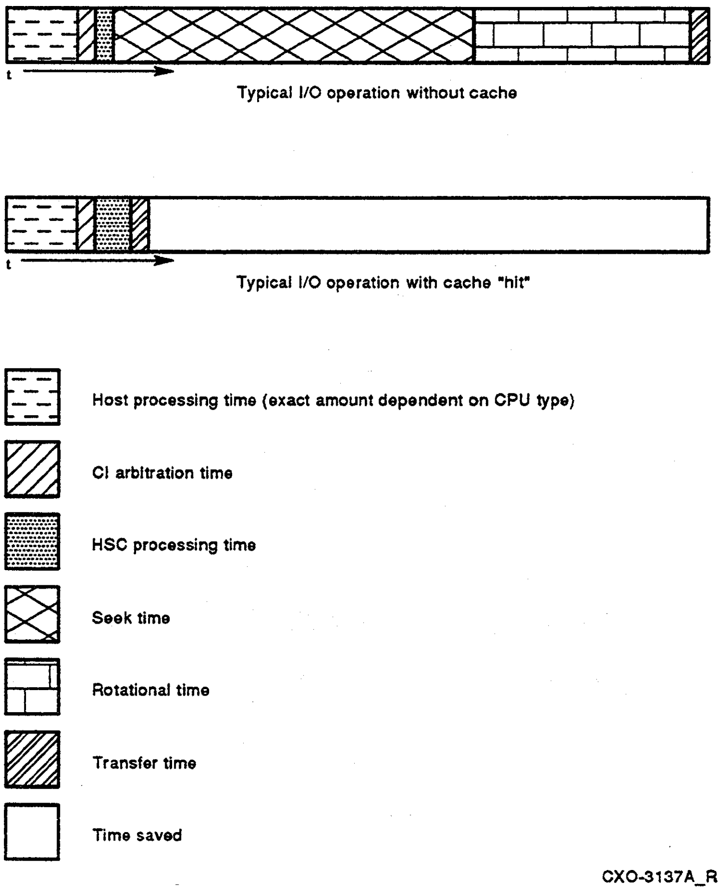
The customer may choose which disk drives are appropriate to participate in cache and may designate up to 20 disk drives on the HSC60 controller and 48 disk drives on the HSC90 controller.

It is recommended that disk drives with the following simultaneous characteristics be designated to participate in cache:

- High I/O rate
- Read intensive
- Small block transfer size
- Frequently accessed data

Cache performance analysis tools will be available on "DSNlink for VMS" to assist in determining the appropriate drives to participate in cache. Drives which have frequent and large writes, or many reads of read-once data, could inhibit the optimum performance of cache as cache misses would become more frequent. A cache miss is when data

Figure 5–2: Cache "Hit" Eliminates Mechanical Delays in an I/O Operation



is searched for in cache, but is not present. After the cache look-up operation resulting in a cache miss, the data must still be retrieved from the disk.

The HSC M.cache option is a 32 megabyte volatile memory based on 1 megabit DRAM technology. The cache software supports cache read and write-through functions. The write-through function ensures that the user data is written on the disk drive before the host is notified of the write operation's being complete. Cache technology is volatile and cache contents will be lost in the event of a power loss. If cache contents become irretrievable through loss of power, HSC reset, or M.cache hardware fault, the user data is always safe and up-to-date on the disk drive. In the case of a cache loss, the information will easily and automatically be reentered into cache as users request frequently used data.

Each disk drive on an HSC60 or HSC90 controller with the cache option can be enabled to share in the cache resource. The disk drives that are enabled to access cache have equal share in the right to use a portion of the cache memory. The shared portion of the memory depends on the rate of requests relative to other drives also sharing in cache. Disk drive caching supports the full complement of disk drive configurations supported by the HSC controller from 1 to 48 disk drives. Note that disk drives participating in HSC caching which are to be VMS shadowed will need to utilize VMS Volume Shadowing Phase II (Host-Based Volume Shadowing). Caching for controller-based shadowed disks is not supported.

HSC controller disk caching has several associated SETSHO commands. These commands control various disk caching parameters that control cache policies. The global and local disk caching commands and parameters are described in the following sections.

5.8.1 Global HSC Controller Cache Commands

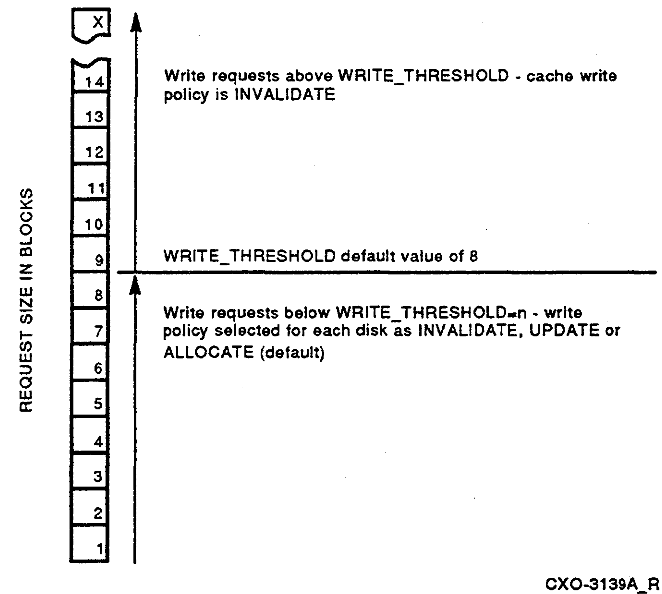
The following SETSHO commands control HSC controller disk caching on a global basis. Modifying these parameters will affect various cache server policies.

- SET SERVER DISK/[NO]CACHE
  Controls the state of the cache server software for the HSC controller. When the cache server is on, disk drives may be enabled for caching; otherwise, all cache server functionality is disabled. This command is dynamic and does not require an HSC controller reboot to take effect.

- SET SERVER CACHE/CACHE_SIZE_THRESHOLD=n
  Sets the cache server read threshold size. The qualifier value *n* represents the maximum size of a read request that will be directed to the cache server for processing. This value is expressed in terms of blocks and may range from one to 64. The default value is eight. The recommended value for VMS systems is eight; for ULTRIX systems, 16. This command is dynamic and does not require an HSC controller reboot to take effect.
- SET SERVER CACHE/WRITE_THRESHOLD=n
  Sets the cache server write threshold size at which the cache server write allocation policy changes. (See section Section 5.8.2.1 for a description of the cache server write allocation policies.) The qualifier value *n* represents the maximum size of a write request that will use the user-settable write allocation policy for the disk. This value is expressed in terms of blocks and may range from zero to 32,767. The default value is eight. The recommended value is one that equals the cache size threshold. This command is dynamic and does not require an HSC controller reboot to take effect. See Figure 5–3.

  Write requests above the qualifier value will use either UPDATE or INVALIDATE as the cache write allocation policy.
- SET SERVER CACHE/ERASE_PURGE_THRESHOLD=n
  Sets the cache server purge threshold size at which the cache server purges cache blocks for the specified disk unit. The qualifier value *n* represents the maximum size of an erase request that will be processed normally by the cache server. Erase requests above the qualifier value will cause the cache server to purge all cache blocks in use by the disk unit. This value is expressed in terms of blocks and may range from zero to 32,767. The default and recommended values are 256. This command is dynamic and does not require an HSC controller reboot to take effect. This parameter should not be changed unless directed by Digital Services.

Figure 5–3: WRITE_THRESHOLD



- SET SERVER CACHE/XDE_SIZE=n
  Sets the cache server index node size. An index node is a cache server data structure that contains one to XDE_SIZE cache blocks where one cache block contains one disk sector's worth of data. The qualifier value *n* represents the number of cache blocks in an index node. This value is expressed in terms of units and may range from one to 16. The default and recommended values are 16. This command requires an immediate HSC controller reboot to take effect. This parameter should not be changed unless directed by Digital Services.

5.8.2 Disk Unit Cache Commands

The following SETSHO commands control HSC controller disk caching on an individual disk unit basis. Modifying these parameters will affect various cache server policies as they apply to each disk unit. All disk unit cache commands are dynamic and do not require an HSC controller reboot to take effect.

- SET [DEVICE] Dnnnn [NO]CACHE
  Controls the cached state of the specified disk unit. Setting a disk unit cached will make I/O requests to the unit eligible for caching. By default, all disk units are disabled from cache processing.

5.8.2.1 Cache Server Write Allocation Policy

The cache server write allocation policy is used to determine the action taken by the cache server when processing a write request. There are three alternatives. The cache server may:

- ALLOCATE cache memory for the request if necessary and store the supplied data into cache memory. If the cache server finds the data already stored in cache memory, it will update the cache memory with the new data.

  This policy is recommended if data written is expected to be referred to later. It is selected by default.
- INVALIDATE cache memory if the data is already found there. If the data is not found in cache memory, no further cache processing occurs; that is, cache memory will not be allocated for the request.

  This policy is recommended if data written is not expected to be referred to later.
- UPDATE cache memory if the data is already found there. If the data is not found in cache memory, no further cache processing occurs; that is, cache memory will not be allocated for the request.

  This policy is recommended if there is uncertainty as to whether the data written will be referred to later.

The preceding write allocation policies are used by the cache server for all write requests that do not exceed the cache write threshold (see SET SERVER CACHE/WRITE_THRESHOLD=n). The *large cache write policy* applies to write requests that exceed the cache write threshold. The large cache write policy is either UPDATE or INVALIDATE and cannot be set by the user.

For requests that do not exceed the cache write threshold, the cache server write allocation policy may be set for each disk unit with the appropriate SETSHO command:

- SET [DEVICE] Dnnnn W_ALLOCATE
  Sets the cache server write allocation policy to ALLOCATE for the disk unit *nnnn*.
- SET [DEVICE] Dnnnn W_INVALIDATE
  Sets the cache server write allocation policy to INVALIDATE for the disk unit *nnnn*.
- SET [DEVICE] Dnnnn W_UPDATE
  Sets the cache server write allocation policy to UPDATE for the disk unit *nnnn*.

5.9 Cache Need Analysis Tool (CNAT)

With the introduction of cache on the HSC controller, it is possible to have I/O response times that are significantly shorter than with previous HSC controller models. This reduced response time translates directly into increased performance since, for a given response time, a much higher I/O rate may be sustained. Similarly, if the I/O rate was to remain the same, the reduced response time would mean a much shorter program run.

Caching works by retaining frequently accessed data within the HSC cache memory. Subsequent requests for this data will be satisfied directly from HSC cache without requiring a disk access. For this to work, however, the same blocks of data on the disk must be read more than once. This type of operation might occur when an application accesses an index portion of an indexed file, when multiple users request the same data, or when multiple host processors request the same range of data blocks.

The HSC Cache Need Analysis Tool (CNAT) is used to depict the potential benefits of installing the HSC Cache option on your controller operating in your environment with your applications.

CNAT consists of two programs designed to run on a VMS system using I/O profiles collected by an HSC controller. The two CNAT programs are:

- LGCOPY—Copies data captured by the DSKLOG utility to a suitable file for analysis.
- LGCACHE—Performs data analysis on the captured data.

With this information, the decision to purchase the HSC Cache option can be objectively evaluated and potential increases in performance accurately depicted.

NOTE

> The HSC Cache option can only be installed on HSC60 or HSC90 controllers. You must upgrade an existing HSC40 or HSC70 controller to an HSC60 or HSC90 controller before installing the HSC Cache option. The HSC50 controller cannot be upgraded to use the HSC Cache option. Contact your Digital sales representative for information on migrating from an HSC50 controller or upgrading your HSC40 or HSC70 controller to an HSC60 or HSC90 controller.

5.9.1 Overview of CNAT Operation

Since cache functions by retaining frequently accessed data in high speed memory, the actual I/O requests over a period of time must be known in order to determine how well cache will work. This is done by capturing all I/O requests issued by the host computers over a period of time, then analyzing these requests to see how effective cache would be in this particular I/O environment.

5.9.1.1 Data Capture

To analyze the I/O stream, special monitoring software within the HSC controller is enabled. This software will write a condensed copy of each I/O command it receives from the host computers to a dedicated disk drive. This logging of I/O commands will proceed in parallel with normal operations and has a negligible impact on performance. The data that is stored on the disk drive includes the type of I/O (read or write), the disk drive to which the command was sent, the beginning logical block of the transfer, and the length of the transfer. The actual data that was transferred is not captured, just the information describing that data.

Since the object of running CNAT is to measure the effects of cache during normal operation, the data capture phase should be run for an amount of time sufficient to capture all normal activities. Although this will vary from one site to another, typical periods of time are from one to two days. If different jobs or processes run at different times during the month, then CNAT may be repeated for each time period of interest.

5.9.1.2 Data Analysis

Once the data has been captured, the next step is to run a program that analyzes the captured data. This program is a simulation of the HSC controller. The program will scan the data file containing the I/O activity and duplicate the actions of HSC Cache. CNAT then creates a data file of which commands have been satisfied by the cache in the HSC controller, and which have been directed to disk. From this data file, the response times for each disk are generated, and the results of what would have happened if HSC cache had been present are predicted. These results can be used to predict future performance under similar conditions (if the time period during which the data was captured was very typical of normal system operation).

5.9.1.3 Interpreting the Results of a CNAT Run

Cache improves performance by returning data directly from HSC memory, bypassing disk accesses. Any time a command is satisfied from cache, it is termed a "hit." If the command must go to disk, it is termed a "miss." Since any data written to disk must actually access the disk, only read commands can generate a hit.

One measure of cache performance is called "hit rate." This is the percentage of commands which result in a cache hit. For example, a hit rate of 50% indicates that half the commands were satisfied from cache and the disk did not have to be accessed.

Another measure of cache performance is response time. On average, a disk access requires from 20 to 50 milliseconds (ms). If the access is satisfied from HSC cache, however, the average time is from 2 to 5 ms, or a small fraction of the time taken on a miss. As the hit rate increases, the percentage of requests having these short response times increases, and the average response time for the disk drive will also decrease. For example, if half of the requests were hits (with a response time of 4 ms) and half were misses (with a response time of 40 ms), then the overall average response time would be 22 ms. With a smaller response time, I/O bound jobs will complete much faster.

The last measure of cache performance is the maximum request rate for a disk drive. In typical operations, the maximum request rate is determined by the longest tolerable response time. For example, an RA92 disk drive can sustain about 35 requests per second with a response time of 50 ms. With caching present, the average response time is much shorter. Therefore, more requests may be sent to this drive before the drive becomes so busy that the response time begins to exceed tolerable limits. With an RA92 disk drive and a cache hit rate of 50%, nearly 75 requests per second may be sent to the drive before the response time reaches 50 ms. Because of this, more work may be sent to the disks than would be possible without cache.

The CNAT analysis program shows both the response times and maximum request rates with and without cache. By examining the cached and non-cached request rates and response times, the increase in performance attainable with cache may be evaluated.

5.9.2 How to Run CNAT

This section describes the steps required to capture the data and analyze the possible effects of using HSC cache.

5.9.2.1 System Requirements

The following equipment and software is required to run CNAT:

- An HSC40, HSC60, HSC70, or HSC90 controller
- HSC40 or HSC70 controllers running HSC software V3.7 or higher; HSC60 or HSC90 controllers running HSC software Version 6.0 or higher (with or without cache enabled)
- One spare RA disk drive (any model) which will be connected to the HSC controller. (This disk will be completely overwritten with data from the data collection.)
- VMS V5.0 or higher. (The CNAT programs supplied with this package were linked under VMS V5.3-1.)

5.9.2.2 Preparing the HSC Controller

Prior to any data capture, special monitoring code within the HSC controller must be enabled. To accomplish this, run the SETSHO utility. Enter the following command to enable the monitoring code (the HSC node in this example is EWOK):

```
CTRL/Y
EWOK> SET SERVER DISK/MSCP
SETSHO-I Your settings require an IMMEDIATE reboot on exit.
SETSHO-Q Rebooting HSC.  Press RETURN to continue, CTRL/Y to abort:
```

Since this command causes special code within the HSC controller to be invoked, a reboot is required. Because of this reboot, this step should be taken when it is convenient to restart the HSC controller.

Entering a return will reboot the HSC controller. Entering a Ctrl/Y will abort the operation. When the reboot has been completed, the monitoring code is enabled. No logging of I/O commands will take place until another HSC utility has been run.

The HSC controller will only log those I/O commands that are sent to disks connected to that HSC controller. Because of this, you should make sure that all disks you wish to monitor are connected to and mounted on the HSC controller under evaluation. Since disks that were originally connected to the HSC controller under evaluation will fail over to the alternate HSC controller when the original HSC controller is rebooted, make sure that you have all disks of interest connected back to the HSC controller under evaluation.

The SETSHO command will cause the logging code to remain enabled even if the HSC controller is later rebooted, so the command only needs to be issued once.

When all data has been captured, the special logging code may be deactivated by entering the following commands to the HSC controller:

```
CTRL/Y
EWOK> SET SERVER DISK/NOMSCP
SETSHO-I Your settings require an IMMEDIATE reboot on exit.
SETSHO-Q Rebooting HSC.  Press RETURN to continue, CTRL/Y to abort:
```

As before, a reboot of the HSC controller is required before this command will take effect.

5.9.2.3 Beginning the Data Capture

To capture the I/O stream, a dedicated disk drive must be connected to the HSC controller under test. This disk will be completely overwritten with the data, and any files on this disk will be lost. After the data capture, the disk must be reinitialized before it may be used with VMS. Any RA disk may be used. The disk must not be mounted by VMS, but it must be available by enabling the disk's port to the HSC controller.

NOTE

The name of the utility on versions of HSC software prior to V6.0 is LGUTIL. As of HSC software V6.0, this utility was renamed to DSKLOG. In the examples that follow, the name DSKLOG is used. If your HSC software version is lower than V6.0, use LGUTIL instead of DSKLOG.

Once the data capture disk is connected, run the logging utility on the HSC controller. The data capture disk will be completely overwritten by the logging software and any VMS files on that disk will be erased. Enter the following commands to enable the DSKLOG utility (assuming the data capture disk is unit 10):

```
CTRL/Y
EWOK> R DSKLOG
DSKLOG> ENABLE D10
    Log:           ENABLED
    Unit:          10
    LBN:           0
    Wrap Count:    0
    MSCP Status:   000000
    Wrap Point:    1216665
    Missed I/O:    0
```

The data capture code is now active and any I/O commands sent to any disk on the HSC controller will be logged to drive 10.

The individual lines in the status message are defined as follows:

- **Log**—Either ENABLED or DISABLED, to indicate the status of the data logging. For data to be captured, the log must be ENABLED.
- **Unit**—The disk unit to which data is being logged. If **Log** is DISABLED, this field is the last unit on which data was captured.
- **LBN**—The last logical block number (LBN) on the data capture disk to which data was written. Each I/O packet occupies 24 bytes, so 3 logical blocks will contain 64 records. To determine the total number of I/O packets captured, divide the LBN field by 3 and then multiply by 64. This value is not exact, but will give a good approximation of how many I/O packets have been sent to the HSC controller.
- **Wrap Count**—DSKLOG continues writing I/O packets until the data capture disk is full. At that time, it wraps back to the beginning of the disk and starts over. The number of times this happens is shown in this field.
- **MSCP Status**—The MSCP status of the last I/O operation. This will usually be zero and may be ignored.
- **Wrap Point**—The number of logical blocks on the data capture disk. To determine how many I/O packets the disk will hold before wrapping, divide this number by 3 and multiply by 64. The length of time before the data wraps depends on both the size of the disk and the I/O rate.

In the previous example, nearly 26 million I/O packets may be captured before data wraps to the beginning of the disk. If the I/O rate to the HSC controller is 200 requests per second, then approximately 129,000 seconds are required before the data wraps (about 36 hours). You can monitor the I/O rate to the HSC controller by using the VTDPY utility. (Refer to the *HSC Controller User Guide* for instructions on how to run the VTDPY utility.)

- **Missed I/O**—This is the number of I/O packets that DSKLOG did not capture. This may happen on an extremely busy system when DSKLOG determines that there are not enough resources to capture the I/O.

Enter Ctrl/Z to exit DSKLOG:

```
DSKLOG> CTRL/Z
DSKLOG-I Exiting.
```

At this point, data is still being captured onto the logging disk even though DSKLOG has been exited. Periodically run DSKLOG to check the status of the data logging operation by entering the following commands:

```
CTRL/Y
EWOK> R DSKLOG
DSKLOG> STATUS
    Log:           ENABLED
    Unit:          10
    LBN:           12
    Wrap Count:    0
    MSCP Status:   000000
    Wrap Point:    1216665
    Missed I/O:    0
```

As shown in the example, the value for **LBN** has changed from 0 to 12 indicating that data has been captured. The values shown here will differ from what you will get with your HSC controller. In this example, 256 I/O packets have been captured. This step may be repeated as often as desired.

5.9.2.4 Ending the Data Capture

Once the time period of interest has passed, enter the following commands to terminate the DSKLOG utility:

```
CTRL/Y
EWOK> R DSKLOG
DSKLOG> DISABLE D10
    Log:           DISABLED
    Unit:          10
    LBN:           225
    Wrap Count:    0
    MSCP Status:   000000
    Wrap Point:    1216665
    Missed I/O:    0
```

A final status message is displayed and disk logging is terminated. In this example, the LBN indicates that 4,800 I/O packets have been captured. DSKLOG does not terminate logging until its internal buffer has been filled. There may be some delay between issuing the DISABLE command and the actual disabling of data logging.

If you plan on copying this data to a VMS file on another disk, the size of that file will be the number of blocks shown for the LBN field. In this example, the number of blocks is 225.

5.9.2.5 Converting the Data

The captured data is now on the dedicated disk (in this case, drive 10 from the previous example). Although the data can be analyzed directly from this disk, you may want to make a copy of the data for later analysis. One reason for creating a copy might be that another data capture run is wanted and there is only one data collection disk. The captured data may be converted to an RMS file which will be placed on a mounted VMS disk. Note that this file may be quite large, depending on how many I/O packets were captured.

To convert the data, the data capture disk must be mounted FOREIGN, as follows:

```
$ MOUNT $3$DUA10:/FOREIGN
%MOUNT-I-MOUNTED, TEST         mounted on _$3$DUA10: (EWOK)
```

Once the disk has been mounted, the copy program may be run. PHY_IO privileges are required to perform this operation:

```
$ RUN LGCOPY
Convert Raw DSKLOG Data - Version 1.1 (14 Jul 91)
```

When asked for the DSKLOG input disk, enter the VMS designator for the data capture disk:

```
DSKLOG input disk (CTRL/Z to exit): $3$DUA10
```

The disk is examined by the program to ensure that it contains valid data. Once this has been verified, the program prompts for an output file name:

```
RMS output file name: TEST.OUT
```

This file will contain the captured data from the data collection disk. The program begins converting the I/O packets and storing them in the specified file:

```
Converting DSKLOG data...
```

Depending on the number of I/O packets captured, this conversion step may take a considerable amount of time. When this process has completed, the total number of records processed is displayed:

```
DSKLOG conversion complete, 4744 records processed.
DSKLOG input disk (CTRL/Z to exit): CTRL/Z
$
```

The number of records processed may not equal the number calculated from the LBN field in the DSKLOG status message. This is normal. Exit the program by entering Ctrl/Z.

5.9.2.6 Analyzing the Data

The final step is to analyze the captured data. The analysis program scans the DSKLOG data. This data may be either in an RMS file or on the original data capture disk. During the scan, the CNAT program LGCACHE evaluates the effects of adding cache to the HSC controller for the workload that was captured. The result of this analysis is a comparative picture of the performance of the I/O subsystem both with and without cache on a per-disk basis. From this analysis, you can see the effects of adding cache to your particular system and determine the potential benefits of cache.

The following is an example of the procedure to use for the analysis. To start the analysis, enter the following command:

```
$ R LGCACHE
HSC Cache Suitability Analysis - Version 1.2 (02 Mar 92)
```

In this example, the file that is to be analyzed has been converted with LGCOPY and is named HSC3.DAT.

When asked for the DSKLOG data file or disk, enter the file name or the number of the data capture disk that contains the DSKLOG data:

```
DSKLOG data file or device: HSC3.DAT
```

NOTE

> If you are analyzing directly from the data capture disk, then this disk must have been mounted FOREIGN. As before, PHY_IO privileges are required to mount FOREIGN.

The program then prompts for a listing file. Enter a file name for the report to be saved in. If you enter Ctrl/Z, the listing file defaults to SYS$OUTPUT.

```
Listing file: HSC1.DATHSC3.LIS
Analyzing DSKLOG data...
```

LGCACHE then begins the analysis of the data. Since this procedure is quite complex, this analysis may take a considerable amount of time. This time will vary, but depends primarily on the number of records captured by the DSKLOG program. Once the analysis has completed, the report is displayed.

The first section of the report is a summary of the DSKLOG data file:

```
DSKLOG Analysis:
      ❶ DSKLOG file: HSC3.DAT
      ❷ Data collection start time: 27-APR-1991 07:49:05.21
      ❸ Data collection stop time: 27-APR-1991 08:22:00.81
      ❹ Scanned data covers 0 hours, 32 minutes
      ❺ Total DSKLOG packets: 96000
      ❻ Total transfer commands: 88880
```

❶ This first data line lists the file name or disk number that contains the DSKLOG data.

❷ This line shows the beginning data collection time.

❸ This line shows the ending data collection time.

❹ This line shows the overall time of the data collection. These times can be used to ensure that the data capture covered the period of interest.

In this example, the total time of 32 minutes is rather short, and might be cause for concern about the validity of the measurements. Unless you are certain that your application has a very short run time, this period should be at least several hours in length.

❺ This line reports the total number of DSKLOG packets analyzed.

❻ This line reports the number of transfer commands. The difference between this number and the DKSLOG packet number is due to other packets that travel between the host computers and the HSC controller, such as commands to bring a disk online or status requests.

Following this summary information, a report is displayed showing the performance of the individual disk drives both with and without cache:

Disk	Requests	NC Resp	Ca Resp	NC Rate	Ca Rate
56	21535	36.2 ms	12.1 ms (33.4%)	18.5	73.6 (3.96x)
55	8880	23.7 ms	22.4 ms (94.2%)	26.7	29.2 (1.10x)
84	6580	28.6 ms	8.8 ms (30.8%)	18.3	96.9 (5.30x)
64	3904	28.8 ms	18.6 ms (64.6%)	16.7	35.7 (2.14x)
* 200	7161	35.2 ms	19.1 ms (54.2%)	12.0	36.0 (2.99x)
54	6560	23.9 ms	22.2 ms (92.7%)	25.2	28.5 (1.13x)
65	2845	26.6 ms	9.9 ms (37.1%)	19.0	82.6 (4.35x)
51	3929	28.2 ms	14.2 ms (50.3%)	17.4	52.4 (3.01x)
59	306	25.7 ms	16.7 ms (64.8%)	19.0	40.2 (2.11x)
50	7975	-	-	-	-
53	87543	31.5 ms	24.8 ms (78.8%)	15.1	23.6 (1.57x)
63	11450	26.0 ms	10.5 ms (40.3%)	24.2	81.3 (3.35x)
62	911	27.3 ms	20.5 ms (75.1%)	17.1	29.3 (1.71x)
58	248	27.3 ms	17.7 ms (65.0%)	16.8	36.5 (2.18x)
60	66	27.6 ms	24.4 ms (88.2%)	16.2	21.1 (1.30x)

This report is divided into several columns, each of which contains specific information that must be evaluated. These columns are:

- **Disk**—This column contains the physical number of the disk. If this number is preceded by an asterisk (*), then that unit is the virtual unit number of a controller-based shadow set. In the previous example, drive 200 is a controller-based shadow set, while all other disks are real units. Note that if the disks are to be both shadowed and cached, host-based caching must be used. The HSC controller does not cache disks in a controller-based shadow set. However, disks in a host-based shadow set may be cached.

  A shadow set is treated in the analysis as though it were a single physical disk. If the shadow set has two or more members, care must be taken in interpreting the data. The values may not be valid since response times are different for multi-member, controller-based shadow sets and single disks. For this reason, shadow sets are flagged with an asterisk to indicate that the data should be viewed with caution.

- **Requests**—This column tallies the number of I/O requests sent to each drive. This is of interest since drives with a low number of requests may not have fully exercised the cache. For example, disk 60 has had only 66 requests. Because of this low number, the performance information for this drive must be viewed with some skepticism.

- **NC Resp**—This column shows the calculated average response time of the drive without caching (Non-Cached Response). In essence, this is the average response time you can expect from the I/O subsystem with your workload for this drive without cache. If this field is a "–", the non-cached response time and all following fields for this disk could not be calculated and the data should be disregarded. In the above example, disk 50 shows this condition. Refer to Section 5.9.3.2 for a detailed explanation of the reasons for this condition.
- **Ca Resp**—This column shows the anticipated average response time of the disk for that same workload when cache is present (Cached Response). A percentage is also shown which represents the percentage of cached response time in relation to non-cached response time.

  For example, disk 56 has an average non-cached response time of 36.2 ms, while the cached response time is 12.1 ms, or 33.4% of the non-cached case. In other words, adding cache will result in this disk drive taking 33.4% of the time for I/O that it took before cache was added. From this, you can conclude that drive 56 is an ideal candidate for caching.
- **NC Rate**—This column shows the calculated requests per second before the average response time rises to 50 ms (a typical value for maximum tolerable response time) when cache is not present (Non-Cached Request Rate). Since response time rises as the load on a disk increases, this figure is a good indication of how much work can be sent to a drive before the response time increases beyond acceptable levels.
- **Ca Rate**—This column shows the calculated requests per second before the average response time rises to 50 ms when cache is present (Cached Request Rate). A multiplier figure is also shown which represents the increase when caching is added.

  For example, disk 56 has a maximum rate without cache of 18.5 requests per second before the response time exceeds 50 ms. With caching, the same disk can now perform 73.6 requests per second, an increase of 3.97 times.

5.9.3 Interpreting the Results of a CNAT Run

When looking at the individual disk performance report, both the decrease in response times and the increase in request rates are the key factors to evaluating the effects of cache. Each has its own merits. The choice of which to use depends on your specific need. In general, the percentage decrease in response time can be translated directly into the decrease in the time taken by the entire application. The increase in I/O can be translated into an increased number of users.

For example, assume that an application ran on disk 56 and consisted of 50% disk and 50% CPU time. Furthermore, assume that this job took 10 minutes to run to completion. With this, we can see that 5 minutes are spent in CPU time and 5 minutes are spent waiting for I/O. Since caching reduces the response time on this disk to 33.4% of its original value, this means that the 5 minutes worth of I/O is now decreased to about 1 minute and 40 seconds. The job itself will now complete in 6 minutes and 40 seconds instead of the original 10 minutes.

Without caching, disk 56 can sustain 18.5 requests per second while adding cache will increase the request rate by a factor of 3.97. In other words, 3.97 times as much I/O can be sent to the disk when cache is present. This usually translates directly into an increased number of users accessing the disk. In this case, you can more than quadruple number of users on a disk without any change in the performance.

The decision of whether to concentrate on response time or request rate depends on your specific requirements. If your jobs take too long to complete and are I/O bound, then response times are the metric of interest. If you want to add more users or I/O streams to a disk and are concerned about the response times degrading, then request rates should be examined.

There are also some cases where cache might not be appropriate. Disk 54, for example, shows an increase in the response time and a decrease in the request rate if cache is added. This might be due to a large percentage of write operations or merely that data is accessed randomly. In any case, cache should be disabled for this drive since it will hinder rather than help performance.

There are also many borderline cases. While it is clear that disks 56, 84, and 50 would receive a tremendous performance boost from cache, disk 60 is not at all certain. Although a 6% reduction in response time and a corresponding 10% increase in request rate is quite good, this performance improvement might be considered marginal. The decision for this case should be based on the intended use of the disk in question. If it is a critical application, then cache would be a worthwhile addition.

If it is not critical, then perhaps caching might not be necessary. In such cases, the report can only provide the anticipated performance impact of adding cache. The benefits of this performance increase must be evaluated on a case-by-case basis.

Once the analysis report has completed, the program prompts for another DSKLOG data file. You may either specify another file or exit the program by entering Ctrl/Z:

```
DSKLOG data file or device:  CTRL/Z
$
```

5.9.3.1 Analyzing Different Applications of Cache

To gain a complete understanding of the effects of cache, it is worthwhile to repeat the data capture and analysis on different workloads. This requires running the DSKLOG program on the HSC controller for each time period of interest, optionally copying the data capture disk to a file with LGCOPY, and analyzing the results with LGCACHE.

By proceeding in this manner, a complete picture of the benefits of cache can be built for your specific applications.

5.9.3.2 Accuracy

As with all analysis and simulation programs, there may be some differences between the results shown by this program and what you see on your system. Specifically, the results shown by the LGCACHE program should be used to compare, not predict, absolute results. The values for response times and request rates are reasonable for typical scenarios, but may vary depending on the specific hardware and software in use.

These inaccuracies are as a result of the following:

- Since DSKLOG does not capture the disk drive type, an RA92 disk drive is assumed for the analysis. Disk drives with higher performance will generally perform better than shown in the analysis.
- Because DSKLOG does not recognize the disk drive type, an ESE storage element will be analyzed as an RA92 disk drive. The HSC controller does not cache an ESE, so the values shown for this disk should be disregarded. Both the cached and non-cached request rates and response times in these cases are meaningless.
- As mentioned previously, controller-based shadow sets (flagged with an asterisk) will be treated as a single, non-shadowed disk. Since the HSC cache does not support controller-based shadowing, the results shown will not be accurate. The shadow set is included to see how the shadow set would behave if it were a single disk and were not shadowed.
- The analysis calculates the average request rate per disk by taking the total number of requests per disk and dividing by the total data capture time. If the disk is only active for a small portion of the data collection time, the results will be inaccurate. To avoid this problem, you should have the data capture running only when the disks are active.
- The results assume that the HSC controller is not more than 80% busy. If the HSC controller is more than 80% busy, then the response times may rise and the request rates may drop because the HSC controller is becoming a bottleneck. This is rarely a problem, and moving active disks to another HSC controller will easily remove the bottleneck.
- In some cases, the measured I/O rate will be higher that would be possible for a single RA92 disk drive. This may occur if the disk being measured is an ESE, a fast magnetic disk drive such as an RA72, or a shadow set, all of which have a very high request rate during the measurement interval. In this instance, it would not be possible to calculate an equivalent response time for an RA92 disk drive, so all fields showing response time and request rates are flagged with a "–".

A sample copy of a complete CNAT run is shown in Example 5–1. This run is identical to that shown earlier in this document and is reproduced here to show the complete series of steps in a CNAT run. Comments not shown in the display but which will help you to to follow the flow are given in italics:

Example 5–1: Sample CNAT Run

```
[CTRL/Y]
EWOK> SET SERVER DISK/MSCP
SETSHO-I Your settings require an IMMEDIATE reboot on exit.
SETSHO-Q Rebooting HSC.  Press RETURN to continue, CTRL/Y to abort:
```

After Rebooting the HSC:

```
[CTRL/Y]
EWOK> R DSKLOG
DSKLOG> ENABLE D10
    Log:           ENABLED
    Unit:          10
    LBN:           0
    Wrap Count:    0
    MSCP Status:   000000
    Wrap Point:    1216665
    Missed I/O:    0
DSKLOG> [CTRL/Y]
DSKLOG-I Exiting.
```

After the data capture:

```
[CTRL/Y]
EWOK> R DSKLOG
DSKLOG> DISABLE D10
    Log:           DISABLED
    Unit:          10
    LBN:           225
    Wrap Count:    0
    MSCP Status:   000000
    Wrap Point:    1216665
    Missed I/O:    0
DSKLOG> [CTRL/Y]
DSKLOG-I Exiting.
```

Copying the data to a VMS disk:

Example 5–1 Cont'd on next page

Example 5–1 (Continued): Sample CNAT Run

```
$ MOUNT $3$DUA10:/FOREIGN
%MOUNT-I-MOUNTED, TEST        mounted on _$3$DUA10: (EWOK)
$ RUN LGCOPY
Convert Raw DSKLOG Data - Version 1.1 (14 Jul 91)
DSKLOG input disk (CTRL/Z to exit): $3$DUA10
RMS output file name: TEST.OUT

Converting DSKLOG data...

DSKLOG conversion complete, 4744 records processed.
DSKLOG input disk (CTRL/Z to exit): CTRL/Z
$
```

Analyzing the data:

```
$ R LGCACHE
HSC Cache Suitability Analysis - Version 1.2 (02 Mar 92)
DSKLOG data file or device: HSC3.DAT
Listing file: HSC1.DATHSC3.LIS
Analyzing DSKLOG data...
DSKLOG Analysis:
        DSKLOG file: HSC3.DAT
        Data collection start time: 27-APR-1991 07:49:05.21
        Data collection stop time: 27-APR-1991 08:22:00.81
        Scanned data covers 0 hours, 32 minutes
        Total DSKLOG packets: 96000
        Total transfer commands: 88880
 Disk  Requests   NC Resp      Ca Resp            NC Rate     Ca Rate
   56    21535    36.2 ms    12.1 ms ( 33.4%)     18.5       73.6 (3.96x)
   55     8880    23.7 ms    22.4 ms ( 94.2%)     26.7       29.2 (1.10x)
   84     6580    28.6 ms     8.8 ms ( 30.8%)     18.3       96.9 (5.30x)
   64     3904    28.8 ms    18.6 ms ( 64.6%)     16.7       35.7 (2.14x)
*  200    7161    35.2 ms    19.1 ms ( 54.2%)     12.0       36.0 (2.99x)
   54     6560    23.9 ms    22.2 ms ( 92.7%)     25.2       28.5 (1.13x)
   65     2845    26.6 ms     9.9 ms ( 37.1%)     19.0       82.6 (4.35x)
   51     3929    28.2 ms    14.2 ms ( 50.3%)     17.4       52.4 (3.01x)
   59      306    25.7 ms    16.7 ms ( 64.8%)     19.0       40.2 (2.11x)
   50     7975       -          -                    -          -
   53    87543    31.5 ms    24.8 ms ( 78.8%)     15.1       23.6 (1.57x)
   63    11450    26.0 ms    10.5 ms ( 40.3%)     24.2       81.3 (3.35x)
   62      911    27.3 ms    20.5 ms ( 75.1%)     17.1       29.3 (1.71x)
   58      248    27.3 ms    17.7 ms ( 65.0%)     16.8       36.5 (2.18x)
   60       66    27.6 ms    24.4 ms ( 88.2%)     16.2       21.1 (1.30x)
DSKLOG data file or device:  CTRL/Z
$
```

Disabling data capture on the HSC controller:

Example 5–1 Cont'd on next page

Example 5–1 (Continued): Sample CNAT Run

```
CTRL/Y
EWOK> SET SERVER DISK/NOMSCP
SETSHO-I Your settings require an IMMEDIATE reboot on exit.
SETSHO-Q Rebooting HSC.  Press RETURN to continue, CTRL/Y to abort:
```

5.10 Cache Performance Analysis Tool (CPAT)

The Cache Performance Analysis Tool (CPAT) monitors cache performance on a disk-by-disk basis and displays important performance information about the effects of cache. CPAT consists of two programs:

- DSTAT—Collects HSC Cache performance statistics
- DSCACHE—Performs analysis on the data collected by DSTAT

The data monitored by the DSTAT program and analyzed by DSCACHE is used by a system manager, along with the guidelines in this document, to select which disks to cache and which disks to remove from caching.

The two CPAT programs also provide dynamic information on the performance of all disks that are currently being cached by the HSC controller. Data is displayed that allows a system manager to adjust the numerous parameters controlling HSC cache operation, thereby yielding even higher performance.

5.10.1 System Requirements

The following equipment is required to run CPAT:

- An HSC60 or HSC90 controller with cache installed
- HSC software V6.0 or higher
- A video terminal capable of 132 columns and direct cursor addressing, such as the VT2xx and VT3xx series
- VMS versions 5.0 and higher

The VMS programs supplied with this package were linked under VMS version 5.5.

NOTE

The HSC Cache option can only be installed on an HSC60 or HSC90 controller. You must upgrade an existing HSC40 or HSC70 controller to an HSC60 or HSC90 controller before installing the HSC Cache option. The HSC50 controller cannot be upgraded to use the HSC Cache option. Contact your Digital sales representative for information on migrating from an HSC50 controller or upgrading your HSC40 or HSC70 controller to an HSC60 or HSC90 controller.

Since DSCACHE requires extensive knowledge of drive performance for accurate analyses, only the following disk types are supported:

- RA70
- RA71
- RA72
- RA73
- RA81
- RA82
- RA90
- RA92

Other drive types will be listed as **Unknown** by the analysis, and no data will be shown.

5.10.2 Restrictions

Two restrictions need to be observed when running this program:

- DSTAT cannot be run, either directly or through DSCACHE, at the same time as the HSC utility VTDPY. Both programs assume exclusive use of the same set of internal statistics counters in HSC memory. Either program will issue an error message if it determines that another program is already running. HSC software V6.0 does not prevent simultaneous access to the counters and can result in erroneous results from both DSTAT and VTDPY if both are run simultaneously.

- CPAT may fail to run when the HSC controller is heavily loaded. If the idle time on the HSC controller is less than 10%, internal limitations of the HSC controller may prevent DSTAT from running properly. The symptom of this condition is an error message stating that there was an error accessing the HSC controller.

5.10.3 Overview of CPAT Operation

Whenever a disk is accessed, code within the HSC controller is activated which will collect statistics about the performance of that disk. The DSTAT utility can be run to display this information on a periodic basis. DSTAT was not designed to be run by humans, however, and presents the information in a very terse format.

DSCACHE runs under VMS. This program makes a connection to the HSC controller over the CI and then runs DSTAT. All information from DSTAT is collected and analyzed by DSCACHE, and the results of this analysis are displayed on the controlling terminal. The display shows the performance effects of cache, as well as several other items designed to assist in choosing which disks to cache or remove from caching.

The following steps are performed in an analysis of cache performance. These steps are presented in more detail in this document:

1. Set your terminal to 132 column mode. This is required since the display uses 132 columns on the screen.
2. Grant yourself DIAGNOSE privileges. This is necessary since the program makes a connection over the CI to the HSC controller.
3. Run the DSCACHE program, answering the questions about which HSC controller to monitor and the length of the scan interval.
4. Once every scan interval, information is displayed about cache performance which you may then interpret and use to tune the cache.

Interpretation of the displayed data is usually done by a system manager. Although the importance of some data might be obvious (such as reduced performance with cache enabled), most is not. As an example, a 10% improvement in the response time is clearly an improvement, but it might be argued that the improvement is so slight that it would be to the advantage of cache as a whole that this disk not be cached.

On the other hand, this disk might be response time critical, and even a 10% improvement might be worthwhile.

For this reason, interpretation and selection of disks to cache or not cache is more of an art than a precise science and will vary from site to site. DSCACHE provides sufficient information to allow you to make an intelligent decision, but it only makes recommendations in fairly simplistic cases. In these cases (such as a performance reduction with cache enabled), the display of the specific disk will be highlighted to assist in seeing potential problems.

5.10.4 Detailed Instructions for Running CPAT

The remainder of this document provides more detailed information on analyzing and tuning the performance of HSC Cache, selecting which drives to remove from caching, and adjusting the various cache parameters. This procedure is presented in the following sequence:

- Run DSCACHE to gather and analyze statistics
- Display and interpret the data
- Tune cache parameters
- Re-run DSCACHE, display and interpret the new data, and retune parameters until satisfactory operation is obtained.

5.10.4.1 Initiating a DSCACHE Run

The terminal used to run the DSCACHE program must be set to 132 column mode and the user must have DIAGNOSE privileges. Failure to do either of these will prevent DSCACHE from running.

Once the preparatory steps have been accomplished, DSCACHE may be run (all user input is shown in bold type):

```
$ RUN DSCACHE
HSC Cache Performance Analysis - Version 1.1 (29 APR 92)
```

When asked for the name of the HSC controller, enter the name of the HSC you wish to analyze:

```
HSC name: HSC001
```

The next question will be the scan time in minutes. Although this will vary depending on the specific site requirements, a good starting value is 5. Note that DSCACHE will analyze and print results based on this time interval, so if 30 is entered, no data will be printed for 30 minutes.

```
Scan time in minutes: 5
```

DSCACHE now attempts to make a connection to the HSC controller over the CI and run the DSTAT program. Any errors that occur (either CI connection or HSC based) are displayed before the program exits.

5.10.4.2 Displaying the Data Output from a CPAT Run

If the connection is successful, the screen is cleared and a message is displayed to show that the program is waiting for data from the HSC controller. This message will remain on the screen for the duration of the scan interval. Once DSCACHE has obtained data from the HSC controller, the data is displayed on the screen.

The first line contains information about the HSC controller itself, and might look as follows:

```
HSC90 V650 HSC001  Id 000000000002 On 07-Apr-1992 10:06:58.82   Up:  21:06 91.5% Idle
```

The last item of information on this line is the percentage of time the HSC controller is idle. If this value is less than 20%, it indicates that the HSC controller is very close to saturation. You should then take steps to reduce the load on the HSC controller. If the value is less than 10%, then internal limitations of the HSC controller may actually cause problems when running DSCACHE.

Following this will be the results of the analysis by the DSCACHE program. The data is printed in three columns of statistics, with nine separate data fields per disk. Since three disks are printed per line, a full complement of 48 disks attached to an HSC90 controller takes 16 lines on the screen.

A sample line of data for a single disk might look like this:

```
Disk S cRsp rdSiz wrSiz  R/S Hits htSz Pg
  44 C  69%  17.0   7.0  5.6  38%  3.0  1
```

The individual fields for each disk are described as follows:

- Disk—This field contains the disk unit number. Note that only the unit number is displayed, not the full VMS number. In the sample line of data, disk 44 is actually $DUA44.
- S—This field shows the status of the disk. Possible values are:
  - C—The disk is cached.
  - O—The disk is on-line, but not cached. No further data will be shown. Although no analysis is possible, the program monitors certain values. If the percentage of reads is greater than 75% (indicating caching might help performance) and the average read size is less than or equal to 8 sectors (the HSC controller default for caching data), the phrase "Consider caching" is displayed. This message is printed in bold video if this condition persists for two consecutive scan periods.
  - U—Unknown drive type. Performance cannot be analyzed and no data will be shown.
- cRsp—This field shows the relative response time of the disk with caching enabled. In the sample line of data, the value of 69% indicates that the average response time over the scan period was 69% of what it would have been if the disk had not been cached. A value of 100% indicates that caching makes no difference in the performance of the disk, while values over 100% indicate that the disk performance is actually worse with caching enabled. If this value is greater than 95% (indicating a very marginal improvement), all data fields for this disk are shown in bold video to highlight the potential problem. If this condition persists for two consecutive scan periods, all fields are shown in reverse video.
- rdSiz—This field represents the average read size in sectors (or blocks) over the scan period. In the sample line of data, the average read size was 17 sectors, or about 8.5 kilobytes.
- wrSiz—This field represents the average write size in sectors (or blocks) over the scan period. In the sample line of data, the average write size was 7 sectors, or about 3.5 kilobytes.
- R/S—This field shows the average requests per second over the scan interval. In the sample line of data, this has a value of 5.6 requests per second. This value may be shown as 0.0, but may not actually be zero. Due to precision and display rounding, it may

be possible for a drive to have very few requests (such as 0.01 per second) and actually show 0.0.

- Hits—This figure represents the cache hit rate. The cache hit rate is defined as the percentage of commands (both read and write) which were satisfied from cache. In the case of drive 44, this has a value of 38%, indicating that approximately 38% of all transfer commands sent to the drive were satisfied from cache and did not have to go to the disk. If this value is less than 10% (indicating a very marginal improvement), all data fields for this disk are shown in bold video to highlight the potential problem. If this condition persists for two consecutive scan periods, all fields are shown in reverse video.
- htSz—This field represents the average size (in sectors) of those commands which resulted in a cache hit. For drive 44, this has a value of 3.0, so we know that over the scan interval, data which was read from cache (38% of all commands) had an average size of 3 sectors, or about 1.5 kilobytes. Contrast this with the average read size of 17 sectors.
- Pg—The final field is the purge ratio. Quite simply, this field attempts to quantify the amount of data the disk purges from cache in relation to not only its data rate, but also the data rate of all other drives which are being cached.

  A value of 1 indicates that the drive is purging cache memory at a rate that is fair with respect to both itself and all other drives. Values greater than 1 indicate that the drive is purging more than its fair share of cache, while values less than 1 indicate that the drive is actually purging less cache memory than might be expected. This figure should be used as a last resort when removing cache from drives, as described in Section 5.10.4.3.2

5.10.4.3 Interpreting the Results of a CPAT Run

When analyzing the DSCACHE output, each of the fields should be examined. The action to take depends on how busy the HSC controller is. The first line of the DSCACHE output contains the percentage of time that the HSC controller is idle. If this value is less than 20%, then the HSC controller is probably saturated and some disks should be removed from caching.

If you feel that some disks should be getting a higher hit rate than is shown, then it is quite possible that other disks are filling cache with data that is never being referenced and, more importantly, purging data from cache that other disks might wish to access. As mentioned earlier, a decision to remove a disk from cache is partially based on site policy. A 10% performance improvement may be grounds for removal at one site, while another would leave a disk cached that had that amount of improvement. Because of this, the guidelines in Section 5.10.4.3.2 can only be considered as suggestions for disk removal. Tuning the cache is relatively straightforward; the decision to cache or not cache disks is more subjective.

5.10.4.3.1 Scan Time

One of the important items to consider is the scan interval of DSCACHE. If this interval is too short, transient conditions will be given greater weight, causing highly erratic analysis results. On the opposite side, scan intervals which are overly lengthy will have a tendency to smooth out conditions which should be highlighted, and will not allow timely diagnosis.

If the object of running CPAT is to tune the HSC Cache for optimal performance, then a reasonable value for DSCACHE scan time is between 10 and 15 minutes. In this manner, complaints by operators and perceived performance differences can quickly be correlated to displayed results.

If long term averaging is desired, then 30 minutes might be more appropriate. This might be useful to see the effects of cache changes if the I/O workload is highly variable. For instantaneous monitoring, a value of one minute is not unreasonable. Although this value is probably too small to allow accurate tuning, it will provide insight into the operation of cache, allowing you to track cache performance with specific applications.

5.10.4.3.2 Disk Removal

A disk drive may be removed from cache for poor performance or for its effect on other disk drives.

A disk may be removed when it performs worse when cached than without caching. This can happen when very little of the data read by the disk is contained in cache. In this case, no benefit is gained, because the data must come from the disk itself. More importantly, the cache code is still executed, since commands which write data to the disk must first check cache to possibly update the data, and commands which read data must load data into cache.

The first field to check for poor performance is the one labeled cRsp (cache response). If this field is over 100%, then it is an indication that the disk has a higher response time with cache than without. Any disk which consistently has a cache response time over 100% should be removed from cache, since its performance will then improve.

A disk with a cache response time slightly less than 100% should be removed unless it is performance-critical because of its effect on other cached disks in the system. For example, a disk with a cache response time of 97% obtains little benefit from cache, but is very likely affecting other cached disks. To aid in identifying this condition, a disk with a cache response time greater than 95% is shown in bold video. If this condition persists for two (or more) consecutive scan intervals, it is shown in reverse video.

Disk removal is the easiest and probably the most productive step in tuning cache. Disks which do not benefit from cache are quickly identified and removed, which not only improves their performance, but also frees up the cache memory they used for other disks to use.

It is important to check the R/S field (requests per second). If the value is quite low, then the amount of data (requests) is probably too low for an accurate analysis. As an example, if a disk shows a rate of 1 request per second and the scan interval is 5 minutes, then only 300 requests have been sampled. Additionally, any response time changes would probably not be noticeable on a disk with a rate as low as this. In general, the performance impact of removing a disk with less than 5 or 10 requests per second is minimal.

5.10.5 Tuning Cache Parameters

Tuning cache is considerably more difficult, since the object is to improve the performance of a disk which is already better with caching than without. Moreover, the improvements tend to have less and less impact as changes continue to be made, so more effort must be expended for smaller results. Finally, changes on any one disk may affect other disks on the system, since cache memory is a resource which is shared among all disks. With a full complement of 48 disks, it is easy to see that cache tuning is a complex task.

Example 5–2 shows a sample CPAT run. For clarity, only part of the header line is shown. In addition, the data has been cut to one column of display instead of the three columns shown on a 132-column printout.

Example 5–2: Sample CPAT Run

```
$ RUN DSCACHE
HSC Cache Performance Analysis - Version 1.1 (29 APR 92)
HSC name: HSC001
Scan time in minutes: 5

HSC90 V650 HSC001  Id 000000000002 On 29-Apr-1992 10:06:58.82   Up:  21:06 91.5% Idle

Disk S cRsp rdSiz wrSiz  R/S Hits htSz Pg
  44 C  69%  17.0   7.0  5.6  38%  3.0  1
  20 C  51%   4.0   4.0 13.5  57%  2.0  1
  23 C  70%   1.7   1.2  0.3  38%  1.4  6
  26 C  66%   1.2   1.9 15.3  39%  1.3  3
  29 C  42%   3.0   1.1 20.4  69%  3.0  0
  32 C 107%   0.5  13.0 20.3   0%  0.0  0
  35 C
  38 C  44%   3.8   1.4 11.7  65%  1.8  2
  44 C  69%  17.0   7.2 15.6  38%  3.0  1
  47 C  76%   4.1   1.5 10.3  33%  4.5  2
  50 C  39%   4.0  12.0  2.1  72%  2.1  1
  53 C  96%   7.0   4.8 30.5  10   2.1  2
```

5.10.5.1 Overall Evaluation

The first step in analysis of the data is to take a quick glance at the display, looking for any obvious problems. Things to look for are excessive response times (remove the disk) and low I/O rates (ignore the disks). In Example 5–2, the first thing to notice is disk 32. At a response time of 107%, it should be removed from cache because its performance is worse with caching than without caching.

Other points to notice from Example 5–2 are:

- Disk 35 has no I/O, so no data is shown. Although it is receiving no benefit from cache, neither is it hurting anything to keep it cached.
- Disk 23 has a negligible I/O rates, so we can probably ignore it for now.
- Disk 50 has a request rate of 2.1 requests per second, so although the cache response time of 39% looks impressive, you will probably not notice its cached response with such a low rate of requests.

5.10.5.2 Marginal Improvement

The next step is to look for disks which have a marginal improvement. If this condition has persisted for a while and the HSC controller is busy, it might pay to remove the disk. In Example 5–2, disk 53 has a cached response time of 96%, a poor performance return for a cached disk. If the HSC controller is busy, we might want to remove it from cache since it may be affecting other disks. This is particularly true since disk 53 has over 30 requests per second, implying a fair amount of cache activity.

5.10.5.3 Read Size

The next step is to examine the average read size. If this size is greater than the cache threshold size in the HSC controller, the data will not be cached. Disk 44 in Example 5–2 has an average read size of 17 sectors. Since the default read threshold is 8 sectors, very few of the read requests from disk 44 will be cached.

In HSC software V6.5, the read threshold is a global parameter. If many disks in the configuration show an average read size of greater than the read threshold, increasing the read threshold may result in a performance improvement. If many disks in the configuration show an average read size smaller than the read threshold, decreasing the threshold may be worthwhile.

There is an interplay between the average read size, the read threshold, and the average hit size. The goal is to have the smallest possible read threshold which results in the best cached response. To do this, raise the read threshold slightly higher than the average read size, then (after viewing the results) reduce it to slightly above the average hit size as seen in the results of the run after raising the read threshold. This two-step process is necessary since the average hit size may change when the read threshold is raised.

5.10.5.4 Write Size

The next step is to examine the average write size. If this value is greater than the write threshold size in the HSC controller, then the caching policy will be UPDATE if the small policy is ALLOCATE or UPDATE, and INVALIDATE if the small policy is INVALIDATE. If the size is less than or equal to the write threshold, the policy may be set by the user. In Example 5–2, the only disks with write sizes greater than 8 sectors (the HSC software default) are drives 32 and 50. Drive 50 has a low request rate, so it probably can be safely ignored.

Modification of the small write policy or the write threshold may be worthwhile. This decision best made with input from someone familiar with the applications being run on the disks of interest.

5.10.5.5 Purge Ratio

The purge ratio is normally the last thing to check, since it is a relatively nebulous figure. It is designed to show how much cache is being purged by a specific drive, relative to the I/O appetite of that drive, relative to all other drives currently being cached. If this drive is purging data at an acceptable rate, then the value will be 1. If the drive is purging twice as much data as would be expected, the value displayed would be 2.

In Example 5–2, drive 26 has a purge ratio of 3, indicating that it is purging data three times more than it should be in relationship to everything else that is happening with the cache. The difficult question to answer is: what value is too high? In general, a high purge ratio only indicates that data is being thrown out of cache more than might be expected. The crucial issue is not how much data is being thrown out, but rather which data is being purged. If the purged data will never be referenced, then no harm has been done. If, on the other hand, another drive might have used that cached data if it had not been purged, then the drive which purged the data has indirectly limited the performance of other drives.

In addition, purging data does take time for the HSC controller to perform. Because of this, subsequent requests to the HSC controller will have to wait. At high request rates, this delay may be noticeable, causing a reduction in the overall performance of the HSC controller. This is not cause for concern if the HSC controller idle time (shown on the first line of the display) is greater than 10%.

Because of the complex nature of this value, it is recommended that it be used as a selection and tuning criteria only as a last resort. This field is displayed in bold video if the purge ratio is greater than 9. Values 10 and greater are grounds for suspicion.

Other than simply removing the offending drive from cache, the only other possible cure for a drive with a high purge ratio would be steps to reduce the amount of data being purged. This typically would mean decreasing the read threshold size, although raising the write threshold size and changing the small write policy to either UPDATE or INVALIDATE may have some effect.

5.10.6 Rerun DSCACHE for Optimum Performance

After making all suggested changes, note the cache response times for each drive and rerun DSCACHE. The only criteria for judging the effectiveness of caching is the cached response time (cRsp). If this value is lower after changing the parameters, then the correct decision was made. If it is higher, then an incorrect decision was made and the process must begin again.

It is also important to note that cache performance will change over time as the I/O workload changes. It is therefore important to make changes slowly and not be surprised to observe the cached response times varying widely from one run to another with no changes at all in the cache parameters. This variation should not be ignored when tuning cache.

5.10.6.1 Order of Analysis

Since cache memory is shared by all disks which are cached, changes to any one disk will very likely affect all other disks being cached. Changes should be done slowly and carefully, letting the system stabilize between changes. Some changes are more drastic than others and will have more effect on the overall system operation. Although not cast in concrete, the following is a suggested ordering for tuning cache:

1. Adjust the cache parameters.
2. Remove any disks which consistently show a response time over 100%.
3. Remove any disks which are consistently highlighted in the display.
4. Remove any disks which have a purge ratio consistently higher than 10.
5. Add any disks flagged by the program as "Consider caching" and return to step 1.

5.10.6.2 Analyzing Different Applications

It should be remembered that different applications may well access disks differently. For example, an order entry system is highly write-intensive and caching might provide little benefit. A report generator, on the other hand, might have only read access to the same files that the order entry system wrote. Because of this, it is important to run DSCACHE when different applications are running in order to build a picture of the different I/O workloads. Since changes to cache are relatively easy to make (with the HSC SETSHO utility), changing workloads could then be dealt with by changing the cache parameters for each application as necessary.

5.10.7 Performing a Deferred Analysis CPAT Run

Although the DSCACHE program is designed to be run interactively, it is possible to collect data and analyze it later. The interpretation of the data remains the same, but the procedure for collecting the data changes somewhat. Basically, the steps are as follows:

1. Connect to the HSC controller from a VMS system with the SET HOST command, creating a log file.
2. Run DSTAT on the HSC controller with the desired scan interval.
3. Analyze the log file with DSCACHE.

5.10.7.1 Limitations On Running Deferred Analysis

In order to accomplish this deferred analysis, three restrictions must be observed:

1. DSTAT cannot be run, either directly or through DSCACHE, at the same time as the HSC utility VTDPY. Both programs assume exclusive use of the same set of internal statistics counters in HSC memory. Either program will issue an error message if it determines that another program is already running. HSC software V6.0 does not prevent simultaneous access to the counters and can result in erroneous results from both DSTAT and VTDPY.
2. In order to perform certain calculations, DSCACHE will not perform an analysis on the first scan contained in the log file. If, for example, the session began at 10:00 AM with a 5-minute scan interval, the analysis would not be done at 10:05 AM (the first scan). The first scan displayed by DSCACHE would be the second scan, at 10:10 AM.

   NOTE

   This restriction only applies when DSCACHE is analyzing a log file. When DSCACHE is run in the interactive mode, all scans will be analyzed.
3. The DSCACHE analysis should be performed on the same system or cluster that the data was collected on. DSCACHE uses unit numbers in the DSTAT output to collect additional data about the actual disk types from the system. If the analysis is done on a

different system, DSCACHE makes assumptions about the drive types that may result in incorrect performance information.

5.10.7.2 Connecting to the HSC Controller

In order to create a log of the data to be analyzed, the first step is to connect to the HSC controller. DIAGNOSE privileges are required to make this connection.

To make the connection, enter the SET HOST command with a log file specified to capture the data (user entered data is shown in bold type):

```
$ SET PROCESS/PRIV=DIAGNOSE
$ SET HOST/HSC/LOG=FOO.LOG HSC001
%HSCPAD-I-LOCPROGEXE, Local program executing - type ^\ to exit, ^Y for prompt

HSC>
```

In this example, the user has connected to the HSC controller named HSC001 and has created a file on VMS called FOO.LOG. This log file will capture all transactions.

5.10.7.3 Running DSTAT

After connecting to the HSC controller, the next step is to run the DSTAT program. This program will collect the raw cache information and print it out on a periodic basis. Since this information is being captured in a log file on VMS, DSCACHE is able to read and analyze the information.

DSTAT prompts for a scan interval. The guidelines for determining the number of minutes between scans are exactly the same as when running DSCACHE interactively.

```
HSC> RUN DSTAT
DSTAT-Q Interval (1 to 90 minutes)? 5
DSTAT is running with a 5 minute measurement increment.
```

Note that when invoking DSTAT, you may also enter the scan interval on the same line that you start DSTAT:

```
HSC> RUN DSTAT 5
DSTAT is running with a 5 minute measurement increment.
```

Every scan interval (5 minutes in the preceding example), DSTAT will print data to the terminal and the VMS log file. The data printed is greater than 80 columns, so although it will be correctly captured and formatted in the log file, it may not display correctly on your screen. The exact contents of the DSTAT data is beyond the scope of this document, and is therefore not covered here.

5.10.7.4 Terminating Data Collection

When it is decided that sufficient information has been captured, terminate DSTAT, break the connection with the HSC controller, and close the VMS log file. First, enter Ctrl/Y to stop DSTAT:

```
Ctrl/Y
DSTAT-I Exiting
HSC>
```

Next, enter Ctrl/\ (Control backslash) to break the connection with the HSC controller:

```
PLAYER>                                   !Control backslash does not echo
%HSCPAD-F-NOLOCEXE, Local program not executing
-SYSTEM-F-ABORT, abort
%HSCPAD-S-END, Control returned to node SOCCER
$
```

At this point, the file FOO.LOG contains a transcript of the entire session, including all the data DSTAT has been printing to the terminal. The next step is to analyze this data.

5.10.7.5 Analyzing the Log File Data

Analysis of the log file data is still done with DSCACHE. The only difference when doing the deferred analysis DSCACHE run is to specify the name of the log file instead of the HSC controller name, and append a /FILE to the name:

```
$ R DSCACHE
HSC Cache Performance Analysis - Version 1.1 (29 APR 92)
```

When asked for the name of the HSC controller, enter the name of the log file you just created, and add /FILE:

```
HSC name: FOO.LOG/FILE
```

DSCACHE now reads the file and displays the analysis of the data, one scan interval at a time. After a single screen has been displayed, DSCACHE will pause and wait for confirmation to proceed. The following message is printed at the bottom of the screen:

```
Pass 1 completed, <CR> for next scan:
```

When you are through examining the current analysis screen, press Return and DSCACHE will analyze the next scan. Proceed through the entire file this way, one screen at a time.

Chapter 6

SETSHO Utility

The SETSHO utility is used to view and change the internal state of the HSC controller. SETSHO allows you to control some of the decision-making processes that relate to hosts and devices connected to the HSC controller. The SETSHO utility can be used to enable automatic device integrity tests and set or show some system parameters.

Only one SETSHO utility process can be active at any time.

When using the SETSHO utility, you can:

- Execute SHOW commands anytime.
- Execute SET commands only when the Secure/Enable switch is in the ENABLE position; otherwise, SETSHO returns an error message.
- Enter only enough letters to make a command unique.
- Enter the HELP command to display descriptions of SET and SHOW commands.

Set and show run simultaneously as a single process. SET commands are used to change parameters; SHOW commands are used to display parameters and states.

6.1 How to Run SETSHO

There are two ways to run SETSHO:

- Enter SET or SHOW at the HSC> prompt, followed by the appropriate SET or SHOW command parameters.
- Enter RUN SETSHO at the HSC> prompt to use SETSHO interactively. The following prompt shows the utility is properly loaded and ready:

  ```
  SETSHO>
  ```

6.2 How to Exit SETSHO

There are several ways to exit SETSHO:

- When you run SETSHO from the HSC> prompt, it exits automatically after every command.
- When you run SETSHO from the SETSHO> prompt:
  - Enter the EXIT command to update the System Configuration Table (SCT). If you change system parameters that require the HSC controller to reboot, the SCT is updated when you execute the EXIT command. Refer to Section 3.6 for a description of the SCT.
  - Enter Ctrl/Y or Ctrl/C to exit SETSHO without changing the SCT.

6.3 How to Concatenate SETSHO Commands

The SETSHO utility allows you to enter several commands on the same command line. You can enter concatenated commands at either the HSC> prompt or the SETSHO> prompt.

If SETSHO detects an error while interpreting or processing one command in a concatenated string, it discards the remaining commands on the command line because they may depend on a previous command to work properly.

To enter concatenated commands:

1. Enter multiple commands separated by a semicolon.
2. Press Return at the end of the concatenated command line.

In the following example of a concatenated command, SETSHO executes each command in the order in which it is entered:

```
SETSHO>SET NAME GREG; ❶ SET ID %X11071789; ❷ SHOW SYSTEM ❸
```

❶ Sets the system name to GREG.

❷ Sets the system identification to 11071789.

❸ Shows system parameters and states.

6.4 SETSHO Commands That Require Immediate Reboot

Some parameter changes require an immediate reboot of the HSC controller before the new values take effect. Parameters, such as system name or system identification, should not be changed while the HSC controller is running. The system name and system identification affect other systems connected to the HSC controller over the CI bus. For this reason, the HSC controller reboots when you exit SETSHO and the new parameters become effective after the reboot. The HSC controller is out of service during the reboot.

An immediate reboot is required if you change parameters with the following commands:

- SET ID
- SET NAME
- SET ODT (if not previously loaded)
- SET REQUESTOR
- SET SCT CLEAR
- SET SERVER DISK/MAX_SECTORS_PER_TRACK

6.4.1 Rebooting From the SETSHO> Prompt

When you run SETSHO from the SETSHO> prompt and change a parameter that requires an immediate reboot, the following message is displayed:

```
SETSHO-I Your settings require an IMMEDIATE reboot on exit.
```

This message is displayed only after the first parameter change that requires an immediate reboot.

When you enter the EXIT command, the following prompt is displayed:

```
SETSHO-Q Rebooting HSC, type Y to continue, CTRL/Y to abort:
```

Enter Y to reboot the HSC controller and implement the new parameters. The following display indicates that the reboot occurred because of a parameter change:

```
INIPIO-I Booting...

    HSC70 Version V600  7-Jan-1990 12:02:30    System HSC001

Copyright 1982 Digital Equipment Corporation.  All Rights Reserved.

SINI-E  Seq 1. at  7-JAN-1990 12:02:30
        Parameter change
        process SETSHO
        PC  011612
        PSW 140001
        Reason 000000
```

The SCT is updated with the new parameters. Refer to Section 3.6 for a description of the SCT.

Enter Ctrl/Y to exit SETSHO and discard the parameter changes. SETSHO displays the following messages:

```
SETSHO-F CTRL/C or CTRL/Y Abort.  No changes made to SCT.
SETSHO-I Program Exit
```

The next reboot does not implement the changes.

6.4.2 Rebooting From the HSC> Prompt

When SETSHO is run from the HSC> prompt and a parameter is changed that requires an immediate reboot, SETSHO displays the following messages:

```
SETSHO-I Your settings require an IMMEDIATE reboot on exit.
SETSHO-Q Rebooting HSC, type Y to continue, CTRL/Y to abort:
```

Enter Y to reboot the HSC controller and implement the new parameters. The HSC controller reboots and displays the reason for the reboot.

Enter Ctrl/Y to abort SETSHO and discard the parameter changes. SETSHO displays the following messages:

```
SETSHO-F CTRL/C or CTRL/Y Abort. No Changes made to SCT.
SETSHO-I Program Exit
```

NOTE

When you change parameters from the HSC> prompt, SETSHO exits automatically after each command.

6.5 SETSHO Commands That Require the ENABLE REBOOT Command

Other parameter changes in SETSHO also require a reboot to take effect, but the reboot does not need to be immediate. These parameters are changed by the following commands:

- SET ALLOCATE DISK
- SET ALLOCATE TAPE
- SET HOST
- SET LOAD
- SET MAX_FORMATTERS
- SET MAX_TAPES
- SET POLLER

The ENABLE REBOOT command allows you to change these parameters and reboot the HSC controller when it is convenient.

6.5.1 Using the ENABLE REBOOT Command

When you change a parameter with one of the commands listed in Section 6.5, the following informational message is displayed:

```
SETSHO-I Your settings require a reboot. Use ENABLE REBOOT.
```

This message is displayed only after the first parameter change that requires the use of the ENABLE REBOOT command.

When you enter the ENABLE REBOOT command, another informational message is displayed:

```
The HSC will reboot on exit.
```

Upon exit, the HSC controller reboots and updates the SCT with the new parameters.

When you change a parameter and enter the EXIT command without entering the ENABLE REBOOT command, the changes are saved on the RX33 boot media. The changes become effective the next time the HSC controller reboots. This feature allows you to change parameters, then reboot when it is convenient.

When you enter a SHOW command to view a parameter you changed without using the ENABLE REBOOT command, the new parameter value is displayed even though the previous value is in effect until the next reboot.

6.5.2 Suppressing Informational Messages with the ENABLE REBOOT Command

To keep the informational messages from displaying each time a parameter is changed that requires the HSC controller to reboot:

1. Enter the ENABLE REBOOT command before you change any parameters. The following informational message is displayed:

   ```
   The HSC will reboot on exit.
   ```

2. Following this message, each time you change a parameter, the SETSHO> prompt is displayed without further informational messages.

3. Enter the EXIT command when you have finished changing parameters. The following prompt is displayed:

```
SETSHO-Q Rebooting HSC, type Y to continue, CTRL/Y  to abort:
```

4. Enter Y to reboot the HSC controller and implement the new parameters. Information is displayed to indicate that the reboot occurred because of a parameter change.

   If you enter Ctrl/Y, you will exit SETSHO and discard the parameter changes. SETSHO displays a message indicating that no changes were made to the SCT. The next reboot does not implement the changes.

6.5.3 Using the ENABLE REBOOT Command Remotely

The ENABLE REBOOT command allows you to remotely boot an HSC controller using the Diagnostic Utility Protocol (DUP). Follow this procedure:

1. Connect to the HSC through DUP.
2. Enter the RUN SETSHO command.
3. Enter the ENABLE REBOOT command.
4. Enter the EXIT command without making any parameter changes.
5. Enter Y at the reboot prompt.

6.6 The SET Commands

This section contains descriptions of the SET commands. The SET commands modify the way the HSC controller operates. These modifications are made to the SCT as described in Section 3.6.

Many SET commands do not take effect until the HSC controller reboots. Some SET commands affect a CI network to such an extent that the HSC controller must reboot to present itself to the other members of the network. Other SET commands require a reboot to internally reorganize the HSC controller.

After a patch has been installed using the PATCH utility, many SETSHO parameters cannot be SET until the HSC controller has been rebooted. The affected parameters are those which require the SCT to be updated. If you try to SET these parameters before rebooting the HSC controller, the following message is displayed:

```
SETSHO-Q MEDIA VERSION MISMATCH.  Correct media problem.
       Press RETURN to continue, CTRL/Y to abort:
```

You can use any of the SETSHO SHOW commands to display the previously set commands before rebooting.

SET ALLOCATE DISK

Sets the disk allocation class.

Format

SET ALLOCATE DISK *allocation-class*

Command Qualifiers	**Defaults**
None	None

Parameters

allocation-class
Specifies the disk allocation class to which the HSC disk server should belong. The allocation class is specified by a number from 0 to 255 (0 indicates no allocation class).

Description

The SET ALLOCATE DISK command sets the disk allocation class in a VAXcluster environment. The initial default value is 0. Refer to the VAXcluster documentation for information on how this command affects the cluster.

Enter the SHOW SYSTEM command to view the setting of the disk allocation class.

The SET ALLOCATE DISK command requires an HSC controller reboot to take effect. Enter the ENABLE REBOOT command.

SET ALLOCATE DISK

Example

The following example shows how to use the SET ALLOCATE DISK command:

Example 6–1: SET ALLOCATE DISK Command

```
SETSHO>SET ALLOCATE DISK 35
```

This command sets the disk allocation class to 35.

SET ALLOCATE TAPE

Sets the tape allocation class.

Format

SET ALLOCATE TAPE *allocation-class*

Command Qualifiers	Defaults
None	None

Parameters

allocation-class
Specifies the tape allocation class to which the HSC tape server should belong. The allocation class is specified by a number from 0 to 255 (0 indicates no allocation class).

Description

The SET ALLOCATE TAPE command sets the tape allocation class in a VAXcluster environment. The initial default value is 0. Refer to the VAXcluster documentation for information on how this command affects the cluster.

Use the SHOW SYSTEM command to view the setting of the tape allocation class.

The SET ALLOCATE TAPE command requires an HSC controller reboot to take effect. Use the ENABLE REBOOT command.

SET ALLOCATE TAPE

Example

The following example shows how to use the SET ALLOCATE TAPE command:

Example 6–2: SET ALLOCATE TAPE Command

```
SETSHO>SET ALLOCATE TAPE 29
```

This command sets the tape allocation class to 29.

SET AUTOMATIC_DIT

Controls initiation of the HSC controller automatic device integrity tests.

Format

SET AUTOMATIC_DIT *sense*

Command Qualifiers	Defaults
None	None

Parameters

sense
Specifies the mode of the automatic device integrity tests.

ENABLE—Enables the execution of automatically scheduled device integrity tests.

DISABLE—Disables the execution of automatically scheduled device integrity tests (see Restrictions).

Restrictions

Do not disable automatic device integrity tests unless directed by Digital Services. These tests can reclaim suspect system resources.

Description

Specifies whether the HSC controller should dedicate the necessary resources to execute the automatic device integrity tests.

There are two automatic device integrity tests:

- Inline memory test—Tests HSC controller data memory buffers that caused a parity error when accessed by a data channel or the port interface module.

SET AUTOMATIC_DIT

- Inline disk device integrity test—Tests disk units declared inoperative by the disk server software.

Enter the SHOW SYSTEM command to view the setting of the automatic device integrity tests.

The SET AUTOMATIC_DIT command does not require an HSC controller reboot to take effect.

Example

The following example shows how to use the SET AUTOMATIC_DIT command:

Example 6–3: SET AUTOMATIC_DIT Command

```
SETSHO>SET AUTOMATIC_DIT ENABLE
```

This command enables the automatic device integrity tests.

SET CI

Displays statistics collected for CI nodes and resets the counters to collect statistics for the CI nodes specified.

Format

SET CI *monitor-node-number*

Command Qualifiers	**Defaults**
None	None

Parameters

monitor-node-number
Specifies the CI node the HSC controller should monitor for statistics. The node number can be a number from 0 to the maximum node number supported by your version of HSC controller and VMS software (refer to the Software Product Description).

Use ALL to direct the HSC controller to collect statistics for all nodes. The factory setting specifies the collection of statistics for all nodes.

Description

Directs the port processor to collect statistics for the specified node. The SET CI command displays the current event counters for the node and resets the event counters to zero.

Enter the SHOW CI command to view and reset the counters without changing the node for which the statistics are being collected.

The SET CI command does not require an HSC controller reboot to take effect.

Examples

The following examples show how to use the SET CI command:

Example 6–4: SET CI Command for Node 12

```
SETSHO>SET CI 12
Statistics previously collected for all nodes:

                Path A          Path B
ACKs:           3117            3244
NAKs:           0               0
No Response:    11445           11162

Discarded Datagrams:  199
Discarded RTNDATS:  0
```

In Example 6–4, the SET CI command requests statistics for node 12.

Example 6–5: SET CI Command for All Nodes

```
SETSHO>SET CI ALL
Statistics previously collected for node number 12:

                Path A          Path B
ACKs:           53              58
NAKs:            1               0
No Response:     1               0

Discarded Datagrams:  0
Discarded RTNDATS:  0
```

In Example 6–5, the SET CI command requests statistics for all nodes.

When you request statistics, SETSHO displays the statistics for all nodes it has been monitoring until the time of your request. It then clears the counters and begins gathering statistics for the requested node(s).

Refer to the SHOW CI command for an explanation of the statistics shown in these examples.

SET CREDIT_MANAGER RESET

Causes the dynamic credit manager (CRMGR) to reset the credits extended to all open, managed connections to their default values and to reset the disk and tape servers' counters to zero.

Format

SET CREDIT_MANAGER RESET

Command Qualifiers	Defaults
None	None

Description

This command causes the credit manager to enter RESET mode. RESET mode attempts to restore the default number of credits to all connections. This mode also resets disk and tape server counters.

The SET CREDIT_MANAGER RESET command should be used when there is little or no activity on the HSC controller. Issuing the command when the HSC controller is heavily loaded will result in the credit manager aborting after 2000 attempts to reset.

A revocation of a credit requires that the host losing the credit respond by returning the credit through a credit response message. The host will be unable to return the credit response message if all credits are in use. Returning credits to the credit manager may therefore require several attempts before the host actually releases the credits.

Use the SHOW CREDIT_MANAGER command to track changes while the SET CREDIT_MANAGER RESET command is active.

SET CREDIT_MANAGER RESET

Example

The following example shows how to use the SET CREDIT_MANAGER RESET command.

Example 6–6: Using the SET CREDIT_MANAGER RESET Command

```
SETSHO>SET CREDIT_MANAGER RESET
```

This command invokes the credit manager's RESET mode of operation.

SET DATE

Sets the HSC system date and time.

Format

SET DATE *date-and-time*

Command Qualifiers	**Defaults**
None	None

Parameters

date-and-time
Specifies the date and time the HSC controller uses. The format for the parameter is:

```
dd-mmm-yyyy[:hh:mm:ss]
```

where:
dd is the day. Use a number from 01 to 31.
mmm is the month. Use the first three letters of the month.
yyyy is the year. Use a number with four digits.
hh is the hour. Use a number from 00 to 23.
mm is the minutes. Use a number from 00 to 59.
ss is the seconds. Use a number from 00 to 59.

Only the day, month, and year fields are required.

Description

Resets the date and time used by all HSC controller processes that report date and time.

When the HSC controller is initially booted, the date is set to 17-NOV-1858:00:00:00 (the astrophysical base date). When the HSC is set on line to hosts, the first host communication with the HSC sets the date and time to the host date and time.

SET DATE

Use the SET DATE command to set the initial date and time when the HSC controller is not on line to a host, or to override the date and time set by a host. The date and time may not be set earlier than the HSC software build date that is displayed when the HSC controller boots. If you omit the optional hour, minute, and second fields of the *date-and-time* parameter, they will default to 0.

Use the SHOW SYSTEM command to view the current date and time.

The SET DATE command does not require an HSC controller reboot to take effect.

Example

The following example shows how to use the SET DATE command:

Example 6–7: SET DATE command

```
SETSHO>SET DATE 22-JAN-1990:15:22:57
```

This command sets the date to January 22, 1990, and the time to 3:22 p.m. and 57 seconds.

SET DEVICE

Controls host access, specifies the cache status, or specifies the cache write allocation policy for a specified storage device.

Format

SET [DEVICE] *unit-id sense*

Command Qualifiers	**Defaults**
None	None

Parameters

unit-id
Specifies to which disk or tape unit the command applies. The format for *unit-id* is:

xnnnn

where:
x is a D, indicating a disk unit, or a T, indicating a tape unit.
nnnn is the unit number.

Unit-id may also be D_ALL only when the sense is [NO]CACHE.

sense
Specifies the type of access granted to the host, the cache status of the device, or the cache write allocation policy associated with the device.

[NO]HOST_ACCESS—Allows/denies host access to the specified storage device.
[NO]CACHE—Controls whether I/O requests to or from the device go through caching hardware. This parameter is valid for disk units only.
W_ALLOCATE—Specifies the cache write allocation policy for the device to be ALLOCATE. Data written to the device will also be written to cache memory. This may cause cache memory to be allocated if the data does not already exist in cache. This parameter is valid for disk units only.

W_INVALIDATE—Specifies the cache write allocation policy for the device to be INVALIDATE. Data written to the device that is also found in cache causes the specific cache memory allocated for the request to be invalidated. Cache memory is then deallocated. This parameter is valid for disk units only.

W_UPDATE—Specifies the cache write allocation policy for the device to be UPDATE. Data that is currently resident in cache will be updated. This parameter is valid for disk units only.

Description

The SET DEVICE command is used to control host access, specify cache status, or specify the cache write allocation policy for a specified storage device.

The SET DEVICE command does not require an HSC controller reboot to take effect.

Changing Host Access

The SET DEVICE NOHOST_ACCESS command is useful if a drive should not be mounted by the operating system or a user.

By default, all drives connected to the HSC controller are set to HOST_ACCESS, meaning the hosts can mount all drives.

A maximum of 48 NOHOST_ACCESS entries can be stored in the SCT.

The SHOW DISKS and SHOW TAPES commands display the settings of HOST_ACCESS for all units.

Changing Drive States

When you change the state of a drive from NOHOST_ACCESS to HOST_ACCESS, you allow host access to the drive.

When you change the state of a drive from HOST_ACCESS to NOHOST_ACCESS, the following may occur:

If the drive is:	These actions take place:
Available (not mounted by any host)	The drive enters the NOHOST_ACCESS state.
Online	The SET DEVICE command is rejected and SETSHO issues an error message. Dismount the drive from the host and try the command again.
Duplicated (more than one drive with the same unit number is connected to the HSC controller)	The NOHOST_ACCESS state is recorded and later activated when the duplicate unit condition is removed and the unit becomes available.
Unknown (due to logical or electrical reasons)	The HSC controller sets the state of the drive to NOHOST_ACCESS when it appears.

SETSHO Action

When the SETSHO utility is directed to change the HOST_ACCESS state of a drive, the following events occur:

- SETSHO notes the change and informs the disk path to change the state of a drive when the EXIT command is issued. This function exists so that if you abort SETSHO with a Ctrl/Y or Ctrl/C, the drive remains in the state that existed before you started SETSHO. SETSHO does not update the SCT or change the drive state until you execute the EXIT command.
- SETSHO marks the HOST_ACCESS state in the SCT. The SCT is preserved across boots; the disk and tape servers examine this table on subsequent boots and when new drives are connected to the HSC controller.
- If you entered the SET DEVICE command at the HSC> prompt, SETSHO exits automatically and the state of the drive changes immediately.

  If you entered the SET DEVICE command from the SETSHO> prompt, make sure you use the EXIT command to exit SETSHO. The state of the drive changes on exit.

Enabling Caching

The SET DEVICE CACHE command is used to enable caching for specific disk units. By default, caching is disabled for all disk units. The CACHE TABLE will accommodate, at most, 48 cached disk units. The SHOW DISKS command displays the cached state of all disk units.

SETSHO Action

When the SETSHO utility is directed to change the cache state and/or policies of a disk unit, the following events occur:

- All changes take effect immediately. However, you must issue the SETSHO EXIT command to update the on-disk copy of the SCT. If you abort SETSHO with a Ctrl/Y or Ctrl/C before the on-disk copy of the SCT has been updated, your changes will not be permanently saved across boots.
- If you entered the SET DEVICE command from the HSC> prompt to change the cache state, SETSHO exits automatically. The drive state and on-disk SCT are both updated immediately.

Specifying the Cache Write Allocation Policy

You may control the cache write allocation policy for disk units with one of the policy parameters of the SET DEVICE command. By default, the cache write allocation policy for all disk units is W_ALLOCATE. The SHOW DISKS command displays the write allocation policy for each cached disk unit.

SETSHO action taken when changing the cache write allocation policy is the same as that for enabling caching. Refer to "SETSHO Action" under the "Enabling Caching" heading for details.

Examples

The following examples show how to use the SET DEVICE command:

Example 6–8: SET DEVICE Dn NOHOST_ACCESS Command

```
SETSHO> SHOW DISKS ❶
Unit     Req     Port     Type     State          Cached   Access   Version
   10     5        3      RA70     Available        No     Host     MC-81, HV-7
   12     4        1      RA70     Available        No     Host     MC-81, HV-7
   13     4        2      RA70     Available        No     Host     MC-79, HV-7
   14     4        0      RA70     Available        No     Host     MC-79, HV-7
   15     4        3      RA70     Available        No     Host     MC-79, HV-7
   78     7        0      RA81     Available        No     Host     MC-7, HV-15

The NOHOST_ACCESS Table is empty. ❷

The CACHE Table is empty.

SETSHO> SET DEVICE D15 NOHOST_ACCESS ❸
SETSHO> SHOW DISKS
Unit     Req     Port     Type     State          Cached   Access      Version
   10     5        3      RA70     Available        No     Host        MC-81, HV-7
   12     4        1      RA70     Available        No     Host        MC-81, HV-7
   13     4        2      RA70     Available        No     Host        MC-79, HV-7
   14     4        0      RA70     Available        No     Host        MC-79, HV-7
   15     4        3      RA70     Available        No     NoHost❹     MC-79, HV-7
   78     7        0      RA81     Available        No     Host        MC-7,  HV-15

Units in NOHOST_ACCESS Table:
        D15 ❺

The CACHE Table is empty.

SETSHO> EXIT ❻
SETSHO-I Program Exit
```

❶ The SHOW DISKS command displays the current state of each disk connected to the HSC controller. Note that all units are host accessible.

❷ No units are shown in the NOHOST_ACCESS table.

❸ Unit 15 is set to NOHOST_ACCESS with the SET DEVICE command.

Example 6–8 Cont'd on next page

Example 6–8 (Continued): SET DEVICE Dn NOHOST_ACCESS Command

---

❹ The SHOW DISKS command shows unit 15 is set to NOHOST_ACCESS.

❺ Unit 15 is now listed in the NOHOST_ACCESS table.

❻ On exit, the SCT is updated and the drive state is changed.

Example 6–9: SET DEVICE Dn W_UPDATE Command

```
SETSHO> SHOW DISKS
Unit     Req      Port      Type      State            Cached       Access    Version
   10     5         3       RA70      Available         No          Host      MC-81, HV-7
   12     4         1       RA70      Available         Yes-A ❶     Host      MC-81, HV-7
   13     4         2       RA70      Available         No          Host      MC-79, HV-7
   14     4         0       RA70      Available         No          Host      MC-79, HV-7
   15     4         3       RA70      Available         No          NoHost    MC-79, HV-7
   78     7         0       RA81      Available         No          Host      MC-7, HV-15

Units in NOHOST_ACCESS Table:
        D15

Units in CACHE Table:
        D12
SETSHO> SET DEVICE D12 W_UPDATE ❷
SETSHO> SHOW DISKS
Unit     Req      Port      Type      State            Cached         Access    Version
   10     5         3       RA70      Available         No            Host      MC-81, HV-7
   12     4         1       RA70      Available         Yes-U ❸       Host      MC-81, HV-7
   13     4         2       RA70      Available         No            Host      MC-79, HV-7
   14     4         0       RA70      Available         No            Host      MC-79, HV-7
   15     4         3       RA70      Available         No            NoHost    MC-79, HV-7
   78     7         0       RA81      Available         No            Host      MC-7, HV-15

Units in NOHOST_ACCESS Table:
        D15

Units in CACHE Table:
        D12
```

❶ The SHOW DISKS display indicates that disk unit 12 is cached and uses a write allocation policy of ALLOCATE as indicated by the letter "A."

❷ The write allocation policy of disk unit 12 is changed using the SET DEVICE command.

❸ Disk unit 12 now shows a write allocation policy of UPDATE as indicated by the letter "U." The SCT is updated immediately with this new information.

SET DUMP

Controls whether the HSC controller provides a system exception dump.

Format SET [NO]DUMP *device*

Command Qualifiers	**Defaults**
None	None

Parameters

device
Specifies the destination of the dump.

CONSOLE—Instructs the HSC controller to print an ASCII dump of internal registers to the console upon failure.

Description

The dump is a useful tool for Digital Services to use in diagnosing both hardware and software problems in the HSC controller. For this reason, keep the system exception dump in the enabled state.

When you execute the SET DUMP CONSOLE command, a summary of the HSC controller state (including system and CPU registers) is displayed on the terminal after a system failure.

To view the current setting of the HSC controller state, use the SHOW SYSTEM command.

The SET DUMP command does not require an HSC controller reboot to take effect.

Example

The following example shows how to use the SET DUMP command:

Example 6–10: SET DUMP Command

```
SETSHO>SET DUMP CONSOLE
```

This command enables a dump to the console.

SET ERROR

Sets the severity level of error messages displayed by the HSC controller on the console and on virtual terminals.

Format

SET ERROR *error-level*

Command Qualifiers	**Defaults**
/[NO]PERMANENT	NOPERMANENT

Parameters

error-level
Specifies the error level to be displayed.

Qualifiers

/[NO]PERMANENT
Specifies whether the error level should be reflected across HSC controller reboots, as well as for the current boot. The default is NOPERMANENT, meaning that the error level setting is not saved across an HSC controller reboot.

Description

Use this command to restrict the number of displayed messages. When you select an error level, the HSC controller displays errors of that level and all errors more severe. The error levels shown in Table 6–1 may be displayed:

Table 6–1: SETSHO Error Levels

Error Level	Error Types Displayed
Success	Success, Info, Warning, Error, Fatal
Info	Info, Warning, Error, Fatal
Warning	Warning, Error, Fatal
Error	Error, Fatal
Fatal	Fatal

This command does not control error messages displayed by utilities run on the console or virtual terminals. This command can only be applied to the following:

- Messages displayed through the central error reporting facility (CERF)
- Messages from the disk server
- Messages from the tape server
- Messages from the CI manager
- Messages from the Executive
- Out-of-band error messages

Use the SHOW ERROR command to view the error level settings.

The SET ERROR command does not require an HSC controller reboot to take effect.

SET ERROR

Example

The following example shows how to use the SET ERROR command:

Example 6–11: SET ERROR Command

```
SETSHO> SHOW ERROR ❶

Error Levels Used Next Re-initialization (/PERMANENT):
        Fatal
        Error
        Warning
        Informational ❷

Error Levels Used Currently (/NOPERMANENT):
        Fatal
        Error
        Warning
        Informational
SETSHO> SET ERROR FATAL ❸
SETSHO> SHOW ERROR

Error Levels Used Next Re-initialization (/PERMANENT):
        Fatal
        Error
        Warning
        Informational ❹

Error Levels Used Currently (/NOPERMANENT):
        Fatal ❺
SETSHO> SET ERROR ERROR/PERMANENT ❻
SETSHO> SHOW ERROR

Error Levels Used Next Re-initialization (/PERMANENT):
        Fatal
        Error ❼

Error Levels Used Currently (/NOPERMANENT):
        Fatal
        Error
```

❶ Shows the severity level of error messages displayed by the HSC controller.

❷ Note that the PERMANENT level (in the SCT) and NOPERMANENT level (in memory) are set to Informational.

Example 6–11 Cont'd on next page

Example 6–11 (Continued): SET ERROR Command

❸ Changes the severity level of errors to be displayed to fatal. Since the /PERMANENT qualifier was not specified, this change will remain in effect only until the next reboot.

❹ Note that the PERMANENT level settings remain the same and do not reflect the change.

❺ The current severity level has been changed to FATAL.

❻ Changes the severity level of errors to be displayed to ERROR. By choosing the error level ERROR, you can also see the more severe level, FATAL. Since the /PERMANENT qualifier was used, this change affects current error levels and error levels to be used after the next reboot.

❼ Note that the PERMANENT and NOPERMANENT level settings reflect the new error level setting, ERROR.

SET EXCEPTION CLEAR

Clears the exception context in the SCT.

Format SET EXCEPTION CLEAR

Command Qualifiers	Defaults
None	None

Description

When the HSC controller boots for reasons other than by power up or pressing the operator control panel Init switch (functionally equivalent methods), the controller determines the reason for the reboot. The HSC controller prints this reason after the initialization and stores it in the SCT. For reboot information refer to Section 6.4.

The SET EXCEPTION CLEAR command clears the reboot reason from the SCT.

Use the SHOW EXCEPTION command to display the reason for the last HSC controller reboot.

The SET EXCEPTION CLEAR command does not require an HSC controller reboot to take effect.

Example

The following example shows how to use the SET EXCEPTION CLEAR command.

Example 6–12: SET EXCEPTION CLEAR Command

```
SETSHO>SET EXCEPTION CLEAR
```

This command clears the exception context from the SCT.

SET HOST

Controls HSC communication to a host node.

Format

SET HOST *sense host-node-number*

Command Qualifiers	Defaults
None	None

Parameters

sense
Specifies the state of HSC communication to a host node.

ENABLE—Allows virtual circuits to be established to the host node.
DISABLE—Does not allow virtual circuits to be established to the host node.

host-node-number
Specifies the CI node number to which the HSC controller allows (or does not allow) virtual circuits to be established. The node number ranges from 0 to the maximum node number supported by your version of the HSC controller and VMS software (see the VMS Software Product Description for the version you are currently running). Use the keyword ALL to allow connections to all nodes.

Description

The CI network consists of HSC controllers and hosts. If a host is disabled by means of the SET HOST command, the HSC controller refuses to establish a virtual circuit to that node.

Use the SHOW HOSTS command to view the current host settings. The factory setting in the SCT enables all hosts.

The SET HOST command requires an HSC controller reboot to take effect. Use the ENABLE REBOOT command.

Example

The following example shows how to use the SET HOST command.

Example 6–13: SET HOST Command

```
SETSHO>SET HOST ENABLE 12
```

This command allows a virtual circuit to be established to host node number 12.

SET ID

Sets the HSC system identification number.

Format

SET ID *system-identification-number*

Command Qualifiers	**Defaults**
None	None

Parameters

system-identification-number
Specifies a hexadecimal number as the new system identification number in the following format:

```
%Xnnnnnnnnnnnn
```

where:
%X—Indicates that a hexadecimal number follows.
nnnnnnnnnnnn—Is a 12-digit hexadecimal number between 1 and 7FFFFFFFFFFF. You do not need to specify all 12 digits.

Restrictions

Because some host operating systems do not track HSC software identification changes (refer to the appropriate manual for the host operating system), ensure that the identification is set to a value specified by the system manager. The system identification must also be set to that number when a new release of HSC software is initially booted.

The SET ID command often requires that a corresponding SET NAME command also be issued.

Description

The system identification is a 48-bit number stored in the SCT that uniquely identifies nodes in the CI configuration. The disk, tape, DUP servers, and CI manager in the HSC controller all use the identification number to communicate with processes on other CI nodes.

The system identification automatically generated by the HSC controller sets the following fields:

<0:7>—The CI node address of the HSC controller.
<8:15>—The complement of the CI node address.
<16:31>—The serial number of the I/O control processor.
<32:47>—Set to zero.

Use the SHOW SYSTEM command to view the system identification.

The SET ID command requires an immediate HSC controller reboot to take effect.

Example

The following example shows how to use the SET ID command.

Example 6–14: SET ID Command

```
SETSHO>SET ID %X110717
```

This command sets the system identification to the hexadecimal number 110717.

SET LOAD

Controls the loading of HSC software modules.

Format

SET [NO]LOAD *load-module*

Command Qualifiers	Defaults
None	None

Parameters

load-module

Specifies which software module to load. The abbreviated names of these modules and their functions are:

CI[1]—CI manager or CI emulator
DF[1]—Disk server and ECC (error correction code) process
DM[1]—Diagnostic monitor (DEMON)
EL[1]—Central error reporting facility (CERF)
TF[1]—Tape server
DUP—Diagnostics utilities protocol server (DUP)

Restrictions

Do not use this command with module options CI, DF, DM, EL, and TF unless directed by a Digital Services representative.

Description

Controls whether a particular software module is loaded during the next controller reboot. This command is used by Digital Customer Services to assist with diagnosing software problems.

Use the SHOW LOAD command to view the software modules the HSC controller will load at the next reboot.

[1] There are restrictions associated with these module options.

The SET LOAD command requires an HSC controller reboot to take effect. Use the ENABLE REBOOT command.

Example

The following example shows how to use the SET LOAD command.

Example 6–15: SET LOAD Command

```
SETSHO>SET NOLOAD DUP
```

This command specifies that the DUP server will not be loaded the next time the HSC controller reboots.

SET MAX_FORMATTERS

Sets the maximum number of tape formatters to be supported by an HSC controller.

Format

SET MAX_FORMATTERS *formatter-count*

Command Qualifiers	Defaults
None	None

Parameters

formatter-count
Specifies the maximum number of formatters that can be connected to the HSC controller. Use a number from 1 to 24.

Description

Sets the maximum number of tape formatters for which program memory is allocated by the tape server when the HSC controller reboots. The default allocates enough program memory to handle the maximum number of formatters that could be connected to the HSC controller. This number is computed by using the number of tape data channels. The default number of formatters is often incorrect, as not every port on every tape data channel is used.

If you add a new formatter and exceed the specified maximum number, the tape server issues the following error message:

```
TAPE-E No Tape Formatter Structures available for Requestor X., Port Y.
       Increase structures via SET MAX_FORMATTERS cmd
```

Increase the number of allocated formatters with the SET MAX_FORMATTERS command.

Use the SET MAX_FORMATTERS command to conserve program memory space.

Use the SHOW MAX_FORMATTERS command to view the setting of this parameter.

The SET MAX_FORMATTERS command requires an HSC controller reboot to take effect. Use the ENABLE REBOOT command.

Example

The following example shows how to use the SET MAX_FORMATTERS command.

Example 6–16: SET MAX_FORMATTERS Command

```
SETSHO>SET MAX_FORMATTERS 8
```

This command sets the maximum number of formatters to eight.

SET MAX_TAPES

Sets the maximum number of tape units to be supported by an HSC controller.

Format

SET MAX_TAPES *tape-unit-count*

Command Qualifiers	Defaults
None	None

Parameters

tape-unit-count
Specifies the maximum number of tape units that can be connected to the HSC controller. Use a number from 1 to 24.

Description

Sets the number of tape units for which program memory is allocated by the tape server when the HSC controller reboots. The default allocates enough program memory to handle the maximum number of tape units that could be connected to the HSC controller. This is computed by using the number of tape data channels. The default number of tape units is often incorrect, as not every port on every tape data channel is used.

If you add a new tape unit that exceeds the maximum number specified, the tape server displays the following error message:

```
TAPE-E No Tape Drive Structures available for Requestor X., Port Y.
       Unit Z.
       Increase structures via SET MAX_TAPES cmd
```

Increase the number of allocated tape units with the SET MAX_TAPES command.

Use the SET MAX_TAPES command to conserve program memory space.

Use the SHOW MAX_TAPES command to view the setting for this parameter.

The SET MAX_TAPES command requires an HSC controller reboot to take effect. Use the ENABLE REBOOT command.

Example

The following example shows how to use the SET MAX_TAPES command.

Example 6–17: SET MAX_TAPES Command

```
SETSHO>SET MAX_TAPES 8
```

This command sets the maximum number of tape units to eight.

SET MEMORY

Controls the use of a word in HSC controller memory.

Format

SET MEMORY *sense memory-address*

Command Qualifiers	**Defaults**
None	None

Parameters

sense
The following conditions can be set with the SET MEMORY command:

ENABLE—Removes a specified memory address from the disabled memory list and makes it available for use.
ENABLE ALL—Clears the disabled memory list and enables all memory locations. Use this command to clear the disabled memory list when a replacement memory board is installed.
DISABLE—Removes a specified memory location from use.

memory-address
Specifies the disabled memory location to be enabled. This is an octal number from 0 to 17777777.

Use ALL to enable all disabled memory locations and all suspect memory locations. However, do not use ALL to disable memory addresses.

Description

The HSC controller maintains a list of bad memory locations in the SCT. Each entry in the list refers to one memory location. When booting, the HSC controller examines this list to determine which portions of memory should not be allocated for use.

Memory addresses are disabled automatically by the HSC controller if two consecutive accesses to the address cause two consecutive parity errors. When a memory location is disabled, the specified memory address is added to the disabled memory list.

The SET MEMORY command does not require an HSC controller reboot to take effect.

Use the SHOW MEMORY command to view the disabled memory list.

Example

The following example shows how to use the SET MEMORY command:

Example 6–18: SET MEMORY Command

```
SETSHO> SET MEMORY ENABLE 23422   ❶
SETSHO> SET MEMORY DISABLE 52346  ❷
SETSHO> SET MEMORY ENABLE ALL     ❸
```

❶ Enables memory location 23422.

❷ Disables memory location 52346.

❸ Enables all disabled memory locations.

SET NAME

Sets the HSC system name.

Format

SET NAME *system-name*

Command Qualifiers	**Defaults**
None	None

Parameters

system-name
Specifies the HSC system name. On a CI network, the system name must be unique and can contain up to eight of the following characters:

- A to Z
- 0 to 9
- Dollar sign ($)
- Underscore (_)

Restrictions

Not all host architectures allow the full range of system names. When the HSC controller is used as a node within a VAXcluster running VMS software, the following restrictions apply to the node name:

- It must consist of six or fewer alphanumeric characters.
- The first character must be alphabetic.
- It cannot contain a dollar sign ($).
- It cannot contain an underscore (_).

If these conditions are not met, VMS hosts cannot communicate with devices connected to the HSC controller.

Because some host operating systems do not track HSC system name changes, use the system name specified by the system manager. Set the system name when a new release of HSC software is initially booted.

The SET NAME command often requires that a corresponding SET ID command also be issued.

Description

The system name identifies the HSC controller to other nodes on the CI network. The system name is used only for identification purposes and is comparable to the DECnet node name in a DECnet network.

The system name is stored in the SCT. (Refer to Section 3.6 for a description of the SCT.) The HSC controller automatically generates a default system name when a new SCT is used. The name the HSC controller generates is six characters in the following format:

```
HSCnnn
```

The three-digit decimal value, *nnn*, is the CI node number. This number may have a prefix of zeros to complete the three-digit value.

The system name is displayed when the HSC controller boots and can also be viewed with the SHOW SYSTEM command.

The SET NAME command requires an immediate HSC controller reboot to take effect.

Example

The following example shows how to use the SET NAME command.

Example 6–19: SET NAME Command

```
SETSHO>SET NAME ENIGMA
```

This command sets the HSC system name to ENIGMA.

SET ODT

Sets On-Line Debugging Technique (ODT) parameters.

Format

SET [NO]ODT *[mode]*

Command Qualifiers	**Defaults**
None	None

Parameters

mode

Specifies if ODT should be enabled and during what circumstances it should be entered. The omission of a parameter specifies that ODT will be loaded and immediately available.

INIT_BPT—Specifies that ODT will be entered at the end of the HSC controller system initialization.
DUMP_BPT—Specifies that ODT will be entered after an exception dump to the device specified by the SET DUMP command.
HOST—Specifies that ODT will be entered after the HSC controller has been reset by a host.

Restrictions

Use this command only when directed by Digital Services.

Description

This command enables or disables the use of software ODT. Entering ODT impedes normal HSC operation and will affect HSC controller failure recovery.

Before you specify how ODT will be entered, load ODT with the following command:

```
SETSHO>SET ODT
```

You can enter ODT in several ways:

- Press Ctrl/p to enter ODT commands manually. The HSC controller displays an asterisk (*) prompt that indicates all normal HSC controller processes have stopped and the HSC controller is ready to accept ODT commands. Exit ODT by entering the ;P command at the ODT prompt.
- Use the SET ODT INIT_BPT command to set the HSC controller to automatically enter ODT at the end of initialization.
- Use the SET ODT DUMP_BPT command to set the HSC controller to automatically enter ODT following an exception dump.
- Use the SET ODT HOST command to set the HSC controller to automatically enter ODT after the HSC controller has been reset by a host.

The SET ODT command causes the HSC controller to reboot when you change the parameter from NOODT to ODT.

Use the SHOW ODT command to view the setting of the ODT flags.

Example

The following example shows how to use the SET ODT command.

Example 6–20: SET ODT Command

```
SETSHO>SET ODT ❶
SETSHO>SET ODT INIT ❷
SETSHO>SET NOODT DUMP ❸
```

❶ Loads ODT in the HSC controller.

❷ Instructs the HSC controller to enter ODT when it has completed initialization.

❸ Instructs the HSC controller not to enter ODT after an exception dump is printed on the console.

SET PERIODIC_DIT

Controls the execution of periodic device integrity tests (DITs).

Format

SET [NO]PERIODIC_DIT *interval*

Command Qualifiers	**Defaults**
None	None

Parameters

interval
Specifies the number of minutes between initiation of the periodic device integrity tests. Use a number from 1 to 59.

Restrictions

Periodic DITs provide an important check of HSC hardware. They should run at one-minute intervals, unless an interval change is directed by Digital Services.

Description

This command controls whether periodic DITs are executed in the HSC controller and how often they are executed. The default frequency is every minute.

Periodic DITs are used to maintain the constant integrity of the HSC control processor, disk data channel(s), and tape data channel(s). Periodic DITs run when CPU time is available and do not impact performance. They should not be disabled under normal circumstances.

The following table shows the function of each periodic DIT:

Test	Function
PRMEMY	Tests portions of the I/O control processor, and control and data memory. It checks: • Control processor control and data memory logic • Control processor parity error detection logic
PRKSDI	Tests the disk data channel. It checks: • Disk data channel control and data memory logic • Disk data channel serialization/deserialization logic
PRKSTI	Tests the tape data channel. It checks: • Tape data channel control and data memory logic • Tape data channel serialization/deserialization logic

Use the SHOW SYSTEM command to view the frequency of periodic device integrity test initiation.

The SET PERIODIC_DIT command does not require an HSC controller reboot to take effect.

Example

The following example shows how to use the SET PERIODIC_DIT command.

Example 6–21: SET PERIODIC_DIT Command

```
SETSHO>SET PERIODIC_DIT 1
```

This command sets the interval between the initiation of the periodic device integrity tests to one minute.

SET POLLER

Sets the HSC controller CI polling variables.

Format

SET POLLER *option [value]*

Command Qualifiers	Defaults
None	None

Parameters

option

Specifies one of several poller parameter options to be modified.

LOW ***value***—Specifies the low node with which polling should begin. Use a number from 0 to 31. The default value is 0.

HIGH ***value***—Specifies the high node with which polling should end. Use a number from 0 to 31. The default value is 31.

NODE ***value***—Specifies the number of nodes to poll with each polling cycle. Use a number from 1 to 32. The default value is 1.

START_RETRY ***value***—Specifies the number of times to retry the START/STACK operation. Use a number from 1 to 20. The default value is 10.

CYCLE ***value***—Specifies the interval (in seconds) between polling cycles. Use a number from 2 to 60. The default value is 2.

DEFAULT—Sets all polling variables to their defaults.

Description

With the SET POLLER command, you can specify:

- A range of nodes to poll
- The number of nodes to poll with each polling cycle
- The number of retries
- The interval between polling cycles
- That all polling variables should be set to their defaults

It is recommended that you use the default values when setting polling variables.

The SET POLLER command requires an HSC controller reboot to take effect. Use the ENABLE REBOOT command.

Example

The following example shows how to use the SET POLLER command.

Example 6–22: SET POLLER Command

```
SETSHO> SET POLLER LOW 2 ❶
SETSHO-I Your settings require a reboot.  Use ENABLE REBOOT.
SETSHO> SET POLLER CYCLE 6 ❷
SETSHO> SHOW POLLER ❸
Lowest address to poll:  2     Highest address to poll:  31
Number of nodes to poll each poll cycle:  1
Times to retry a START/STACK:  20
Seconds between poll cycles:  6
SETSHO> SET POLLER HIGH 30 ❹
SETSHO> SET POLLER START_RETRY 10 ❺
SETSHO> SHOW POLLER ❻
Lowest address to poll:  2     Highest address to poll:  30
Number of nodes to poll each poll cycle:  1
Times to retry a START/STACK:  10
Seconds between poll cycles:  6
```

❶ Specifies that polling should begin with node 2.

❷ Specifies a 6-second interval between polling cycles.

Example 6–22 Cont'd on next page

SET POLLER

Example 6–22 (Continued): SET POLLER Command

---

❸ Displays the values set by the previous commands.

❹ Specifies that polling should end with node 30.

❺ Specifies that the START/STACK operation should be retried 10 times.

❻ Displays the changes made with the previous commands.

SET PROMPT

Sets the HSC console and terminal prompts.

Format

SET PROMPT *prompt-string*

Command Qualifiers	Defaults
None	None

Parameters

prompt-string

Specifies the HSC controller prompt string which can contain up to 10 of the following characters:

- A to Z
- 0 to 9
- Dollar sign ($)
- Underscore (_)

A greater-than sign and a space (>) is automatically appended to the prompt.

Description

When a new RX33 boot media is first initialized, the prompt is set to the default name: HSC. Once you specify a new prompt, it is stored in the SCT and saved on the media for future reboots.

The SET PROMPT command does not require an HSC controller reboot to take effect.

Example

The following example shows how to use the SET PROMPT command.

Example 6–23: SET PROMPT Command

```
HSC>RUN SETSHO
SETSHO>SET PROMPT NEW_PROMPT
SETSHO>EXIT
SETSHO-I PROGRAM EXIT
NEW_PROMPT>
```

This command changes the prompt from HSC> to NEW_PROMPT>.

SET REQUESTOR

Controls the type of microcode loaded into a K.si requestor.

Format

SET REQUESTOR *requestor-number*

Command Qualifiers	Defaults
/TYPE	None

Parameters

requestor-number
Specifies the requestor into which the microcode will be loaded. Use a number from 2 to 9. This requestor must be a K.si module.

Qualifiers

/TYPE=data_channel_type

DISK indicates that disk microcode should be loaded.

TAPE indicates that tape microcode should be loaded.

Restrictions

The requestor must correspond to the type of device that is connected to it. Make sure a data channel configured as a tape data channel is connected to a tape drive, and a data channel configured as a disk data channel is connected to a disk drive. If a unit is not connected to the proper data channel, the unit is declared inoperative.

If a unit is declared inoperative, connect the unit to the proper data channel and use the SET REQUESTOR command to reconfigure the requestor.

SET REQUESTOR

Description

The SET REQUESTOR n/TYPE=data_channel_type command changes the type of microcode that is loaded into a specified K.si requestor module. The microcode type, disk or tape, must match the attached disk or tape device types.

Under most circumstances during an HSC controller reboot, the HSC software loads the correct microcode type into the K.si modules. To determine the microcode type previously loaded into each K.si module, the boot software examines the system configuration table on the boot medium. If accurate information cannot be obtained, the software examines the K.si module hardware to determine the microcode type previously loaded. If both methods fail, disk microcode is loaded into the K.si module.

Use the SHOW REQUESTORS command to verify that the correct microcode type has been loaded into the K.si modules whenever you suspect otherwise. You may want to perform this action after adding to or changing the configuration of the devices attached to the HSC controller backplane. If the SHOW REQUESTORS display indicates that a K.si module has the wrong microcode type, use the SET REQUESTOR n/TYPE=data_channel_type to install the correct microcode.

After you have set the microcode type using the SET REQUESTOR n/TYPE=data_channel_type command, you are prompted for an automatic reboot upon exiting SETSHO. New K.si microcode will **not** be loaded unless you affirmatively acknowledge this reboot prompt and allow the HSC controller to reboot.

Example

The following example shows how to use the SET REQUESTOR command with an automatic reboot on exit:

Example 6–24: SET REQUESTOR Command

```
SETSHO> SHOW REQUESTORS ❶
Req      Status  Type        Version                  Microcode Loaded
0        Enabled P.ioj
1        Enabled K.ci        MC- 54 DS- 2 Pila-0 K.pli-0     n/a
2/A      Enabled K.si        MC- 12 DS- 4             disk
3/B      Enabled K.sdi       MC- 40 DS- 3             n/a
4/C      Enabled K.sdi       MC- 42 DS- 3             n/a
5/D      Enabled K.sdi       MC- 40 DS- 3             n/a
6/E      Enabled K.sdi       MC- 42 DS- 3             n/a
7/F      Enabled K.si        MC- 11 DS- 4             disk
8/M      Enabled K.sdi       MC- 39 DS- 3             n/a
9/N      Enabled K.sdi       MC- 42 DS- 3             n/a
SETSHO> SET REQUESTOR 2/TYPE=TAPE ❷
SETSHO-I Your settings require an IMMEDIATE reboot on exit.
SETSHO> SHOW REQUESTORS
Req      Status  Type        Version                  Microcode Loaded
0        Enabled P.ioj
1        Enabled K.ci        MC- 54 DS- 2 Pila-0 K.pli-0     n/a
2/A      Enabled K.si        MC- 12 DS- 4             tape ❸
3/B      Enabled K.sdi       MC- 40 DS- 3             n/a
4/C      Enabled K.sdi       MC- 42 DS- 3             n/a
5/D      Enabled K.sdi       MC- 40 DS- 3             n/a
6/E      Enabled K.sdi       MC- 42 DS- 3             n/a
7/F      Enabled K.si        MC- 11 DS- 4             disk
8/M      Enabled K.sdi       MC- 39 DS- 3             n/a
9/N      Enabled K.sdi       MC- 42 DS- 3             n/a
SETSHO> EXIT
SETSHO-Q Rebooting HSC, type Y to continue, CTRL/Y to abort: Y ❹

INIPIO-I  Booting...

    HSC70 Version V600   7-Jan-1990 21:30:15    System HSC006

Copyright 1982 Digital Equipment Corporation.  All Rights Reserved.
```

Example 6–24 Cont'd on next page

Example 6–24 (Continued): SET REQUESTOR Command

```
Ctrl/Y
HSC> RUN SETSHO
SETSHO> SHOW REQUESTORS
Req     Status   Type            Version                  Microcode Loaded
0       Enabled P.ioj
1       Enabled K.ci            MC- 54 DS- 2 Pila-0 K.pli-0    n/a
2/A     Enabled K.si            MC- 12 DS- 4         tape  ❺
3/B     Enabled K.sdi           MC- 40 DS- 3         n/a
4/C     Enabled K.sdi           MC- 42 DS- 3         n/a
5/D     Enabled K.sdi           MC- 40 DS- 3         n/a
6/E     Enabled K.sdi           MC- 42 DS- 3         n/a
7/F     Enabled K.si            MC- 11 DS- 4         disk
8/M     Enabled K.sdi           MC- 39 DS- 3         n/a
9/N     Enabled K.sdi           MC- 42 DS- 3         n/a
```

❶ A SHOW REQUESTORS command shows that all K.si requestors are loaded with disk microcode.

❷ The SET REQUESTOR n/TYPE=data_channel_type command is now used to reset the K.si in requestor 2 as a tape data channel. Note that the message on the next line reminds you that you must accept the reboot upon exiting SETSHO to have tape microcode loaded into the requestor.

❸ The SHOW REQUESTORS command now shows that the reconfiguration command has been accepted by the system. However, since a reboot has yet to occur, disk microcode is still loaded and operating in requestor 2, even though the display indicates that tape microcode is loaded.

❹ Answering Y to the reboot prompt starts the reboot sequence.

❺ After the HSC controller reboots, another SHOW REQUESTORS command shows requestor 2 has been loaded with new microcode.

SET SCOPE

Identifies the terminal as a hardcopy device or video display.

Format

SET [NO]SCOPE

Command Qualifiers	Defaults
/[NO]PERMANENT	NOPERMANENT

Qualifiers

/[NO]PERMANENT

Specifies whether the terminal line settings should be reflected across HSC controller reboots. The default is NOPERMANENT.

Description

This command identifies the ASCII serial line being used as a hardcopy or a video terminal connection. This command has no effect on virtual terminals.

The terminal setting is used by utility programs within the HSC controller, as well as by the HSC terminal service (which controls character input and output).

The Delete key on the terminal functions differently, depending on whether you specify the terminal as hardcopy or video display:

- If you use the SET SCOPE command (identifying your terminal as video display), the Delete key erases the character to the left of the cursor position.
- If you use the SET NOSCOPE command (identifying your terminal as a hardcopy device), the text being erased appears on your printout surrounded with backslash (\ ) characters.

Use the SHOW LINES command to view the state of each terminal.

SET SCOPE

The SET SCOPE command does not require an HSC controller reboot to take effect.

NOTE

Use of the SET SCOPE/PERMANENT command is not recommended if the HSC controller is to be left unattended. If the HSC controller crashes with this command enabled, the terminal displays the first page of data and then hangs. The HSC controller cannot recover after a crash without operator intervention.

Example

The following example shows how to set the terminal line to act as a video (scope) terminal and then display the setting.

Example 6–25: SET SCOPE Command

```
SETSHO> SET SCOPE     ❶
SETSHO> SHOW LINES    ❷
Device   CSR      Attributes
TT0      177560  NoScope Enabled
TT2      177530  Scope   Enabled   ❸
TT4      000000  Scope   Enabled Pseudo-Terminal
TT5      000000  NoScope Enabled Pseudo-Terminal
DX0      177400  Boot Device (SY:)
DX1      177400
```

❶ Sets the terminal line to act as a video terminal.

❷ Displays the state of all terminals.

❸ Shows that your terminal line is set to act as a video terminal.

SET SCT CLEAR

Causes the HSC controller to reset the user SCT to its default settings.

Format SET SCT CLEAR

Command Qualifiers	Defaults
None	None

Description

The SCT is a file (SCT.INI) that is maintained on the RX33 boot media. The SCT stores all permanent HSC controller configuration information and most of the SETSHO parameters. For more information about the SCT, refer to Section 3.6.

It is recommended that you use the default SCT parameters set at the factory. If site-specific parameters are set, all parameters will need to be reset each time a new HSC software version is installed.

Using the SET SCT CLEAR command is equivalent to holding in the Fault switch during the initial phase of reboot. Both actions return the SCT to the default settings. After the HSC controller boots, the displayed message indicates that the default SCT is in use.

The SET SCT CLEAR command requires an immediate HSC controller reboot to take effect.

SET SCT CLEAR

Example

The following example shows how to use the SET SCT CLEAR command.

Example 6–26: SET SCT CLEAR Command

```
SETSHO>SET SCT CLEAR
```

This command causes the HSC controller to reboot when you exit SETSHO.

SET SERVER CACHE

Sets cache server parameter values.

Format

SET SERVER CACHE

Command Qualifiers	Defaults
/CACHE_SIZE_THRESHOLD	8
/WRITE_THRESHOLD	8
/ERASE_PURGE_THRESHOLD	256
/XDE_SIZE	16

Qualifiers

/CACHE_SIZE_THRESHOLD=n
Sets the cache server read threshold size. The qualifier value *n* represents the maximum size of a read request that will be directed to the cache server for processing. This value is expressed in terms of blocks and may range from 1 to 64. The recommended value for VMS systems is 8; for ULTRIX systems, 16.

/WRITE_THRESHOLD=n
Sets the cache server write threshold size at which the cache server write allocation policy changes. See Section 5.8.2.1 for a description of the cache server write allocation policies. The qualifier value *n* represents the maximum size of a write request that will use the user-settable write allocation policy for the disk. Write threshold is expressed in terms of blocks and may range from 0 to 32,767. The recommended value is one that equals the cache size threshold. Write requests above the qualifier value will use either UPDATE or INVALIDATE as the cache write allocation policy.

/ERASE_PURGE_THRESHOLD=n
Sets the cache server purge threshold size at which the cache server purges cache blocks for the specified disk unit. The qualifier value *n* represents the maximum size of an erase request that will be processed normally by the cache server. Erase requests above the qualifier value will cause the cache server to purge all cache blocks in use by the disk

unit. This value is expressed in terms of blocks and may range from 0 to 32,767. The recommended value is 256.

/XDE_SIZE=n

Sets the cache server index node size. An index node is a cache server data structure that contains 1 to XDE_SIZE cache blocks where one cache block contains one disk sector's worth of data. The qualifier value *n* represents the number of cache blocks in an index node. This value is expressed in terms of units and may range from 1 to 16. The recommended value is 16.

Restrictions

Use the XDE_SIZE qualifier only when directed by Digital Services.

Description

Use the SET SERVER CACHE command to set global caching parameters. Modifying these cache server parameters will affect various cache server policies. Use the SHOW SERVER CACHE command to view cache server parameters.

Example

The following example shows how to use the SET SERVER CACHE command.

Example 6–27: SET SERVER CACHE/CACHE_SIZE_THRESHOLD=4

```
SETSHO>SET SERVER CACHE/CACHE_SIZE_THRESHOLD=4
```

This command sets the maximum size of a read request that will be directed to the cache server for processing to four blocks.

SET SERVER DISK

Sets disk server parameter values.

Format

SET SERVER DISK

Command Qualifiers	Defaults
/[NO]CACHE	NOCACHE
/DRIVE_TIMEOUT	2
/MAX_SECTORS_PER_TRACK	74
/[NO]VARIANT_PROTOCOL	VARIANT_PROTOCOL

Qualifiers

/[NO]CACHE

Globally enables/disables disk caching. Caching will only be enabled if the HSC controller contains the appropriate hardware.

/DRIVE_TIMEOUT=n

Sets the drive timeout interval to *n* seconds. Changing this qualifier affects failover timing. This qualifier should be kept at its default value or the value set at installation. A drive timeout value of 0 is invalid. Valid drive timeout values range from 1 to 24.

/MAX_SECTORS_PER_TRACK=n

Adjusts the maximum sectors per track value for any disk drive attached to the HSC controller. This value is used to allocate data structures for use by the disk server. This qualifier requires an immediate HSC controller reboot to take effect. Valid maximum sectors per track values range from 74 to 100.

/[NO]VARIANT_PROTOCOL

Enables/disables variant SDI (standard disk interconnect) protocols for the HSC disk server. Note that this command is used to turn enhanced performance mode on or off at the HSC controller level. Enhanced mode is actually enabled on each individual ESE20 when the drive is brought online to the HSC disk server.

SET SERVER DISK

Restrictions

Use the DRIVE_TIMEOUT qualifier only when directed by Digital Services.

Description

Use the SHOW SERVER DISK command to view disk server parameters.

Examples

The following examples show how to use the SET SERVER DISK command.

Example 6–28: SET SERVER DISK/DRIVE_TIMEOUT=4

```
SETSHO>SET SERVER DISK/DRIVE_TIMEOUT=4
```

This command sets the disk drive timeout period to 4 seconds.

Example 6–29: SET SERVER DISK/VARIANT

```
SETSHO> SET SERVER DISK/VARIANT_PROTOCOL
SETSHO> SHOW SERVER DISK
Disk Server Options Enabled:
        Variant Protocol
        Disk Drive Controller Timeout: 2 seconds
        Maximum Sectors per Track: 74 sectors
SETSHO> SET SERVER DISK/NOVARIANT_PROTOCOL
SETSHO> SHOW SERVER DISK
Disk Server Options Enabled:
        Disk Drive Controller Timeout: 2 seconds
        Maximum Sectors per Track: 74 sectors
```

This command turns variant SDI protocols for the HSC disk server on and off.

Example 6–30: SET SERVER DISK/CACHE

```
SETSHO> SHOW SERVER DISK
Disk Server Options Enabled:
        Variant Protocol
        Disk Drive Controller Timeout: 2 seconds
        Maximum Sectors per Track: 74 sectors
SETSHO> SET SERVER DISK/CACHE
SETSHO-I You must EXIT SETSHO to update the drive cache state.
SETSHO> SHOW SERVER DISK
Disk Server Options Enabled:
        Variant Protocol
        Disk Caching
        Disk Drive Controller Timeout: 2 seconds
        Maximum Sectors per Track: 74 sectors
```

This command globally enables disk caching.

6.7 The SHOW Commands

This section contains descriptions of the SHOW commands. The SHOW commands display the entries in the SCT. The SCT is described in Section 3.6.

SHOW commands display information about HSC controller states and parameters. SHOW commands do not modify HSC controller parameters, therefore, they do not require an HSC controller reboot.

Since some SET commands only become effective after using the ENABLE REBOOT command, the parameter value displayed with a SHOW command may differ from the value the HSC controller is currently using. Refer to Section 6.6 for a description of the set commands that require the use of the ENABLE REBOOT command.

SHOW ALL

Displays information about numerous HSC controller states and parameters.

Format

SHOW ALL

Command Qualifiers	Defaults
None	None

Description

Displays information equivalent to that displayed by using the following SHOW commands:

- SHOW CI
- SHOW CONNECTIONS
- SHOW CREDIT_MANAGER
- SHOW DISKS
- SHOW ERROR
- SHOW EXCEPTION
- SHOW HOSTS
- SHOW LINES
- SHOW LOAD
- SHOW MEMORY
- SHOW ODT
- SHOW POLLER
- SHOW REQUESTORS
- SHOW SERVER CACHE
- SHOW SERVER DISK
- SHOW SYSTEM
- SHOW TAPES
- SHOW VIRTUAL_CIRCUITS

SHOW ALL

Refer to the individual SHOW command descriptions for further information on these commands.

SHOW CI

Shows the CI counters.

Format

SHOW CI

Command Qualifiers	Defaults
None	None

Description

The SHOW CI command displays the event counters returned by the port processor module. After displaying them, the port processor module resets the event counters to zero and continues collecting statistics for the same node(s).

The statistics gathered are defined as follows:

ACK—An immediate CI positive acknowledgment was correctly received from the target node following a message or data packet transfer from the HSC controller. This is the successful result of a packet transfer attempt.

NAK—An immediate CI negative acknowledgment was correctly received from the target node following a message or data packet transfer from the HSC controller. This indicates the target node was not able to accept the packet transfer, usually because the target node did not have an available buffer to receive the item. The HSC controller normally retries a protocol message or data packet.

No Response—No immediate response was received from the target node following a message or data packet transfer from the HSC controller. This might indicate:

- The target node did not receive the packet as being correct.
- The target node was busy on the alternate path.

SHOW CI

- The HSC controller did not properly receive the acknowledgment as being correct.

The HSC controller normally retries a protocol message or data packet.

Use the SET CI command to specify the node that should be monitored.

Example

The following is an example of the SHOW CI screen display.

Example 6–31: SHOW CI Screen Display

```
SETSHO>SHOW CI

Statistics previously collected for all nodes:
                Path A          Path B
ACKs:           984             969
NAKs:           0               0
No Response:    3863            3859

Discarded Datagrams:  0
Discarded RTNDATs:    0
```

SHOW CONNECTIONS

Displays information about all virtual circuits and connections the HSC controller has with other nodes.

Format

SHOW CONNECTIONS

Command Qualifiers	Defaults
None	None

Description

With the SHOW CONNECTIONS command, you can display:

- The node number of all nodes that have an established virtual connection to the HSC controller.
- The system identification numbers and names of these nodes.
- The disk and tape server connections for each node, the state of each connection, the number of credits extended to the node, and the connection reference number if specified by the host at the time the connection was established.
- A summary of all connections.

SHOW CONNECTIONS

Example

The following is an example of the SHOW CONNECTIONS screen display.

Example 6–32: SHOW CONNECTIONS Screen Display

```
SETSHO>SHOW CONNECTIONS

Node 14, VC State: OPEN ❶
System ID:  %X00000000FCBF      Name:  EAGLE❷
        Connection VMS$DISK_CL_DRVR -> MSCP$DISK        State:  OPEN (AVAIL) ❸
                Credits:  24
        Connection VMS$TAPE_CL_DRVR -> MSCP$TAPE        State:  OPEN (AVAIL)
                Credits:  12

Node 15, VC State: OPEN
System ID:  %X0000000020C5      Name:  TURKEY
        Connection VMS$DISK_CL_DRVR -> MSCP$DISK        State:  OPEN (AVAIL)
                Credits:  24     Connection Reference Number: 1❹
        Connection VMS$TAPE_CL_DRVR -> MSCP$TAPE        State:  OPEN (AVAIL)
                Credits:  12
Total of 2 Virtual Circuits, 4 Open Connections ❺
SETSHO-I Program Exit
```

❶ Displays the number of the node to which a virtual circuit has been established, and the status of that circuit.

❷ Displays the system identification and node name.

❸ Displays the following information for node 14:

- Connections with the disk and tape servers have been established.
- The connection states are OPEN (available).
- The default number of credits allowed for a disk connection is 24 and for a tape connection is 12.

❹ Displays the connection reference number established by the host.

❺ Displays a summary of the connections.

SHOW CREDIT_MANAGER

Displays the status of the dynamic credit manager.

Format

SHOW CREDIT_MANAGER

Command Qualifiers	**Defaults**
None	None

Description

The SHOW CREDIT_MANAGER command displays system information, the state of the dynamic credit manager (CRMGR), the number of SPECIAL mode invocations, and information about each active connection.

Refer to the example for a listing of the information displayed by the SHOW CREDIT_MANAGER command.

SHOW CREDIT_MANAGER

Example

The following is an example of the SHOW CREDIT_MANAGER screen display.

Example 6–33: SHOW CREDIT_MANAGER Screen Display

```
SETSHO>SHOW CREDIT_MANAGER

10-Feb-1992 18:43:09.15 Boot:  3-Feb-1992 14:27:52.35   Up: 172:15
Version:    V650        System ID: %X00000000FE01       Name: HSC001
CRMGR is ENABLED        SPECIAL mode invocations: 0
----------------------------------------------------------------------------------
---Host----  -----REMOTE-----  CURRENT  DEFAULT  CON  SRV  SRV   CON    CON
(# ) Name--  -----SERVER-----  CREDITS  CREDITS  HWM  HWM  TOT   CRW    CTR
----------------------------------------------------------------------------------
(16) FIFE    VMS$TAPE_CL_DRVR        6        6    6  137   62     0      1
(16) FIFE    VMS$DISK_CL_DRVR       12       12   12  173   60     0      1
(19) CLRNET  VMS$TAPE_CL_DRVR        6        6    6  137   62     0      1
(19) CLRNET  VMS$DISK_CL_DRVR       12       12   12  173   60     0      1
(22) BASSAX  VMS$TAPE_CL_DRVR       28        6   40  137   62    33   6055
(22) BASSAX  VMS$DISK_CL_DRVR       12       12   67  173   60    44   5498
(26) HORN    VMS$TAPE_CL_DRVR        6        6   30  137   62    22   6719
(26) HORN    VMS$DISK_CL_DRVR       12       12   40  173   60     1   4521
(30) ZYMBEL  VMS$TAPE_CL_DRVR       16        6   40  137   62    18   2710
(30) ZYMBEL  VMS$DISK_CL_DRVR       12       12   30  173   60     0    775
```

The column headers in the display have the following meanings:

- **HOST #**—Port number of the host.
- **HOST NAME**—Name of the host.
- **REMOTE SERVER**—Indicates whether it is a disk or tape connection by displaying the name of the remote application.
- **CURRENT CREDITS**—Number of credits granted to the connection.
- **DEFAULT CREDITS**—Number of credits normally granted when the connection is first opened.
- **CON HWM** (Connection High Water Mark)—Highest number of credits granted to the connection from the time the connection was first opened.

Example 6–33 Cont'd on next page

Example 6–33 (Continued): SHOW CREDIT_MANAGER Screen Display

- **SRV HWM** (Server High Water Mark)—Highest number of credits granted by the server since the HSC booted or since the last SET CREDIT_MANAGER RESET command was issued.
- **SRV TOT** (Server Total)—Current total of credits granted by the server to all connections of the same type (all disk, all tape).
- **CON CRW** (Connection Credit Waits)—A relative measure representing possible "credit waits" encountered from the host side of the connection. A credit wait indicates that a credit was not available to the host when a host application needed to send a command to the HSC controller. This condition forces the host application to wait for a credit. The credit manager's main function is to minimize credit waits by dynamically allocating credits to connections requiring credits.
- **CON CTR** (Connection Counter)—A bookeeping entry that tracks the number of credit transactions issued to a connection by the credit manager. Each credit transaction represents a grant or revocation of one or more credits. Upon opening the connection, the CON CTR value is 1 since it takes one transaction to establish the initial credits.

SHOW DISKS

Displays the statistics related to all disk drives connected to the HSC controller.

Format

SHOW DISKS

Command Qualifiers	**Defaults**
None	None

Description

The SHOW DISKS command displays the unit number, requestor slot, port, type, state, cache state, cache write allocation policy (if cached), host access state, disk microcode, and hardware revision levels for all disks connected to the HSC controller.

Example

The following is an example of the SHOW DISKS screen display.

Example 6–34: SHOW DISKS Screen Display

```
SETSHO> SHOW DISKS
Unit    Req     Port    Type    State           Cached  Access  Version
   10    5        3     RA70    Available        No     Host    MC-81, HV-7
   12    4        1     RA70    Available        Yes-U  Host    MC-81, HV-7
   13    4        2     RA70    Available        No     Host    MC-79, HV-7
   14    4        0     RA70    Available        No     Host    MC-79, HV-7
   15    4        3     RA70    Available        No     NoHost  MC-79, HV-7
   78    7        0     RA81    Available        No     Host    MC-7, HV-15

Units in NOHOST_ACCESS Table:
        D15

Units in CACHE Table:
        D12
```

This example shows the status of all disks connected to the HSC controller.

Example 6–35: SHOW Dn Screen Display

```
SETSHO> SHOW D12
Unit    Req     Port    Type    State           Cached  Access  Version
   12    4        1     RA70    Available        Yes-U  Host    MC-81, HV-7

The unit is NOT in the NOHOST_ACCESS table.

The unit IS in the CACHE table.
```

This example shows the status of disk unit 12.

SHOW ERROR

Displays the current error level settings.

Format SHOW ERROR

Command Qualifiers	Defaults
None	None

Description

Displays the severity level of error messages for the current operation and for the next HSC controller initialization. This applies only to messages from the disk server, tape server, CI manager, executive, and out-of-band errors.

The error message levels determine the minimum severity level of errors the HSC controller displays on the console and virtual terminals. The following error levels may be displayed:

Table 6–2: SETSHO Error Levels

Error Level	Error Types Displayed
Success	Success, Info, Warning, Error, Fatal
Info	Info, Warning, Error, Fatal
Warning	Warning, Error, Fatal
Error	Error, Fatal
Fatal	Fatal

Use the SET ERROR command to change the error level settings.

Example

The following examples demonstrate use of the SHOW ERROR screen display.

Example 6–36: SHOW ERROR Screen Display

```
SETSHO>SHOW ERROR

Error Levels Used Next Re-initialization (/PERMANENT):
        Fatal
        Error
        Warning
        Informational

Error Levels Used Currently (/NOPERMANENT):
        Fatal
        Error
        Warning
        Informational
```

This example displays the error levels that will be used after the next reinitialization and the error levels currently being used.

Example 6–37: SHOW ERROR Screen Display After Entering a SET ERROR FATAL Command

```
SETSHO> SET ERROR FATAL
SETSHO> SHOW ERROR

Error Levels Used Next Re-initialization (/PERMANENT):
        Fatal
        Error
        Warning
        Informational

Error Levels Used Currently (/NOPERMANENT):
        Fatal
```

This example shows the result of entering a SET ERROR FATAL command. This condition is not preserved across the boot because the command was executed without using the /PERMANENT qualifier. Therefore, the display indicates that four levels of error will be reported after the next reinitialization.

Example 6–38: SHOW ERROR After a SET ERROR ERROR/PERMANENT Command

```
SETSHO> SET ERROR ERROR/PERMANENT
SETSHO> SHOW ERROR

Error Levels Used Next Re-initialization (/PERMANENT):
        Fatal
        Error

Error Levels Used Currently (/NOPERMANENT):
        Fatal
        Error
```

This example shows that during the current operation of the HSC controller, only errors of severity level ERROR and greater are displayed. This condition is preserved across the boot because the command was executed using the /PERMANENT qualifier.

SHOW EXCEPTION

Displays the reason for the last HSC system exception.

Format SHOW EXCEPTION

Command Qualifiers	**Defaults**
None	

Description

When the HSC controller initiates an automatic reboot (system exception), it records the reason for the reboot in the SCT.

The SHOW EXCEPTION command displays the reason for the reboot.

SHOW EXCEPTION

Examples

The following is an example of the SHOW EXCEPTION screen display.

Example 6–39: SHOW EXCEPTION Screen Display

```
SETSHO>SHOW EXCEPTION ❶

Last Reboot Caused by Parameter change
       Process SETSHO
       PC  007276
       PSW 140001
       Reason 000000
```

❶ Shows the last reboot was caused by a SETSHO request—a parameter was changed that required the HSC controller to reboot. The following information is displayed:

- Process SETSHO—the process initiating the exception
- PC xxxxxx—the program counter
- PSW xxxxxx—the processor status word
- Reason—the reason for the reboot

The numeric statistics (represented by xxxxxx in the list) are version dependent and may change from one software release to the next.

Example 6–40: SHOW EXCEPTION Screen Display

```
SETSHO> SHOW EXCEPTION ❶
SETSHO-I No Exception Logged.
```

❶ Shows no exception was logged.

SHOW HOSTS

Shows a list of disabled hosts.

Format SHOW HOSTS

Command Qualifiers	Defaults
None	None

Description

Displays those host nodes for which communication has been disabled by the SET HOST DISABLE command. The HSC controller maintains a list of nodes and their status. SETSHO lists only those nodes for which communication is disabled.

Example

The following is an example of the SHOW HOSTS screen display.

Example 6–41: SHOW HOSTS Screen Display

```
SETSHO>SHOW HOSTS

All hosts are enabled. ❶
SETSHO>SET HOST DISABLE 8 ❷
SETSHO>SET HOST DISABLE 14 ❸
SETSHO>SHOW HOSTS
Disabled Host Node Numbers: ❹
  Node 8
  Node 14
Total of 2 hosts disabled.
```

❶ Shows all hosts are enabled but does not list node numbers.

❷ Disables communication with host 8.

❸ Disables communication with host 14.

❹ A SHOW HOSTS command displays a list of the disabled hosts by node number.

SHOW LINES

Displays settings of the terminal lines.

Format SHOW LINES

Command Qualifiers	**Defaults**
None	None

Description

Displays the status of the ASCII serial ports and drives.

The load devices are:

TT—This is a serial line or pseudo-terminal. Attributes can be:

- SCOPE/NOSCOPE—Specifies whether the device is a video display terminal or hardcopy device.
- ENABLED—Specifies whether or not the HSC controller recognizes input from the terminal. If no terminal or serial device is connected on the line when the HSC controller boots, the line is set to disabled.
- PSEUDO-TERMINAL—Specifies a DUP terminal, not a physical terminal.

DX—This is an RX33 drive. If the HSC controller boots from this drive, the attribute *Boot Device (SY:)* is noted.

Example

The following is an example of the SHOW LINES screen display.

Example 6–42: SHOW LINES Screen Display

```
SETSHO>SHOW LINES

Device    CSR      Attributes
TT0      177560  NoScope Enabled
TT2      177530  Scope   Enabled
TT4      000000  NoScope Enabled Pseudo-Terminal
TT5      000000  NoScope Enabled Pseudo-Terminal
DX0      177400  Boot Device (SY:)
DX1      177400
```

In this example, four terminals (TT0, TT2, TT4, and TT5) and two RX33 drives (DX0 and DX1) are displayed. The HSC controller was booted from DX0.

SHOW LOAD

Displays the software modules loaded on reboot.

Format SHOW LOAD

Command Qualifiers	Defaults
None	None

Description

Displays the software modules to be loaded the next time the HSC controller is initialized.

The modules that can be loaded are:

- CI—CI manager or CI emulator
- DF—Disk server and ECC process
- DM—Diagnostic monitor (DEMON)
- EL—Central error reporting facility (CERF)
- TF—Tape server
- DUP—Diagnostics utilities protocol (DUP) server

This list of loaded modules can be modified with the SET LOAD command.

Example

The following is an example of the SHOW LOAD screen display.

Example 6–43: SHOW LOAD Screen Display

```
SETSHO>SHOW LOAD

Modules loaded next reboot:
        Central Error Reporting Facility
        Diagnostic Execution Monitor (DEMON)
        DUP
```

The display in this example shows that the central error reporting facility, diagnostic monitor (DEMON), and DUP will be loaded during the next reboot. Also, if a disk data channel is present, the HSC controller will load the disk server; if a tape data channel is present, the HSC controller will load the tape server.

SHOW MAX_FORMATTERS

Displays the maximum number of tape formatters that may be connected to the HSC controller.

Format

SHOW MAX_FORMATTERS

Command Qualifiers	Defaults
None	None

Description

The maximum number of formatters displayed will be allocated space in program memory the next time the HSC controller is initialized.

Example

The following is an example of the SHOW MAX_FORMATTERS screen display.

Example 6–44: SHOW MAX_FORMATTERS Screen Display

```
SETSHO>SHOW MAX_FORMATTERS

Maximum Formatters: 24
```

In this example, up to 24 formatters will be allocated program memory space.

SHOW MAX_TAPES

Displays the maximum number of tape units that may be connected to the HSC controller.

Format

SHOW MAX_TAPES

Command Qualifiers	Defaults
None	None

Description

The maximum number of tape units displayed will be allocated space in program memory the next time the HSC controller is initialized.

Example

The following is an example of the SHOW MAX_TAPES screen display.

Example 6–45: SHOW MAX_TAPES Screen Display

```
SETSHO>SHOW MAX_TAPES

Maximum Tape Drives: 24
```

In this example, up to 24 tape units will be allocated program memory space.

SHOW MEMORY

Displays the disabled memory list, the suspect memory list, and the maximum and actual memory available.

Format

SHOW MEMORY

Command Qualifiers	Defaults
None	None

Description

Displays the contents of the suspect and disabled memory lists, as well as the maximum and actual memory available. All lists are normally maintained by the HSC software and updated only at boot time.

The first time a memory location causes a parity error, or fails the power up memory diagnostics, the address of the failing memory location is added to the suspect memory list. If the same location later causes another parity error, the address of the failing memory location is removed from the suspect memory list and added to the disabled memory list. If a memory location appears in the disabled memory list, the HSC controller does not allocate it for use.

The disabled memory list can also be maintained manually with the SET MEMORY command.

Example

The following is an example of the SHOW MEMORY screen display.

Example 6–46: SHOW MEMORY Screen Display

```
SETSHO>SHOW MEMORY

Disabled Memory List:
No entries found

Suspect Memory List:
No entries found

Maximum Memory Available:

Program Memory: 524288 words
Control Memory: 131072 words
Data Memory:    262144 words

Actual Memory Available:

Program Memory: 524288 words
Control Memory: 131040 words❶
Data Memory:    262144 words
```

❶ Actual control memory available is always 32 words less than maximum control memory available due to HSC controller hardware and software restrictions.

SHOW ODT

Displays the ODT settings in the SCT.

Format SHOW ODT

Command Qualifiers	Defaults
None	None

Description

The ODT settings are:

- **ODT**—ODT is loaded and available.
- **INIT_BPT**—ODT will be entered at the end of HSC controller initialization.
- **DUMP_BPT**—ODT will be entered after an exception dump to the device specified by the SET DUMP command.
- **HOST_Reset_ODT**—ODT will be entered after the HSC controller has been reset by the host.

Example

The following is an example of the SHOW ODT screen display.

Example 6–47: SHOW ODT Screen Display

```
SETSHO>SHOW ODT

Current ODT Setting:
        ODT ❶
        DUMP_BPT ❷
```

❶ ODT is loaded.

❷ ODT will be entered following an HSC system exception.

SHOW POLLER

Displays the values of the CI polling variables.

Format SHOW POLLER

Command Qualifiers	**Defaults**
None	None

Description

The following CI polling variables are displayed:

- The lowest and highest node numbers polled.
- The number of nodes polled at each poll cycle.
- The number of START/STACK retries allowed.
- The time interval in seconds between polling cycles.

Example

The following is an example of the SHOW POLLER screen display.

Example 6–48: SHOW POLLER Screen Display

```
SETSHO>SHOW POLLER

Lowest address to poll:  0   Highest address to poll:  31
Number of nodes to poll each poll cycle:  1
Times to retry a START/STACK:  10
Seconds between poll cycles:  2
```

SHOW POOL

Displays memory pool sizes.

Format

SHOW POOL

Command Qualifiers	Defaults
None	None

Description

Displays the quantity of free control memory blocks, short lifetime control memory blocks, and data buffers available for use by software processes and data channels in the HSC controller.

These numbers may change each time the SHOW POOL command is issued.

Example

The following example shows a typical number of free structures in a SHOW POOL screen display.

Example 6–49: SHOW POOL Screen Display

```
SETSHO>SHOW POOL

Free Lists
2576 - Control Blocks
  32 - Short Lifetime Control Blocks
 887 - Data Buffers
```

SHOW REQUESTORS

Displays information about each requestor.

Format SHOW REQUESTORS

Command Qualifiers	Defaults
None	None

Description

The following information is displayed for each requestor:

- Status (enabled or disabled)
- Type (P.ioj, K.ci, K.si, K.sdi, K.sti, or Empty)
- Microcode version

If the requestor is a K.si or loadable K.ci, the microcode loaded is also displayed.

Example

The following is an example of the SHOW REQUESTORS screen display.

Example 6–50: SHOW REQUESTORS Screen Display

```
SETSHO>SHOW REQUESTORS
Req     Status   Type           Version                  Microcode Loaded
0       Enabled P.ioj
1       Enabled K.ci            MC- 73 DS- 3 Pila-64 K.pli-15   CI
2/A     Enabled K.si            MC- 17 DS- 3             tape
3/B     Enabled K.sti           MC- 27 DS- 2             n/a
4/CJ    Enabled K.si/8          MC- 12 DS- 4             8disk
5/DK    Enabled K.si/8          MC- 12 DS- 4             8disk
6/EL    Enabled K.si/8          MC- 12 DS- 4             8disk
7/F     Enabled K.sdi           MC- 42 DS- 3             n/a
8/M     Enabled K.si            MC- 12 DS- 4             disk
9/N     Enabled K.si            MC- 12 DS- 4             disk
```

In this example, requestor 2 is a 4-port K.si module that is configured as a tape data channel. Requestors 4, 5, and 6 are 8-port K.si modules that are configured as disk data channels. Requestors 8 and 9 are 4-port K.si modules that are configured as disk data channels. Note that this SHOW REQUESTORS display may not represent an advisable HSC controller configuration. It is intended to illustrate the various combinations of displays only.

SHOW SERVER CACHE

Displays the status of the cache server.

Format

SHOW SERVER CACHE

Command Qualifiers	Defaults
None	None

Description

The status and parameters used by the cache server are displayed.

Example

The following is an example of the SHOW SERVER CACHE screen display.

Example 6–51: SHOW SERVER CACHE Screen Display

```
SETSHO> SHOW SERVER CACHE
Cache Status
        Supervisor mode initialized
        Cache hardware present
        ILCACH run
        Cache tests good
        Cache Size Threshold (SC$CST):  8. blocks
        ERASE Purge Threshold: 256. blocks
        WRITE Threshold:  8. blocks
        Transfer Defined Extent size (SC$XDE): 16. blocks
```

SHOW SERVER DISK

Displays the status of the disk server.

Format

SHOW SERVER DISK

Command Qualifiers	Defaults
None	None

Description

The options and parameters used by the disk server are displayed.

Example

The following is an example of the SHOW SERVER DISK screen display.

Example 6–52: SHOW SERVER DISK Screen Display

```
SETSHO>SHOW SERVER DISK
Disk Server Options Enabled:
        Variant Protocol
        Disk Caching
        Disk Drive Controller Timeout: 2 seconds
        Maximum Sectors per Track: 74 sectors
```

SHOW SYSTEM

Displays various HSC system parameters, many of which may be set individually.

Format SHOW SYSTEM

Command Qualifiers	**Defaults**
None	None

Description

The SHOW SYSTEM command displays the following parameters:

- System date and time.
- System boot time.
- Total uptime accumulated since last boot.
- HSC software version number.
- System identification number.
- System name.
- Operator control panel status.
- HSC controller model.
- System dump flag status.
- Device integrity tests status.
- Disk and tape allocation class values.

Example

The following is an example of the SHOW SYSTEM screen display.

Example 6–53: SHOW SYSTEM Screen Display

```
SETSHO>SHOW SYSTEM
12-Jan-1990 13:38:40.71 ❶ Boot:  7-Jan-1990 16:05:27.51 ❷ Up: 117:33 ❸
Version: V600 ❹           System ID: %X00000000FE01 ❺   Name: HSC001 ❻
Front Panel:  Enabled ❼                                 HSC Type: HSC70 ❽
Console Dump:  Enabled ❾
Automatic DITs:  Enabled ❿
Periodic DITs:  Enabled, Interval = 1
Disk Allocation Class:    0                   Tape Allocation Class:  0 ⓫
Disk Drive Controller Timeout: 2 seconds
Maximum Tape Drives:  24
Maximum Formatters:  24
```

❶ System date and time. This is set by the host when establishing the first virtual circuit or by using the SET DATE command.

❷ The time the HSC controller was booted. This number, called *absolute boot time*, represents the first setting of the system date and time.

❸ Up time (hours and minutes). This is the amount of time the HSC controller has been running since it was booted.

❹ Software version. This number changes every release to reflect the latest software version number; it is used for reporting purposes.

❺ System identification. This number is set automatically by the HSC controller and can be modified with the SET ID command.

❻ System name. This name is set automatically by the HSC controller and can be modified with the SET NAME command.

❼ Front panel status. This shows the current state of the Secure/Enable switch on the operator control panel.

❽ HSC controller model.

❾ Settings of the automatic dump flags. These are modified with the SET DUMP command.

Example 6–53 Cont'd on next page

Example 6–53 (Continued): SHOW SYSTEM Screen Display

---

(10) Diagnostic flags and intervals. These values can be modified with the SET AUTOMATIC_DIT and SET PERIODIC_DIT commands.

(11) Disk and tape allocation class values. These values can be modified with the SET ALLOCATE DISK and SET ALLOCATE TAPE commands.

SHOW TAPES

Displays the statistics related to all tape units connected to the HSC controller.

Format

SHOW TAPES

Command Qualifiers	Defaults
None	None

Description

The tape unit number, requestor slot, port, type of tape unit, state of the tape unit, and version numbers are displayed.

Example

The following is an example of the SHOW TAPES screen display.

SHOW TAPES

Example 6–54: SHOW TAPES Screen Display

```
SETSHO>SHOW TAPES
Unit    Req     Port    Type    State                   Version
  122    2        0     TA81    Offline   , Host  DMC - 0,  DHV - 0
                                Density: GCR 6250        FMC - 15, FHV - 6
  123    2        1     TA81    Offline   , Host  DMC - 0,  DHV - 0
                                Density: GCR 6250        FMC - 15, FHV - 6
  400    7        1     TA90    Available, Host  DMC - 23, DHV - 11
                                Density: COMPACTED       FMC - 24, FHV - 5
  401    8        1     TA90    Available, Host  DMC - 23, DHV - 11
                                Density: NORMAL          FMC - 24, FHV - 5

The Tape NOHOST_ACCESS Table is empty.
```

This example shows the status of all tapes connected to the HSC controller.

SHOW VIRTUAL_CIRCUITS

Displays the virtual circuit table for all nodes to which the HSC controller has established virtual circuits.

Format SHOW VIRTUAL_CIRCUITS

Command Qualifiers	Defaults
None	None

Description

The virtual circuit table contains a listing of active node numbers, node names, and their path statuses.

Example

The following is an example of the SHOW VIRTUAL_CIRCUITS screen display.

Example 6–55: SHOW VIRTUAL_CIRCUITS Screen Display

```
SETSHO>SHOW VIRTUAL_CIRCUITS
Virtual Circuits Status
 Node          Open State
 14 (Bison)    Path A  Path B
 15 (Trout)    Path A  Path B
Total of 2 Virtual Circuits
```

This example shows that the HSC controller has a virtual circuit open to node 15 and node 14. Both CI paths are functioning correctly.

6.8 SETSHO Messages

This section describes the different SETSHO messages. The messages are divided into six levels of severity, from least severe to most severe. In each message, a letter appears following SETSHO–. This letter is a code that indicates the severity of the problem. The following table explains each message code.

Table 6–3: SETSHO Message Codes

Code	Description	Refer to
Q	Inquiry. Requires an operator response.	Section 6.8.1.
S	Success. Notification of successful completion of a requested action.	Section 6.8.2.
I	Information. Usually, no response or action is necessary.	Section 6.8.3.
W	Warning. Usually, no action is required.	Section 6.8.4.
E	Error. Notification of detected error condition.	Section 6.8.5.
F	Fatal. The system reboots.	Section 6.8.6.

6.8.1 SETSHO Inquiry Messages

SETSHO–Q Correct media problem. Press RETURN to continue, CTRL/Y to abort:

Explanation: SETSHO has detected some type of media problem. This message is usually preceded by another, more descriptive E-level error message which may provide more information.

Action: Press Return to retry or continue from the failed operation. Additional user action may be needed based on a preceding error message.

SETSHO–Q Rebooting HSC. Press RETURN to continue, CTRL/Y to abort:

Explanation: The HSC controller must be rebooted to activate the changed SETSHO parameters.

Action: Enter Y if you would like to activate the SETSHO changes, otherwise, press Ctrl/Y to abort the changes.

6.8.2 SETSHO Success Message

SETSHO–S The HSC will reboot on exit

Explanation: This message is a reminder that the HSC controller will automatically reboot when it exits.

Action: None.

6.8.3 SETSHO Informational Messages

SETSHO–I Program Exit.

Explanation: The SETSHO utility has completed processing and is exiting.

Action: None.

SETSHO–I *device–type* unit *unit–id* not found.

Explanation: The unit specified is not known to the disk or tape server.

Action: If the unit is correctly connected to the HSC controller, contact Digital Services for assistance in verifying the configuration.

SETSHO–I Disk caching is disabled.

Explanation: A command that affects global caching or caching on a unit is issued when disk caching is disabled.

Action: Make sure the HSC controller has the proper cache hardware. If the correct hardware is installed, try to enable disk caching by using the SET SERVER DISK/CACHE command.

NOTE

Use the SHOW SERVER DISK or SHOW SERVER CACHE command to see the cache state.

If you have enabled global disk caching (SET SERVER DISK/CACHE) and have enabled caching for the unit (SET Dn CACHE) and the disk unit is still not cached, the problem may be with the cache hardware. Contact Digital Services if you suspect a cache hardware malfunction.

SETSHO–I No *device–type* units found

Explanation: No units of the specified type were found.

Action: If the units are correctly connected to the HSC controller, contact Digital Services for assistance with verifying the configuration.

SETSHO–I No Exception Logged

Explanation: The SHOW EXCEPTION command requests the HSC controller to show the reason for the last reboot, but no reason was logged. The following may have caused this message since the last exception was logged:

- The HSC controller was last rebooted from power up (or the Init switch).
- The SCT has been reset to factory settings (which also resets the exception log).

Action: None.

SETSHO–I No virtual circuits are open

Explanation: No virtual circuits are open.

Action: None.

SETSHO–I Not enough resources to complete your request

Explanation: To complete certain operations, SETSHO must acquire HSC system resources and communicate with other software and hardware elements in the HSC controller. When trying to execute a command, SETSHO found the HSC controller did not contain enough system resources.

Action: This may be a transient condition. Try the request again later. If you suspect a hardware failure, contact Digital Services for assistance.

SETSHO–I Your settings require an IMMEDIATE reboot on exit

Explanation: You changed a parameter with a SET command that requires an immediate reboot of the HSC controller for the new value to take effect.

Action: When you have finished changing parameters, exit SETSHO and respond to the reboot prompt.

SETSHO–I Your settings require a reboot. Use ENABLE REBOOT

Explanation: You changed a parameter with a SET command that requires the HSC controller to reboot for the new value to take effect.

Action: Enter the ENABLE REBOOT command before you exit SETSHO.

6.8.4 SETSHO Warning Messages

SETSHO–W All permanent changes lost

Explanation: Specifying the SET SCT CLEAR command resets the SCT back to the original factory settings. Any permanent changes made up to this point in a SETSHO interactive session are lost.

Action: None.

SETSHO–W Both PERMANENT and NOPERMANENT parameters set.
All NOPERMANENT parameters will be lost on reboot.

Explanation: Changes were made to both PERMANENT and NOPERMANENT parameters.

Action: Verify that you did not set both PERMANENT and NOPERMANENT parameters to the SET ERROR command.

SETSHO–W For VMS systems, the HSC name cannot contain a dollar sign ($)

Explanation: The HSC controller name specified in the SET NAME command contains a dollar sign ($) character. Under certain conditions, this is a restriction.

Action: Refer to the description of the SET NAME command and reenter the HSC controller name.

SETSHO–W For VMS systems, the HSC name cannot contain an underscore (_)

Explanation: The HSC controller name specified in the SET NAME command contains an underscore (_) character. Under certain conditions, this is a restriction.

Action: Refer to the description of the SET NAME command and reenter the HSC controller name.

SETSHO–W For VMS systems, the HSC name must begin with an alphabetic character

Explanation: The HSC controller name specified in the SET NAME command does not begin with an alphabetic character. Under certain conditions, this is a restriction.

Action: Refer to the description of the SET NAME command and reenter the HSC controller name.

SETSHO–W For VMS systems, the HSC name must consist of six or fewer alphanumeric characters

Explanation: The HSC controller name specified in the SET NAME command exceeds the six-character limit. Under certain conditions, this is a restriction.

Action: Refer to the description of the SET NAME command and reenter the HSC controller name.

SETSHO–W Invalid Address—*address*

Explanation: The address specified is not a valid HSC controller memory address.

Action: Reenter the SET MEMORY command with a valid address.

SETSHO–W Invalid Hex Number—*hexadecimal_number*

Explanation: The number specified is not a valid hexadecimal number.

Action: Enter a valid hexadecimal number.

6.8.5 SETSHO Error Messages

SETSHO–E 4-port K.si cannot be loaded with 8-port microcode

Explanation: In configuring a 4-port K.si module with the SET REQUESTOR command, you specified it to be loaded with 8-port K.si microcode.

Action: Reenter the SET REQUESTOR command, specifying either 4-port K.si microcode or an 8-port K.si module.

SETSHO–E 8-port K.si cannot be loaded with 4-port microcode

Explanation: In configuring an 8-port K.si module with the SET REQUESTOR command, you specified it to be loaded with 4-port microcode.

Action: Reenter the SET REQUESTOR command, specifying either 8-port K.si microcode or a 4-port K.si module.

SETSHO–E Address *address* not mapped to physical memory

Explanation: Information normally displayed by the credit manager is not available.

Action: Reboot the HSC controller. If the problem persists, submit an SPR.

SETSHO–E Cannot correctly write the system configuration table (SCT)

Explanation: SETSHO cannot correctly update the SCT with the permanent change(s) specified.

Action: Check the error code, correct the problem, and allow SETSHO to retry the operation. The system load media must be write enabled.

SETSHO–E Command cannot be negated

Explanation: You illegally negated a SET command or qualifier.

Action: This command cannot be negated. Please consult the documentation for the command to achieve the desired result.

SETSHO–E Command was unrecognized: *your entry*

Explanation: A command was entered incorrectly (generally a misspelled command).

Action: Reenter the command correctly.

SETSHO–E CRDMGR process not in PCB table

Explanation: The HSC credit manager process is not running.

Action: Reboot the HSC controller. If the problem persists, submit an SPR.

SETSHO–E Disabled Memory List is full. Your address is not saved

Explanation: The disabled memory list is of finite length and can hold only a small number of entries. SETSHO cannot add the specified memory location to the list.

Action: Call Digital Services to examine memory allocation.

SETSHO–E Illegal character *character* in System Name

Explanation: The system name contains an illegal character.

Action: Reenter the SET NAME command with valid characters.

SETSHO–E Invalid range on credits per connection. Valid range is from *min-credits* to *max-credits*

Explanation: The number of credits you have assigned per connection to a host is outside the allowable range.

Action: Reenter the SET CREDITS command using a credit value within the allowable range.

SETSHO–E Invalid range on host id. Valid range is from *min-host* to *max-host*

Explanation: You have specified a host identification outside the allowable range.

Action: Reenter the SET CREDITS command using a host identification within the allowable range.

SETSHO–E Invalid range on memory address. Valid range is from 0 to 16777777

Explanation: The memory address specified is out of range.

Action: Reenter the SET MEMORY command specifying an octal number from 0 to 16777777.

SETSHO–E Invalid range on *parameter*. Valid range is from *low–value* to *high–value*

Explanation: You specified a parameter value that is out of range.

Action: Reenter the command using a parameter value within the proper range.

SETSHO–E Low node address greater than high node address

Explanation: The SET POLLER command specified a low node number (at which polling should begin) that was greater than the high node number.

Action: Reenter the SET POLLER command with a low node number less than the high node number.

SETSHO-E Media version mismatch.

Explanation: The software currently running on the HSC controller does not match the software version of the media currently in the load device. These versions must match if you wish to change a system parameter with a SET command.

Action: Make sure the media currently in the load device is the media from which the HSC controller was booted.

SETSHO–E Requestor disabled

Explanation: You have issued a SET REQUESTOR command to a requestor that is present in the HSC controller backplane, but is disabled.

Action: Reenter the SET REQUESTOR command to the correct slot.

SETSHO–E Requestor slot empty

Explanation: You have issued a SET REQUESTOR command to an unoccupied backplane slot.

Action: Reenter the SET REQUESTOR command to the correct slot.

SETSHO–E The host interface module K.ci is not present. Check the error code and correct the error

Explanation: A command that requires interrogation of the host interface module (K.ci) was specified. That module is not present or is not working.

Action: Install a host interface module (K.ci) in the HSC controller.

SETSHO–E The NOHOST table for *device–type* is full. The state of this unit cannot be preserved across boot

Explanation: The HSC controller has two NOHOST tables—one for disk and one for tape units. Each table has capacity for 48 units. The table into which you wanted to insert a unit is already full.

Action: Use the SET DEVICE *unit–id* HOST_ACCESS command to remove an existing unit entry from the table and make room for the new unit.

SETSHO–E This command works only with disk units

Explanation: A tape unit was specified on a command that works only with disk units.

Action: Reenter the command again, specifying a disk unit. The syntax for a disk unit is D*nnnn*, where *nnnn* is the unit number.

SETSHO–E This is not a loadable requestor

Explanation: You have issued a SET REQUESTOR command to a K.sdi or K.sti module. These modules cannot be reconfigured.

Action: Reenter the SET REQUESTOR command to the correct slot.

SETSHO–E Time not correctly set

Explanation: The date (and time) specified with the SET DATE command is not correctly set. You cannot specify a date/time combination that is earlier than the HSC system build time (shown on the console when the HSC controller boots).

Action: Enter a valid date/time string.

SETSHO–E You cannot specify a value when specifying NOPERIODIC_DIT

Explanation: The SET NOPERIODIC_DIT command and an interval value were specified. This is not legal. In this context, NOPERIODIC_DIT means no periodic device integrity tests will run.

Action: Reenter the command without the interval value.

SETSHO–E Your command was incomplete. Reenter with all parameters.

Explanation: You entered a SET command and failed to enter the parameters.

Action: Reenter the SET command with the appropriate parameters.

6.8.6 SETSHO Fatal Message

SETSHO–F CTRL/C or CTRL/Y Abort. No changes made to SCT.

Explanation: Ctrl/C or Ctrl/Y was entered while SETSHO was running. None of the permanent changes (those that are saved across boots and are stored in the SCT) were saved. Temporary changes are in effect.

Action: Restart SETSHO.

Chapter 12

VTDPY UTILITY

The VTDPY utility gathers and displays system statistics. VTDPY displays system throughput, disk and tape drive status, and the status of processes running on the HSC controller. VTDPY also indicates which nodes have virtual circuits, connections, and multiple connections to the HSC controller.

The VTDPY utility requires a video terminal and does not display on a hardcopy printer. Attach a VT100- (with Advanced Video Option), VT220-, or VT320-series terminal (set at 9600 baud) to the EIA port of the HSC controller.

The following sections show how to use the VTDPY utility.

12.1 How to Run VTDPY

CAUTION

Do not run VTDPY under the following conditions:

- Over a host-HSC controller connection that was established with the VMS SET HOST/HSC command on VMS versions prior to Version 4.6.
- While running the Cache Performance Analysis Tool (CPAT). Attempting to run CPAT and VTDPY simultaneously results in a fatal error to either CPAT or VTDPY, depending upon which program is running when the other is started.

To initiate VTDPY, enter the following command at the HSC> prompt:

```
HSC>RUN VTDPY [update-interval]
```

The *update-interval* is in seconds, from 4 to 60. Higher update intervals have less impact on HSC controller performance. enter Ctrl/Z to use the default update interval of 30 seconds.

If you do not enter an update interval when you initiate VTDPY, the following prompt is displayed:

```
VTDPY-Q Interval (seconds) ?
```

If you enter an update interval outside the allowable range, VTDPY displays an error message. Refer to Section 12.3 for a description of this message.

Enter Ctrl/Y or Ctrl/C to terminate VTDPY and clear the screen.

12.1.1 Using the VTDPY Control Keys

Use the control key sequences given in Table 12–1 to work the VTDPY display.

Table 12–1: VTDPY Control Keys

Control Key Sequence	Function
Ctrl/A	Displays disk status on the next and all subsequent refreshes. Calculates new "Free List" and "Pool Size" values.
Ctrl/B	Displays tape status on the next and all subsequent refreshes. Calculates new "Free List" and "Pool Size" values.
Ctrl/C	Terminates VTDPY and clears the screen.
Ctrl/D	Displays disk status on the next refresh. Thereafter, tape status and disk status are alternately displayed on subsequent refreshes. Calculates new "Free List" and "Pool Size" values.
Ctrl/E	Displays tape status on the next refresh. Thereafter, disk status and tape status are alternately displayed on subsequent refreshes. Calculates new "Free List" and "Pool Size" values.
Ctrl/F	Displays available memory segments and their sizes. Calculates new "Free List" and "Pool Size" values.
Ctrl/V	Displays host path status information (A, B, or a diamond) on the next refresh only. Calculates new "Free List" and "Pool Size" values.
Ctrl/W	Refreshes the screen, resets to alternating disk/tape status display, and calculates new "Free List" and "Pool Size" values.
Ctrl/Y	Terminates VTDPY and clears the screen.

Portions of the VTDPY display are continuously updated at the update interval selected. The display changes as the internal state of the HSC controller changes. The field values relating to HSC memory—"Free List" and "Pool Size"—do not change with these continuous updates. These memory statistics are updated only when the screen is refreshed using specific control key sequences, such as Ctrl/W.

12.2 How to Interpret the VTDPY Display Fields

This section describes the major fields in the VTDPY display. An example of the VTDPY screen is shown, followed by an explanation of each field of the screen. The overall screen is shown in Figure 12–1.

Figure 12–1: VTDPY Display

```
HSC90  V600  HSC003  Id  000000FC03  On-18-Dec-1990  10:02:43.13   Up:  120:18

   2.5% Idle        14.8% Data B/W Used      106 Work Requests/Sec      85 Sectors/Sec          243 Records/Sec          82 Cache Hits/Sec

     Free Lists            Process      Pr  St  Time%                     Disk Status, refresh time is 10 seconds
   Ctrl Blks    1977 +          Kernel             9.0%      D#    S     IO/S     IOs    HITs    D#    S  IO/S    IOs  HITs      D#     S   IO/S    IOs   HITs
   SLCB/DCB       48 +      4  VTDPY    11  Rn      .1%      D44   A                             D2016 C     4     43     7      D3032  A
   Buffers       855 +     50  DEMON    11  B1               D115  E      24     236             D2017 O     4     39            D3033  A
   WHE          1023 +     52  PDEMON    7  B1               D116  E      24     240             D2018 A                         D3034  C     34    343    343
                           54  PSCHED   13  Rn     2.5%      D171  C      12     123      94     D2019 C     6     56    49      D3035  C     99     86     56
                           72  DISK      9  B1    46.9%      D172  A                             D2020 C     1      5     0      D3036  C     12    116    112
     Pool Sizes           110  ECC       6  B1      .0%      D173  C       8      79       1     D2021 C     0      2     2      D3037  A
   Common       6160 +    114  CASH      8  B1    10.3%      D174  A                             D2022 C     1      9     0
   Kernel       9164 +    132  HOST      4  B1    22.5%      D175  C       1       9       6     D2023 O     4     40
   Program   1255232 +    134  POLLER    5  B1               D176  C       4      37      34     D2024 O     0      4
   Control     20088 +    136  SCSDIR    5  B1     8.7%      D177  A                             D2025 O     2     24
                                                             D1010 O      21     205             D2026 O     0      0
                                                             D1011 O       0       4             D2027 O     0      0
         Host Connections                                    D1012 C       1      13      11     D2028 O    14    142
                    111111111122222222223333333333           D1013 C       3      29      20     D2029 O    13    133
          0123456789012345678901234567890123456789           D1014 C       2      21      21     D2030 C     4     43    43
         0......M...M...C...V.......M.M.........             D1015 C       5      47      17     D2031 O     0      0
        40........................................
```

CXO-3128A_R

Field

```
HSC90 ❶ V600 ❷ HSC003 ❸ Id 0000000FC03 ❹ On
18-DEC-1990  10:02:43.13 ❺ UP: 120.18 ❻
```

Description

❶ HSC controller model number.

❷ HSC system software base level.

❸ System name.

❹ HSC controller identification number, given as a hexadecimal number unique in the cluster.

❺ System date and time.

❻ Hours and minutes the HSC controller has been running since the last boot or reboot.

Field

```
2.5% Idle ❶ 14.8% Data B/W Used ❷ 106 Work Requests/Sec
❸ 85 Sectors/Sec ❹
243 Records/Sec ❺ 82 Cache Hits/Sec ❻ * ❼
```

Description

❶ Percentage of current P.io module idle time.

❷ Shows the percentage of HSC data bus bandwidth used. This display is instantaneous and may often show 0% even when the HSC controller is busy because the bandwidth was zero at the instant the sample was taken.

❸ Average number of work requests per second. This includes MSCP and TMSCP messages.

❹ Number of disk data sectors transferred per second. This number is normalized to match the update interval.

❺ Number of tape data records transferred per second. This number is normalized to match the update interval.

❻ Number of times data was found and obtained from cache. This number is normalized to match the update interval.

❼ The asterisk indicates that the rate information displayed is outdated. This may be due to insufficient processor time available to VTDPY on heavily loaded HSC systems.

Field

```
   Free Lists
CTRL Blks    1977 + ❶
SLCB/DCB       48 + ❷
Buffers       855 + ❸
WHE          1023 + ❹

   Pool Sizes       ❺
Common       6160 +
Kernel       9164 +
Program   1255232 +
Control     20088 +
```

Description

This field shows the quantity of available memory and memory structures. The memory and memory structures are used by various components of HSC controller software for the purposes of communication and data transfer. The units displayed are:

❶ CTRL Blks—Number of blocks

❷ SLCB/DCB—Number of structures

❸ Buffers—Number of buffers

❹ WHE—Number of structures

❺ Pool Sizes—Bytes of memory

The numbers are usually followed by plus signs. Minus signs indicate the system is in memory deficit. During memory deficit, the HSC controller slows down and, if the deficit lasts long enough, the HSC controller could crash.

The “Free Lists” and “Pool Sizes” values are updated every time the screen is refreshed using control key sequences (for example, by entering Ctrl/W). The plus (+) and minus (-) signs are updated at every update interval.

Field

```
    Host Connections
              1111111111222222222233333333333 ❶
  0123456789012345678901234567890123456789
 0.......M...M...C...V.......M.M.......... ❷
40........................................ ❸
```

Description

Indicates host connection status.

❶ The first and second lines are used to determine host node numbers 0-39. Each digit on the first line is read with the digit directly below it to form the numbers 10-39.

❷ The third line indicates the status of the host connections.

- **C** indicates one connection to that host. In this example, node 15 shows one connection.
- **M** indicates multiple connections to that host. Because each host can make a separate connection to each of the disk, tape, and DUP servers, this field frequently shows multiple connections. In this example, nodes 7, 11, 27, and 29 show multiple connections.
- **V** indicates that only a virtual circuit is open and no connection is present. This usually means the host is in a transitional state. This example shows node 19 with only a virtual circuit open.
- If no letter corresponds to the node number, that host does not have any connection to the HSC controller.

❸ The fourth line describes the connection status for host node numbers above 40. To determine these host node numbers, add the base number 40 at the far left to the numbers above the display in the first and second lines.

Field

```
   Host Path Status
           111111111122222222223333333333
  0123456789012345678901234567890123456789
 0.......^...A...^...B.......A.^..........
40........................................
```

Description

When you enter Ctrl/V, the Host Connections display toggles to an alternate Host Path Status display for one update interval only. This display contains CI path status information. If one path (A or B) becomes inoperative, this display alternates with the Host Connections display until the bad path is operational again.

The symbols in this example have the following meanings:

- A solid diamond symbol (represented by a caret (^) in this example) indicates both paths are operating normally (normal operation).
- An **A** or **B** indicates only one CI path is operational.

  If an **A** is displayed, path A is active but path B is not.
  If a **B** is displayed, path B is active but path A is not.

  These conditions indicate a possible hardware problem.

The example shows that nodes 7, 15, and 29 have both paths operating, nodes 11 and 27 have only path A operating, and node 19 has only path B operating.

Field

```
  Process Pr St  Time%
    Kernel        9.0%
  4 VTDPY  11 Rn   .1%
 50 DEMON  11 Bl
 52 PDEMON  7 Bl
 54 PSCHED 13 Rn  2.5%
 72 DISK    9 Rn 46.9%
110 ECC     6 Bl   .0%
114 CASH    8 Bl 10.3%
132 HOST    4 Bl 22.5%
134 POLLER  5 Bl
130 SCSDIR  5 Bl  8.7%
```

Description

The fields in this example contain process, statistical, and status information. The following list describes the column entries (from left to right):

- The first column indicates the process number (4, 50, and so on).
- The **Process** column shows the names of various processes. The first entry in this column indicates the operating system, Kernel. Other names in the **Process** column are described in Table 12–2.

Table 12–2: Process Description

Process Name	Description
VTDPY	Video terminal display utility
DEMON	Diagnostics execution monitor (for demand and automatic device integrity tests)
PDEMON	Periodic diagnostics execution monitor (for periodic device integrity tests)
PSCHED	Periodic device integrity tests scheduler (this is the HSC controller idle loop)

Table 12–2 (Continued): Process Description

Process Name	Description
DISK	Disk server (displayed when the disk server is loaded)
ECC	Error correction code process (displayed when the disk server is loaded)
CASH	Cache server (displayed when the cache server is loaded)
HOST	Host interface manager process (always present)
POLLER	Host processor poller (displayed when a connection is present)
SCSDIR	Host directory request processor
TAPE	Tape server
TTRASH	Tape error log processor (displayed when the tape server is loaded)

- The **Pr** column shows the priority of the process (11, 11, 7, and so on).
- The **St** column shows the status of the process: either running (Rn) or blocked (Bl).
- The **Time%** column shows the percentage of P.io time that each currently running process is using (9.0%, .1%, 2.5%, and so on).

Not all active processes are necessarily shown. Because of limited space on the screen, the display of some processes may be truncated and the CPU time percentages may not total 100 percent, depending on the polling interval of the data sample.

Field

Disk Status, refresh time is 10 seconds

D#	S	IO/S	IOs	HITs	D#	S	IO/S	IOs	HITs	D#	S	IO/S	IOs	HITs
D44	A				D2016	C	4	43	7	D3032	A			
D115	E	24	236		D2017	O	4	39		D3033	A			
D116	E	24	240		D2018	A				D3034	C	34	343	343
D171	C	12	123	94	D2019	C	6	56	49	D3035	C	9	86	56
D172	A				D2020	C	1	5	0	D3036	C	12	116	112
D173	C	8	79	1	D2021	C	0	2	2	D3037	A			
D174	A				D2022	C	1	9	0					
D175	C	1	9	6	D2023	O	4	40						
D176	C	4	37	34	D2024	O	0	4						
D177	A				D2025	O	2	24						
D1010	O	21	205		D2026	O	0	0						
D1011	O	0	4		D2027	O	0	0						
D1012	C	1	13	11	D2028	O	14	142						
D1013	C	3	29	20	D2029	O	13	133						
D1014	C	2	21	21	D2030	C	4	43	43					
D1015	C	5	47	17	D2031	O	0	0						

Description

This area of the display alternates between disk and tape drive status when both device types are connected to the HSC controller. To display disk drive status only, use the Ctrl/A control key sequence. This example shows disk drive status.

The disk status display of VTDPY:

- shows the activity on a drive-by-drive basis.
- may be used as a tool in the allocation and evaluation of HSC cache.
- assists in evaluating which drives benefit the most from caching by displaying information containing:
  - the drives having the greatest demands made on them.
  - the number of input/output (IO) requests per second.
  - the cache read hits compared to all other drives or the HSC controller.

- the ratio between total inputs or outputs (IO) during this measuring interval and cache read hits.

For disk heading definitions refer to Table 12–3. For disk status codes refer to Table 12–4.

Table 12–3: VTDPY Disk Drive Heading Definitions

Column Heading	Definition	Meaning
D#	Disk drive number	An ordered list of known drive numbers connected to this HSC controller
S	Drive status code	Characters that indicate the current drive's status (see Table 12–4 for drive status code definitions)
IO/S	Input or output requests per second	The IO rate on a per drive basis
IOs	Total input or output requests during this measuring interval	The request count for each drive
HITs	Total cache read hits during this measuring interval	The cache read hits for each drive that has caching enabled

Table 12–4: Disk Drive Status Codes

Status Character	Definition
O	Drive is online.
A	Drive is available.
C	Drive is online and caching is enabled.
E	Drive is online and is an ESE-type drive in enhanced mode (if this ESE drive was in compatibility mode, an O would be displayed).
D	HSC controller is connected to duplicate units (two or more drives with the same unit number). Drive is disabled.
U	Drive is in an undefined state.
X	A single host has exclusive access to a drive in any state: available, online, or offline. This indicator is for ULTRIX systems only.
Y	A single host has exclusive access to a drive and the drive is online with caching enabled. This indicator is for ULTRIX systems only.

Field

```
      Tape Status, refresh time is 10 seconds
 T#    S IO/S    IOs          T#    S IO/S    IOs
  T14 A                     T1412 O    4     43
  T15 O   24    236         T1413 A
  T16 O    4     40
  T17 O    2     24
  T18 F
  T19 O    0      0
  T20 A
  T21 O   20    199
T1300 A
T1301 A
T1302 A
T1303 F
T1304 F
T1305 A
T1306 A
T1307 A
```

Description

This area of the display alternates between disk and tape drive status when both device types are connected to the HSC controller. To display tape drive status only, use the Ctrl/B control key sequence. This example shows tape drive status.

The tape status display of VTDPY shows the activity on a drive-by-drive basis. For tape heading definitions refer to Table 12–5. For tape status codes refer to Table 12–6.

Table 12–5: VTDPY Tape Drive Heading Definitions

Heading	Definition	Meaning
T#	Tape drive number	An ordered list of known drive numbers connected to this HSC controller
S	Drive status code	Characters that indicate the current drive's status (see Table 12–6 for drive status code definitions)
IO/S	Input or output requests per second	The IO rate on a per drive basis
IOs	Total inputs or outputs during this measuring interval	The request count for each drive

Table 12–6: Tape Drive Status Codes

Status Code	Definition
O	Drive is online
A	Drive is available
F	No tape is mounted on the drive

12.3 VTDPY Messages

This section describes the messages VTDPY may display.

12.3.1 VTDPY Error Messages

VTDPY–E Illegal Interval Value (4 to 60 seconds)

Explanation: You have entered an update interval that is outside the allowable range. VTDPY prompts again for the update interval.

Action: Enter a value within the specified range.

12.3.2 VTDPY Fatal Messages

VTDPY–F DSTAT and VTDPY may not run concurrently

Explanation: Due to the use of a common set of statistics variables, the DSTAT and VTDPY utilities may not run concurrently. The DSTAT utility is used by the Cache Performance Analysis Tool (CPAT).

Action: Wait until CPAT (or the DSTAT utility) is terminated before running VTDPY.

VTDPY–F Insufficient Common Pool

Explanation: Indicates insufficient memory to run VTDPY.

Action: Try VTDPY again when the demands on memory are reduced. Look for disabled memory by entering the SHOW MEMORY command at the HSC> prompt.

Chapter 13

SCTSAV Utility

The SCTSAV utility is used when installing updates of HSC controller software. This utility saves you the steps of printing out the system configuration table (SCT) and reentering the values when installing the update. SCTSAV also circumvents the need for multiple reboots of the HSC controller which were previously required when manually entering parameter changes using the SETSHO utility.

The SCTSAV utility cannot be used to install an initial version of HSC software on a new HSC controller. Use the procedure described in detail in the current *HSC Software Release Notes* for installing the HSC software.

The SCTSAV utility reads the current SCT parameters from memory, translates them to the new software version, and writes them to the SCT.INI file residing on the new version media. The new version media can then be booted with the saved HSC parameters.

All HSC parameters that are current in the SCT are written to the new version media. However, there may be new HSC parameter values associated with the new version software. After booting with the new version of the HSC software, any new HSC software parameters will contain default values and must be updated using the appropriate SETSHO commands.

13.1 Restrictions on Running SCTSAV

The SCTSAV utility is supplied on the distribution media of the new version of HSC software and is compatible with one particular software version. However, the SCTSAV utility returns a fatal error under the following circumstances:

- If you try to run SCTSAV a second time after running it and rebooting the new media. Once SCTSAV has executed and the new version software is booted, the SCTSAV utility will no longer load. You will get the following message if you try to run SCTSAV again on an HSC controller that is running the new software:

  ```
  KMON--F File Not a Loadable Program Image
  ```

  SCTSAV is a "one time" utility that only works with first installation of the new version software.
- If you insert the new version media into any boot device of the HSC controller, then boot (with or without holding the Fault button in) before running SCTSAV, you will get the following fatal SCTSAV error when you subsequently run SCTSAV:

  ```
  SCTSAV--F SCTSAV cannot determine the source of the SCT file
  ```

- If you use SCTSAV to update new SCT parameters on one HSC controller, then insert the same media in the boot device of another HSC controller running a previous version of HSC software and run SCTSAV without rebooting, you will get the following fatal SCTSAV error:

  ```
  SCTSAV--F SCTSAV cannot determine the source of the SCT file
  ```

  For this reason, you must make any backup copies of the new version HSC software media **before** running the SCTSAV utility and installing the new software.

13.2 How to Run SCTSAV

Use the following procedure to install a new version of HSC software with the SCTSAV utility.

CAUTION

Be sure to make all preinstallation backup copies of the new HSC software media **before** running the SCTSAV utility. This is because SCTSAV returns a fatal error once it has written the SCT file on the new media.

1. Follow the disk and tape failover procedure detailed in the software installation section of the current *HSC Software Release Notes*.
2. Remove the diskette containing the previous version of HSC software from the HSC controller boot device.
3. Remove the write-protect tab from the new HSC software diskette.
4. Insert the diskette containing the new HSC software into the HSC controller boot device.
5. Enter the following command:

```
HSC> RUN SCTSAV

SCTSAV--I HSC parameters have been copied to the new version media
SCTSAV--I Program exit
```

   The SCTSAV utility takes only a few seconds to run. If you get a fatal error while running SCTSAV, the SCT.INI file could be in error and result in an incorrect SCT after reboot. In this unlikely event, go to the procedure given in Section 13.4 to install the new HSC software.

13.3 SCTSAV Example

Example 13–1 shows a successful run of the SCTSAV utility.

Example 13–1: Sample SCTSAV Utility Run

```
Ctrl/C

HSC> RUN SCTSAV

SCTSAV--I HSC parameters have been copied to the new version media
SCTSAV--I Program exit
```

13.4 Recovering from a Fatal SCTSAV Error

The SCTSAV utility has been designed to preserve data integrity. However, unpredictable hardware failures could cause the saved SCT parameters to be unusable.

In the unlikely event that you get a fatal error while running SCSAV, the SCT.INI file could contain incorrect data caused by the error. Use the following procedure to recover from a fatal SCTSAV error:

1. Verify that the disk and tape failover procedures detailed in the software installation section of the current *HSC Software Release Notes* have been correctly followed. Ensure that the diskette containing the "old" version of HSC software is installed in the HSC controller boot device.
2. Run the SETSHO utility and use the following commands to save the SCT parameters on the old media to hardcopy:
   - SHOW SYSTEM
   - SHOW REQUESTORS
3. If the HSC controller has the HSC Cache option installed, save the output from the following commands to hardcopy:
   - SHOW DISKS

- SHOW SERVER CACHE
- SHOW SERVER DISK

4. Install the new media and boot the HSC controller by pressing the Init and Fault buttons on the operator control panel (OCP). Release the Fault button when the following message appears:

   ```
   INIPIO--I Booting...
   ```

5. After the HSC controller has successfully booted with the new media, use the SETSHO utility to enter the saved hardcopy parameters into the SCT table.
6. Reenter the above SHOW commands and verify that all parameters are correctly set.

This procedure is the same as the one described in detail in the current *HSC Software Release Notes* for installing HSC software when you are running a version of HSC software that is more than one level older than the version you are installing (for example, going from V5.0A to V6.5 and skipping over V6.0).

13.5 SCTSAV Messages

This section contains a listing of the messages that may be displayed while running the SCTSAV utility.

13.5.1 SCTSAV Informational Messages

SCTSAV–I CTRL/Y or CTRL/C Abort

Explanation: The SCTSAV utility has been aborted by the user.

Action: None.

SCTSAV–I HSC parameters have been copied to the new version media

Explanation: The SCTSAV utility has successfully copied the SCT parameters to the new version media.

Action: None.

SCTSAV–I Program exit

Explanation: The SCTSAV utility has terminated. This message is printed for all exiting conditions, including a successful run or a fatal error.

Action: If an error has occurred, rerun the SCTSAV utility.

13.5.2 SCTSAV Inquiry Messages

SCTSAV–Q Write enable unit. Press Return to continue, or CTRL/Y to exit

Explanation: This error occurs along with a WRITE PROTECTED warning message.

Action: You can either write enable the media or exit the SCTSAV utility.

13.5.3 SCTSAV Warning Messages

SCTSAV–W Unit is write protected

Explanation: The HSC software media comes with a write-protect tab in place to prevent accidental writing of the media during installation. However, SCTSAV writes to this media during its run.

Action: Remove the diskette from the drive and peel the write-protect tab off. Reinstall the diskette and continue with the software installation procedure.

13.5.4 SCTSAV Fatal Messages

SCTSAV–F Cannot read the new version syscom file

Explanation: The new version software media cannot be read without an error occurring. This condition could be due to a hardware failure of the boot device or because the media is not properly inserted.

Action: Verify that the media has been properly inserted in the boot device. If correct, call Digital Services. Install the new version media using the procedure given in Section 13.4.

SCTSAV–F Could not verify the new version media
HSC SCT parameters were not properly copied
Boot the new version media holding in the fault button

Explanation: The HSC controller hardware did not report any read/write errors, but the saved HSC SCT parameters have failed verification. This is a data error that could be due to faulty media or a hardware problem.

Action: Call Digital Services. Install the new version media using the procedure given in Section 13.4.

SCTSAV–F Insufficient resources to run, no xfrbs

Explanation: Memory resources to run the SCTSAV utility could not be allocated. This message could be caused by a memory failure.

Action: Call Digital Services. Install the new version media using the procedure given in Section 13.4.

SCTSAV–F SCTSAV cannot determine the source of the SCT file

Explanation: The SCT has already been written by the SCTSAV utility or by a reboot of the HSC controller. Therefore, SCTSAV cannot validate the SCT and run to completion.

Action: Install the new version media using the procedure given in Section 13.4.

SCTSAV–F The HSC parameters did not properly copy to the new version media
Boot the new version media holding in the fault button

Explanation: The SCT does not contain proper values after the write operation and is in an undefined condition.

Action: You must manually set the SCT parameters in the new version media using the procedure described in Section 13.4.

SCTSAV–F Write failure during write check, status: *xxx* (O)

Explanation: The new version software media cannot be written without an error. This condition could be due to a hardware failure of the boot device. The octal byte given in *xxx* is an error status value.

Action: Record the octal status value *xxx* and call Digital Services. Install the new version media using the procedure given in Section 13.4.

Appendix A

Command Prompt and TTDR Errors

This appendix describes the keyboard monitor (KMON) prompt, its error messages, and the terminal driver facility (TTDR) error messages.

The KMON prompt is referred to in this manual as the HSC> prompt. The term "KMON prompt" is used in this appendix because the error messages associated with this prompt are prefixed by the letters KMON. A user can change the prompt by using the SET PROMPT command.

A.1 KMON Prompt

When you enter Ctrl/Y, the HSC controller displays the KMON prompt:

```
HSC>
```

Always enter an accompanying program name when you enter the RUN command at the KMON prompt. Otherwise, the system prompts for a program name.

If you press any key (except the Break key or Control keys) and the HSC controller is unprepared to accept input, the HSC console terminal beeps. The Break key is an exception because it is a direct instruction to the HSC hardware to stop the I/O control processor. Control keys are direct input to the software.

A.2 KMON Prompt Messages

This section describes the KMON prompt messages. Most of the messages are classified as fatal messages.

A.2.1 KMON Prompt Informational Message

KMON–I Program Load Aborted

Explanation: You entered Ctrl/C or Ctrl/Y at the terminal during a program load. The HSC controller terminates the loading of the program.

Action: Run the program again.

A.2.2 KMON Prompt Fatal Messages

KMON–F All Utility Partitions in Use

Explanation: The HSC software has a finite number of partitions available to run utilities. This message is displayed if you enter a RUN *filename* command and every available partition is in use by an executing utility.

Action: Either terminate a currently executing utility by entering Ctrl/C on the console terminal, or wait for the utility to complete.

KMON–F Demand Device Integrity Test Request Already Pending

Explanation: The HSC controller can run only one demand device integrity test at a time. (A demand device integrity test is requested by an explicit RUN *filename* command on the keyboard, as opposed to an automatic device integrity test run at the discretion of the HSC software.) This message is issued when a device integrity test is already running.

Action: Either terminate the currently running device integrity test by entering Ctrl/C on the console terminal, or wait for the device integrity test to complete.

KMON–F Device Integrity Test Monitor Not In Memory

Explanation: The diagnostic monitor (the diagnostic/HSC software interface) that all device integrity tests use is not currently loaded in memory. The diagnostic monitor is required to run any device integrity test.

Action: Use the SETSHO utility to execute the SET LOAD DM command. This command loads the diagnostic monitor the next time the HSC controller reboots.

KMON–F Device Integrity Test Monitor Too Busy; Try Again Later

Explanation: This message is issued in response to a RUN *filename* command. It indicates that the HSC software common pool did not contain enough free space to allocate the diagnostic request block (DRB) data structure necessary to run a device integrity test.

Action: This is a transient condition. Run the device integrity test again later.

KMON–F Error Reading Program File

Explanation: This message is issued in response to a RUN *filename* command. It indicates that a hardware problem with the load device is preventing a normal load of the requested program.

Action: Check the disk drive to make sure the RX33 diskette is properly mounted. If the load medium has been in service for a long time, it may be approaching the end of its useful life; try another load medium. If the error persists, call Digital Customer Services.

KMON–F File Not a Loadable Program Image

Explanation: This message is issued in response to a RUN *filename* command. It indicates that the requested program is not a proper utility or device integrity test (files with a file type of .UTL or .DIA).

Action: Select another program to run.

KMON–F Illegal Indirect Device or File Name

Explanation: This message is issued in response to the *@filename* command. It indicates that the command file name you supplied is in an illegal format. Indirect file support is an unsupported feature of the HSC controller.

Action: Use a command file name of the correct format: FILENAME.COM.

KMON–F Illegal Device or Program Name

Explanation: This message is issued in response to the RUN *filename* command. It indicates that the device specified in the filename does not exist or the filename is illegal.

Action: Correct the filename and enter the RUN command again.

KMON–F Insufficient Common Pool

Explanation: This message is issued in response to a RUN *filename* command. It indicates that although the program was successfully loaded, the common pool of the HSC controller did not contain enough contiguous free space to allocate an input buffer for the requested program.

Action: This is a transient condition. Run the program again later.

KMON–F Insufficient Free Memory to Load Program

Explanation: This message is issued in response to a RUN *filename* command. It indicates that although the HSC controller found the program, there were not enough free contiguous 4 kilobyte sections of program memory to load the program.

Action: This may be a transient condition if many utilities or device integrity tests are running. If so, wait for one of these programs to finish, or terminate a program by entering Ctrl/C to free memory space currently in use by these programs.

If the problem is not transient, or if the suggested solution does not solve the problem, do one or both of the following:

- Use the SETSHO command SET [NO]LOAD *module-name* to eliminate loading of unneeded modules at HSC controller boot time.

- Use the SET MAX_TAPE and SET MAX_FORMATTER commands to reduce the amount of memory the tape server allocates for internal structures. Refer to Chapter 6 for details.

KMON–F Invalid or Ambiguous Command

Explanation: The command you entered at the KMON prompt (HSC>) was not one of the following:

- RUN
- SET
- SHOW
- DIRECT
- PURGE
- CRASH
- Ctrl/Z (EXIT)

Action: Enter a valid command.

KMON–F Load File Disabled by Software

Explanation: The program specified in the RUN *filename* command was flagged in its image as disabled. This program is not loadable and cannot be executed with the RUN command.

Action: None.

KMON–F No Media Mounted on Specified Unit

Explanation: This message is issued in response to a RUN *filename* command. It indicates there is no media mounted in the device specified in the filename parameter.

Action: Either run the program from another device or mount a diskette in the specified drive.

KMON–F Operator panel in SECURE position.

Explanation: You entered a RUN *filename* command or a SETSHO SET command at the KMON prompt when the Secure/Enable switch was in the SECURE position. The HSC controller can only execute SETSHO SHOW commands when the Secure/Enable switch is in the SECURE position.

Action: Place the Secure/Enable switch in the ENABLE position.

KMON–F Process Not Runnable on Demand

Explanation: This message is issued in response to a RUN *filename* command. Although the program specified was successfully loaded, it cannot be run on a terminal. Therefore, the program load was aborted.

Action: None.

KMON–F Program Already Executing

Explanation: The program specified in the RUN *filename* command is already executing on another terminal. Only one copy of any program can execute at a time.

Action: Either wait for the currently executing program to finish or terminate the program by entering Ctrl/C on the terminal on which the program is running.

KMON–F Program File Not Found on Specified Unit

Explanation: The program specified in the RUN *filename* command was not found on the unit specified.

Action: Run the program from a different unit. Inspect the contents of the unit with the DIRECT command.

A.3 DIRECT Error Messages

This section describes the DIRECT error messages.

DIRECT–F Command Syntax Error

Explanation: A syntax error was made in entering the DIRECT command.

Action: Reenter the DIRECT command using the correct syntax.

DIRECT–F Corrupted HSC directory structure

Explanation: An error was detected while reading the directory structure of the diskette.

Action: Use a different diskette. Verify that the diskette is not corrupted.

DIRECT–F Fatal I/O Error

Explanation: An error was detected while reading information from the device.

Action: Verify that the diskette is of a type recognized by the HSC controller. Verify that there are no hardware problems with the device.

DIRECT–F Invalid HSC volume

Explanation: The diskette was not of a type recognized by the HSC controller.

Action: Use the proper diskette type in the HSC controller load device.

A.4 TTDR Error Messages

This section describes the TTDR error messages.

TTDR–F Error Reading Indirect File

Explanation: This message is issued when the HSC terminal server is unable to read a block from the indirect command file. Indirect file support is an unsupported feature of the HSC controller.

Action: None.

TTDR–F Error Allocating Memory for Indirect File

Explanation: This message is issued when the HSC terminal server is unable to allocate a buffer in which to read a block of the indirect command file. Indirect file support is an unsupported feature of the HSC controller.

Action: None.

TTTDR–F Indirect Command File Not Found

Explanation: This message is issued when the HSC terminal server is unable to find the specified file. Indirect file support is an unsupported feature of the HSC controller.

Action: None.

TTDR–F Input Timeout

Explanation: The HSC terminal server has a timer that begins whenever any prompt is issued. After 5 minutes, the timer expires. The HSC terminal server issues the message and forces a Ctrl/Y in response to the prompt.

Action: Rerun the program that issued the prompt. Enter a response immediately after prompts are issued.

Appendix B

Exception Codes and Messages

Certain software inconsistencies can cause an exception (crash) in the HSC controller. This appendix describes all HSC controller exception codes caused by software inconsistencies. It provides a description of the exception codes, the facility or program reporting them, and the action you should take. For ease of reference, these codes are arranged in numerical order (octal radix).

To determine which exception code caused a particular crash, refer to the crash dump printed on the terminal. Note that the code number, but not the text, appears on hardcopy printouts.

If you do not find the exception code noted in the printout, the exception was caused by hardware. For such cases, save the subsystem exception dump and contact Digital Services or submit an Software Performance Report (SPR) as described in Section B.2.

The HSC controller crash dump in Example B–1 shows where to look and how to interpret the information in the crash dump.

Example B–1: Crash Dump Example

```
-*  SUBSYSTEM EXCEPTION   *-      V600           HSCxx  HSC007 (1)
         at 02-Aug-1990 00:13:34.20       up    0 00:13:34.20
User (2)  Pc: 000002 caused by (20      ) IOT (3)
PSW:  140004
CRASH (4) active, PCB addr = 036322
R0-R5:
000000    126104   000000   000000   000000   000000
Kernel SP: 000774
Kernel Stack:
017214 (5) 016334   007410   077406   077406   077406  077406   077406
077406    077406   100016   077506   077506   077406  077406   077406
Supervisor SP: 000650 (6)
Supervisor Stack:
052525 (7) 052525   025252   025252   025252   025252   025252   025252
025252   025252   025252   025252   025252   025252   025252   025252
User SP: 000250
User Stack:
005000 (8) 000110   010001   104064   000000   000520  000000   000000
000000    000000   000000   000000   000000   000000  000000   000000
KPAR(0-7):
(9)
    .
    .
    .
Status of requestors(1-9):
000001 (10) 000206   000205   000205   000205   000205  000205   000205
(PC-6) to (PC):
NXM    003407   000004   046534
Booting..
```

(1) This line calls out a crash and indicates the HSCxx is at software version number V600. The last field is the assigned node name (set with SET NAME).

(2) This line indicates the processor mode in which the crash occurred. This can be either Kernel or User.

(3) This three-letter mnemonic indicates the type of crash. The example mnemonic IOT indicates that this is a software inconsistency. Any other combination of letters, such as NXM (nonexistent memory) would designate a crash outside the scope of this appendix.

Such exceptions require further analysis by Digital Services.

4. The initial name on this line identifies the process active at the time of the crash. It is valid only during user-mode crashes. Use this name as a crosscheck when looking up the crash description.
5. If the mode notation is Kernel, check the first word of the Kernel Stack for the crash code.
6. If the HSC controller has an M.cache module installed, the crash dump will contain a Supervisor SP and a Supervisor Stack dump. This information does not appear on HSC controllers that do not have an operational M.cache module installed.
7. If the mode notation is Superv, check the first word of the Supervisor Stack for the crash code.
8. Because the mode notation in this example indicated User, check the User Stack for the crash code number. This code is always the first word of the stack (in this case, 005000).
9. The following ellipsis replaces other unnecessary stack dump information.
10. This line denotes the identity and status of each requestor. See Table B–1 for a listing of normal status codes for a requestor, and refer to the *HSC Controller Service Manual* for a listing of the crash status codes for requestors.

Table B–1: Normal Operation Status Codes for K-Requestors

Status Code (Octal)	Description
001	K.ci host interface
002	K.sdi disk data channel module
004	K.si data channel module with no microcode loaded
007	8-port K.si data channel module with microcode loaded
010	K.ci2 host interface with no microcode loaded
076	Secondary P.io module
203	K.sti tape data channel module
205	4-port K.si data channel module with disk microcode loaded
206	4-port K.si data channel module with tape microcode loaded

Table B–1 (Continued): Normal Operation Status Codes for K-Requestors

Status Code (Octal)	Description
211	K.ci2 host interface with microcode loaded
212	8-port K.si data channel module with no microcode loaded
277	P.ioc module
377	No requestor present

B.1 SINI-E Error Printout

The following SINI-E error example appears immediately upon reboot after a subsystem exception. Information contained in this error message is a condensation of the crash dump information.

Example B–2: SINI-E Exception Code

```
SINI-E Seq 1. at 17-Nov-1858 00:00:02.00, Out-of band 000602 ❶
        Software inconsistency ❷
        Process CRASH  ❸
        PC  000002
        PSW 140004
        Stack dump:  005000  000110  010001
```

❶ The out-of-band message number is used for troubleshooting.

❷ This line defines the cause of the crash.

❸ This line and the following three lines duplicate the applicable information in the crash dump.

B.2 Submitting a Software Performance Report

Some of the exception messages listed in this appendix suggest submitting a Software Performance Report (SPR) with a copy of the crash dump. Before submitting the SPR, contact the Customer Support Center or your local field office to find out if additional information will be needed. Submit an SPR only after eliminating other possibilities, such as hardware-related problems.

When you submit an SPR, check the appropriate exception code in this appendix for information needed to analyze the crash. Include all the requested information with the SPR.

B.3 Exception Messages

In each of the exception messages, **Facility:** indicates the process(es) running at the time the crash occurred. The first name listed is the major process. The second name is the module of the process that generated the exception. This module may be a subprocess of the main process or simply a different code module. Include the crash dump message and any other applicable hardcopy information with an Software Performance Report (SPR) submission.

001002 ($CPUM1)
Previous mode not user

Facility: EXEC, EXEC

Explanation: During a context switch of user processes, the previous mode (as indicated by the program status word (PSW)) was not user mode.

Action: Submit an SPR with the crash dump.

001003 ($CEXPCB)
EXEC PCB was scheduled

Facility: EXEC, EXEC

Explanation: During process scheduling, the EXEC process control block (PCB) was scheduled. This dummy PCB is used only for loading the process and should never be scheduled.

Action: Submit an SPR with the crash dump.

001004 ($CDEBCAC)
Cache setting in PDR is in incorrect state

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. A page descriptor register (PDR) directed to program memory does not have "disable cache" set. A PDR directed to data memory does have "disable cache" set.

Action: Submit an SPR with the crash dump.

001005 ($CPUM2)
Previous mode not user

Facility: EXEC, EXEC

Explanation: During a context switch of user processes, the previous mode, as indicated by the program status word (PSW), was not user mode.

Action: Submit an SPR with the crash dump.

001006 ($CCB4)
Spurious Interrupt from K at Control Bus Level 4

Facility: EXEC, EXEC

Explanation: One of the data channel requestor modules, or the K.ci, interrupted the P.ioc module at level four, but, upon queue examination, no elements were shown (an element should be on the level 4 interrupt queue).

Action: Save any crash dump before rebooting. Contact Digital Services or submit an SPR.

001007 ($CCB5)
Spurious Interrupt from K at Control Bus Level 5

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. One of the data channel requestor modules, or the K.ci, interrupted the P.ioc at level 5, yet, upon queue examination, no elements were shown (an element should be on the level 5 interrupt queue)

Action: Contact Digital Services or submit an SPR. Save any crash dump before rebooting.

001010 ($CDC1)
Downcount failed

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. During processing of the level 5 interrupt queue, a down count operation failed.

Action: Submit an SPR with the crash dump.

001011 ($CDC2)
Downcount failed

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. During processing of the level 5 interrupt queue, a down count operation failed.

Action: Submit an SPR with the crash dump.

001012 ($CACQ)
Acquire on Semaphore with address of 0

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. The ACQ$P system service was called with a semaphore address of 0.

Action: The process specified as active is the offender. Submit an SPR with the crash dump.

001013 ($CAML)
Acquire Multiple on Semaphore with address of 0

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. The AMLT$P system service was called with a semaphore address of 0.

Action: The process specified as active is the offender. Submit an SPR with the crash dump.

001014 ($CRLP)
Release on Semaphore with address of 0

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. The REL$P system service was called with a semaphore address of 0.

Action: The process specified as active is the offender. Submit an SPR with the crash dump.

001015 ($CRRTI)
RRTI$ on Semaphore with address of 0

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. The RRTI$P system service was called with a semaphore address of 0.

Action: The process specified as active is the offender. Submit an SPR with the crash dump.

001016 ($CRTI1)
RRTI$ found Semaphore count non-zero

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. When exiting, the RRTI$ routine found an inconsistency in a semaphore count word.

Action: The process specified as active is the offender. Submit an SPR with the crash dump.

001017 ($CRTI2)
RRTI$ found Semaphore count non-zero

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. When exiting, the RRTI$ routine found an inconsistency in a semaphore count word.

Action: The process specified as active is the offender. Submit an SPR with the crash dump.

001020 ($CRCPP)
Receive/Dequeue from Queue with address of 0

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. One of the RCV$P FROM$P or DEQ$P FROM$P system services was called with a queue head address of 0.

Action: The process specified as active is the offender. Submit an SPR with the crash dump.

001021 ($CRCCP)
Receive/Dequeue from Queue with address of 0

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. One of the RCV$C FROM$P or DEQ$C FROM$P system services was called with a queue head address of 0.

Action: The process specified as active is the offender. Submit an SPR with the crash dump.

001022 ($CRCCV)
Receive/Dequeue from Queue with address of 0

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances.

Action: The process specified as active is the offender. Submit an SPR with the crash dump.

001023 ($CRMPP)
Receive/Dequeue Maybe from Queue with address of 0

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. The RCVM$P system service was called with a queue head address of 0.

Action: The process specified as active is the offender. Submit an SPR with the crash dump.

001024 ($CRMCP)
Receive/Dequeue Maybe from Queue with address of 0

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. The RCVM$C system service was called with a queue head address of 0.

Action: The process specified as active is the offender. Submit an SPR with the crash dump.

001025 ($CRMCV)
Receive/Dequeue Maybe from Queue with address of 0

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. The RCVM$W system service was called with a queue head address of 0.

Action: The process specified as active is the offender. Submit an SPR with the crash dump.

001026 ($CRAMCV)
Receive All-Maybe from Queue with address of 0

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. One of the RCAM$C FROM$P or RCAM$C FROM$W system services was called with a queue head address of 0.

Action: The process specified as active is the offender. Submit an SPR with the crash dump.

001027 ($CSPP)
Send/Enqueue to Queue with address of 0

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. One of the SEND$P TO$P or ENQ$P TO$P system services was called with a queue head address of 0.

Action: The process specified as active is the offender. Submit an SPR with the crash dump.

001030 ($CSCP)
Send/EnQueue to Queue with address of 0

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. One of the SEND$C TO$P or ENQ$C TO$P system services was called with a queue head address of 0.

Action: The process specified as active is the offender. Submit an SPR with the crash dump.

001031 ($CSCV)
Send/Enqueue to Queue with invalid target queue specified

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. One of the SEND$C TO$W or ENQ$C TO$W system services was called with an incorrect target queue address.

Action: The process specified as active is the offender. Submit an SPR with the crash dump.

001032 ($CSHPP)
Send/Enqueue-to-Head to Queue with address of 0

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. One of the SNDH$P TO$P or ENQH$P TO$P system services was called with a queue head address of 0.

Action: The process specified as active is the offender. Submit an SPR with the crash dump.

001033 ($CSHCP)
Send/Enqueue-to-Head to Queue with address of 0

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. One of the SNDH$C TO$P, ENQH$C TO$P, SNDH$C TO$P, or ENQH$C TO$P system services was called with a queue head address of 0.

Action: The process specified as active is the offender. Submit an SPR with the crash dump.

001034 ($CIHPP)
Insert at Head to Queue with address of 0

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. The INSH$P TO$P system service was called with a queue head address of 0.

Action: The process specified as active is the offender. Submit an SPR with the crash dump.

001035 ($CIHCP)
Insert at Head to Queue with address of 0

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. The INSH$C TO$P system service was called with a queue head address of 0.

Action: The process specified as active is the offender. Submit an SPR with the crash dump.

001036 ($CUPCV)
Up count to Counter with address of 0

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. The UPC$ system service was called with a queue head address of 0.

Action: The process specified as active is the offender. Submit an SPR with the crash dump.

001037 ($CDWCV)
Down count to Counter with address of 0

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. The DWNC$ system service was called with a queue head address of 0.

Action: The process specified as active is the offender. Submit an SPR with the crash dump.

001040 ($CSTTM)
Set Timer operation to active timer

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. The SETTM$ system service was called to set a timer that is already active.

Action: The process specified as active is the offender. Submit an SPR with the crash dump.

001041 ($CSNZ1)
Release of Semaphore with address of 0

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. During some circumstances, a semaphore will require a down count without subsequent scheduling considerations. This typically happens when a process enters hibernation or exits. During the implicit release operation, the semaphore had an address of 0.

Action: Submit an SPR with the crash dump.

001042 ($CTOVR)
Time-of-day overflowed

Facility: EXEC, EXEC

Explanation: During an update of the current time of day, the executive detected an overflow. This can happen if a node on the CI sets a false time to the HSC controller.

Action: Contact Digital Services or submit an SPR. Save the crash dump for inspection. You may reboot the HSC controller.

001043 ($CPWFL)
Power Failure

Facility: EXEC, EXEC

Explanation: The processor is still operating five seconds after a power failure indication. Therefore, CRONIC concludes that the power failure indication was false.

Action: Contact Digital Services or submit an SPR.

001201 ($CNOHIBER)
Process on Recoverable List not Hibernating

Facility: EXEC, EXECLOAD

Explanation: Before loading a utility or diagnostic, the loader examined the recoverable memory list of cached programs to determine whether or not a program might be loaded from memory instead of from the load device. When a program was found on the recoverable memory list, its state was not hibernate state. This software inconsistency should not be seen under normal circumstances.

Action: Submit an SPR with the crash dump, noting previous activity with the program requested.

001202 ($CIMAGE)
Memory extent encroaches defined area

Facility: EXEC, EXECLOAD

Explanation: The process to be loaded specified additional memory or buffer space, as specified on the loadable file header (LFHEADER) directive. When the additional memory was allocated and mapped to the process, it had encroached upon the loaded area. This exception can also indicate that the process image did not start on a 4K word boundary.

Action: Submit an SPR with the crash dump.

001203 ($CNOPROC)
No code parent process loaded

Facility: EXEC, EXECLOAD

Explanation: When a process was loaded, its PCB specified it should execute and share code associated with another process. When attempting to locate the code parent, the loader found that the parent was not loaded.

Action: Submit an SPR with the crash dump.

001204 ($CALLOCATE)
Insufficient Kernel Pool

Facility: EXEC, EXECLOAD

Explanation: When EXEC attempted to allocate either a PCB (Z.) or an address descriptor (A.) structure from kernel pool for a new process, kernel pool was inadequate to support the additional structures.

Action: Submit an SPR with the crash dump.

001205 ($CLFAO)
FAO overrun

Facility: EXEC, EXECLOAD

Explanation: The formatted ASCII output (FAO) string returned during formatting of a module version mismatch message was too large for the buffer.

Action: Submit an SPR with the crash dump. If possible, send a copy of the RX33 diskette.

001401 ($CBUSY)
Performed receive when already busy with request

Facility: EXEC, EXECRDWR

Explanation: The READ$/WRITE$ service, while in its exception routine, was already busy with one request while a RCV$P operation was performed.

Action: Submit an SPR with the crash dump.

001402 ($CNOLOADED)
Requested driver not loaded

Facility: EXEC, EXECRDWR

Explanation: A process within the HSC software specified a READ$ or WRITE$ operation with a device control block (DDCB) for a device not configured on that model. For example, a program specified a transfer for a TU58 tape drive on an HSC controller. Because the device is not configured on the system, the driver is not loaded.

Action: Submit an SPR with the crash dump, describing activity on the HSC controller at the time of the exception. The process listed as active may be the READ$/WRITE$ service, and not the process that performed the offending request.

001403 ($CDDCB)
Invalid DDCB specified

Facility: EXEC, EXECRDWR

Explanation: A request to the READ$/WRITE$ service specified a DDCB that was invalid, or it specified an invalid device type in the DD$TYPE field.

Action: Submit an SPR with the crash dump, describing activity on the HSC controller at the time of the exception. The process listed as active may be the READ$/WRITE$ service and not the process that performed the offending request.

001501
Motor not Running

Facility: EXEC, EXECRX33

Explanation: The motor was not running when the motor shutdown timer expired.

Action: Submit an SPR with the crash dump.

001502
Non-RX33 command requested

Facility: EXEC, EXECRX33

Explanation: The RX33 driver received an CRONIC transfer request (XFRB), but the XFRB specified a DDCB for a non-RX33 device.

Action: Submit an SPR with the crash dump.

001503
Invalid Unit Number

Facility: EXEC, EXECRX33

Explanation: The DDCB specified an RX33 device, but the unit requested was not 0 or 1.

Action: Submit an SPR with the crash dump.

001504
Zero byte count transfer

Facility: EXEC, EXECRX33

Explanation: A transfer was requested with a zero byte count.

Action: Submit an SPR with the crash dump.

001505
Invalid byte count

Facility: EXEC, EXECRX33

Explanation: A transfer was requested with a byte count that was not a multiple of 512 (sector size).

Action: Submit an SPR with the crash dump.

001506
Invalid internal byte count

Facility: EXEC, EXECRX33

Explanation: The remaining byte count of a partially completed transfer was not a multiple of 512. The original (requested) byte count was a multiple of 512.

Action: Submit an SPR with the crash dump.

001507
RX33 hardware registers are incorrect

Facility: EXEC, EXECRX33

Explanation: RX33 disk drive hardware signaled successful completion of an I/O operation, but the hardware registers (current sector, current track, or memory address register) did not contain the expected values.

Action: Contact Digital Services or submit an SPR.

001510
Invalid Head Select

Facility: EXEC, EXECRX33

Explanation: The software attempted to select a head other than 0 or 1.

Action: Submit an SPR with the crash dump.

001511
Memory Management

Facility: EXEC, EXECRX33

Explanation: Relocation is not enabled in the memory management hardware.

Action: Submit an SPR with the crash dump.

001512
Invalid Virtual Address

Facility: EXEC, EXECRX33

Explanation: The virtual address passed in the XFRB is not in page 4.

Action: Submit an SPR with the crash dump.

001513
Unexpected Interrupt from RX33

Facility: EXEC, EXECRX33

Explanation: An unexpected interrupt was received from the RX33 controller. This condition is not detected until a command is about to be issued; that is, the crash does not happen when the interrupt is detected.

Action: If the problem persists, submit an SPR with the crash dump.

001514
Invalid Internal Unit Number

Facility: EXEC, EXECRX33

Explanation: The unit number index value is not 0 or 2.

Action: Submit an SPR with the crash dump.

001515
Non-Existent Memory

Facility: EXEC, EXECRX33

Explanation: The RX33 controller returned an NXM error.

Action: Contact Digital Services or submit an SPR.

001601 ($CPAG1)
TYPE$ crosses page boundaries

Facility: EXEC, EXECTT

Explanation: A process requested a TYPE$ system service (or an ACPT$ service with a prompt) specifying a buffer that crosses a memory management page boundary. This is a restriction of the driver.

Action: Submit an SPR with the crash dump, describing activity at the time of the exception.

001602 ($CPAG2)
ACPT$ crosses page boundaries

Facility: EXEC, EXECTT

Explanation: A process requested an ACPT$ system service specifying a buffer that crosses a memory management page boundary. This is a restriction of the driver.

Action: Submit an SPR with the crash dump, describing activity at the time of the exception.

001603 ($CNOPCB)
PCB not found on run queue

Facility: EXEC, EXECTT

Explanation: EXEC failed to locate the PCB in the RUN queue for the process excepted by a keyboard command.

Action: Submit an SPR with the crash dump.

001701 ($CPAGE)
READ$ or WRITE$ crossed page boundary

Facility: EXEC, EXECTU58

Explanation: A request to the TU58 tape drive specified a buffer that crossed a memory management page boundary. This is a restriction of the driver.

Action: Submit an SPR with the crash dump, describing activity at the time of the exception.

002001
Exception routine invoked for unknown reason

Facility: DEMON

Explanation: DEMON's exception routine was activated, but not for Ctrl/Y, Ctrl/C, or a diagnostic timeout.

Action: Submit an SPR with the crash dump. If a certain sequence of HSC controller operations induced this crash, include a description of that sequence.

002002
Insufficient free memory to allocate a program stack

Facility: DEMON

Explanation: When DEMON was initialized, it could not allocate enough free program memory for use as a stack.

Action: Notify Digital Services.

002003
DEMON was initiated when there was no diagnostic to run

Facility: DEMON

Explanation: DEMON did a receive on its work queue and received a nondiagnostic request.

Action: Submit an SPR with the crash dump. If a certain sequence of HSC controller operations induced this crash, include a description of that sequence.

002004
Failure in periodic control or data memory test

Facility: DEMON, PRMEMY

Explanation: One of the periodic control or data memory interface tests detected a failure. Failures in these tests are fatal, and the HSC controller must reboot after displaying a message describing the failure.

Action: Notify Digital Services. Save the crash dump and the error message preceding the crash dump.

002005
Failure in periodic K.sdi or K.sti test

Facility: DEMON, PRKSDI, PRKSTI

Explanation: The periodic K.sdi/K.si or K.sti/K.si module tests detected a failure. Failures in these tests are fatal, and the HSC controller must reboot after displaying a message describing the type of error and requestor number of the failed module.

Action: Notify Digital Services. Save the crash dump and all error messages immediately preceding the crash dump.

002006
ILDISK received illegal queue address

Facility: DEMON, ILDISK

Explanation: ILDISK requested exclusive access to a drive's state area. The acquire operation should return the control memory address of the attention/available service queue for the specified drive. The address returned was zero, an illegal address for a queue.

Action: If a certain sequence of HSC controller operations induced this crash, include a description of that sequence. Also note if the problem occurs only when a particular disk drive is tested.

002007
ILDISK received illegal buffer descriptor

Facility: DEMON, ILDISK

Explanation: ILDISK received a buffer descriptor from the free buffer queue. A consistency check on the buffer descriptor failed because the descriptor indicated the buffer was not in the HSC controller's buffer memory. A software problem is the most likely cause of this crash.

Action: Submit an SPR with the crash dump. If a certain sequence of HSC controller operations induced this crash, include a description of that sequence. Also note if the problem occurs only when a particular disk drive is tested.

002010
ILDISK detected inconsistency in exception routine

Facility: DEMON, ILDISK

Explanation: ILDISK's internal flags indicated exclusive ownership of a drive's state area, but the address of the K.sdi/K.si control area was not available. When ILDISK has exclusive ownership of a drive state area, the address of the K.sdi/K.si control area should always be available. A software problem is the most likely cause of this crash.

Action: Submit an SPR with the crash dump. If a certain sequence of HSC controller operations induced this crash, include a description of that sequence. Also note if the problem occurs only when a particular disk drive is tested.

002011
An ILEXER disk I/O request failed to complete

Facility: DEMON, ILEXER

Explanation: ILEXER attempted to abort all outstanding disk I/O requests. After waiting two minutes, the program found that one or more I/O requests had not completed. The HSC controller crashes and reboots because ILEXER cannot exit with a request outstanding.

Action: Submit an SPR with the crash dump. If a certain sequence of HSC controller operations induced this crash, include a description of that sequence. Also note if the problem occurs only when a particular disk drive is tested.

002012
An ILEXER tape I/O request failed to complete

Facility: DEMON

Explanation: ILEXER attempted to abort all outstanding tape I/O requests. After waiting four minutes, the program found that one or more I/O requests had not completed. The HSC controller crashed and rebooted because ILEXER cannot exit with a request outstanding.

Action: Submit an SPR with the crash dump. If a certain sequence of HSC controller operations induced this crash, include a description of that sequence. Also note if the problem occurs only when a particular tape drive or formatter is tested.

002014
ILTAPE timed-out waiting for Drive State Area

Facility: DEMON, ILTAPE

Explanation: ILTAPE requested exclusive access to a tape formatter for testing. ILTAPE timed out because the request did not complete within 60 seconds.

Action: Submit an SPR with the crash dump. Also include a summary of any tape error messages immediately preceding the crash. If a certain sequence of HSC controller operations caused this crash, include a description of that sequence. Also note if the problem occurs only when a particular tape drive or formatter is used.

002015
ILTAPE detected inconsistency after a command failure

Facility: DEMON, ILTAPE

Explanation: ILTAPE issued a command to the HSC tape diagnostic interface, but the command failed. In the process of preparing an error message, ILTAPE found that the command opcode was an illegal or unknown value.

Action: Submit an SPR with the crash dump. Also include a summary of any tape error messages immediately preceding the crash. If a certain sequence of HSC controller operations caused this crash, include a description of that sequence. Also note if the problem occurs only when a particular tape drive or formatter is used.

002016
ILTAPE detected inconsistency while restoring a TACB

Facility: DEMON, ILTAPE

Explanation: ILTAPE could not return a tape diagnostic structure to the table of tape access control blocks (TACBs) because the table showed that no TACBs were in use.

Action: Submit an SPR with the crash dump. Also include a summary of any tape error messages immediately preceding the crash. If a certain sequence of HSC controller operations induced this crash, include a description of that sequence. Also note if the problem occurs only when a particular tape drive or formatter is used.

002017
ILTAPE detected inconsistency in exception routine

Facility: DEMON, ILTAPE

Explanation: ILTAPE's internal flags indicated exclusive ownership of a drive state area, but the address of the K.sti/K.si control area was not available. When ILTAPE has exclusive ownership of a drive state area, the address of the K.sti/K.si control area should always be available. A software problem is the most likely cause of this crash.

Action: Submit an SPR with the crash dump. If a certain sequence of HSC controller operations caused this crash, include a description of that sequence. Also note if the problem occurs only when a particular tape drive is tested.

003001
Illegal format type specified

Facility: CERF

Explanation: An illegal format type was specified in an error message to CERF.

Action: Submit an SPR with the crash dump.

003002
Output length too long

Facility: CERF

Explanation: When CERF processed an MSCP error message, the FAO output of the text string was too long for CERF's buffer.

Action: Submit an SPR with the crash dump.

003003
Output length too long

Facility: CERF

Explanation: When CERF processed an out-of-band message, the FAO output of the text string was too long for CERF's buffer.

Action: Submit an SPR with the crash dump.

004002
BMB reserved but not found

Facility: DISK, many

Explanation: A big memory buffer (BMB) was reserved through a system function but was not found when the table of BMBs was searched.

Action: Submit an SPR with the crash dump. Specify which process was running and make note of the activity on the system at the time of the crash.

004004
Invalid action byte in Connection Block

Facility: DISK, SDI

Explanation: The subprocess within the disk path that processes requests from the CI manager received a connection block with an invalid action byte.

Action: Submit an SPR with the crash dump.

004005
Datagram received from a connection

Facility: DISK, MSCP

Explanation: The main MSCP disk command server process received a nonsequenced message from some connection.

Action: Submit an SPR with the crash dump. Note all levels of host software running in the cluster.

004006
MSCP message size exceeded maximum

Facility: DISK, MSCP

Explanation: The main MSCP disk command server process received a sequenced message, with a length greater than the MSCP maximum, from some connection.

Action: Submit an SPR with the crash dump. Note all levels of host software running in the cluster.

004007
Invalid error signaled by K.ci

Facility: DISK, MSCP

Explanation: The main MSCP command server received an MSCP command packet, with invalid error bits set, from the K.ci.

Action: Submit an SPR with the crash dump. Note all levels of host software running in the cluster and the revision level of the K.ci microcode.

004010
Server queue on work queue with no items

Facility: DISK, many

Explanation: The main disk process received a subprocess work queue with no attached work items from the main work queue.

Action: Submit an SPR with the crash dump. Note the currently running process.

004011
Invalid module number

Facility: DISK, many

Explanation: The main disk process detected an invalid module number when it tried to switch to a different internal process represented by the module number.

Action: Submit an SPR with the crash dump. Note the current process running.

004013
State change to ONLINE requested via gatekeeper

Facility: DISK, SDI

Explanation: The state change processor within the sequential command gatekeeper received a DUCB extension requesting a state change to *online*. This crash indicates an improper use of the state change mechanism.

Action: Submit an SPR with the crash dump.

004014
Inconsistent drive state detected

Facility: DISK, SDI

Explanation: The state change processor within the sequential command gatekeeper received a DUCB extension containing a different state than the current state in the DUCB. This crash indicates an improper use of the state change mechanism.

Action: Submit an SPR with the crash dump.

004015
Improper state change for shadow member

Facility: DISK, SDI

Explanation: The sequential gatekeeper mechanism completes all outstanding I/O for a shadow unit before allowing a state change to take place on any of the members of the shadow set. This crash indicates the mechanism failed to operate properly.

Action: Submit an SPR with the crash dump.

004016
Disk Unit Table (DUT) inconsistency

Facility: DISK, many

Explanation: The disk server either tried to add a unit to the disk unit table (DUT) when it was already there or tried to remove a unit from the DUT that was not present. This crash indicates improper sequencing of actions to add a unit to or remove a unit from the DUT.

Action: Submit an SPR with the crash dump.

004017
Invalid diagnostic HMB

Facility: DISK, MSCP

Explanation: The diagnostic interface within the disk path received a host message block (HMB) with a nonzero length field in the HM$LOF word.

Action: Submit an SPR with the crash dump. List any HSC utilities or diagnostics running at the time of the crash.

004021
Diagnostic release of disk unit while disk is online

Facility: DISK, MSCP

Explanation: A diagnostic or utility attempted to release a disk unit while the disk unit was still in the online state. HSC diagnostics and utilities must put the drive in the available state before releasing the unit for general use.

Action: Submit an SPR with the crash dump. Specify any HSC utilities or diagnostics running at the time of the crash.

004025
Invalid error recovery attempted on K.ci detected error

Facility: DISK, ERROR

Explanation: The disk server began error processing on an error detected by K.ci; however, the error recovery actions for that error were invalid.

Action: If this crash occurs immediately after a boot, try rebooting with a backup copy of the HSC software. Otherwise, submit an SPR with the crash dump.

004026
Invalid error recovery attempted on K.sdi/K.si detected error

Facility: DISK, ERROR

Explanation: The disk server began error processing on an error detected by a K.sdi/K.si; however, the error recovery actions taken by the disk server for that error were invalid.

Action: If this crash occurs immediately after a boot, try rebooting with a backup copy of the HSC software. Otherwise, submit an SPR with the crash dump.

004027
Invalid disk characteristics for operation

Facility: DISK, ERROR

Explanation: An arithmetic operation to compute some disk parameter caused an overflow or produced a result outside the allowed range. It is also possible, though unlikely, that a disk is supplying invalid characteristics to the HSC controller.

Action: If possible, get the number of the requestor involved from the last error log printed on the console or from the system error log. Contact Digital Services. If no disk or K.sdi/K.si hardware problem exists, submit an SPR with the crash dump.

004030
S bit not set in Fragment Request Block error state

Facility: DISK, ERROR

Explanation: The S bit in the K control area port subarea for a drive in fragment request block (FRB) error state was not set as expected.

Action: Contact Digital Services or submit an SPR with the crash dump.

004031
DT$ERQ not zero in Fragment Request Block error state

Facility: DISK, ERROR

Explanation: The FRB error queue in the Disk Rotational Access Table (DRAT) being processed by error recovery was not zero as expected upon returning from retrying a transfer in FRB error state.

Action: If possible, get the number of the requestor involved from the last error log printed on the console or from the system error log. Contact Digital Services or submit an SPR with the crash dump.

004032
Unable to get to Fragment Request Block error state

Facility: DISK, ERROR

Explanation: Error recovery was unable to place a disk port in the FRB error state to perform an error recovery operation.

Action: Reboot the HSC controller. If this error persists, submit an SPR with the crash dump.

004033
Non-ECC/EDC errors remaining after ECC correction

Facility: DISK, ERROR

Explanation: ECC error correction should take place after all other errors, except EDC, have been corrected. This crash occurs because other error indicators are set after ECC correction takes place.

Action: Submit an SPR with the crash dump.

004034
Level B error recovery retry in wrong state

Facility: DISK, ERROR

Explanation: A level B error recovery retry operation was attempted without the drive port being in FRB error state.

Action: Submit an SPR with the crash dump.

004035
Level C error recovery retry in wrong state

Facility: DISK, ERROR

Explanation: A level C error recovery retry operation was attempted without the drive port being in FRB error state.

Action: Submit an SPR with the crash dump.

004036
Dialog Control Block state is busy with empty Dialog Control Block queue

Facility: DISK, ERROR

Explanation: The drive state indicator in the K control area indicates a K.sdi/K.si module is processing a dialog control block (DCB), but the DCB queue is empty. This could possibly indicate a malfunctioning K.sdi/K.si.

Action: Contact Digital Services. If possible, get the number of the requestor involved from the last error log. If no hardware problem exists, submit an SPR with the crash dump. Note all K.sdi/K.si microcode revisions.

004037
Invalid error queue address in route

Facility: DISK, ERROR

Explanation: When the disk server attempted to route an FRB to an error queue, the error queue address in the route descriptor was invalid.

Action: Submit an SPR with the crash dump.

004040
Undefined error bit in error word

Facility: DISK, ERROR

Explanation: The error recovery routine IDENTIFY found an undefined bit in the error word stored by either a K.sdi/K.si module or K.ci module.

Action: If possible, get the number of the requestor involved from the last error log printed on the console or from the system error log. Contact Digital Services. If no hardware problem exists, submit an SPR with the crash dump.

004041
No buffer found in Fragment Request Block when expected

Facility: DISK, ERROR

Explanation: The error recovery routine MAPBUF expected to map a buffer but found the buffer address to be zero.

Action: Submit an SPR with the crash dump.

004042
Fragment Request Block not in error state for level D I/O operation

Facility: DISK, ERROR

Explanation: A call to the error recovery subroutine LVLDIO was made without the port being in FRB error state.

Action: Submit an SPR with the crash dump.

004043
Stack too deep to save in thread block

Facility: DISK, ERROR

Explanation: A call to the error recovery subroutine LVLDIO was made with too many items on the stack to save in a thread block.

Action: Submit an SPR with the crash dump.

004044
Buffer not found for specified error

Facility: DISK, ERROR

Explanation: A call to the error recovery subroutine RCDHMX specified a buffer that was not in the list of buffers for the specified FRB.

Action: Submit an SPR with the crash dump.

004046
DRAT not found for Fragment Request Block retirement

Facility: DISK, ERROR

Explanation: While attempting to retire an FRB by simulating route completion, the error recovery subroutine RETIRE could not locate the associated DRAT.

Action: If possible, get the number of the requestor involved from the last error log printed on the console or from the system error log. Contact Digital Services or submit an SPR. Note the K.sdi/K.si microcode revision levels.

004050
DRAT queue not empty for shadow copy

Facility: DISK, MSCP

Explanation: After obtaining exclusive use of a drive, the shadow copy code found that the DRAT queue for the drive was not empty.

Action: Submit an SPR with the crash dump.

004051
Inconsistent result for repair operation

Facility: DISK, MSCP

Explanation: An impossible combination of results was found at the end of a shadow repair operation.

Action: Submit an SPR with the crash dump.

004052
Known drive not found in the Disk Unit Table (DUT)

Facility: DISK, MSCP

Explanation: When the disk server attempted to remove a known disk unit from the DUT, the unit was not found in that table.

Action: Submit an SPR with the crash dump. Note any utilities or diagnostics running at the time of the crash.

004055
Attempt to enable drive interrupt that is already enabled

Facility: DISK, many

Explanation: The ARM subroutine was called to enable the K.sdi/K.si to interrupt the disk server for certain drive state changes; however, interrupts were already enabled.

Action: Submit an SPR with the crash dump. Note the process running at the time of the crash.

004056
Attempt to enable drive interrupt when previous state change is pending

Facility: DISK, many

Explanation: The ARM subroutine was called to enable the K.sdi/K.si to interrupt the disk server for drive state changes; however, a drive state change was being processed.

Action: Submit an SPR with the crash dump. Note the process running at the time of the crash.

004057
Invalid drive state change requested

Facility: DISK, many

Explanation: The SCHSQM subroutine was called to schedule a state change operation for a drive that has been declared inoperative but whose state is still recorded as available.

Action: Submit an SPR with the crash dump. Note the process running at the time of the crash.

004070
Nonzero status for SUCCESSful Dialog Control Block

Facility: DISK, SDI

Explanation: Although a DCB (SDI command) completed with a status of SUCCESS, either the DCB error word indicated an error, or the SDI response opcode was invalid.

Action: If possible, get the number of the requestor involved from the last error log printed on the console or from the system error log.

Contact Digital Services. If no K.sdi/K.si hardware problem exists, submit an SPR with a crash dump. Note all K.sdi/K.si microcode revision levels.

004072
Dialog Control Block state is busy with empty Dialog Control Block queue

Facility: DISK, many

Explanation: The drive state indicator in the K control area indicates a DCB is being processed by the K.sdi/K.si module, but the DCB queue is empty.

Action: If possible, get the number of the requestor involved from the last error log printed on the console or from the system error log. Contact Digital Services or submit an SPR. Note all K.sdi/K.si microcode revision levels.

004073
K.sdi is not responding

Facility: DISK, SDI

Explanation: A K.sdi/K.si module failed to process an immediate DCB within a preset time. The lower byte of the second word on the stack is the failing requestor number.

Action: If possible, get the number of the requestor involved from the system error log. If the error persists, it is likely that the associated K.sdi/K.si is broken. Contact Digital Services.

004076
Wrong Port State for Dialog Control Block (DCB)

Facility: DISK, SDI

Explanation: Either the SDI interface was in use when not expected, the "process DCB" bit was not set when expected to be set, or the SDI interface received an error DCB when the disk port was not in DCB error state.

Action: Submit an SPR with the crash dump.

004100
No thread block for operation

Facility: DISK, SDI

Explanation: A thread block was not available to the SDI interface in order to suspend the current process.

Action: Submit an SPR with the crash dump.

004101
Stack too deep to suspend process in thread block

Facility: DISK, SDI

Explanation: The DCBWAIT routine was called with too many words on the stack to suspend the process in a thread block.

Action: Submit an SPR with the crash dump.

004106
DRAT allocation failure

Facility: DISK, many

Explanation: There was not enough free control memory to allocate a DRAT for a specific drive type.

Action: Submit an SPR with the crash dump.

004107
A command did not complete after the drive was declared inoperative

Facility: DISK, MSCX

Explanation: Since no progress was made on executing a command after receiving several MSCP GET COMMAND STATUS commands to trace its progress, the drive was declared inoperative in an attempt to complete the command. The outstanding command however, still failed to complete within an additional timeout period.

Action: Submit an SPR with the crash dump. Note the drive type of the drive identified in the error message and any errors reported by the disk server prior to the crash.

004110
Get Command Status processing overflow

Facility: DISK, MSCX

Explanation: Processing of the MSCP GET COMMAND STATUS command determined that the calculated status will result in an overflow.

Action: Submit an SPR with the crash dump.

004111
A timer's link field values are inconsistent with its current operational state

Facility: DISK, many

Explanation: A timer was in a state that prevented adding or removing it from an active list.

Action: Submit an SPR with the crash dump.

004112
Inconsistent shadow member state detected

Facility: DISK, many

Explanation: A unit is incorrectly marked as a member of a shadow set, or the shadow unit links are inconsistent given the current state of the shadow unit.

Action: Submit an SPR with the crash dump.

004113
NO DRAT list is invalid

Facility: DISK, many

Explanation: The NO DRAT list was found to be invalid when declaring a drive inoperative.

Action: Submit an SPR with the crash dump.

004114
Connection closed after delay in attention processing

Facility: DISK, AVLATT

Explanation: While the disk server was waiting to acquire resources to send an attention message to the host, the associated disk connection closed.

Action: Submit an SPR with the crash dump.

004115
DCB address inconsistency

Facility: DISK, SDI

Explanation: While processing an error on a seek DCB, the current seek DCB address was inconsistent with the DCB address stored in the DRAT.

Action: Submit an SPR with the crash dump.

004116
Bad error completion queue in Dialog Control Block

Facility: DISK, MSCP

Explanation: An invalid error completion queue was found in the DCB when it was being set up for a seek operation.

Action: Submit an SPR with the crash dump.

004117
No DRAT was found on the K.sdi DRAT list when expected

Facility: DISK, many

Explanation: The DRAT list was empty when the disk server expected to find a DRAT queued to the K.sdi/K.si DRAT list.

Action: Submit an SPR with the crash dump.

004120
Too many DRATs in use during an enhanced ESE transfer operation

Facility: DISK, MSCP

Explanation: The number of DRATs in use for a transfer to an ESE in the enhanced mode of operation has exceeded the maximum value allowed.

Action: Submit an SPR with the crash dump.

004121
Replacement Block Number (RBN) access during an ESE enhanced mode transfer

Facility: DISK, MSCP

Explanation: The disk server is preparing to perform an enhanced performance mode transfer operation to an RBN on an ESE, but the ESE has no RBNs.

Action: Submit an SPR with the crash dump.

004122
Invalid DRAT bit set for ESE in enhanced performance mode of operation

Facility: DISK, MSCP

Explanation: A DRAT on the K.si DRAT list did not have the "Set D-bit on completion" flag set as expected.

Action: Submit an SPR with the crash dump.

004123
DCB K.si list inconsistency for ESE in enhanced mode of operation

Facility: DISK, many

Explanation: More than one nonseek DCB was queued to the K.si DCB work queue during I/O rundown on an ESE in enhanced mode of operation. Only one nonseek DCB is expected to be active at a time while running in enhanced mode.

Action: Submit an SPR with the crash dump.

004124
Buffer count inconsistency for ESE in enhanced mode of operation

Facility: DISK, MSCP

Explanation: During ESE enhanced mode transfer processing, the DRAT buffer count indicated that the DRAT was full. However, the "DRAT full" flag was not set.

Action: Submit an SPR with the crash dump.

004125
Too many disk ports

Facility: DISK (LOADER)

Explanation: You have connected more disk ports to the HSC controller than the disk server can support.

Action: Refer to the configuration guidelines for the HSC. If the HSC is configured properly, contact Digital Services.

004126
Invalid fragmentation loop count while fragmenting a transfer

Facility: DISK, MSCP

Explanation: When breaking down a transfer command into smaller fragments, a disk server count indicates that there are more FRBs to be initialized; however, the pointer to these FRBs is zero.

Action: Submit an SPR with the crash dump. If the problem is reproducible, note conditions and configurations under which problem occurs.

004127
Invalid deferred seek queue

Facility: DISK, MSCP

Explanation: The disk server, in trying to queue a new master FRB to the deferred seek queue, has discovered that the list is corrupt.

Action: Submit an SPR with the crash dump. If the problem is reproducible, note conditions and configurations under which problem occurs.

004130
No buffer descriptor for primary revectored block

Facility: DISK, ERROR

Explanation: When trying to save the buffer descriptor associated with a primary revectored block, the HSC software disk server has discovered that the buffer descriptor pointer is zero.

Action: Submit an SPR with the crash dump. If the problem is reproducible, note conditions and configurations under which problem occurs.

004131
Invalid return searching for outstanding command

Facility: DISK, MSCX

Explanation: The HSC software disk server received an MSCP GET COMMAND STATUS command from a host node and called a routine to search for the outstanding command. This routine returns to a location based on where the outstanding command is found. In this case, the return was invalid.

Action: Submit an SPR with the crash dump. If the problem is reproducible, note conditions and configurations under which the problem occurs.

004132
Active Disk Rotational Access Table on port for which format operation is scheduled

Facility: DISK, MSCP

Explanation: The disk server received a request to do a format operation on a particular port; however, the port is already processing a DRAT.

Action: Submit an SPR with the crash dump. If the problem is reproducible, note conditions and configurations under which the problem occurs.

004133
FRB in error recovery is not identified

Facility: DISK,ERROR

Explanation: When the HSC software disk server places a fragment request block (FRB) in the error recovery state, it stores the location of that FRB. This error occurs when the stored value of that location is found to be zero while the drive is in an FRB error recovery state.

Action: Submit an SPR with the crash dump.

005000
User-Invoked CRASH

Facility: CRASH

Explanation: The user entered the CRASH command at the HSC> prompt.

Action: If this crash occurred due to a reason other than entering the CRASH command, submit an SPR with the crash dump. Otherwise, no action is necessary.

005001
ECC self-diagnostic string too big for FAO

Facility: ECC

Explanation: A self-diagnostic string generated for the ECC process was too big to print with the allocated formatted ASCII output (FAO) buffer.

Action: Submit an SPR with the crash dump.

005002
No ECC errors to correct

Facility: ECC

Explanation: An FRB without any errors was sent to the error correction code (ECC) process.

Action: Submit an SPR with the crash dump.

005003
Cannot allocate Extended Function Control Block to print self–diagnostic messages

Facility: ECC

Explanation: The ECC process failed to allocate an extended function request block (XFRB) for printing messages during self-diagnostics.

Action: Submit an SPR with the crash dump.

005004
ECC found more than a 10-bit symbol error

Facility: ECC

Explanation: The ECC process received a buffer containing more than a 10-bit symbol error. Error recovery processing should never pass on such a buffer.

Action: Submit an SPR with the crash dump.

006000
This class of crashes is for tape path software inconsistency errors

Facility: TAPE, TFxxxx

Explanation: A software inconsistency error occurred.

Action: Submit an SPR with the crash dump. Specify the utilities or diagnostics active at the time of the crash.

006001
An STI GET LINE STATUS failed

Facility: TAPE, TFATNAVL

Explanation: When issued to the tape data channel, the standard tape interconnect (STI) command GET LINE STATUS returned with a failure. This command should not fail when issued to a working tape data channel.

Action: Contact Digital Services or submit an SPR.

006003
Received an illegal Connection Block (CB) from the CIMGR

Facility: TAPE, TFCI

Explanation: A connection block (CB) with an illegal opcode was sent to the tape server.

Action: Submit an SPR with the crash dump.

006004
An illegal diagnostic Opcode was received

Facility: TAPE, TFDIAG

Explanation: A diagnostic HMB with an illegal opcode was sent to the tape diagnostic interface.

Action: Submit an SPR with the crash dump. Specify the utilities or diagnostics active at the time of the crash.

006005
Diagnostics trying to acquire assigned drive state area

Facility: TAPE, TFDIAG

Explanation: Diagnostics are trying to acquire the previously assigned drive state area.

Action: Submit an SPR with the crash dump. Specify the diagnostics or utilities active at the time of the crash.

006006
Inconsistencies during drive state area acquisition

Facility: TAPE, TFDIAG

Explanation: The software context word KT$SFW is not equal to the tape formatter control block (TFCB) address and/or the DIALOG list head is nonzero when diagnostics are trying to acquire the drive state area.

Action: Submit an SPR with the crash dump. Indicate the utilities or diagnostics active at the time of the crash.

006007

No Block Header buffer supplied by BACKUP

Facility: TAPE, TFDIAG

Explanation: BACKUP did not supply the initial block header buffer descriptor.

Action: Submit an SPR with the crash dump. Include details of the backup operation.

006010

No buffers supplied by the disk server for an HSC backup operation, yet the status was successful

Facility: TAPE, TFDIAG

Explanation: No disk data block buffers were supplied in the HMB for the backup operation yet the status was successful. General Register 3 points to the windowed control memory address of the HMB in question. General Register 0 should point to the buffer descriptor list for the backup operation.

Action: Submit an SPR with the crash dump. Include details of the BACKUP operation.

006011

Could not allocate an XFRB

Facility: TAPE, TFLIB

Explanation: The tape server could not allocate an extended function control block (XFRB) through ALOCB, a CRONIC system service.

Action: Submit an SPR with the crash dump.

006012

Required CIMGR functionality not yet implemented

Facility: TAPE, TFMSCP

Explanation: The host sent the tape server a command packet with an opcode that was not a sequenced message.

Action: Submit an SPR with the crash dump. Indicate the host software version.

006013
Required CIMGR functionality not yet implemented

Facility: TAPE, TFMSCP

Explanation: The tape server received a host command packet longer than allowed (36 bytes).

Action: Submit an SPR with the crash dump. Indicate the host software version.

006014
Required CIMGR functionality not yet implemented

Facility: TAPE, TFMSCP

Explanation: The tape server received a host command packet with a status that is currently illegal.

Action: Contact Digital Services or submit an SPR.

006015
Could not find correct Tape Drive Control Block (TDCB) pointer

Facility: TAPE, TFSEQUEN

Explanation: A call to remove a host's access to a drive resulted in the tape server searching the current chain of tape drive control blocks (TDCBs) in that host's HCB. Inability to find the correct TDCB pointer resulted in this crash.

Action: Submit an SPR with the crash dump.

006016
Unable to allocate an HDB

Facility: TAPE, TFSEQUEN

Explanation: The tape server's attempt to add a host access, which requires allocation of a host drive block (HDB), failed for lack of resources.

Action: Submit an SPR with the crash dump.

006017
Tape formatter does not support chosen density

Facility: TAPE, TFSEQUEN

Explanation: The tape formatter does not support a density that the HSC controller supports. General Register 4 points to the TDCB for the drive in question.

Action: Submit an SPR with the crash dump. Include the host software version and tape formatter revision.

006020
An invalid density is set in the Tape Drive Control Block (TDCB)

Facility: TAPE, TFSEQUEN

Explanation: An invalid density was set in the TDCB.

Action: Submit an SPR with the crash dump.

006021
Read-reverse emulation not flagged

Facility: TAPE, TFSEQUEN

Explanation: The tape server entered the read-reverse emulation code without read-reverse emulation being flagged.

Action: Submit an SPR with the crash dump.

006022
Route pointer for read-reverse emulation zero

Facility: TAPE, TFSEQUEN

Explanation: The tape server entered the read-reverse emulation code with a record data truncated error without having the route pointer set in the HMB.

Action: Submit an SPR with the crash dump.

006023
Requested transfer larger than 64 Kb

Facility: TAPE, TFSEQUEN

Explanation: The requested transfer size for a read reverse is larger than 64 kilobytes.

Action: Submit an SPR with the crash dump.

006024
Read-reverse emulation not flagged

Facility: TAPE, TFSEQUEN

Explanation: The tape server entered the read-reverse emulation short retry code without read-reverse emulation being flagged. Read-reverse emulation is flagged in the TDCB at offset TD.FLAGS bit TDF.RREVEM.

Action: Submit an SPR with the crash dump.

006025
Read-reverse emulation not flagged

Facility: TAPE, TFSEQUEN

Explanation: The tape server entered the read-reverse emulation long retry code without read-reverse emulation being flagged.

Action: Submit an SPR with the crash dump.

006026
KT$SEM is less than or equal to zero

Facility: TAPE, TFSEQUEN

Explanation: The K control area offset KT$SEM is zero.

Action: Submit an SPR with the crash dump.

006031
No available stacks

Facility: TAPE, TFSERVER

Explanation: There are no available stacks for a process trying to suspend.

Action: Submit an SPR with the crash dump.

006033
Top of user stack for a resume is not set to server return

Facility: TAPE, TFSERVER

Explanation: The top of the user stack on a process resume is not set to the server return routine.

Action: Submit an SPR with the crash dump.

006035
Hit end of subprocess list

Facility: TAPE, TFSERVER

Explanation: The tape server scheduler hit the end of its work list, but it should never reach the end of this list.

Action: Call Digital Services or submit an SPR with the crash dump.

006037
Trying to Queue a DCB to the K.sti when it is blocked for error

Facility: TAPE, TFST1

Explanation: The tape server is trying to queue a command to the head of the K.sti Dialog Queue while the requestor is blocked for error. This error condition must be cleared before inserting commands to the head of this queue.

006041
A Get Line Status DCB operation timed out

Facility: TAPE, TFSTI

Explanation: A Get Line Status DCB timed out after two minutes. Since this DCB is only issued to the requestor and not the formatter it should complete right away.

Action: If it does not, call Digital Services or submit an SPR.

006043
Buffer descriptor address missing

Facility: TAPE, TXREVERSE

Explanation: The next address is missing from the linked list of buffer descriptors in an FRB.

Action: Submit an SPR with the crash dump.

006044
Unexpected Fragment Request Block (FRB) error received

Facility: TAPE, TFERR

Explanation: The tape server received an error from a software station rather than a hardware station.

Action: Submit an SPR with the crash dump.

006045
Unknown Fragment Request Block (FRB) error received

Facility: TAPE, TFERR

Explanation: An unidentifiable error is flagged in a FRB.

Action: Submit an SPR with the crash dump.

006046
K.ci did not return a Fragment Request Block (FRB)

Facility: TAPE, TFERR

Explanation: Transfer request blocks (TRBs) have associated FRBs that point to data buffers. When a TRB is received in error, the FRBs must be deallocated. If an FRB is held by K.ci and not returned within 20 seconds, this crash occurs.

Action: Call Digital Services or submit an SPR.

006047
Invalid down count occurred on a Host Message Block (HMB) chain

Facility: TAPE, TFERR

Explanation: In the process of *catching* HMBs in order to restart them as part of TRB error recovery, an invalid down count operation takes place.

Action: Submit an SPR with the crash dump.

006050
A software inconsistency was found while purging TRB's

Facility: TAPE, TFERR

Explanation: While purging TRBs, consistency checks are done on the sequence numbers of all the TRBs being removed. The dependencies on associated DCBs are checked as well. The associated DCB for a TRB about to be removed wasn't found so this inconsistency error occurs.

Action: Submit an SPR with the crash dump.

006052
No free control blocks available to re-transfer

Facility: TAPE, TFERR

Explanation: An attempt to collect free control blocks (FCBs) during transfer error recovery has failed after waiting the timeout period for a free FCB.

Action: Submit an SPR with the crash dump.

006054
Unable to locate a FCB

Facility: TAPE, TFSEQUEN

Explanation: The tape server attempted to bring a drive online, but the attempt failed because of lack of resources.

Action: Call Digital Services or submit an SPR with the crash dump.

006056
Out of timer pool

Facility: TAPE, TFSEQUEN

Explanation: The tape server attempted to initiate a rewind, but failed due to lack of timer pool.

Action: Call Digital Services or submit an SPR with the crash dump.

006060
Invalid record size supplied by Backup

Facility: TAPE, TFDIAG

Explanation: HSC BACKUP supplied an invalid record size; 8, 16, and 32 kilobytes are the only record sizes supported.

Action: Call Digital Services or submit an SPR with the crash dump.

006075
Reserved DCB resource is zero

Facility: TAPE, TFSTI

Explanation: A software inconsistency occurred where an internal resource for a DCB was zero.

Action: Submit an SPR with the crash dump.

006076
Reserved DCB resource is zero

Facility: TAPE, TFSTI

Explanation: A software inconsistency occurred where an internal resource for a DCB was zero.

Action: Submit an SPR with the crash dump.

007000
This class of crashes includes CIMGR software consistency errors

Facility: CIMGR, many

Explanation: This message indicates the existence of a software consistency error.

Action: Submit an SPR with the crash dump. Specify the utilities or diagnostics active at the time of the crash.

007001
Received a sequence message without a credit

Facility: CIMGR, CIDIRECT

Explanation: The SCS$DIRECT process received a sequence message in a host message block (HMB) flagged by the K.ci as not having a credit for the connection. General Register 1 has the address of the HMB in error.

Action: Submit an SPR with the crash dump. Include the HMB.

007002
Failed to acquire a control block from K.ci

Facility: CIMGR

Explanation: The POLLER process could not obtain a control block from the K.ci to resend a timed-out STACK datagram.

Action: Call Digital Services or submit an SPR.

007003
K.ci is hung

Facility: CIMGR

Explanation: During the polling interval (60 seconds), the CIMGR ensures K.ci is still running. This trap indicates it is not.

Action: Contact Digital Services or submit an SPR.

007004
K.ci detected an unrecoverable error and stopped

Facility: CIMGR

Explanation: K.ci sent its control area to the CIMGR exception process. K.ci does this whenever it detects a nonrecoverable hardware error.

Action: Contact Digital Services or submit an SPR.

007005
K.ci path status check failed

Facility: CIMGR

Explanation: K.ci did not respond to a path status check within 30 seconds.

Action: If no hardware problem exists, submit an SPR with the crash dump.

007006
System name is corrupted

Facility: CIMGR

Explanation: During initialization, the CIMGR discovered the system name in the SCT was corrupted.

Action: Release the Online switch (out) on the HSC controller. Reboot the HSC controller by holding the Fault switch in until the State indicator blinks. This will bypass using the SCT on the boot device. Run SETSHO to reset the system name and ID, then reboot the HSC again before pushing in the Online switch on the front panel.

007007
HMB received with wrong number of BMB

Facility: CIMGR

Explanation: CIMGR received an HMB with the wrong number of BMBs, or CIMGR detected an inconsistent state.

Action: Contact Digital Services or submit an SPR.

007011
Connection incarnation inconsistent

Facility: CIMGR

Explanation: While a connection is in the process of opening, the incarnation of that connection is flagged as formative. The final step of opening the connection is to remove the flag. This crash indicates the flag was prematurely removed, indicating a state inconsistency for the connection.

Action: Submit an SPR with the crash dump.

007012
Connection incarnation mismatch

Facility: CIMGR

Explanation: The incarnation of an opening connection is kept in both the connection block (CB) and the connection block vector table. As a connection opens, a check is made to ensure these incarnations agree. A disagreement indicates a dangling reference to an old incarnation of the connection.

Action: Submit an SPR with the crash dump.

007013
Inconsistent connection state due to a VC closure

Facility: CIMGR

Explanation: CIMGR attempted an illegal state transition on a connection. The state transition was initiated by a virtual circuit (VC) closure. General Register 2 points to the CB.

Action: Submit an SPR with the crash dump. Include the CB.

007014
Unable to retrieve resource from K.ci during a disconnect

Facility: CIMGR

Explanation: During a disconnect, the CIMGR was unable to retrieve the resources from the K.ci associated with the credits on that connection.

Action: Submit an SPR with the crash dump.

007015
K.ci did not respond to notification of a VC closure

Facility: CIMGR

Explanation: The K.ci did not respond to notification of a VC closure within the 30-second time limit.

Action: Contact Digital Services or submit an SPR.

007016
Illegal connection state

Facility: CIMGR

Explanation: CIMGR detected an illegal CB state.

Action: Submit an SPR with the crash dump.

007017
Attempt to deallocate a Connection Block without an incarnation

Facility: CIMGR

Explanation: A CB did not have a valid incarnation at the time it was deallocated.

Action: Submit an SPR with the crash dump.

007020
Failure to retrieve SCS resources from K.ci

Facility: CIMGR

Explanation: When CIMGR tried to allocate resources for use across a virtual circuit, the count of data memory resources was incorrect. The HMB for serializing VC traffic must have two BMBs.

Action: Submit an SPR with the crash dump.

007021
The count of waiters for virtual circuit resources went negative

Facility: CIMGR

Explanation: While processing the list of waiters for virtual circuit transmission resources, CIMGR detected a nonempty list to indicate a negative number of waiters.

Action: Submit an SPR with the crash dump.

007022
Invalid BMB address

Facility: CIMGR

Explanation: An HMB arrived at the resource collector with an invalid BMB address attached to it.

Action: Enter the SHOW REQUESTORS command to view the K.pli microcode revision level. If it is less than revision 45, contact your Digital Services representative for the update. Otherwise submit an SPR with the crash dump and note the disk configuration.

007023
SCS buffer retrieval failure

Facility: CIMGR, CISUBRS

Explanation: Attempt to retrieve SCS buffer failed when SB$SBS indicated it was available.

Action: Submit an SPR with the crash dump.

007024
I/O Rundown did not complete 10 minutes after virtual circuit closure

Facility: CIMGR

Explanation: After closing a VC, the CIMGR starts a ten minute timer to allow servers to complete I/O rundown. If the timer expires, the CIMGR crashes the HSC to make it possible to reestablish all VCs. because the previously established connections were not closed, a virtual circuit could not be reopened.

Action: Submit an SPR with the crash dump.

07025
Unable to obtain an HMB structure to send a START datagram to host to close VC

Facility: CIMGR, CISUBRS

Explanation: When the HSC controller needs to close a virtual circuit, the CIMGR module issues a START datagram. If the CIMGR is unable to obtain an HMB after thirty tries at one-second intervals, this exception is issued.

Action: Submit an SPR with the crash dump and console log. Note if the problem occurred under heavy load.

07026
Unable to obtain a BMB structure to send a START datagram to host to close VC

Facility: CIMGR, CISUBRS

Explanation: When the HSC controller needs to close a virtual circuit, the CIMGR module issues a START datagram. If the CIMGR is unable to obtain a BMB after thirty tries at one-second intervals, this exception is issued.

Action: Submit an SPR with the crash dump and console log. Note if the problem occurred under heavy load.

07027
Unable to obtain a System Block when attempting to send a START datagram to host to close VC

Facility: CIMGR, CISUBRS

Explanation: When the HSC controller needs to close a virtual circuit, the CIMGR module issues a START datagram. This exception code is issued if the CIMGR is unable to obtain a system block (SB).

Action: Submit an SPR with the crash dump and console log.

007030
Possible K.ci hardware error detected after loss of all virtual circuits

Facility: CIMGR, CISUBRS

Explanation: When all virtual circuits to the HSC controller are closed, the CIMGR opens a 20-second window during which certain error conditions are monitored. If any of the error conditions occur, the HSC controller crashes. If a hardware failure exists, it will be identified during reboot of the HSC controller through display of an OCP error code.

Action: If an OCP error code is displayed during reboot, contact Digital Services. Otherwise, treat this code as a transient condition unless it becomes a frequent occurrence.

012001
Connection Block not found

Facility: DUP

Explanation: When DUP receives an HMB, DUP tries to find a reference to the connection block in the DG$ structures. DUP was unable to find a reference to the connection block.

Action: Submit an SPR with an exception dump or startup message indicating the contents of the stack.

012002
Illegal BMB count

Facility: DUP

Explanation: The HMB (MSCP packet carrier) has an illegal number of BMBs allocated. DUP allows only one BMB. Therefore, the HMB is invalid.

Action: Submit an SPR with an exception dump or startup message indicating the contents of the stack. The second word of the stack contains the windowed address of the HMB.

012003
Illegal HMB Opcode

Facility: DUP

Explanation: The opcode specified in the HM$LOF field of the HMB was not equal to HML$RM. HMB opcodes must indicate the HMB is for a sequenced message.

Action: Submit an SPR with an exception dump or startup message indicating the contents of the stack.

012004
Illegal HMB Error

Facility: DUP

Explanation: The error specified in the HM$ERR field of the HMB was not equal to 0, HME$EC, or HME$NC.

Action: Submit an SPR with an exception dump or startup message indicating the contents of the stack.

012021
Invalid Connection Block

Facility: DUP

Explanation: The DUP process received a connection block with an invalid value in the CB$ACT field. The CB$ACT field contains the action to be performed by the DUP Server.

Action: Submit an SPR with an exception dump or startup message indicating the contents of the stack.

012024
Bad Down Count

Facility: DUP

Explanation: DUP initiates a return of the endpacket to the host by down counting the reference counter in the related control block. The down count should return a one.

Action: Submit an SPR with an exception dump or startup message indicating the contents of the stack.

012036
Connection Broken

Facility: DUP

Explanation: While DUP was preparing to send a message to the K.ci, the connection to the host was broken. The connection was broken after DUP did an extensive check to ensure the connection existed.

Action: Submit an SPR with the crash dump.

020001
Illegal Cache Diagnostic Opcode

Facility: CACHE, CAUPD

Explanation: The cache server update processing code received a message whose operation code was not within the range of operation codes recognized by the cache server.

Action: Submit an SPR with the crash dump.

020002
Illegal HMB Block Type

Facility: CACHE

Explanation: The block type specified in the host message block (HMB) operation code is not one recognized by the cache server. The only valid HMB block type code is HML$TP.

Action: Submit an SPR with the crash dump.

020003
Illegal HMB Opcode

Facility: CACHE

Explanation: The operation code specified in the HM$LOF field of the HMB did not indicate a sequenced message. All messages received by this facility of the cache server must be sequenced.

Action: Submit an SPR with the crash dump.

020004
Illegal HMB Request Type

Facility: CACHE

Explanation: This cache server processes diagnostic and utility requests only. However, the message received was not one of these types.

Action: Submit an SPR with the crash dump.

020020
Illegal Error Condition

Facility: MSCP

Explanation: The M.cache module indicated the presence of an error condition, but the cache server could not find the error condition in any of the hardware-software interface data structures.

Action: Submit an SPR with the crash dump. Ask Digital Services to perform diagnostics on the M.cache module.

020040
Insufficient Free Cache Block Pages

Facility: CAUPD

Explanation: The M.cache module supplies more cache memory than the cache server is able to map to its data structures. This condition may be caused by faulty M.cache hardware.

Action: Submit an SPR with the crash dump.

020060
No AE. found for this IN.

Facility: CASH

Explanation: The cache server data structures appear to be corrupt. In this case, the cache server cannot find an array entry for a particular index node.

Action: Submit an SPR with the crash dump.

020100
Data Buffer/Sector Count Inconsistency

Facility: CASH, MSCP

Explanation: The cache server has detected a data buffer/sector count inconsistency. The sector count and number of attached data buffers should agree in value, but they do not.

Action: Submit an SPR with the crash dump.

042001
FAO message buffer overflow

Facility: DIRECT

Explanation: The program DIRECT was attempting to output the formatted directory end message, but the length of that message was longer than the allotted FAO output buffer.

Action: Submit an SPR with the crash dump.

043001
Wrong HMB received when trying to bring source online

Facility: DKCOPY

Explanation: DKCOPY sent a HMB to the disk server requesting the source unit be brought online in a shadow set. When the completion queue of this HMB was checked, it pointed to a different, and incorrect, HMB.

Action: Submit an SPR with the crash dump.

043002
Bad down count when trying to bring source online

Facility: DKCOPY

Explanation: DKCOPY issued a command to the disk server to bring the source unit online. When the online operation completed, DKCOPY decremented a count of outstanding commands. The count value, however, was found to be invalid.

Action: Submit an SPR with the crash dump.

043003
Wrong HMB received when trying to issue a GET COMMAND STATUS to the target unit of the copy operation

Facility: DKCOPY

Explanation: DKCOPY sent a HMB to the disk server requesting it to send a GET COMMAND STATUS (GCS) command to the target unit. When the completion queue of this HMB was checked, it pointed to a different, and incorrect, HMB.

Action: Submit an SPR with the crash dump.

043004
Bad count value discovered when trying to issue a GET COMMAND STATUS to the target unit

Facility: DKCOPY

Explanation: DKCOPY issued a GCS command operation to the target unit to check on the progress of the copy operation. When the GCS end message was returned to DKCOPY from the disk server, DKCOPY decremented a count of outstanding commands. The count value, however, was found to be invalid.

Action: Submit an SPR with the crash dump.

043005
Bad downcount when trying to bring target unit online

Facility: DKCOPY

Explanation: DKCOPY issued a command to the disk server to bring the target unit online and initiate a shadow copy operation. When the operation completed, DKCOPY decremented a count of outstanding commands. The count value, however, was found to be invalid.

Action: Submit an SPR with the crash dump.

043006
Bad downcount when trying to issue abort command to target unit

Facility: DKCOPY

Explanation: DKCOPY issued a command to the disk server to abort the shadow copy operation. When the abort operation completed, DKCOPY decremented a count. The count value, however, was found to be invalid.

Action: Submit an SPR with the crash dump.

043007
Wrong host message block HMB received after issuing AVL command to shadow unit

Facility: DKCOPY

Explanation: DKCOPY sent a HMB to the disk server requesting that the shadow unit used to facilitate the copy operation be made available. When the completion queue of this HMB was checked, it pointed to a different, and incorrect, HMB.

Action: Submit an SPR with the crash dump.

043010
Bad down count when trying to issue AVL command to shadow unit

Facility: DKCOPY

Explanation: DKCOPY issued a command to the disk server to put the created shadow unit into an available state. When this command completed, DKCOPY decremented a count of outstanding commands. The count value, however, was found to be invalid.

Action: Submit an SPR with the crash dump.

046001
Missing disk rotational access table (DRAT) for FORMAT TRACK operation

Facility: FORMAT

Explanation: A DRAT that was to be put on its completion queue was not found on the DRAT queue.

Action: Submit an SPR with the crash dump.

051001
An XFRB was not acquired to print messages

Facility: SETSHO, SSMAIN

Explanation: SETSHO was not able to acquire an XFRB. A crash was initiated because the lack of an XFRB prevents communication between the HSC controller and the console.

Action: Submit an SPR with the crash dump.

051002
Failed to properly send HMB to K.ci

Facility: SETSHO, SSMAIN

Explanation: SETSHO sent an HMB to the K.ci and a crash was initiated because SETSHO did not receive confirmation of the HMB from the K.ci within the required time.

Action: Submit an SPR with the crash dump.

051003
Too many characters intended for console printout

Facility: SETSHO, SSMAIN

Explanation: SETSHO called formatted ASCII output (FAO) routines and generated more characters than the allocated buffer would allow. The maximum buffer size is 510 characters.

Action: Submit an SPR with the crash dump.

051004
The SCT (System Control Table) crossed a page boundary

Facility: SETSHO, SSMAIN

Explanation: The SCT must remain within one page in memory. The crash may indicate an incorrectly padded SCT.

Action: Submit an SPR with the crash dump.

051101
Failed in sending HMB to disk server for SET Dn [NO]HOST

Facility: SETSHO

Explanation: SETSHO sent an HMB to the disk server to set a disk drive to HOST or NOHOST access. The crash was initiated because the confirmation of this command was not received within the required time.

Action: Submit an SPR with the crash dump.

051102
Failed in sending HMB to tape server for SET Tn [NO]HOST

Facility: SETSHO

Explanation: SETSHO sent an HMB to the tape server to set a tape drive to HOST or NOHOST access. The crash was initiated because the confirmation of this command was not received within the required time.

Action: Submit an SPR with the crash dump.

051201
Failed in sending HMB to disk server for SHOW Dn

Facility: SETSHO

Explanation: SETSHO sent an HMB to the disk server to show a specified disk drive. The crash was initiated because the confirmation of this command was not received within the required time.

Action: Submit an SPR with the crash dump.

051202
Failed in sending HMB to tape server for SHOW Tn

Facility: SETSHO

Explanation: SETSHO sent an HMB to the tape server to show a specified tape drive. The crash was initiated because the confirmation of this command was not received within the required time.

Action: Submit an SPR with the crash dump.

051203
SCT crash context table contained too many characters

Facility: SETSHO

Explanation: The SCT crash context table contained too many characters. When SETSHO called formatted ASCII output (FAO) routines, it generated more characters than the allocated buffer size would allow. The maximum buffer size is 510 characters.

Action: Submit an SPR with the crash dump. To clear the condition, reset the SCT to factory settings by holding in the Fault button while pressing the Init button. You may release the Fault button when the "INIPIO-I Booting ..." message appears. The HSC should remain offline until the SCT is reset with user-supplied values.

052001 ($CDWMATH)
Doubleword math not consistent

Facility: SINI

Explanation: During calculation and allocation of control blocks, which are allocated as doublewords, the number of words in the control blocks was not a doubleword multiple.

Action: Submit an SPR with the crash dump.

052002 ($CDIV10)
Divide operation set overflow

Facility: SINI

Explanation: During allocation of control blocks (set as 80 percent of available control memory), a divide operation set the PSW overflow bit.

Action: Submit an SPR with the crash dump.

052003 ($CMUL8)
Multiply operation set overflow

Facility: SINI

Explanation: During allocation of control blocks (set as 80 percent of available control memory), a multiply operation set the PSW overflow bit.

Action: Submit an SPR with the crash dump.

061001
XCALL stack overflow

Facility: DIAGINT

Explanation: The DDUSUB transfer routines use a stack allocated from common pool for XCALLs (cross-address space calls) from the disk server. The low word of this stack is initialized to a special value that should never change. This crash occurs when the routine DDUTIO is called. The low word of the stack contains a value different than the initialization value.

Action: Submit an SPR with the crash dump. Note the diagnostics or utilities running at the time of the crash.

062001 ($CNOWINDOW)
Process does not have windows declared

Facility: SUBLIB, ERTYP

Explanation: A process requesting an out-of-band error log be issued by the ERTYP$ service in SUBLIB does not have windows declared in its process control block (PCB) declaration. A window set is required to use this service.

Action: Submit an SPR with the crash dump.

062003 ($NKCNTAR)
Data channel control table inconsistency

Facility: SUBLIB

Explanation: A table of bandwidth values has an entry that does not correspond to a known data channel control area.

Action: Submit an SPR with the crash dump. Include the disk and tape configuration.

Index

A

Air filter • 1–12
Allocation class
  reported • 6–108
Automatic device integrity tests • 6–13
Automatic load balancing
  tools • 5–14
Automatic reboot • 3–6

B

BACKUP • 7–1
  tape specifics
    density • 7–9
    error • 7–9
  using more than one tape drive • 7–4
BACKUP/RESTOR
  examples • 7–17
BACKUP error-level error messages • 7–33
BACKUP error messages • 7–23
BACKUP fatal messages • 7–27
BACKUP informational messages • 7–20
BACKUP messages • 7–20
  error • 7–23
  fatal • 7–27
  success • 7–20
  warning • 7–22
BACKUP Messages
  informational messages • 7–20
BACKUP prompts
  change date • 7–6
  change reel • 7–12
  depress return • 7–11
BACKUP prompts (cont'd)
  mount tape • 7–11
  NO OPERATOR • 7–10
  record size transfer • 7–8
  rejected tape units • 7–4
  retain volume • 7–11
  save-set expiration date • 7–6
  save-set name • 7–4
  tape specifics
    size • 7–9
  tape unit numbers • 7–3
  volume labels • 7–7
    two ways to name • 7–7
BACKUP Prompts
  disk unit number • 7–3
BACKUP success messages • 7–20
BACKUP utility • 7–1
BACKUP warning messages • 7–22
Block size recommendations • 5–16
Boot, device names • 4–5
Boot, self-test • 3–4
Booting remotely using ENABLE REBOOT • 6–7
Boot procedure • 3–1
Boot time • 6–108
Break key • 4–1
Broadcast messages • 4–3

C

Cache
  overview • 5–23
  participating • 5–23
  performance • 5–23
  performance analysis tools • 5–24

Cache commands
disk drive • 5–28
disk unit • 5–28
SET [DEVICE] Dnnnn [NO]CACHE • 5–28
disk unit cache
SET [DEVICE] Dnnnn [NO]CACHE • 5–28
global • 5–25
SET SERVER CACHE/CACHE_SIZE_THRESHOLD=n • 5–26
SET SERVER CACHE/ERASE_PURGE_THRESHOLD=n • 5–26
SET SERVER CACHE/WRITE_THRESHOLD=n • 5–26
SET SERVER DISK/[NO]CACHE • 5–25
Cache need analysis tool (CNAT) • 5–29
Cache performance analysis tool (CPAT) • 5–48
Cache server
write allocation policy • 5–28
action • 5–28
Care, customer • 1–12
Central error reporting facility • 6–31, 6–94
CERF • 6–31, 6–94
see central error reporting facility • 6–1
Changing drive states • 6–22
Changing parameters
from the SETSHO prompt • 6–4
requiring ENABLE REBOOT • 6–5
Changing Parameters
requiring immediate reboot • 6–3
Changing parameters from the HSC> prompt • 6–5
Changing parameters from the SETSHO> prompt • 6–4
CI manager • 6–40, 6–94
CI node number • 6–15, 6–36, 6–39, 6–49, 6–75, 6–90, 6–113
CI responder • 6–40, 6–94
Cleaning the filter • 1–11
Clear exception • 6–34
Command
DIR • 4–5
Command prompt and TTDR errors • A–1
Commands • 4–4
CRASH • 4–7
EXIT • 4–8
PURGE • 4–7
RUN • 4–5
SET • 4–5
Commands (cont'd)
SHOW • 4–5
SHOW SYSTEM • 1–9
Commands requiring immediate reboot • 6–3
Commands that require ENABLE REBOOT • 6–5
Commands to communicate with the HSC controller • 4–4
Concatenating commands • 6–2
Configuration
for maximum performance • 5–6
multiple drives on one DCM • 5–8
Configuration flexibility • 5–10
Configuring
for connectivity • 5–10
for performance • 5–4
adding drives to lower priority DCMs • 5–7
data access across multiple drives on the HSC • 5–8
device placement specifics • 5–9
Connectivity
configuration • 5–10
Console dump • 6–28
Control blocks • 6–103
Control characters
at the HSC> prompt
beep • 4–2
bell • 4–2
command prompt • 4–2
Ctrl/O • 4–2
Ctrl/P • 4–2
Ctrl/Q • 4–2
Ctrl/R • 4–2
Ctrl/S • 4–2
Ctrl/U • 4–2
Ctrl/Y • 4–2
Ctrl/Z • 4–2
DEL • 4–2
HSC>prompt • 4–2
Control characters or special key characters • 4–2
Conventions used in this document • xviii
COPY messages • 9–6
error • 9–8
fatal • 9–9
informational • 9–6
warning • 9–6
COPY prompts
enter source unit • 9–3
enter target unit • 9–3

COPY prompts (cont'd)
mount source medium • 9–4
mount target medium • 9–5
perform verification pass • 9–4
really perform COPY • 9–4
COPY utility • 9–1
avoid running under heavy load conditions • 9–2
example • 9–5
how to use it • 9–2
initiating • 9–3
CRASH command • 4–7
Ctrl/C, automatic • 4–3

D

Data access across multiple drives on the HSC • 5–8
Data buffers • 6–103
Data channel module • 1–5
Data channel modules • 5–2
Date and time • 6–19, 6–108
automatic set • 6–19
manual set • 6–19
DCM • 5–2
adding drives to lower priority DCMs • 5–7
adding multiple drives on one DCM • 5–8
configuration for disk or tape • 5–2
description • 5–2
priority • 5–4
utilization on the HSC • 5–4
DC Power Switch • 2–4
DEL
at the HSC> prompt • 4–2
DEMON
see diagnostic monitor • 6–1
Device Integrity Test • 6–13
Device names • 4–5
Device placement specifics • 5–9
application issuing large transfer size • 5–10
paging, swapping, image activation disk drives • 5–9
shadowed disk drives • 5–9
Device specific configuration requirements • 5–2
Diagnostic and utilities protocol server • 6–94
Diagnostic monitor • 6–40, 6–94
Diagnostics, self test • 1–6
Diagnostics utilities protocol server • 6–40
Diagnostic Utility Protocol (DUP) • 5–22
Differences between HSC BACKUP and host BACKUP • 7–1
DIGITAL Standard Disk Format • 10–1
DIR command • 4–5
DIRECT error messages
fatal • A–7
DKCOPY error codes • 8–7
DKCOPY example operations • 8–4
DKCOPY messages • 8–8
error • 8–11
fatal • 8–8
informational messages • 8–12
success message • 8–12
DKCOPY prompts
all input correct • 8–2
enter source unit • 8–2
enter target unit • 8–2
DKCOPY utility • 8–1
how to use it • 8–1
initiation • 8–2
Document structure • xvii
Drive state
available • 6–23
duplicated • 6–23
online • 6–23
unknown • 6–23
Drive_timeout • 6–69
DUMP
to terminal • 6–28
DUP • 6–92
see diagnostics and utilities protocol • 6–1
DUP server • 6–94

E

ENABLE REBOOT
commands that require • 6–5
ENABLE REBOOT Command
booting the HSC remotely • 6–7
how to use • 6–6
suppressing informational messages • 6–6
EP–ESE performance considerations • 5–3
Error information
SINI-E printout • B–4
Error levels • 6–30, 6–84
SETSHO error messages • 6–114

Error message codes • 1–11
Error messages, BACKUP • 7–23
Error messages, RESTOR • 7–35
Example COPY operation • 9–5
Examples, BACKUP/RESTOR • 7–17
Exception codes and messages • B–1
Exception messages listing • B–5 to B–70
Exit command • 4–8
EXIT command • 4–8
Exiting SETSHO • 6–2

F

Fatal messages, BACKUP • 7–27
Fatal messages, RESTOR • 7–41
Fault switch • 2–8

G

Glossary of terms • Glossary–1

H

Host connection
  Computer Interconnect (CI) • 1–4
  Mass Storage Control Protocol (MSCP) • 1–4
  star coupler • 1–4
  system communication architecture (SCA) • 1–4
Host level tools
  diagnostic utility protocol • 5–22
  preferred path function • 5–17
How to boot the HSC • 3–4
How to change parameters from the HSC> prompt • 6–5
How to change parameters from the SETSHO> prompt • 6–4
How to clean front door filter • 1–11
How to clean the filter • 1–11
How to concatenate commands • 6–2
How to exit SETSHO • 6–2
How to load the RX33 • 3–4
How to operate the HSC • 4–1
How to run SETSHO • 6–2
How to use BACKUP • 7–3
How to use ENABLE REBOOT • 6–6
How to use the terminal • 4–1
HSC BACKUP and host BACKUP comparison • 7–2
HSC controller
  automatic reboot • 3–6
  how to boot • 3–4
  in a cluster environment • 1–4
  initializing • 1–6
  operating software
    CRONIC • 1–6
  power on • 1–6
HSC controller applications • 1–1
HSC controller overview • 1–1
HSC controller parameters • 6–72
HSC controller saturation • 5–12
  data rate • 5–13
  request rate • 5–12
HSC controller states • 6–72
HSC crashes • B–1
HSC figures
  basic cluster configuration • 1–4
HSC software • 1–7
  Central Error Reporting Facility (CERF) • 1–10
  CI Exerciser • 1–9
  CI Responder • 1–9
  device integrity tests • 1–9
  Diagnostics Utilities Protocol (DUP) • 1–9
  error indications • 1–10
    console message format • 1–10
    error message code • 1–10
    error message format • 1–11
    output message format • 1–10
    terminal message format • 1–10
  utility programs
    user-loadable • 1–8

I

Immediate Reboot • 6–3
Informational messages, BACKUP • 7–20
Informational messages, RESTOR • 7–34
Initialization • 1–6
Initiating BACKUP • 7–3
Initiating DKCOPY • 8–2
Initiating restor • 7–13
Init switch • 2–7
Inline device integrity tests • 6–108

In line disk device integrity test • 6–13
In line memory test • 6–13
In line tape device integrity test • 6–13
Input control characters • 4–2

K

Keyboard timeout • 4–3
KMON messages • A–2
KMON prompt • A–1
KMON prompt, defined • A–1
KMON prompt messages
  fatal • A–2
  informational • A–2

M

Maximum configurations • 1–5
Messages BACKUP • 7–20
messages RESTOR • 7–34
Multiple drives on one DCM • 5–8
Multiple drives on the HSC • 5–8

O

OCP
  see operator control panel • 6–1
OCP switches • 2–6
ODT • 6–50
ODT, accidental • 4–2
Online indicator • 2–8
Operator control panel • 6–108, 6–109
Operator control panel switches • 2–6
  blank indicators • 2–9
  fault indicator • 2–8
  init indicator • 2–7
  online switch • 2–8
  power indicator • 2–7
  state indicator • 2–7
Operator control panel switches and indicators • 2–6
Out-of-band error messages • 6–31

P

Performance
  cache • 5–23
  configuration • 5–4
  device placement specifics • 5–9
  host level tools • 5–17
  overview • 5–1
Performance configurations • 5–1
  by type of disk or tape drive • 5–6
Performance considerations
  block size recommendations • 5–16
  EP–ESE • 5–3
  pipeline errors and pipeline error reporting • 5–14
Periodic device integrity tests • 6–52, 6–108
Pipeline errors and pipeline error reporting • 5–14
Preface • xvii
Preferred path function • 5–17
Preventive maintenance • 1–12
PRKSDI
  see periodic device integrity test • 6–1
PRKSTI
  see periodic device integrity test • 6–1
PURGE command • 4–7
PURGE command, purpose • 4–7

Q

Quick disconnect
  when • 4–3

R

Rebooting from the HSC> prompt • 6–5
Rebooting from the SETSHO> prompt • 6–4
Recoverable memory list, defined • 4–7
RESTOR • 7–1
  how to use RESTOR • 7–13
  RUN RESTOR • 7–13
RESTOR error messages • 7–35
RESTOR fatal messages • 7–41
RESTOR informational messages • 7–34
RESTOR messages • 7–34
  error • 7–35
  fatal • 7–41
  informational • 7–34

RESTOR messages (cont'd)
- success • 7–34
- warning • 7–35

RESTOR prompts
- enter disk unit number • 7–13
- enter save-set name • 7–14
- enter tape unit numbers • 7–13
- mount tape • 7–15
- NO OPERATOR • 7–14
- press Return • 7–15
- save-set expired • 7–16

RESTOR success message • 7–34
RESTOR warning messages • 7–35
RUN BACKUP • 7–3
RUN command • 4–5
Running SETSHO • 6–2
RX330 system diskette
- how to load the diskette • 3–4

RX33 cover plate • 3–4
RX33 disk drive description • 3–1
RX33 load procedure • 3–4
RX33 system diskette
- description of • 3–3

RXFMT example operation • 11–4
RXFMT messages • 11–4
- error • 11–7
- fatal • 11–7
- informational • 11–5
- status • 11–5
- warning • 11–6

RXFMT prompts
- enter unit to format • 11–2
- mount diskette • 11–3
- really perform format • 11–2

RXFMT utility • 11–1
- avoid using under heavy load conditions • 11–2
- how to use it • 11–1
- initiation • 11–2

S

Save-set
- file name • 7–4

SCT • 3–6
SCT.INI file • 3–7
SCTSAV • 13–1 to 13–8
- boot • 13–1

SCTSAV (cont'd)
- example • 13–4
- fatal error • 13–4
- file not loadable • 13–2
- messages • 13–5
  - fatal • 13–6
  - informational • 13–5
  - inquiry • 13–6
- non-booted • 13–1
- running • 13–3
- SCT.INI • 13–1
- SHOW LINES • 13–1

Secure/Enable switch • 6–109
Self test diagnostics • 1–6
Serial number • 6–38
SET ALLOCATE DISK • 6–9
SET ALLOCATE TAPE • 6–11
SET AUTOMATIC_DIT • 6–13
SET CI • 6–15
SET command • 4–5
SET command examples
- SET ALLOCATE DISK • 6–10
- SET ALLOCATE TAPE • 6–12
- SET AUTOMATIC DIT • 6–14
- SET CI • 6–16
- SET DATE • 6–20
- SET DEVICE • 6–26
- SET DUMP CONSOLE • 6–29
- SET EXCEPTION CLEAR • 6–35
- SET HOST • 6–37
- SET ID • 6–39
- SET LOAD • 6–41
- SET MAX_FORMATTERS • 6–43
- SET MAX_TAPES • 6–45
- SET MEMORY • 6–47
- SET NAME • 6–49
- SET ODT • 6–51
- SET PERIODIC DIT • 6–53
- SET POLLER • 6–56
- SET PROMPT • 6–58
- SET REQUESTOR • 6–62
- SET SCOPE • 6–64
- SET SCT CLEAR • 6–66
- SET SERVER CACHE • 6–68
- SET SERVER DISK • 6–70

SET commands • 6–8
- ALLOCATE DISK • 6–9
- ALLOCATE TAPE • 6–11

SET commands (cont'd)
AUTOMATIC_DIT • 6–13
CI • 6–15
CREDIT_MANAGER RESET • 6–17
DATE • 6–19
DEVICE
[NO]CACHE • 6–21
W_ALLOCATE • 6–21
W_UPDATE • 6–21
DEVICE D_ALL • 6–21
DEVICE [NO]HOST_ACCESS • 6–21
Dn • 6–21
DUMP • 6–28
D_ALL • 6–21
ERROR • 6–30
EXCEPTION CLEAR • 6–34
HOST DISABLE • 6–36
HOST ENABLE • 6–36
ID • 6–38
LOAD • 6–40
MAX_FORMATTERS • 6–42
MAX_TAPES • 6–44
MEMORY • 6–46
MEMORY DISABLE • 6–46
MEMORY ENABLE • 6–46
MEMORY ENABLE ALL • 6–46
NAME • 6–48
system name • 6–48
NODUMP • 6–28
NOSCOPE • 6–63
ODT • 6–50
PERIODIC_DIT • 6–52
POLLER • 6–54
PROMPT • 6–57
REQUESTOR • 6–59
SCOPE • 6–63
SCT CLEAR • 6–65
SERVER CACHE • 6–67
SERVER DISK • 6–69
SET CREDIT_MANAGER RESET • 6–17
SET DATE • 6–19
SET DEVICE • 6–21
changing drive states • 6–22
SET Dn • 6–21
SET DUMP • 6–28
SET D_ALL • 6–21
Set ERROR
types • 6–30
SET ERROR • 6–30
SET EXCEPTION CLEAR • 6–34
SET HOST • 6–36
SET ID • 6–38
SET LOAD • 6–40
SET MAX_FORMATTERS • 6–42
SET MAX_TAPES • 6–44
SET MEMORY • 6–46
SET NAME • 6–48
SET NOSCOPE • 6–63
SET ODT • 6–50
SET PERIODIC_DIT • 6–52
SET POLLER • 6–54
SET PROMPT • 6–57
SET REQUESTOR • 6–59
SET SCOPE • 6–63
SET SCT CLEAR • 6–65
SET SERVER CACHE • 6–67
SET SERVER DISK • 6–69
SETSHO
concatenate commands • 6–2
how to exit • 6–2
how to run it • 6–2
immediate reboot • 6–3
reboot from the SETSHO> prompt • 6–4
SETSHO message codes
description • 6–114
SETSHO messages • 6–114
codes • 6–114
error • 6–119
fatal • 6–123
informational • 6–115
success • 6–115
warning • 6–117
SETSHO utility • 6–1
Short lifetime control blocks • 6–103
SHOW ALL • 6–73
SHOW CI • 6–75
SHOW command • 4–5
SHOW command examples
SHOW CI • 6–76
SHOW CONNECTIONS • 6–78
SHOW CREDIT_MANAGER • 6–81
SHOW DISKS • 6–82
SHOW ERROR • 6–85
SHOW EXCEPTION • 6–89
SHOW LINES • 6–93

SHOW command examples (cont'd)
  SHOW LOAD • 6–95
  SHOW MAX_FORMATTERS • 6–96
  SHOW MAX_TAPES • 6–97
  SHOW MEMORY • 6–99
  SHOW ODT • 6–101
  SHOW POLLER • 6–102
  SHOW POOL • 6–103
  SHOW REQUESTORS • 6–105
  SHOW SERVER • 6–106, 6–107
  SHOW SYSTEM • 6–110
  SHOW TAPES • 6–112
  SHOW VIRTUAL_CIRCUITS • 6–113
Show commands
  LINES • 13–1
SHOW commands • 6–72
  ALL • 6–73
  CI • 6–75
  CONNECTIONS • 6–77
  CREDIT_MANAGER • 6–79
  description of • 6–72
  DISKS • 6–82
  ERROR • 6–84
  EXCEPTION • 6–87
  HOSTS • 6–90
  LINES • 6–92
  LOAD • 6–94
  MAX_FORMATTERS • 6–96
  MAX_TAPES • 6–97
  MEMORY • 6–98
  ODT • 6–100
  POLLER • 6–102
  POOL • 6–103
  REQUESTORS • 6–104
  SERVER CACHE • 6–106
  SERVER DISK • 6–107
  SYSTEM • 6–108
  TAPES
    status • 6–111
  VIRTUAL_CIRCUITS • 6–113
SHOW CONNECTIONS • 6–77
SHOW CREDIT_MANAGER • 6–79
SHOW DISKS
  status of • 6–82
SHOW ERROR • 6–84
SHOW EXCEPTION • 6–87
SHOW HOSTS • 6–90
SHOW LINES • 6–92
SHOW LOAD • 6–94
SHOW MAX_FORMATTERS • 6–96
SHOW MAX_TAPES • 6–97
SHOW MEMORY • 6–98
SHOW ODT • 6–100
SHOW POLLER • 6–102
SHOW POOL • 6–103
SHOW REQUESTORS • 6–104
SHOW SERVER CACHE • 6–106
SHOW SERVER DISK • 6–107
SHOW SYSTEM • 6–108
SHOW TAPES • 6–111
SHOW VIRTUAL_CIRCUITS • 6–113
SINI errors
  SINI-E error printout • B–4
Software inconsistencies • B–1
Software Performance Report • 7–20
Software version • 6–108
Special character
  DEL • 4–2
Special system diskette information • 9–1
Standard Disk Interconnect (SDI) • 1–4
Standard Tape Interconnect (STI) • 1–4
Storage unit connection • 1–4
Submitting an SPR • B–5
Success message, RESTOR • 7–34
Success messages, BACKUP • 7–20
Suppressing informational messages with ENABLE
    REBOOT • 6–6
Switch, Secure/Enable • 6–109
Switches and indicators • 2–1
  AC power switch • 2–1
  DC power switch • 2–1
  secure/enable switch
    enable indicator • 2–4
      operator restrictions • 2–4
SYSCOM.INI file • 3–6
System configuration table • 3–6
  template SCT • 3–6
  user SCT • 3–7
System diskette information • 9–1
  longevity • 9–1
  write protecting • 9–2
System dump • 6–28, 6–108
System exception • 6–28, 6–34, 6–87

System ID • 6–38, 6–108
System name • 6–108

T

Tape allocation class • 6–11
Tape configurations
  SHOW REQUESTOR • 5–16
Tape formatter • 6–42, 6–96
Tape units • 6–44, 6–97
Time and date • 6–19, 6–108
To determine number of DCMs configured on the HSC • 5–16
Tools for automatic load balancing • 5–14
TTDR error messages
  fatal • A–7

U

Uptime • 6–108
Using ENABLE REBOOT • 6–6

V

VERIFY example • 10–3
VERIFY messages • 10–6
  fatal • 10–16
  informational • 10–6
  warning • 10–12
VERIFY prompts
  enter disk unit number • 10–2
  print informational messages • 10–3
  report transient errors by block • 10–3
  was unit just formatted • 10–2
VERIFY utility • 10–1
  how to use it • 10–1
  initiation • 10–2
Virtual circuit • 6–36, 6–113
Virtual terminal • 6–63
Volume shadowing • 1–6
VTDPY disk drive heading definitions • 12–14
VTDPY disk drive status code definitions • 12–14
VTDPY Display • 12–5
VTDPY fields
  interpretation • 12–4
VTDPY messages • 12–17
  error • 12–17
  fatal • 12–17
VTDPY prompts
  enter update interval • 12–2
VTDPY tape drive heading definitions • 12–16
VTDPY tape drive status codes • 12–16
VTDPY utility • 12–1
  control keys • 12–2
  disk status display • 12–13
  how to run it • 12–1
  initialization • 12–1
  process description • 12–11
  tape status display • 12–15

W

Warning messages, BACKUP • 7–22
Warning messages, RESTOR • 7–35