Compaq StorageWorks™

HSJ80 Array Controller
ACS Version 8.5J-2

Troubleshooting Resources Guide

First Edition (August 2000)
Part Number: EK–J80TR–SA. A01
Compaq Computer Corporation

Printed in the U.S.A.

HSJ80 Array Controller ACS Version 8.5J-2 Troubleshooting Resources Guide
First Edition (August 2000)
Part Number: EK–J80TR–SA. A01

Contents

Chapter 2

Utilities and Exercisers

Chapter 3

Event Reporting Templates

Figures

Tables

About This Guide

This guide is a troubleshooting resource for HSJ80 array controllers running array controller software (ACS) versions 8.5J and 8.5J-2. This guide contains information on various utilities, software templates, and event reporting codes.

This guide does not contain information about:

- The operating environments to which the controller might be connected, nor does this guide contain detailed information about subsystem enclosures or their components. See the documentation that accompanied these peripherals for this information.
- Replacement procedures for hardware and software components, and subsystem upgrade procedures. See the controller maintenance and service guide that accompanied the array controller for this information.

Intended Audience

This publication is for use by *Compaq StorageWorks* DS–BA356–MW controller enclosure and Model 2200 Ultra SCSI controller enclosure customers and employees who are responsible for maintaining the subsystems.

How This Guide is Arranged

This guide discusses troubleshooting resources pertaining to the HSJ80 array controller. The guide is organized as follows:

Chapter 1, Troubleshooting Information

This chapter provides information and guidelines for troubleshooting the array controller, cache module, and external cache battery (ECB).

Chapter 2, Utilities and Exercisers

This chapter describes the various utilities and exercisers used to operate and maintain HSJ80 subsystems.

Chapter 3, Event Reporting Templates

This chapter describes the various event logs used by the array controller software to report significant events to the host systems.

Chapter 4, ASC/ASCQ, Repair Action, and Component Identifier Codes

This chapter describes the ASC/ASCQ, recommended repair action, and component identifier codes. A table of each code type is provided, in ascending order, that describes each code value.

Chapter 5, Instance Codes

This chapter describes the instance code structure and provides a table of valid instance codes in ascending order.

Chapter 6, Last Failure Codes

This chapter describes the last failure code structure and provides a table of valid last failure codes in ascending order.

Glossary

Index

Conventions

This guide uses the text conventions in Table 1 and special notices provided within this section.

Text Conventions

Table 1 Text Conventions

Convention	Meaning
Bold	Keyboard keys appear in boldface. For example: **Enter/Return** or **Y**(es) key
SMALL CAPS	Used to indicate the status of an LED. For example: FLASHING means turning on and off, ON means on, and OFF means off
ALLCAPS	Command syntax that must be entered exactly as shown and for commands discussed within text, for example: SET FAILOVER COPY=OTHER_CONTROLLER "Use the SHOW SPARESET command to show the contents of the spareset."
`Monospaced`	Screen display.
italic	User entered command variable or numeric value, for example: SHOW *RAIDset-name* or SET THIS_CONTROLLER CACHE_FLUSH_TIMER=*nn*
	Identifies the first use of *Compaq* specific trademarks or service marks in this document, for example: *Compaq* and *StorageWorks*
	Reference to other publications, for example: "See the *HSJ80 Array Controller ACS Version 8.5J Release Notes* for details."
	Adds emphasis to text, for example: "*Do not* use the following command...."
. . .	Indicates that a portion of an example or figure has been omitted.

Table 1 Text Conventions (Continued)

Convention	Meaning
"this controller"	The controller serving the current CLI session through a local or remote terminal.
"other controller"	The controller in a dual-redundant pair that is connected to the controller serving the current CLI session.

Special Notices

This guide does not contain detailed descriptions of standard safety procedures. However, this guide does contain warnings for procedures that might cause personal injury and cautions for procedures that might damage the controller or its related components. Look for these symbols when performing the procedures in this guide:

WARNING: A warning indicates the presence of a hazard that can cause personal injury if precautions in the text are not observed.

CAUTION: A caution indicates the presence of a hazard that might damage hardware, corrupt software, or cause a loss of data.

IMPORTANT: An important note is a type of note that provides information essential to the completion of a task. Users can disregard information in a note and still complete a task, but they should not disregard an important note.

NOTE: A note provides additional information that is related to the completion of an instruction or procedure.

Getting Help

After exhausting the information in this guide, obtain further information and help using the Compaq website at http://www.compaq.com/storage. The website maintains information on this product as well as the latest drivers and Flash ROM images. The website also provides access to worldwide Compaq technical support phone numbers through the "Contact Us" link.

Related Publications

Table 2 lists documents related to the use of the controller, cache module, and external cache battery.

Table 2 Related Publications

Document Title	Part Number
HSJ80 Array Controller ACS Version 8.5J-2 Maintenance and Service Guide	EK–J80MS–SA
HSJ80 Array Controller ACS Version 8.5J-2 Installation and Configuration Guide	AA–RN17A–TE
HSJ80 Array Controller ACS Version 8.5J-2 Configuration Planning Guide	EK–HSJCP–PA
HSJ80 Array Controller ACS Version 8.5J-2 CLI Reference Guide	EK–HSJCL–RA
HSJ80 Array Controller ACS Version 8.5J-2 Software Solution Kit Overview	EK–HSJSO–OA
HSJ80 Array Controller ACS Version 8.5J-2 for OpenVMS Release Notes	EK–HSJAA–RA
DS-BA356-MW Controller Enclosure Upgrade/Add-on Kit Quick Setup Guide	EK–356MW–QA
DS-BA356-MW Controller Enclosure Upgrade/Add-on Kits Installation Guide	EK–356MW–IA
DS-BA356-MW Controller Enclosure User Guide	EK–356MW–UA
Command Console V2.3 for MA6000 User's Guide	AA–RMBDA–TE
Model 2100 and 2200 Ultra SCSI Controller Enclosure User Guide	EK–SE2C8–UA
The RAIDBOOK—A Source for RAID Technology	RAID Advisory Board

Chapter 1

Troubleshooting Information

This chapter provides guidelines for troubleshooting the controller, cache module, and external cache battery (ECB). See enclosure documentation for information on troubleshooting enclosure hardware, such as the power supplies, cooling fans, and environmental monitoring unit (EMU).

Typical Installation Troubleshooting Checklist

The following checklist identifies many of the problems that occur in a typical installation. After identifying a problem, use Table 1–1 to confirm the diagnosis and fix the problem.

If an initial diagnosis points to several possible causes, use the tools described in this chapter and then those in Chapter 2 to further refine the diagnosis. If a problem cannot be diagnosed using the checklist and tools, contact a Compaq authorized service provider for additional support.

To troubleshoot the controller and supporting modules:

1. Check the power to the enclosure and enclosure components.
   - Are power cords connected properly?
   - Is power within specifications?
2. Check the component cables.
   - Are bus cables to the controllers connected properly?
   - For DS–BA356–MW enclosures, are ECB cables connected properly?

3. Check each program card to make sure the card is fully seated.
4. Check the operator control panel (OCP) and devices for LED codes.

   See "Flashing OCP Pattern Display Reporting," page 1-10, and "Solid OCP Pattern Display Reporting," page 1-12, to interpret the LED codes.
5. Connect a local terminal to the controller and check the controller configuration with the following command:

   ```
   SHOW THIS_CONTROLLER FULL
   ```

   Make sure that the ACS version loaded is correct and that pertinent patches are installed. Also, check the status of the cache module and the supporting ECB.

   In a dual redundant configuration, check the "other controller" with the following command:

   ```
   SHOW OTHER_CONTROLLER FULL
   ```
6. Using the fault management utility (FMU), check for Last Failure or "memory-system failure" entries.

   Show these codes and translate the Last Failure Codes they contain. See Chapter 2, "Displaying Failure Entries" and "Translating Event Codes" sections.

   If the controller failed to the extent that the controller cannot support a local terminal for FMU, check the host error log for the Instance or Last Failure Codes. See Chapter 5 and Chapter 6 to interpret the event codes.
7. Check device status with the following command:

   ```
   SHOW DEVICES FULL
   ```

   Look for errors such as "misconfigured device" or "No device at this PTL." If a device reports misconfigured or missing, check the device status with the following command:

   SHOW *device-name*
8. Check storageset status with the following command:

   ```
   SHOW STORAGESETS FULL
   ```

   Make sure that all storagesets are normal (or normalizing if the storageset is a RAIDset or mirrorset). Check again for misconfigured or missing devices using step 7.

9. Check unit status with the following command:

   SHOW UNITS FULL

   Make sure that all units are available or online. If the controller reports a unit as unavailable or offline, recheck the storageset the unit belongs to with the following command:

   SHOW *storageset-name*

   If the controller reports that a unit has lost data or is unwriteable, recheck the status of the devices that make up the storageset. If the devices are operating normally, recheck the status of the cache module. If the unit reports a media format error, recheck the status of the storageset and storageset devices.

Troubleshooting Table

After diagnosing a problem, use Table 1–1 to resolve the problem.

Table 1–1 Troubleshooting Table (Sheet 1 of 6)

Symptom	Possible Cause	Investigation	Remedy
Reset button not lit.	No power to subsystem.	Check power to subsystem and power supplies on controller enclosure.	Replace cord or (DS–BA356–MW enclosure only) AC input box.
	Failed controller.	If the foregoing check fails to produce a remedy, check OCP LED codes.	Replace controller.
Reset button lit steadily; other LEDs also lit.	Various.	See OCP LED Codes.	Follow repair action using Table 1–2.
Reset button blinking; other LEDs also lit.	Device in error or FAIL set on corresponding device port with other LEDs lit.	SHOW *device* FULL.	Follow repair action using Table 1–3.

Table 1–1 Troubleshooting Table (Sheet 2 of 6)

Symptom	Possible Cause	Investigation	Remedy
Cannot set failover to create dual-redundant configuration.	Incorrect command syntax.	See the controller CLI reference guide for the SET FAILOVER command.	Use the correct command syntax.
	Different software versions on controllers.	Check software versions on both controllers.	Update one or both controllers so that both controllers are using the same software version.
	Incompatible hardware.	Check hardware versions.	Upgrade controllers so that they are using compatible hardware.
	Controller previously set for failover.	Make sure that neither controller is configured for failover.	Use the SET NOFAILOVER command on both controllers, then reset "this controller" for failover.
	Failed controller.	If the foregoing checks fail to produce a remedy, check for OCP LED codes.	Follow repair action using Table 1–2 or Table 1–3.
Nonmirrored cache: controller reports failed DIMM in Cache A or B.	Improperly installed DIMM.	Remove cache module and make sure that the DIMM is fully seated in the slot.	Reseat DIMM.
	Failed DIMM.	If the foregoing check fails to produce a remedy, check for OCP LED codes.	Replace DIMM.
Mirrored cache: "this controller" reports DIMM 1 or 2 failed in Cache A or B.	Improperly installed DIMM in "this controller" cache module.	Remove cache module and make sure that DIMMs are installed properly.	Reseat DIMM.
	Failed DIMM in "this controller" cache module.	If the foregoing check fails to produce a remedy, check for OCP LED codes.	Replace DIMM in "this controller" cache module.
Mirrored cache: "this controller" reports DIMM 3 or 4 failed in Cache A or B.	Improperly installed DIMM in "other controller" cache module.	Remove cache module and make sure that the DIMMs are installed properly.	Reseat DIMM.
	Failed DIMM in "other controller" cache module.	If the foregoing check fails to produce a remedy, check for OCP LED codes.	Replace DIMM in "other controller" cache module.

Table 1–1 Troubleshooting Table (Sheet 3 of 6)

Symptom	Possible Cause	Investigation	Remedy
Mirrored cache: controller reports battery not present.	Memory module was installed before the cache module was connected to an ECB.	DS–BA356–MW enclosure: ECB cable not connected to cache module. Model 2200 enclosures: ECB not installed or seated properly in backplane.	DS–BA356–MW enclosure: Connect ECB cable to cache module, then restart both controllers by pushing their reset buttons simultaneously. Model 2200 enclosures: install or reseat ECB.
Mirrored cache: controller reports cache or mirrored cache has failed.	Primary data and the mirrored copy data are not identical.	SHOW THIS_CONTROLLER indicates that the cache or mirrored cache has failed. Spontaneous FMU message displays: “Primary cache declared failed - data inconsistent with mirror,” or “Mirrored cache declared failed - data inconsistent with primary.”	Enter the SHUTDOWN command on controllers that report the problem. (This command flushes the contents of cache to synchronize the primary and mirrored data.) Restart the controllers that were shut down.

Table 1–1 Troubleshooting Table (Sheet 4 of 6)

Symptom	Possible Cause	Investigation	Remedy
Invalid cache.	Mirrored-cache mode discrepancy. This discrepancy might occur after installing a new controller. The existing cache module is set for mirrored caching, but the new controller is set for unmirrored caching. (This discrepancy might also occur if the new controller is set for mirrored caching but the existing cache module is not.)	SHOW THIS_CONTROLLER indicates "invalid cache." Spontaneous FMU message displays: "Cache modules inconsistent with mirror mode."	Connect a terminal to the maintenance port on the controller reporting the error and clear the error with the following command—all on one line: CLEAR_ERRORS THIS_CONTROLLER INVALID_CACHE NODESTROY_UNFLUSHED_ DATA. See the controller CLI reference guide for more information.
	Cache module might erroneously contain unflushed write-back data. This might occur after installing a new controller. The existing cache module might indicate that the cache module contains unflushed write-back data, but the new controller expects to find no data in the existing cache module. (This error might also occur if installing a new cache module for a controller that expects write-back data in the cache.)	SHOW THIS_CONTROLLER indicates "invalid cache." No spontaneous FMU message.	Connect a terminal to the maintenance port on the controller reporting the error, and clear the error with the following command—all on one line: CLEAR_ERRORS THIS_CONTROLLER INVALID_CACHE DESTROY_UNFLUSHED_ DATA. See the controller CLI reference guide for more information.

Table 1–1 Troubleshooting Table (Sheet 5 of 6)

Symptom	Possible Cause	Investigation	Remedy
Cannot add device.	Illegal device.	See product-specific release notes that accompanied the software release for the most recent list of supported devices.	Replace device.
	Device not properly installed in enclosure.	Check that the device is fully seated.	Firmly press the device into the bay.
	Failed device.	Check for presence of device LEDs.	Follow repair action in the documentation provided with the enclosure or device.
	Failed power supplies.	Check for presence of power supply LEDs.	Follow repair action in the documentation provided with the enclosure or power supply.
	Failed bus to device.	If the foregoing checks fail to produce a remedy, check for OCP LED codes.	Replace enclosure.
Cannot configure storagesets.	Incorrect command syntax.	See the controller CLI reference guide for the ADD *storageset* command.	Reconfigure storageset with correct command syntax.
	Exceeded maximum number of storagesets.	Use the SHOW command to count the number of storagesets configured on the controller.	Delete unused storagesets.
	Failed battery on ECB. (An ECB or UPS is required for RAIDsets and mirrorsets.)	Use the SHOW command to check the ECB battery status.	Replace the ECB if required.
Cannot assign unit number to storageset.	Incorrect command syntax.	See the controller CLI reference guide for correct syntax.	Reassign the unit number with the correct syntax.
Unit is available but not online.	This is normal. Units are “available” until the host accesses them, at which point their status is changed to “online.”	None	None
Host cannot see device.	Broken cables.	Check for broken cables.	Replace broken cables.

Table 1–1 Troubleshooting Table (Sheet 6 of 6)

Symptom	Possible Cause	Investigation	Remedy
Host cannot access unit.	Host files or device drivers not properly installed or configured.	Check for the required device special files.	Configure device special files as described in the getting started manual that accompanied the software release.
	Invalid Cache	See the description for the invalid cache symptom on page 1–6.	See the description for the invalid cache symptom.
	Units have lost data.	Issue the SHOW UNITS command.	CLEAR_ERRORS *unit-number* LOST_DATA.
Host log file or maintenance terminal indicates that a forced error occurred when the controller was reconstructing a RAIDset or mirrorset.	Unrecoverable read errors might have occurred when controller was reconstructing the storageset. Errors occur if another member fails while the controller is reconstructing the storageset.	Conduct a read scan of the storageset using the appropriate utility from the host operating system.	Rebuild the storageset, then restore storageset data from a backup source. While the controller is reconstructing the storageset, monitor the host error log activity or spontaneous event reports on the maintenance terminal for any unrecoverable errors. If unrecoverable errors persist, note the device on which they occurred, and replace the device before proceeding.
	Host requested data from a normalizing storageset that did not contain the data.	Use the SHOW *storageset-name* command to see if all storageset members are “normal.”	Wait for normalizing members to become normal, then resume I/O to them.

Significant Event Reporting

Controller fault management software reports information about significant events that occur. These events are reported by:

- Maintenance terminal displays
- Host error logs
- OCP LEDs

Some events cause controller operation to halt; others allow the controller to remain operable. Both types of events are detailed in the following sections.

Reporting Events That Cause Controller Operation to Halt

Events that cause the controller to halt operations are reported three possible ways:

- a flashing OCP pattern display
- a solid OCP pattern display
- Last Failure reporting

Use Table 1–2 to interpret *FLASHING* OCP patterns and Table 1–3 to interpret *solid* (*ON*) OCP patterns. In the Error column of the solid OCP patterns, there are two separate descriptions. The first denotes the actual error message that appears on the terminal, and the second provides a more detailed explanation of the designated error.

Use the following legend to interpret both tables as indicated:

- ■ = reset button FLASHING (in Table 1–2) or ON (in TABLE 1–3)
- ❑ = reset button OFF
- ● = LED FLASHING (in Table 1–2) or ON (in TABLE 1–3)
- ❍ = LED OFF

NOTE: If the reset button is FLASHING and an LED is ON, either the devices on that LED bus do not match the controller configuration, or an error occurred in one of the devices on that bus. Also, a single LED that is turned ON indicates a failure of the drive on that port.

Flashing OCP Pattern Display Reporting

Certain events can cause a *FLASHING* display of the OCP LEDs. Each event and the resulting pattern is described in Table 1–2.

IMPORTANT: Remember that a solid black pattern represents a FLASHING display. A white pattern indicates OFF.

All LEDs FLASH at the same time and at the same rate.

Table 1–2 FLASHING OCP Pattern Displays and Repair Actions

Pattern	OCP Code	Error	Repair Action
■❍❍❍❍❍●	1	Program card EDC error.	Replace program card.
■❍❍❍●❍❍	4	Timer zero on the processor is bad.	Replace controller.
■❍❍❍●❍●	5	Timer one on the processor is bad.	Replace controller.
■❍❍❍●●❍	6	Processor Guarded Memory Unit (GMU) is bad.	Replace controller.
■❍❍●❍●●	B	Nonvolatile Journal Memory (JSRAM) structure is bad because of a memory error or an incorrect upgrade procedure.	Verify the correct upgrade (see the controller release notes and Cover Letters, if available). If error continues, replace controller.
■❍❍●●❍●	D	One or more bits in the diagnostic registers did not match the expected reset value.	Press the reset button to restart the controller. If this does not correct the error, replace the controller.
■❍❍●●●❍	E	Memory error in the JSRAM.	Replace controller.
■❍❍●●●●	F	Wrong image found on program card.	Replace program card or replace controller if needed.
■❍●❍❍❍❍	10	Controller Module memory is bad.	Replace controller.
■❍●❍❍●❍	12	Controller Module memory addressing is malfunctioning.	Replace controller.
■❍●❍❍●●	13	Controller Module memory parity is not working.	Replace controller.

Legend:

■ = reset button FLASHING ❑ = reset button OFF ● = LED FLASHING ❍ = LED OFF

Table 1–2 FLASHING OCP Pattern Displays and Repair Actions (Continued)

Pattern	OCP Code	Error	Repair Action
■❍●❍●❍❍	14	Controller Module memory controller timer has failed.	Replace controller.
■❍●●❍❍●	15	The Controller Module memory controller interrupt handler has failed.	Replace controller.
■❍●●●●❍	1E	During the diagnostic memory test, the Controller Module memory controller caused an unexpected Non-Maskable Interrupt (NMI).	Replace controller.
■●❍❍●❍❍	24	The card code image changed when the contents were copied to memory.	Replace controller.
■●●❍❍❍❍	30	The JSRAM battery is bad.	Replace controller.
■●●❍❍●❍	32	First-half diagnostics of the Time of Year Clock failed.	Replace controller.
■●●❍❍●●	33	Second-half diagnostics of the Time of Year Clock failed.	Replace controller.
■●●❍●❍●	35	The processor bus-to-device bus bridge chip is bad.	Replace controller.
■●●●❍●●	3B	There is an unnecessary interrupt pending.	Replace controller.
■●●●●❍❍	3C	There was an unexpected fault during initialization.	Replace controller.
■●●●●❍●	3D	There was an unexpected maskable interrupt during initialization.	Replace controller.
■●●●●●❍	3E	There was an unexpected NMI during initialization.	Replace controller.
■●●●●●●	3F	An invalid process ran during initialization.	Replace controller.

Legend:

■ = reset button FLASHING ❑ = reset button OFF ● = LED FLASHING ❍ = LED OFF

Solid OCP Pattern Display Reporting

Certain events cause a *solid* display of the OCP LEDs. Each event and the resulting pattern is described in Table 1–3.

Information related to the solid OCP patterns is automatically displayed on the maintenance terminal (unless disabled with the FMU) using %FLL formatting, as detailed in the following examples:

Table 1–3 Solid OCP Pattern Displays and Repair Actions (Sheet 1 of 4)

Pattern	OCP Code	Error	Repair Action
❑❍❍❍❍❍❍	0	Catastrophic controller or power failure.	Check power. If good, reset controller. If problem persists, reseat controller module and reset controller. If problem is still evident, replace controller module.
■❍❍❍❍❍❍	0	No program card detected or kill asserted by other controller. Controller unable to read program card.	Make sure that the program card is properly seated while resetting the controller. If the error persists, try the card with another controller; or replace the card. Otherwise, replace the controller that reported the error.
■●❍❍●❍●	25	Recursive Bugcheck detected. The same bugcheck has occurred three times within 10 minutes, and controller operation has halted.	Reset the controller. If this fault pattern is displayed repeatedly, follow the repair action(s) associated with the Last Failure code that is repeatedly terminating controller execution.
■●❍❍●●❍	26	Indicated memory module is missing. Controller is unable to detect a particular memory module.	Insert memory module (cache board).
■●❍❍●●●	27	Memory module has insufficient usable memory.	Replace indicated DIMM(s). (This indication is only provided when Fault LED logging is enabled).

Legend:

■ = reset button ON ❑ = reset button OFF ● = LED ON ❍ = LED OFF

Table 1–3 Solid OCP Pattern Displays and Repair Actions (Sheet 2 of 4)

Pattern	OCP Code	Error	Repair Action
■●○●○○○	28	An unexpected Machine Fault/NMI occurred during Last Failure processing. A machine fault was detected while a Non-Maskable Interrupt was processing.	Reset the controller.
■●○●○○●	29	EMU protocol version incompatible. The microcode in the EMU and the software in the controller are not compatible.	Upgrade either the EMU microcode or the software (refer to the Release Notes that accompanied the controller software).
■●○●○●○	2A	All enclosure I/O modules are not of the same type. Enclosure I/O modules are a combination of single-ended and differential.	Make sure that the I/O modules in an extended subsystem are either all single-ended or all differential, not both.
■●○●○●●	2B	Jumpers not terminators found on backplane. One or more SCSI bus terminators are either missing from the backplane or broken.	Make sure that enclosure SCSI bus terminators are installed and that there are no jumpers. Replace the failed terminator if the problem continues.
■●○●●○○	2C	Enclosure I/O termination power out of range. Faulty or missing I/O module causes enclosure I/O termination power to be out of range.	Make sure that all of the enclosure device SCSI buses have an I/O module. If problem persists, replace the failed I/O module.
■●○●●●●	2F	Memory module has illegal DIMM configuration.	Verify that DIMMs are installed correctly.
■●●○○○○	30	An unexpected bugcheck occurred before subsystem initialization completed. An unexpected Last Failure occurred during initialization.	Reinsert controller. If that does not correct the problem, reset the controller. If the error persists, try resetting the controller again, and replace the controller if no change occurs.

Legend:

■ = reset button ON ❑ = reset button OFF ● = LED ON ○ = LED OFF

Table 1–3 Solid OCP Pattern Displays and Repair Actions (Sheet 3 of 4)

Pattern	OCP Code	Error	Repair Action
■●●❍❍❍●	31	ILF$INIT unable to allocate memory. Attempt to allocate memory by ILF$INIT failed.	Replace controller.
■●●❍❍●❍	32	Code load program card write failure. Attempt to update program card failed.	Replace program card.
■●●❍❍●●	33	Nonvolatile program memory (NVPM) structure revision too low. NVPM structure revision number is less than the one that can be handled by the software version attempting to be executed.	Verify that the program card contains the latest software version. If the error persists, replace controller.
■●●❍●❍●	35	An unexpected bugcheck occurred during Last Failure processing. Last Failure Processing interrupted by another Last Failure event.	Reset controller.
■●●❍●●❍	36	Hardware-induced controller reset expected. Automatic hardware reset failed.	Replace controller.
■●●❍●●●	37	Software-induced controller reset expected. Software-induced reset failed.	Replace controller.
■●●●❍❍❍	38	Controller operation halted. Last Failure event required termination of controller operation, for example: SHUTDOWN via the command line interpreter (CLI).	Reset controller.
■●●●❍❍●	39	NVPM configuration inconsistent. Device configuration within the NVPM is inconsistent.	Replace controller.

Legend:

■ = reset button ON ❑ = reset button OFF ● = LED ON ❍ = LED OFF

Table 1–3 Solid OCP Pattern Displays and Repair Actions (Sheet 4 of 4)

Pattern	OCP Code	Error	Repair Action
■●●●❍●❍	3A	An unexpected NMI occurred during Last Failure processing. Last Failure processing interrupted by a Non-Maskable Interrupt (NMI).	Replace controller.
■●●●❍●●	3B	NVPM read loop hang. Attempt to read data from NVPM failed.	Replace controller.
■●●●●❍❍	3C	NVPM write loop hang. Attempt to write data to NVPM failed.	Replace controller.
■●●●●❍●	3D	NVPM structure revision greater than image. NVPM structure revision number is greater than the one that can be handled by the software version attempting to execute.	Replace program card with one that contains the latest software version.
■●●●●●●	3F	DAEMON diagnostic failed hard in non-fault tolerant mode. DAEMON diagnostic detected critical hardware component failure; controller can no longer operate.	Verify that cache module is present. If the error persists, replace controller.

Legend:

■ = reset button ON ❑ = reset button OFF ● = LED ON ❍ = LED OFF

Last Failure Reporting

Last failures are automatically displayed on the maintenance terminal (unless disabled via the FMU) using %LFL formatting. The example below details an occurrence of a Last Failure report:

```
%LFL--HSJ> --13-JAN-1999 04:39:45 (time not set)-- Last Failure Code: 20090010
Power On Time: 0.Years, 14.Days, 19.Hours, 58.Minutes, 42.Seconds
Controller Model: HSJ80
Serial Number: AA12345678 Hardware Version: 0000(00)
Software Version: V085j-2(50)
Informational Report
Instance Code: 0102030A
Last Failure Code: 20090010 (No Last Failure Parameters)
Additional information is available in Last Failure Entry: 1.
```

In addition, Last Failures are reported to the host error log using Template 01, following a restart of the controller. See Chapter 4 for a more detailed explanation of this template.

Reporting Events That Allow Controller Operation to Continue

Events that do not cause controller operation to halt are displayed in one of two ways:

- Spontaneous event log
- CLI event reporting

Spontaneous Event Log

Spontaneous event logs are automatically displayed on the maintenance terminal (unless disabled with the FMU) using %EVL formatting, as illustrated in the following examples:

```
%EVL--HSJ> --13-JAN-1999 04:32:47 (time not set)-- Instance Code: 0102030A (not yet
reported to host)
Template: 1.(01)
Power On Time: 0.Years, 14.Days, 19.Hours, 58.Minutes, 43.Seconds
Controller Model: HSJ80
Serial Number: AA12345678 Hardware Version: 0000(00)
Software Version: V085j-2(50)
Informational Report
Instance Code: 0102030A
Last Failure Code: 011C0011
Last Failure Parameter[0.] 0000003F

%EVL--HSJ> --13-JAN-1999 04:32:47 (time not set)-- Instance Code: 82042002 (not yet
reported to host)
Template: 13.(13)
Power On Time: 0.Years, 14.Days, 19.Hours, 58.Minutes, 43.Seconds
Controller Model: HSJ80
Serial Number: AA12345678 Hardware Version: 0000(00)
Software Version: V085j-2(50)
Header type: 00 Header flags: 00
Test entity number: 0F Test number Demand/Failure: F8 Command: 01
Error Code: 0008 Return Code: 0005 Address of Error: A0000000
Expected Error Data: 44FCFCFC Actual Error Data: FFFF01BB
Extra Status(1): 00000000 Extra Status(2): 00000000 Extra Status(3): 00000000
Instance Code: 82042002
HSJ>
```

Spontaneous event logs are reported to the host error log using SCSI Sense Data Templates 01, 05, 11, 12, 13, 14, 32, 33, 34, 41, 51, 57, 61, and 71, plus the Disk Copy Data Correlation Event Log. See Chapter 3 for a more detailed explanation of items.

CLI Event Reporting

CLI event reports are automatically displayed on the maintenance terminal (unless disabled with the FMU) using %CER formatting, as shown in the following example:

```
%CER--HSJ> --13-JAN-1999 04:32:20 (time not set)-- Previous controller-
operation stopped with display of solid fault code, OCP Code: 3F
HSJ>
```

Running the Controller Diagnostic Test

During startup, the controller automatically tests the device ports, host ports, cache module, and value-added functions. If intermittent problems are experienced with one of these components, run the controller diagnostic test in a continuous loop, rather than restarting the controller repeatedly.

Use the following steps to run the controller diagnostic test:

1. Connect a terminal to the controller maintenance port.
2. Start the self-test with one of the following commands:

   SELFTEST THIS_CONTROLLER

   SELFTEST OTHER_CONTROLLER

   NOTE: The self-test runs until an error is detected or until the controller reset button is pressed.

If the self-test detects an error, the self-test saves information about the error and produces an OCP LED code for a “daemon hard error.” Restart the controller to write the error information to the host error log, then check the host error log for a “built-in self-test failure” event report. This report will contain an instance code, located at offset 32 through 35, that can be used to determine the cause of the error. See Chapter 2, “Translating Event Codes” for help on translating instance codes.

ECB Charging Diagnostics

Whenever restarting the controller, the diagnostic routines automatically check the charge of each ECB battery. If the battery is fully charged, the controller reports the battery as good and rechecks the battery every 24 hours. If the battery is charging, the controller rechecks the battery every 4 minutes. A battery is reported as being either above or below 50 percent in capacity. A battery below 50 percent in capacity is referred to as being low.

The 4-minute polling continues for the maximum allowable time to recharge the battery—up to 10 hours for a DS–BA356–MW enclosure, or 3.5 hours for a Model 2200 enclosure. If the battery does not charge sufficiently after the alloted time, the controller declares the battery as "failed."

Battery Hysteresis

When charging an ECB battery, write-back caching is allowed as long as a previous down-time did not drain more than 50 percent of ECB battery capacity. When an ECB battery is operating below 50 percent capacity, the battery is considered to be low and write-back caching is disabled.

CAUTION: Compaq recommends replacing the ECB every 2 years to prevent battery failure.

NOTE: If an uninterruptible power supply (UPS) is used for backup power and set to DATACENTER_WIDE, the controller does not check the battery. See the controller configuration planning guide, controller installation and configuration guide and controller CLI reference guide for information about the UPS switches.

Caching Techniques

The cache module supports the following caching techniques to increase subsystem read and write performance:

- Read caching
- Read-ahead caching
- Write-through caching
- Write-back caching

Read Caching

When the controller receives a read request from the host, the controller reads the data from the disk drives, delivers the data to the host, and stores the data in the supporting cache module. Subsequent reads for the same data will take this data from the supporting cache module rather than accessing the data from the disk drives. This process is called read caching.

Read caching can decrease the subsystem response time to many host read requests. If the host requests some or all of the cached data, the controller satisfies the request from the supporting cache module rather than from the disk drives. By default, read caching is enabled for all storage units.

For more details, refer to following CLI commands in the controller CLI reference guide:

SET *unit-number* MAXIMUM_CACHED_TRANSFER=*nn*

SET unit-number MAX_READ_CACHED_TRANSFER_SIZE=*nn*

SET *unit-number* READ_CACHE

Read-Ahead Caching

Read-ahead caching begins when the controller has already processed a read request, and the controller receives a subsequent read request from the host. If the controller does not find the data in the cache memory, the controller reads the data from the disk drives and sends this data to the cache memory.

During read-ahead caching, the controller anticipates subsequent read requests and begins to prefetch the next blocks of data from the disk drives as the controller sends the requested read data to the host. These are parallel actions. The controller notifies the host of the read completion, and subsequent sequential read requests are satisfied from the cache memory. By default, read-ahead caching is enabled for all disk units.

Write-Through Caching

When the controller receives a write request from the host, the controller places the data in the supporting cache module, writes the data to the disk drives, then notifies the host when the write operation is complete. This process is called write-through caching because the data actually passes through—and is stored in—the cache memory along the way to the disk drives.

If read caching is enabled for a storage unit, write-through caching is automatically enabled.

Write-Back Caching

Write-back caching improves the subsystem response time to write requests by allowing the controller to declare the write operation "complete" as soon as the data reaches the supporting cache memory. The controller performs the slower operation of writing the data to the disk drives at a later time. For more details, refer to following CLI commands in the controller CLI reference guide:

SET *unit-number* MAXIMUM_CACHED_TRANSFER=*nn*

SET unit-number MAX_WRITE_CACHED_TRANSFER_SIZE=*nn*

SET *unit-number* WRITEBACK_CACHE

By default, write-back caching is enabled for all units. The controller will only provide write-back caching to a unit if the cache memory is nonvolatile, as described in the next section.

By default, the controller expects to use an ECB as the backup power source for the cache module. However, if the subsystem is protected by a UPS, use one of the following CLI commands to instruct the controller to use the UPS:

SET *controller* UPS=NODE_ONLY

SET *controller* UPS=DATACENTER_WIDE

Fault-Tolerance for Write-Back Caching

The cache module supports nonvolatile memory and dynamic cache policies to protect the availability of cache module unwritten (write-back) data.

Nonvolatile Memory

Except for disaster-tolerant supported mirrorsets, the controller provides write-back caching for storage units while the controller cache memory is nonvolatile. In other words, to enable write-back caching requires connecting a backup power source (ECB) to the cache module to preserve the unwritten cache data during a power failure. If the cache memory were volatile—meaning that a backup power supply is not connected to protect the cache memory—the unwritten cache data would be lost during a power failure.

By default, the controller expects to use an ECB as the backup power source for the supporting cache module. However, if the subsystem is backed up using a UPS, two options are available that tell the controller to use the UPS with one of the following commands:

- For BA370 enclosure only: use both the ECB and the UPS together with the following command:

  SET *controller* UPS=NODE_ONLY

- Use only the UPS as the backup power source with the following command:

  SET *controller* UPS=DATACENTER_WIDE

NOTE: See the controller CLI reference guide for detailed descriptions of these commands.

Cache Policies Resulting from Cache Module Failures

If the controller detects a full or partial failure of the supporting cache module or ECB, the controller automatically reacts to preserve the unwritten data in the supporting cache module. Depending upon the severity of the failure, the controller chooses an interim caching technique—also called the cache policy—until the cache module or ECB is repaired or replaced.

Table 1–4 shows the cache policies resulting from a full or partial failure of cache module A (Cache A) in a dual-redundant controller configuration. The consequences shown in Table 1–4 are the same for Cache B failures.

Table 1–5 shows the cache policies resulting from a full or partial failure of the ECB connected to Cache A in a dual-redundant controller configuration. The consequences shown in Table 1–5 are the opposite for an ECB failure connected to Cache B.

- If the ECB is at least 50% charged, the ECB is still good and is charging.
- If the ECB is less than 50% charged, the ECB is low, but still charging.

Table 1–4 Cache Policies—Cache Module Status

Cache Module Status		Cache Policy	
Cache A	**Cache B**	**Unmirrored Cache**	**Mirrored Cache**
Good.	Good.	Data loss: None Cache policy: Both controllers support write-back caching. Failover: None	Data loss: None Cache policy: Both controllers support write-back caching. Failover: None
Multibit cache memory failure.	Good.	Data loss: Forced error and loss of write-back data for which the multibit error occurred. Controller A detects and reports the lost blocks. Cache policy: Both controllers support write-back caching. Failover: None	Data loss: None. Controller A recovers Controller A lost write-back data from the mirrored copy on Cache B. Cache policy: Both controllers support write-back caching. Failover: None

Table 1–4 Cache Policies—Cache Module Status (Continued)

Cache Module Status		Cache Policy	
Cache A	**Cache B**	**Unmirrored Cache**	**Mirrored Cache**
DIMM or cache memory controller chip failure.	Good.	Data loss: Write-back data that was not written to media when failure occurred was not recovered. Cache policy: Controller A supports write-through caching only; Controller B supports write-back caching. Failover: In transparent failover, all units failover to Controller B. In multiple-bus failover with host-assist, only those units that use write-back caching, such as RAIDsets and mirrorsets, failover to Controller B. All units with lost data become inoperative until they are cleared using the CLEAR LOST_DATA command. Units that did not lose data operate normally on Controller B. In single-controller configurations, RAIDsets, mirrorsets, and all units with lost data become inoperative. Although lost data errors can be cleared on some units, RAIDsets and mirrorsets remain inoperative until the nonvolatile memory on Cache A is repaired or replaced.	Data loss: Controller A recovers all of Controller A write-back data from the mirrored copy on Cache B. Cache policy: Controller A supports write-through caching only; Controller B supports write-back caching. Failover: In transparent failover, all units failover to Controller B and operate normally. In multiple-bus failover with host-assist, only those units that use write-back caching, such as RAIDsets and mirrorsets, failover to Controller B.
Cache Board Failure.	Good.	Same as for DIMM failure.	Data loss: Controller A recovers all of Controller A write-back data from the mirrored copy on Cache B. Cache policy: Both controllers support write-through caching only. Controller B cannot execute mirrored writes because Cache A cannot mirror Controller B unwritten data. Failover: None

Table 1–5 Resulting Cache Policies—ECB Status

Cache Module Status		Cache Policy	
Cache A	**Cache B**	**Unmirrored Cache**	**Mirrored Cache**
At least 50% charged.	At least 50% charged.	Data loss: None Cache policy: Both controllers continue to support write-back caching. Failover: None	Data loss: None Cache policy: Both controllers continue to support write-back caching. Failover: None
Less than 50% charged.	At least 50% charged.	Data loss: None Cache policy: Controller A supports write-through caching only; Controller B supports write-back caching. Failover: In transparent failover, all units failover to Controller B. In multiple-bus failover with host-assist, only those units that use write-back caching, such as RAIDsets and mirrorsets, failover to Controller B. In single-controller configurations, the controller only provides write-through caching to the units.	Data loss: None Cache policy: Both controllers continue to support write-back caching. Failover: None
Failed.	At least 50% charged.	Data loss: None Cache policy: Controller A supports write-through caching only; Controller B supports write-back caching. Failover: In transparent failover, all units failover to Controller B and operate normally. In multiple-bus failover with host-assist, only those units that use write-back caching, such as RAIDsets and mirrorsets, failover to Controller B. In single-controller configurations, the controller only provides write-through caching to the units.	Data loss: None Cache policy: Both controllers continue to support write-back caching. Failover: None

Table 1–5 Resulting Cache Policies—ECB Status (Continued)

Cache Module Status		Cache Policy	
Cache A	**Cache B**	**Unmirrored Cache**	**Mirrored Cache**
Less than 50% charged.	Less than 50% charged.	Data loss: None Cache policy: Both controllers support write-through caching only. Failover: None	Data loss: None Cache policy: Both controllers support write-through caching only. Failover: None
Failed.	Less than 50% charged.	Data loss: None Cache policy: Both controllers support write-through caching only. Failover: In transparent failover, all units failover to Controller B and operate normally. In multiple-bus failover with host-assist, only those units that use write-back caching, such as RAIDsets and mirrorsets, failover to Controller B. In single-controller configurations, the controller only provides write-through caching to the units.	Data loss: None Cache policy: Both controllers support write-through caching only. Failover: None
Failed.	Failed.	Data loss: None Cache policy: Both controllers support write-through caching only. Failover: None. RAIDsets and mirrorsets become inoperative. Other units that use write-back caching operate with write-through caching only.	Data loss: None Cache policy: Both controllers support write-through caching only. Failover: None. RAIDsets and mirrorsets become inoperative. Other units that use write-back caching operate with write-through caching only.

Enabling Mirrored Write-Back Cache

Before configuring dual-redundant controllers and enabling mirroring, make sure the following conditions are met:

- Each cache module is configured with the same size cache, 512 MB.
- Diagnostics indicate that both caches are good.
- Both cache modules have an ECB connected and the UPS switch is set by the following command:

  SET *controller* NOUPS (no UPS is connected)

- Both cache modules either:
  - Have an ECB connected and the UPS switch is set by one of the following commands:

    SET *controller* NOUPS (no UPS is connected)

  - Do not have an ECB connected and the UPS switch is set by the following command:

    SET *controller* UPS=DATACENTER_WIDE

  NOTE: No unit errors are outstanding (for example, lost data or data that cannot be written to devices).

- Both controllers are started and configured in failover mode.

For important considerations when configuring a subsystem for mirrored caching, see the controller installation and configuration guide. To add or replace DIMMs in a mirrored cache configuration, see the controller maintenance and service guide.

Chapter 2

Utilities and Exercisers

This chapter describes the utilities and exercisers available to aid in troubleshooting and maintaining the controllers, cache modules, and ECBs. These utilities and exercisers include:

- Fault Management Utility (FMU)
- Video Terminal Display (VTDPY) Utility
- Disk Inline Exerciser (DILX)
- Tape Inline Exerciser (TILX)
- Format and Device Code Load Utility (HSUTIL)
- Configuration (CONFIG) Utility
- Code Load and Code Patch (CLCP) Utility
- Clone (CLONE) Utility
- Field Replacement Utility (FRUTIL)
- Change Volume Serial Number (CHVSN) Utility

Fault Management Utility (FMU)

The FMU provides a limited interface to the controller fault management software. Use FMU to:

- Display the last failure and memory-system-failure entries that the fault management software stores in the controller non-volatile memory.
- Translate many of the code values contained in event messages. For example, entries might contain code values that indicate the cause of the event, the software component that reported the event, the repair action, and so on.
- Display the instance codes that identify and accompany significant events which do not cause the controller to halt operation.
- Display the last-failure codes that identify and accompany failure events which cause the controller to halt operations. Last-failure codes are sent to the host only after the affected controller is restarted.
- Control the display characteristics of significant events and failures that the fault management system displays on the maintenance terminal. See “Controlling the Display of Significant Events and Failures,” page 2-5, for specific details on this feature.

Displaying Failure Entries

The controller stores the 16 most recent last-failure reports as entries in its non-volatile memory. The occurrence of any failure event halts operation of the controller on which it occurred.

> **NOTE:** Memory system failures are reported through the last failure mechanism but can be displayed separately.

Use the following steps to display the last-failure entries:

1. Connect a PC or a local terminal to the controller maintenance port.
2. Start FMU with the following command:

   RUN FMU

3. Show one or more of the entries with the following command:

   SHOW *event_type entry# FULL*

   where:

   - *event-type* is LAST_FAILURE or MEMORY_SYSTEM_FAILURE

- *entry#* is ALL, MOST_RECENT, or 1 through 16
- *FULL* displays additional information, such as the Intel i960 stack and hardware component register sets (for example, the memory controller, FX, host port, and device ports, and so on).

4. Exit FMU with the following command:

```
EXIT
```

The following example shows a last-failure entry. The Informational Report—the lower half of the entry—contains the last failure code, reporting component, and so forth that can be translated with FMU to learn more about the event.

```
Last Failure Entry: 4. Flags: 006FF300
Template: 1.(01) Description: Last Failure Event
 Occurred on 28-JUN-2000 at 15:29:28
Power On Time: 0. Years, 14. Days, 19. Hours, 51. Minutes, 31. Seconds
Controller Model: HSJ80
Serial Number: AA12345678 Hardware Version: 0000(00)
Controller identifier:
 Unique Device Number: 000105060200 Model: 45.(2D) Class:1.(01)
Software Version: V085j-2(50)
Node Name: "HSJB6" CI Node Number: 4.(04)
Informational Report
Instance Code: 0102030A Description:
 An unrecoverable software inconsistency was detected or an intentional
 restart or shutdown of controller operation was requested.
Reporting Component: 1.(01) Description:
 Executive Services
Reporting component's event number: 2.(02)
Event Threshold: 10.(0A) Classification:
 SOFT. An unexpected condition detected by a controller software component
 (e.g., protocol violations, host buffer access errors, internal
 inconsistencies, uninterpreted device errors, etc.) or an intentional
 restart or shutdown of controller operation is indicated.
Last Failure Code: 20090010 (No Last Failure Parameters)
Last Failure Code: 20090010 Description:
 This controller requested this controller to shutdown.
Reporting Component: 32.(20) Description:
 Command Line Interpreter
Reporting component's event number: 9.(09)
Restart Type: 1.(01) Description: No restart
```

Translating Event Codes

Use the following steps to translate the event codes in the fault management reports for spontaneous events and failures.

1. Connect a PC or a local terminal to the controller maintenance port.
2. Start FMU with the following command:

   RUN FMU

3. Show one or more of the entries with the following command:

   DESCRIBE *code_type code#*

   where:

   - *code_type* is one of those listed in Table 2–1
   - *code#* is the alpha-numeric value displayed in the entry
   - code types marked with an asterisk (*) require multiple code numbers (see Chapter 3 for types codes used in the various templates, Chapter 4 for ASC, ASCQ, Repair Action, and Component ID codes, Chapter 5 for Instance Codes, and Chapter 6 for Last Failure Codes)

Table 2–1 Event Code Types

Event Code Type	Event Code Type
ASC_ASCQ_CODE*	REPAIR_ACTION_CODE
COMPONENT_CODE	RESTART_TYPE
CONTROLLER_UNIQUE_ASC_ASCQ_CODE*	SCSI_COMMAND_OPERATION_CODE*
DEVICE_TYPE_CODE	SENSE_DATA_QUALIFIERS*
EVENT _THRESHOLD_CODE	SENSE_KEY_CODE
INSTANCE_CODE	TEMPLATE_CODE
LAST_FAILURE_CODE	

The following examples show the FMU translation of a last-failure code and an instance code.

```
FMU>DESCRIBE LAST_FAILURE_CODE 206C0020
Last Failure Code: 206C0020
Description: Controller was forced to restart in order for new controller
code image to take effect.
Reporting Component: 32.(20)
Description: Command Line Interpreter
Reporting component's event number: 108.(6C)
Restart Type: 2.(02)
Description: Automatic hardware restart

FMU>DESCRIBE INSTANCE 026e0001
Instance Code: 026E0001
Description: The device specified in the Device Locator field has been
reduced from the Mirrorset associated with the logical unit. The nominal
number of members in the mirrorset has been decreased by one. The reduced
device is now available for use.
Reporting Component: 2.(02)
Description: Value Added Services
Reporting component's event number: 110.(6E)
Event Threshold: 1.(01) Classification:
IMMEDIATE. Failure or potential failure of a component critical to proper
controller operation is indicated; immediate attention is required.
```

Controlling the Display of Significant Events and Failures

Use the SET command to control how the fault management software displays significant events and failures.

Table 2–2 describes various SET commands that can be entered while running FMU. These commands remain in effect only as long as the current FMU session remains active, unless the PERMANENT qualifier is entered (the last entry in the table).

Table 2–2 FMU SET Commands

Command	Result
SET EVENT_LOGGING SET NOEVENT_LOGGING	Enable and disable the spontaneous display of significant events to the local terminal; preceded by "%EVL" (see example on page 1–17). By default, logging is enabled (SET EVENT_LOGGING). When logging is enabled, the controller spontaneously displays information about the events on the local terminal. Spontaneous event logging is suspended during the execution of CLI commands and operation of utilities on a local terminal. Because these events are spontaneous, logs are not stored by the controller.
SET LAST_FAILURE LOGGING SET NOLAST_FAILURE LOGGING	Enable and disable the spontaneous display of last failure events; preceded by "%LFL" (see example on page 1–16). By default, logging is enabled (SET LAST_FAILURE LOGGING). The controller spontaneously displays information relevant to the sudden termination of controller operation. In cases of automatic hardware reset (for example, power failure or pressing the controller reset button), the fault LED log display is inhibited because automatic resets do not allow sufficient time to complete the log display.
SET *log_type* REPAIR_ACTION SET *log_type* NOREPAIR_ACTION	Enable and disable the inclusion of repair action information for event logging or last-failure logging. By default, repair actions are not displayed for these log types (SET *log_type* NOREPAIR_ACTION). If the display of repair actions is enabled, the controller displays any of the recommended repair actions associated with the event.
SET *log_type* VERBOSE SET *log_type* NOVERBOSE	Enable and disable the automatic translation of event codes that are contained in event logs or last-failure logs. By default, this descriptive text is not displayed (SET *log_type* NOVERBOSE). See "Translating Event Codes," page 2-4, for instructions to translate these codes manually.
SET PROMPT SET NOPROMPT	Enable and disable the display of the CLI prompt string following the log identifier "%EVL," or "%LFL," or "%FLL." This command is useful if the CLI prompt string is used to identify the controllers in a dual-redundant configuration (see the controller CLI reference guide for instructions to set the CLI command string for a controller). If enabled, the CLI prompt will be able to identify which controller sent the log to the local terminal. By default, the prompt is set (SET PROMPT).
SET TIMESTAMP SET NOTIMESTAMP	Enable and disable the display of the current date and time in the first line of an event or last-failure log. By default, the timestamp is set (SET TIMESTAMP).

Table 2–2 FMU SET Commands (Continued)

Command	Result
SET FMU_REPAIR_ACTION SET FMU_NOREPAIR_ACTION	Enable and disable the inclusion of repair actions with SHOW LAST_FAILURE and SHOW MEMORY_SYSTEM_FAILURE commands. By default, the repair actions are not shown (SET FMU NOREPAIR_ACTION). If repair actions are enabled, the command outputs display all of the recommended repair actions associated with the instance or last-failure codes used to describe an event.
SET FMU VERBOSE SET FMU NOVERBOSE	Enable and disable the inclusion of instance and last failure code descriptive text with SHOW LAST_FAILURE and SHOW MEMORY_SYSTEM_ FAILURE commands. By default, this descriptive text is not displayed (SET FMU_NOVERBOSE). If the descriptive text is enabled, it identifies the fields and their numeric content that comprise an event or last-failure entry.
SET CLI_EVENT_REPORTING SET NOCLI_EVENT_REPORTING	Enable and disable the asynchronous errors reported at the CLI prompt (for example, “swap signals disabled” or “shelf (enclosure) has a bad power supply”); preceded by “%CER” (see example on page 1–18). By default, these errors are reported (SET CLI_EVENT_REPORTING). These errors are cleared with the CLEAR ERRORS_CLI command.
SET FAULT_LED_LOGGING SET NOFAULT_LED_LOGGING	Enable and disable the solid fault LED event log display on the local terminal. Preceded by “%FLL.” By default, logging is enabled (SET FAULT_LED_LOGGING). When enabled, and a solid fault pattern is displayed in the OCP LEDs, the fault pattern and its meaning are displayed on the maintenance terminal. For many of the patterns, additional information is also displayed to aid in problem diagnosis. In cases of automatic hardware reset (for example, power failure or pressing the controller reset button), the fault LED log display is inhibited because automatic resets do not allow sufficient time to complete the log display.
SHOW PARAMETERS	Displays the current settings associated with the SET command.
SET *command* PERMANENT	Preserves the SET command across controller resets.

Video Terminal Display (VTDPY) Utility

The VTDPY utility, through various screens, displays configuration and performance information for the HSJ80 storage subsystem and is used to check the subsystem for communication problems. Information displayed includes:

- Processor utilization
- Virtual storage unit activity and configuration
- Cache performance
- Device activity and configuration
- Host port activity and configuration

NOTE: All VTDPY screen displays are 132 characters wide. However, for readability purposes, the sample screens in this section are not complete screens as viewed on the terminal.

Restrictions with VTDPY

The following restrictions apply when using VTDPY:

- The VTDPY utility requires a serial maintenance terminal that supports ANSI control sequences or a graphics display that emulates an ANSI-compatible terminal.
- Only one VTDPY session can be run on a controller at a time.
- VTDPY does not display information for passthrough devices.

Running VTDPY

Use the following steps to run VTDPY:

1. Connect a serial maintenance terminal to the controller maintenance port.

IMPORTANT: The terminal must support ANSI control sequences.

2. Set the terminal to NOWRAP mode to prevent the top line of the display from scrolling off of the screen.
3. Press **Enter**/**Return** to display the CLI prompt (CLI>).
4. Start VTDPY with the following command:

```
RUN VTDPY
```

Use the key sequences and commands listed in Table 2–3 to control VTDPY.

Table 2–3 VTDPY Key Sequences and Commands

Command	Action
Ctrl/C	Enables command mode; after entering **Ctrl/C**, enter one of the following commands and press **Enter**/**Return**: DISPLAY CACHE DISPLAY DEFAULT DISPLAY DEVICE DISPLAY HOST DISPLAY PORT 1 DISPLAY PORT 2 DISPLAY STATUS EXIT or QUIT HELP INTERVAL *seconds* (to change update interval) REFRESH or UPDATE
Ctrl/G	Updates screen
Ctrl/O	Pauses (and resumes) screen updates
Ctrl/R	Refreshes the current screen display
Ctrl/Y	Exits VTDPY

Commands can be abbreviated to the minimum number of characters necessary to identify the command. Enter a question mark (**?**) after a partial command to see the values that can follow the supplied command.

For example: if **DISP ?** (DISP <space> ?) is entered, the utility will list CACHE, DEFAULT, and other possibilities.

Upon successfully executing a command—other than HELP—VTDPY exits command mode. Pressing **Enter**/**Return** without a command also causes VTDPY to exit command mode.

VTDPY Help

Entering **HELP** at the VTDPY prompt (VTDPY>) displays information about VTDPY commands and keyboard shortcuts. See Figure 2–1 below:

NOTE: The ^ symbol denotes the **Ctrl** key on the keyboard.

```
VTDPY> HELP
Available VTDPY commands:
^C - Prompt for commands
^G or ^Z - Update screen
^O - Pause/Resume screen updates
^Y - Terminate program
^R or ^W - refresh screen
DISPLAY CACHE - Use 132 column unit caching statistics display
DISPLAY DEFAULT - Use 132 column system performance display
DISPLAY DEVICE - Use 132 column device performance display
DISPLAY HOST - Use 132 column Host Ports statistics display
DISPLAY PORT 1 - Use 132 column Host Port 1 performance display
DISPLAY PORT 2 -Use 132 column Host Port 2 performance display
DISPLAY STATUS - Use 132 column controller status display
EXIT - Terminate program (same as QUIT)
INTERVAL <seconds> - Change update interval
HELP - Display this help message
REFRESH - Refresh the current display
QUIT - Terminate program (same as EXIT)
UPDATE - Update Screen Display
```

Figure 2–1. VTDPY commands and shortcuts generated from the Help command

VTDPY Display Screens

VTDPY displays storage subsystem information using the following display screens:

- Default Screen
- Controller Status Screen
- Cache Performance Screen
- Device Performance Screen
- Host Ports Statistics Screen
- Host Port 1 and 2 Detailed Statistics Screen

Choose any of the screens by entering **DISPLAY** at the VTDPY prompt, followed by the screen name. For example: display the cache performance screen using the VTDPY following command:

```
DISPLAY CACHE
```

Each display screen is shown in the following sections. Screen interpretations are presented following the various screens.

Default Screen

The DEFAULT screen, shown in Figure 2–2, consists of the following sections and subsections:

- Screen header, which includes:
  - Controller ID data
  - Subsystem performance
  - Controller up-time
  - Current date and time
- Controller/processor utilization
- Host port 1 and 2 packet data brief
- Full unit performance

```
VTDPY> DISPLAY DEFAULT

HSJ80 S/N: ZG94900033 SW: V085J-2 HW: H0-01  60.1% Idle  63210 KB/S  2577 Rq/S
                                                  Up: 13 20:58:52 28-JUN-2000 10:33:41
                              PORT/NODE
 Pr Name Stk/Max  Typ Sta  CPU% Port 1 NodeID 12      Unit ASWC12  KB/S Rd% Wr% Cm% Ht%
  0 NULL   0/  0       Rn  60.1 NAME J80012          D0001x  aFF     0   0   0   0   0
  4 MAIN  40/  3  FNC  Rn  32.8 SysID 4200100C4CD9    D0002o^ aFF  2417  42  57   0  98
 15  DUP  10/  1  FNC  Bl   0.3 Path A  Pkts  Pkts/S  D0003o^ aFF     0   0   0   0   0
 18 RMGR  40/  4  FNC  Rn   3.3 Rcv    31296    1039  D0004o^ aFF   174   0 100   0   0
 20 DS_1  40/  3  FNC  Bl   3.3 Ack    31434    1044  D0005o^ aFF  1020 100   0   0 100
                              Oth       94       3  D0006o^ aFF  2709  37  62   0  97
                              Path B  Pkts  Pkts/S
                              Rcv    31368    1042
                              Ack    31221    1037
                              Oth       97       3
                              Port 2 NodeID 13
                              NAME J80013
                              SysID 4200100D4ED9
                              Path A  Pkts  Pkts/S
                              Rcv    45230    1502
                              Ack    45183    1501
                              Oth       96       3
                              Path B  Pkts  Pkts/S
                              Rcv    45028    1495
                              Ack    45070    1497
                              Oth       96       3
```

Figure 2–2. Sample of the VTDPY default screen

Controller Status Screen

The STATUS screen, shown in Figure 2–3, consists of the following sections:

- Screen header, which includes:
  - Controller ID data
  - Subsystem performance
  - Controller up-time
  - Current date and time
- Controller/processor utilization
- Device port configuration
- Host port configuration
- Brief unit performance

NOTE: Figure 2–3 applies to “this controller” only. To see “other controller” connections, run VTDPY again on the “other controller.”

```
VTDPY>DISPLAY STATUS

HSJ80 S/N: ZG94900033 SW: V085J-2 HW: H0-01  64.6% Idle   6045 KB/S 2228 Rq/S
                                        Up: 13 20:58:52 28-JUN-2000 10:33:41
                                Target
 Pr Name Stk/Max Typ Sta  CPU%           1111111           Unit  ASWC12 KB/S
  0 NULL   0/  0     Rn  64.6   0123456789012345           D0001 x  aFF    0
  4 MAIN  40/  3 FNC Rn  27.3  P1DDDDDDHh                  D0002 o^ aFF 1827
 15  DUP  10/  1 FNC Bl   2.6  o2DDDDDDHh                  D0003 o^ aFF    0
 18 RMGR  40/  4 FNC Rn   5.0  r3      Hh                  D0004 o^ aFF  447
 20 DS_1  40/  3 FNC Bl   0.3  t4DD DDDHh                  D0005 o^ aFF 1024
                               5D D D Hh                  D0006 o^ aFF 2746
                               6      Hh
                             Port 1       Port 2
                             Connections  Connections
                              0123456789  0123456789
                             0MM........  0.....M..M
                             1.M....      1.....
                             2            2
                             3            3
                             Path Status  Path Status
                             Connections  Connections
                              0123456789  0123456789
                             0^^........  0.....^..^
                             1.^....      1.....
                             2            2
                             3            3
```

Figure 2–3. Sample of the VTDPY status screen

Cache Performance Screen

The CACHE screen, shown in Figure 2–4, consists of the following sections:

- Screen header, which includes:
  - Controller ID data
  - Subsystem performance
  - Controller up-time
  - Current date and time
- Unit status
- Unit I/O activity

```
VTDPY>DISPLAY CACHE

HSJ80 S/N: ZG94900033 SW: V085J-2 HW: H0-01  51.9% Idle   6445 KB/S 2297 Rq/S
                                        Up: 13 20:58:52 28-JUN-2000 10:33:41
Unit    ASWC12    KB/S  Rd%  Wr%  Cm%  Ht%  Ph%  MS%  Purge  BlChd  BlHit  RH%
D0001   x  aFF       0    0    0    0    0    0    0      0      0      0    0
D0002   o^ aFF    2301   44   55    0   96    0    4      0  16120  60000    0
D0003   o^ aFF     326  100    0    0   98    0    2     36   2592  18924   11
D0004   o^ aFF     410   16   83    0  100    0    0    975  20100   4116    0
D0005   o^ aFF     828  100    0    0  100    0    0      0      0  48880    0
D0006   o^ aFF    2577   39   60    0   97    0    3   2557  48916  60000    0
```

Figure 2–4. Sample of the VTDPY cache screen

Device Performance Screen

The DEVICE screen, shown in Figure 2–5, consists of the following sections:

- Screen header, which includes:
  - Controller ID data
  - Subsystem performance
  - Controller up-time
  - Current date and time
- Device port configuration (upper left)
- Device performance (center)
- Device port performance (lower left)

```
VTDPY>DISPLAY DEVICE

HSJ80 S/N: ZG94900033 SW: V085J-2 HW: H0-01  53.6% Idle   2843 KB/S 166 Rq/S
                                      Up: 13 20:58:52 28-JUN-2000 10:33:41

       Target         P TL   ASWF    Rq/S  RdKB/S  WrKB/S Que  Tg  CR  BR  ER
            111111    D1000  a          0       0       0   0   1   0   0   0
  0123456789012345    D1010  a          0       0       0   0   1   0   0   0
P1DDDDDDHh            D1020  a          0       0       0   0   1   0       0
o2DDDDDDHh            D1030  a          0       0       0   0   1   0   0   0
r3      Hh            D1040  a          0       0       0   0   1   0   0   0
t4DD DDDHh            D1060  a          0       0       0   0   1   0   0   0
 5D D D Hh                                                          0
 6      Hh                                                         0

Port Rq/S RdKB/S WrKB/S CR BR TR
  1     0      0      0  0  0  0
  2     0      0      0  0  0  0
  3     0      0      0  0  0  0
  4    84      0    172  0  0  0
  5    81      0   2670  0  0  0
  6     0      0      0  0  0  0
```

Figure 2–5. Sample of regions on the VTDPY device screen

Host Ports Statistics Screen

The HOST screen, shown in Figure 2–6, consists of the following sections:

- Screen header, which includes:
  - Controller ID data
  - Subsystem performance
  - Controller up-time
  - Current date and time
- Host port 1 packet data full
- Host port 1 configuration
- Host port 2 packet data full
- Host port 2 configuration

```
VTDPY>DISPLAY HOST

HSJ80 S/N: ZG94900033 SW: V085J-2 HW: H0-01   73.3% Idle   4155 KB/S 1249 Rq/S
                                                   Up: 13 20:58:52 28-JUN-2000 10:33:41
Port 1    Node ID   12                        Port 2    Node ID   13
Name      J80012                              Name      J80013
  Path A   Pkts     Pkts/S                    Path A     Pkts     Pkts/S
Rcv       26579        885                    Rcv        9763        325
Ack       26620        887                    Ack        9775        325
Nak           3          0    Port 1          Nak           0          0    Port 2
Nor          95          3    Connections     Nor          96          3    Connections
RNak         58          1     0123456789     RNak          4          0     0123456789
CRC           0          0    0MM........     CRC           5          0    0......M..M
CDrop         0          0    1.M....         CDrop         0          0    1......
Retry         0          0    2               Retry         0          0    2
  Path B   Pkts     Pkts/S    3                 Path B   Pkts     Pkts/S    3
Rcv       26534        884    Path Status     Rcv        9820        327    Path Status
Ack       26483        882     0123456789     Ack        9796        326     0123456789
Nak           0          0    0^^........     Nak           0          0    0......^..^
Nor          93          3    1.^....         Nor          96          3    1......
RNak         59          1    2               RNak          5          0    2
CRC           1          0    3               CRC           0          0    3
CDrop         0                                CDrop         0
Retry         0          0                     Retry         0          0

DGD           0          0                     DGD           0          0
CWait         0          0                     CWait         0          0
```

Figure 2–6. Sample of the VTDPY host screen

Host Port 1 and 2 Detailed Statistics Screen

The host PORT 1 and PORT 2 screens consist of the following sections (see example in Figure 2–7):

- Screen header, which includes:
  - Controller ID data
  - Subsystem performance
  - Controller up-time
  - Current date and time
- Host port 1 or 2 node statistics
- Host port 1 or 2 error totals
- Host port 1 or 2 node totals

```
VTDPY>DISPLAY PORT 1

HSJ80 S/N: ZG94900033 SW: V085J-2 HW: H0-01   60.3% Idle   6052 KB/S 2333 Rq/S
                                                        Up: 13 20:58:52 28-JUN-2000 10:33:41
Port 1  CI Node Number 12  SCS Name J80012
              Path A             Path B                        Path A             Path B
Nd   CW   Rcv   Ack   Nak  Nor  Rcv   Ack   Nak  Nor  Nd   CW   Rcv   Ack   Nak  Nor  Rcv   Ack   Nak  Nor
0     0     5     0     0    0    5     5     0    0  16    0     0     0     0    0    0     0     0    0
1     0  1284  1265     0    7 1206  1225     0   10  17    0     0     0     0    0    0     0     0    0
2     0     0     0     0   12    0     0     0   12  18    0     0     0     0    0    0     0     0    0
3     0     0     0     0   12    0     0     0   12  19    0     0     0     0    0    0     0     0    0
4     0     0     4     0    0    0     0     0    0  20    0     0     0     0    0    0     0     0    0
5     0     0     0     0   12    0     0     0   12  21    0     0     0     0    0    0     0     0    0
6     0     0     0     0   12    0     0     0   12  22    0     0     0     0    0    0     0     0    0
7     0     0     4     0    0    0     0     0    0  23    0     0     0     0    0    0     0     0    0
8     0     0     0     0   12    0     0     0   12  24    0     0     0     0    0    0     0     0    0
9     0     0     3     0    0    0     0     0    0  25    0     0     0     0    0    0     0     0    0
10    0     0     3     0    0    0     0     0    0  26    0     0     0     0    0    0     0     0    0
11    0  2240 22593     0    1 2260 22431     0    0  27    0     0     0     0    0    0     0     0    0
12    0     0     0     0    0    0     0     0    0  28    0     0     0     0    0    0     0     0    0
13    0     0     0     0   12    0     0     0   12  29    0     0     0     0    0    0     0     0    0
14    0     4     4     0    0    4     4     0    0  30    0     0     0     0    0    0     0     0    0
15    0     0     0     0   12    0     0     0   12  31    0     0     0     0    0    0     0     0    0
                                                          ___ ______ ______ ___ ___ ______ ______ ___ ___
CRC:      0                                    Total  0  23720 23881  3  92 23841 23679  0  94
RNak:    64                           Port 2 Total  0  45220 45225  0  96 45042 45033  0  97
DGD:      0
```

Figure 2–7. Sample of the VTDPY host port 1 screen

Interpreting VTDPY Screen Information

Refer to the sample VTDPY screens in the previous section as needed while the various sections of these screens are interpreted in this section. The six VTDPY screens display information in the following screen subsections:

- Screen Header
- Unit Performance Data Fields
- Device Performance Data Fields
- Device Port Performance Data Fields
- Host Port Configuration
- Device Port Configuration
- Controller/Processor Utilization
- Host Port Packet Data
- Host Port Error Totals
- Host Port Node Statistics
- Host Port Node Totals

Each screen subsection is described in the following sections.

Screen Header

The screen header is the first line of data on every display screen. The header shows information about the overall performance of the HSJ80 storage subsystem and is further divided into the following four subsections:

- Controller ID data
- Subsystem performance data
- Controller up-time data
- Current date and time

The controller ID data appears as follows:

```
HSJ80    S/N: xxxxxxxxxxxx    SW: xxxxxxx    HW: xx-xx
```

where:

- HSJ80: string represents the controller model name and number.

- S/N: depicts an alpha-numeric serial number.
- SW: depicts a software version number.
- HW: depicts a hardware revision number.

The subsystem performance data appears as follows:

```
xxx.x% Idle   xxxxxx KB/S   xxxxx RQ/S
```

where:

- xxx.x% Idle displays the controller policy processor up-time.
- KB/S displays cumulative data transfer rate in kilobytes per second.
- RQ/S displays cumulative unit request rate in requests per second.

The controller up-time data shows the up-time of the HSJ80 controller in days, hours and minutes in the following format:

```
Up:   days   hh:mm:ss
```

The current date and time is displayed as follows:

```
day-month-year   hh:mm:ss
```

Common Data Fields

Some VTDPY displays contain common data fields, such as the DEFAULT, STATUS, CACHE, and DEVICE screens. Table 2–4 provides a description of common data fields on DEFAULT, STATUS, and CACHE screens.

Table 2–4 VTDPY — Common Data Fields Column Definitions: Part 1

Column	Contents		
Pr	Thread priority		
Name	Thread name or NULL (idle)		
Stk/Max	Allocated stack size in 512 byte pages and maximum number of stack pages actually used		
Typ	Thread type:		
	FNC	=	functional thread
	DUP	=	device utility/exerciser (DUP) local program threads
	NULL	=	null thread. Special thread type that only executes when no other thread type is executable.

Table 2–4 VTDPY — Common Data Fields Column Definitions: Part 1 (Continued)

Column	Contents		
Sta	Status:		
	BI	=	waiting for completion of a process currently running
	Io	=	waiting for input or output
	Rn	=	actively running
CPU%	Percentage of central processing unit resource consumption		

Other common data fields in the VTDPY in the DEFAULT, STATUS, CACHE, and DEVICE screens are described in Table 2–5.

Table 2–5 VTDPY — Common Data Fields Column Definitions: Part 2

Column	Contents		
Port	Port 1 or 2, representing Host Port 1 or 2, respectively.		
NodeID	Node identifier		
Name	Node name; up to 6 characters maximum		
SysID	System ID; up to 12 characters maximum		
Path A	Denotes activity on Path A of Host Port 1 or 2		
Path B	Denotes activity on Path B of Host Port 1 or 2		
Pkts	Number of packets pertaining to Path A or B		
	Rcv	=	number of packets received on this Port/Path
	Ack	=	number of packets acknowledged on this Port/Path
	Oth	=	number of packets whose status resulted in something other than acknowledged on this Port/Path
Pkts/S	rate of packet processing in packets per second		
	Rcv	=	number of packets received on this Port/Path
	Ack	=	number of packets acknowledged on this Port/Path
	Oth	=	number of packets whose status resulted in something other than acknowledged on this Port/Path

Unit Performance Data Fields

VTDPY displays virtual storage unit performance information in a block of tabular data in the DEFAULT, STATUS, and CACHE screens only. Each of these screens displays the unit performance data in a different format, as follows:

- DEFAULT screen uses the full format (see Figure 2–2).
- STATUS screen uses a brief format (see Figure 2–3).
- CACHE screen uses the maximum format (see Figure 2–4).

Although these displays show unit performance in three different formats, the displays share common data fields, with the brief format displaying the least information, the full format supplying more information, and the maximum format displaying the maximum amount of available information. See Table 2–6 for a description of each field on these screens.

Table 2–6 VTDPY — Unit Performance Data Fields Column Definitions

Column	Contents		
Unit	Kind of unit and the unit number. Unit types include:		
	C	=	CD-ROM drive
	D	=	disk drive or CD-ROM drive
	I	=	invisible device
	L	=	medium changer or loader
	O	=	optical memory device
	P	=	passthrough device
	T	=	tape device
	?	=	unknown device type

Table 2–6 VTDPY — Unit Performance Data Fields Column Definitions (Continued)

Column	Contents		
A	Availability of the unit:		
	a	=	available to “other controller”
	d	=	offline, unit disabled for servicing
	e	=	online, unit mounted for exclusive access by a user
	f	=	offline, media format error
	i	=	offline, unit inoperative
	m	=	offline, maintenance mode for diagnostic purposes
	o	=	online, Host can access this unit through “this controller”
	r	=	offline, rundown set with the SET NORUN command
	v	=	offline, no volume mounted due to lack of media
	x	=	online, Host can access this unit through “other controller”
	l	=	for disk devices only, indicating the device is failsafe locked
		=	(space) unknown availability
S	Spindle state of a virtual storage disk unit:		
	^	=	disk device spinning at correct speed; tape loaded
	>	=	disk device spinning up
	<	=	disk device spinning down
	v	=	disk device stopped spinning
		=	(space) unknown spindle state or device is not a disk unit
W	Write-protection state of the virtual storage device		
	W	=	for disk drives, indicating the device is hardware write-protected
		=	(space) device is not a disk unit
C	Caching state of the device:		
	a	=	read, write-back, and read-ahead caching enabled
	b	=	read and write-back caching enabled
	c	=	read and read-ahead caching enabled
	p	=	read-ahead caching enabled
	r	=	read caching only
	w	=	write-back caching is enabled
		=	(space) caching disabled

Table 2–6 VTDPY — Unit Performance Data Fields Column Definitions (Continued)

Column	Contents
1 2	Access type for Host Ports 1 and 2
	F = read/write or full access
	N = none or no access
	R = read-only access
KB/S	Average amount of data transferred to and from the unit during the last update interval in kilobyte increments per second.
Rd%	Percentage of data transferred between the host and the unit that were read from the unit.
Wr%	Percentage of data transferred between the host and the unit that were written to the unit.
Cm%	Percentage of data transferred between the host and the unit that were compared. A compare operation can accompany a read or a write operation, so this column is not the sum of columns Rd% and Wr%.
Ht%	Cache-hit percentage for data transferred between the host and the unit.
Ph%	Partial cache hit percentage of data transferred between the host and the unit.
MS%	Cache miss percentage of data transferred between the host and the unit.
Purge	Number of blocks purged from the write-back cache during the last update interval.
BlChd	Number of blocks added to the cache in the last update interval.
BlHit	Number of cached data blocks hit in the last update interval.
RH%	Read cache-hit percentage for data transferred between the host and the unit.

Device Performance Data Fields

VTDPY displays up to 42 devices in the device performance region (see Figure 2–5, center) of the DEVICE screen only. See Table 2–7 for a description of each field.

Table 2–7 VTDPY — Device Performance Data Fields Column Definitions

Column	Contents		
PTL	Type of device and the device port-target-LUN (PTL) address:		
	D	=	disk drive
	P	=	passthrough device
	?	=	unknown device type
		=	(space) no device configured at this location
A	Allocation state. Availability of the device:		
	a	=	available to “other controller”
	A	=	available to “this controller”
	u	=	unavailable, but configured on “other controller”
	U	=	unavailable, but configured on “this controller”
		=	(space) unknown allocation state
S	Spindle state of the device:		
	^	=	disk device spinning at correct speed; tape loaded
	>	=	disk device spinning up
	<	=	disk device spinning down
	v	=	disk device stopped spinning
		=	(space) unknown spindle state
W	Write-protection state of the device		
	W	=	for disk drives, indicating the device is hardware write-protected
		=	(space) other device type
F	Fault status of a device		
	F	=	unrecoverable device fault. Device fault LED is ON.
		=	(space) no fault detected
Rq/S	Average I/O request rate for the device during the last update interval. Requests can be up to 8 KB and generated by host requests or cache flush activity.		

Table 2–7 VTDPY — Device Performance Data Fields Column Definitions (Continued)

Column	Contents
RdKB/S	Average read data transfer rate to the device in KB/s during the previous update interval.
WrKB/S	Average write data transfer rate to the device in KB/s during the previous update interval.
Que	Maximum number of transfer requests waiting to be transferred to the device during the last screen update interval.
Tg	Maximum number of requests queued to the device during the last screen update interval. If the device does not support tagged queuing, the maximum value is 1.
CR	Number of SCSI command resets that occurred since VTDPY was started.
BR	Number of SCSI bus resets that occurred since VTDPY was started.
TR	Number of SCSI target resets that occurred since VTDPY was started.

Device Port Performance Data Fields

VTDPY displays a device port performance region (see Figure 2–5, lower left) on the DEVICE screen only. See Table 2–8 for a description of each field.

Table 2–8 VTDPY — Device Port Performance Data Fields Column Definitions

Column	Contents
Port	SCSI device ports 1 through 6.
Rq/S	Average I/O request rate for the device during the last update interval. Requests can be up to 8 KB and generated by host requests or cache flush activity.
RdKB/S	Average read data transfer rate to the device in KB/s during the previous update interval.
WrKB/S	Average write data transfer rate to the device in KB/s during the previous update interval.
CR	Number of SCSI command resets that occurred since VTDPY was started.
BR	Number of SCSI bus resets that occurred since VTDPY was started.
TR	Number of SCSI target resets that occurred since VTDPY was started.

Host Port Configuration

VTDPY displays host port configuration information in a block of tabular data in the STATUS and HOST screens only. The data is displayed for both host Port 1 and host Port 2 independently, although the format is the same for both. Host port configuration display data includes:

```
Port x
Connections
0123456789
0
1
2
3
Path Status
0123456789
0
1
2
3
```

Table 2–9 Host Port Configuration Data

Field Label	Description
Port x	Represents Host Ports 1 and 2 respectively. The value of "x" is either 1 or 2.
Connections	Represents the 32 possible virtual circuit connects (0 through 31) to the host port and the status of each connection.
	C = a single connection exists for this virtual circuit
	M = multiple connections exist for this virtual circuit
	V = no connection to this virtual circuit
	. = (period) no virtual circuits exist
Path Status	Represents the virtual circuit path status for the corresponding connections defined in the Connections portion of this display.
	A = a good cable for path A only
	B = a good cable for path B only
	X = crossed cables
	^ = good cables for paths A and B
	. = (period) no connection

Device Port Configuration

VTDPY displays device port configuration information in a block of tabular data in the DEVICE and STATUS screens only. The information is arranged in a grid with the port numbers listed along the vertical axis and the targets on each port listed along the horizontal axis. The word "Port" is spelled out vertically to denote the port numbers. The screen shows the usage of each port/target combination with a code in the array as shown below. Fields in the information are explained after the example.

```
          Target
               111111
     123456789012345
   P1DDDD Hh
   o2DDDD Hh
   r3DDDD Hh
   t4DDDD Hh
    5DDDD Hh
    6DDDD Hh
```

Table 2–10 Device Map Column Definitions

Column	Contents		
Port	SCSI ports 1 through 6.		
Target	SCSI targets 0 through 15. Single controllers occupy 7; dual-redundant controllers occupy 6 and 7.		
	D	=	disk drive or CD-ROM drive
	F	=	foreign device
	H	=	"this controller"
	h	=	"other controller" in dual-redundant configurations
	P	=	passthrough device
	?	=	unknown device type
		=	(space) no device at this port/target location

Controller/Processor Utilization

VTDPY displays information on policy processor threads using a block of tabular data in the DEFAULT and STATUS screens only. Thread data is located on the left side of both screens (see Figure 2–2 and Figure 2–3) and contains fields described in Table 2–11 and Table 2–12.

Table 2–11 Controller/Processor Utilization Definitions

Column	Contents		
Pr	Thread priority. The higher the number, the higher the priority.		
Name	Thread name. For DUP Local Program threads, use the name in the Name field to invoke the program.		
Stk/Max	Allocated stack size in 512-byte pages. The Max column lists the number of stack pages actually used.		
Typ	Thread type:		
	FNC	=	Functional thread. Those threads that are started when the controller boots and never exits.
	DUP	=	DUP local program threads. Those threads that are only active when run either from a DUP connection or through the command line interpreter RUN command.
	NULL	=	a special type of thread that only executes when no other thread is executable.
Sta	Current thread state:		
	Bl	=	The thread is blocked waiting for timer expiration, resources, or a synchronization event.
	Io	=	A DUP local program is blocked waiting for terminal I/O completion.
	Rn	=	The thread is currently executable.
CPU%	Shows the percentage of execution time credited to each thread since the last screen update. The values might not total 100% due to rounding errors and the fact that there might not be enough room to display all of the threads. An unexpected amount of time can be credited to some threads because the controller firmware architecture allows code from one thread to execute in the context of another thread without a context switch.		

Table 2–12 VTDPY Thread Descriptions

Thread	Description
CLI	A local program that provides an interface to the controller command line interpreter thread.
CLIMAIN	Command line interpreter (CLI).
CONFIG	A local program that locates and adds devices to a configuration.
DILX	A local program that exercises disk devices.
DIRECT	A local program that returns a listing of available local programs.
DS_0	A device error recovery management thread.
DS_1	The thread that handles successful completion of physical device requests.
DS_HB	The thread that manages the device and controller error indicator lights and port reset buttons.
DUART	The console terminal interface thread.
DUP	The DUP protocol thread.
FMTHRD	The thread that performs error log formatting and fault reporting for the controller.
FOC	The thread that manages communication between the controllers in a dual controller configuration.
HP_MAIN	Host port work queue handler. Handles all work from the host port such as new I/O and completion of I/O.
MDATA	The thread that processes metadata for nontransportable disks.
NULL	The process that is scheduled when no other process can be run.
NVFOC	The thread that initiates state change requests for the other controller in a dual controller configuration.
REMOTE	The thread that manages state changes initiated by the other controller in a dual controller configuration.
RMGR	The thread that manages the data buffer pool.
RECON	The thread that rebuilds the parity blocks on RAID 5 storagesets when needed and manages mirrorset copy operations when necessary.
SCS	The SCS directory thread.
TILX	A local program that exercises tape devices.
VA	The thread that provides logical unit services independent of the host protocol.
VTDPY	A local program that provides a dynamic display of controller configuration and performance information.

Host Port Packet Data

VTDPY displays host port packet data in a brief and full formats. Both formats use a block of tabular data in the single screen: the DEFAULT screen provides brief information and the HOST screen provides full information. The data for each format is displayed independently for both host port 1 and 2, and described in Table 2–13.

An example of the *brief* format is displayed as follows:

```
PORT/NODE
Port x NodeID xx
Name xxxxxx
SysId xxxxxxxxxxxx
Path A Pkts Pkts/S
Rcv     0    0
Ack     0    0
Oth     0    0
Path B Pkts Pkts/S
Rcv     0    0
Ack     0    0
Oth     0    0
```

An example of the *full* format is displayed as follows:

```
PORT/NODE
Port x NodeID xx
Name xxxxxx
SysId xxxxxxxxxxxx
Path A Pkts Pkts/S
Rcv     0    0
Ack     0    0
Nak     0    0
Nor     0    0
RNak    0    0
CRC     0    0
CDrop   0    0
Retry   0    0
Path B Pkts Pkts/S
Rcv     0    0
Ack     0    0
Nak     0    0
Nor     0    0
RNak    0    0
CRC     0    0
CDrop   0    0
Retry   0    0

DGD     0    0
Cwait   0    0
```

Table 2–13 Host Port Packet Data Descriptions

Column	Description
Port x	The value of x is either 1 or 2 representing Host Port 1 or 2, respectively.
NodeID xx	The value of xx is the node identifier.
Name	Node name that is up to 6 characters.
SysId	System ID name that is up to 12 characters.
Path A	Activity on Path A of the Port (either 1 or 2) since the last screen update.
Path B	Activity on Path B of the Port (either 1 or 2) since the last screen update.

Table 2–13 Host Port Packet Data Descriptions (Continued)

Column	Description		
Pkts	Number of packets pertaining to Path A or Path B and their processing as follows:		
	Rcv	=	Total number of packets received on this Port/Path since the last screen update.
	Ack	=	Number of packets acknowledged on this Port/Path since the last screen update.
	Nak	=	Number of received packets with Negative Acknowledgment response on this Port/Path since the last screen update.
	Nor	=	Number of transmitted packets having No Response on Transmit on this Port/Path since the last screen update.
	RNak	=	Number of transmitted packets Receiving a Negative Acknowledgment on this Port/Path since the last screen update.
	CRC	=	Number of received packets containing a bad cyclic redundancy check character since the last screen update.
	CDrop	=	Number of receive packet attempts where the carrier signal dropped during the packet reception.
	Retry	=	Number of transmitted packets that went through during a subsequent delayed retry.
	Oth	=	Number of packets whose status resulted in something other than acknowledged on this Port/Path since the last screen update.
Pkts/S	Rate of packet processing in packets per second for Paths A and B. Just as it was for Pkts, the data displayed is also delimited by packets received, packets acknowledged, and other.		
DGD	Number of datagrams discarded and their rate of occurrence since the last screen update.		
Cwait	Number of credit waits and their rate of occurrence since the last screen update.		

Host Port Error Totals

VTDPY displays host port error totals in the host PORT 1 and host PORT 2 detailed statistics screens only. Totals only pertain to the specific host port number screen being displayed. See “Host Port Error Total Fields” section for a description of the fields used to collect the host port error totals.

Table 2–14 Host Port Error Total Fields

Column	Description
RNak	Total number of negative acknowledgments returned on received packets for all virtual circuit nodes on the host port number screen being displayed since the last screen update.
CRC	CRC is the total number of cyclic redundancy check character errors found for all virtual circuit nodes on the host port number screen being displayed since the last screen update.
DGD	DGD is the total number of discarded data grams enacted for all virtual circuit nodes on the host port number screen being displayed since the last screen update.

Host Port Node Statistics

VTDPY displays host port node statistics in two blocks of tabular data in the host PORT 1 and host PORT 2 detailed statistics screens only. These blocks adjoin one another and cover the 32 possible node addresses. The left most block on the screen also presents some port static data shown in the header area. The left portion of the host port statistics subsection is shown first, followed by a representation of the right portion of the host port statistics subsection. The display format is shown below and described in Table 2–15.

```
Port x  CI Node Number xx  SCS Name xxxxxx
             Path A              Path B
Nd  CW  Rcv  Ack  Nak  Nor  Rcv  Ack  Nak  Nor
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
```

Table 2–15 Host Port Node Statistics Descriptions

Column	Description
Port x	The value of x is either 1 or 2 representing Host Port 1 or 2, respectively.
CI Node Number xx	The value of xx is a two-digit Computer Interconnect (CI) node number for the port.
SCS Name	CINode name that is up to 6 characters.
Path A and Path B	Denote the two paths for the Port number being displayed.
Nd	Denotes the node number from 0 through 15 on the left portion of the host port node statistics subsection and 16 through 31 on the right portion of the host port node statistics subsection.
CW	Number of credit waits for the specific node number since the last screen update.
Rcv	Total number of packets received for the specific node and path since the last screen update.
Ack	Number of packets acknowledged for the specific node and path since the last screen update.
Nak	Number of received packets with Negative Acknowledgment response for the specific node and path since the last screen update.
Nor	Number of transmitted packets having No Response on Transmit for the specific node number and path since the last screen update.

Host Port Node Totals

VTDPY displays host port node totals for the Host Port 1 and Host Port 2 detailed STATISTICS screens only. These totals pertain to the 32 virtual circuit nodes shown in the host port node statistics blocks as described in the previous section.

The example below shows the host port node statistics blocks shown virtually as a contiguous list. The host port node totals appear under the host port node statistics subsection.

```
                        Path A                  Path B
            Nd  CW  Rcv  Ack  Nak  Nor   Rcv  Ack  Nak  Nor
            0
            .
            .
            .
           31
          Total   0    0    0    0    0     0    0    0    0
  Port x Total   0    0    0    0    0     0    0    0    0
```

The “Total” line refers to the summation results of each column of the host port being displayed.

The “Port x Total” line refers to the summation results of each column of the host port node statistics for the other host port. Therefore, when this line appears in the Host Port 1 detailed STATISTICS screen, then x would be 2 for the other host port statistics (see Table 2–7).

Disk Inline Exerciser (DILX)

Use DILX to check the data transfer capability of disk drives.

Checking for Disk Drive Problems

DILX generates intense read/write loads to the disk drive while monitoring drive performance and status. Run DILX on as many disk drives as desired, but since this utility creates substantial I/O loads on the controller, Compaq recommends stopping host-based I/O activity during the test.

Finding a Disk Drive in the Subsystem

Use the following steps to find a disk drive or device in the subsystem:

1. Connect a PC or a terminal to the controller maintenance port.
2. Show the devices that are configured on the controller with the following command:

   SHOW UNITS

3. Find the specific device in the enclosure with the following command:

   LOCATE *unit-number*

   This command causes the device LED to blink continuously.

4. Enter the following command to turn off the LED:

   LOCATE CANCEL

Testing the Read Capability of a Disk Drive

Use the following steps to test the read capability of a disk drive:

1. From a host console, dismount the logical unit that contains the disk drive being tested.
2. Connect a terminal to the controller maintenance port that accesses the disk drive being tested.
3. Run DILX with the following command:

   RUN DILX

IMPORTANT: Use the auto-configure option to test the read and write capabilities of every disk drive in the subsystem.

CAUTION: *Do not* exercise passthrough devices using DILX in auto-configure mode. This option might cause tape or optical devices in the subsystem to become unreliable.

4. Enter **N**(o) to decline the auto-configure option and to allow testing of a specific disk drive.
5. Enter **Y**(es) to accept the default test settings and to run the test in read-only mode.
6. Enter the unit number of the specific disk drive to test.

   For example: to test D107, enter the number 107.
7. To test more than one disk drive, enter the appropriate unit numbers when prompted. Otherwise, enter **N**(o) to start the test.

NOTE: Use the control sequences listed in Table 2–16 to control DILX during the test.

Table 2–16 DILX and TILX Control Sequences

Command	Action
Ctrl/C	Stops the test.
Ctrl/G	Displays the performance summary for the current test and continues testing.
Ctrl/Y	Stops the test and exits DILX or TILX.

Testing the Read and Write Capabilities of a Disk Drive

Run a DILX basic function test to test the read and write capability of a disk drive. During the basic function test, DILX runs the following four tests.

NOTE: DILX repeats the last three tests until the time entered in step 6 on page 2-39 expires.

- **Write test.** Writes specific patterns of data to the disk drive (see Table 2–17). DILX does not repeat this test.
- **Random I/O test.** Simulates typical I/O activity by issuing read, write, access, and erase commands to randomly-chosen LBNs. The ratio of these commands can be manually set, as well as the percentage of read and write data that are compared throughout this test. This test takes 6 minutes.

- **Data-transfer test.** Tests throughput by starting at an LBN and transferring data to the next unwritten LBN. This test takes 2 minutes.
- **Seek test.** Stimulates head motion on the disk drive by issuing single-sector erase and access commands. Each I/O uses a different track on each subsequent transfer. The ratio of access and erase commands can be manually set. This test takes 2 minutes.

Table 2–17 Data Patterns for Phase 1: Write Test

Pattern	Pattern in Hexadecimal Numbers
1	0000
2	8B8B
3	3333
4	3091
5	0001, 0003, 0007, 000F, 001F, 003F, 007F, 00FF, 01FF, 03FF, 07FF, 0FFF, 1FFF, 3FFF, 7FFF
6	FIE, FFFC, FFFC, FFFC, FFE0, FFE0, FFE0, FFE0, FE00, FC00, F800, F000, F000, C000, 8000, 0000
7	0000, 0000, 0000, FFFF, FFFF, FFFF, 0000, 0000, FFFF, FFFF, 0000, FFFF, 0000, FFFF, 0000, FFFF
8	B6D9
9	5555, 5555, 5555, AAAA, AAAA, AAAA, 5555, 5555, AAAA, AAAA, 5555, AAAA, 5555, AAAA, 5555, AAAA, 5555
10	DB6C
11	2D2D, 2D2D, 2D2D, D2D2, D2D2, D2D2, 2D2D, 2D2D, D2D2, D2D2, 2D2D, D2D2, 2D2D, D2D2, 2D2D, D2D2
12	DB6D, B6DB, 6DB6, DB6D, B6DB, 6DB6, DB6D, B6DB, 6DB6, DB6D, B6DB, 6DB6, DB6D
13, ripple 1	0001, 0002, 0004, 0008, 0010, 0020, 0040, 0080, 0100, 0200, 0400, 0800, 1000, 2000, 4000, 8000
14, ripple 0	FIE, FFFD, FFFB, FFF7, FFEF, FFDF, FFBF, FF7F, FEFF, FDFF, FBFF, F7FF, EFFF, BFFF, DFFF, 7FFF
15	DB6D, B6DB, 6DB6, DB6D, B6DB, 6DB6, DB6D, B6DB, 6DB6, DB6D, B6DB, 6DB6, DB6D
16	3333, 3333, 3333, 1999, 9999, 9999, B6D9, B6D9, B6D9, B6D9, FFFF, FFFF, 0000, 0000, DB6C, DB6C
17	9999, 1999, 699C, E99C, 9921, 9921, 1921, 699C, 699C, 0747, 0747, 0747, 699C, E99C, 9999, 9999
18	FFFF

Use the following steps to test the read and write capabilities of a specific disk drive:

CAUTION: Running this test on the disk drive will erase all data on the disk. Make sure that the disk drives used do not contain customer data.

1. From a host console, dismount the logical unit that contains the disk drive that needs testing.
2. Connect a terminal to the controller maintenance port that accesses the disk drive being tested.
3. Run DILX with the following command:

   ```
   RUN DILX
   ```

IMPORTANT: Use the auto-configure option to test the read and write capabilities of every disk drive in the subsystem.

CAUTION: *Do not* exercise passthrough devices using DILX in auto-configure mode. This option might cause tape or optical devices in the subsystem to become unreliable.

4. Enter **N**(o) to decline the auto-configure option and to allow testing of a specific disk drive.
5. Enter **N**(o) to decline the default settings.

   NOTE: To ensure that DILX accesses the entire disk space, enter 120 minutes or more in the next step. The default setting is 10 minutes.

6. Enter the number of minutes desired for running the test.
7. Enter the number of minutes between the display of performance summaries.
8. Enter **Y**(es) to include performance statistics in the summary.
9. Enter **Y**(es) to display both hard and soft errors.
10. Enter **Y**(es) to display the hex dump.
11. Press **Enter**/**Return** to accept the hard-error limit default.
12. Press **Enter**/**Return** to accept the soft-error limit default.
13. Press **Enter**/**Return** to accept the queue depth default.

14. Enter **1** to run the basic function test option.
15. Enter **Y**(es) to enable phase 1, the write test.
16. Enter **Y**(es) to accept the default percentage of requests that DILX issues as read requests during phase 2, the random I/O test.

    DILX issues the balance as write requests.
17. Enter **0** to select ALL for the data patterns that DILX issues for write requests.
18. Enter **Y**(es) to perform the initial write pass.
19. Enter **Y**(es) to allow DILX to compare the read and write data.
20. Press **Enter**/**Return** to accept the default percentage of reads and writes that DILX compares.
21. Enter the unit number of the specific disk drive to be tested.

    For example: to test D107, enter the number 107.
22. To test more than one disk drive, enter the appropriate unit numbers when prompted. Otherwise, enter **N**(o) to start the test.

NOTE: Use the command sequences shown in Table 2–16 to control the test.

DILX Error Codes

Table 2–18 explains the error codes that DILX might display during and after testing.

Table 2–18 DILX Error Codes

Error Code	Message and Explanation
1	`Illegal Data Pattern Number found in data pattern header.` Explanation: DILX read data from the disk and discovered that the data did not conform to the pattern that DILX had previously written.
2	`No write buffers correspond to data pattern.` Explanation: DILX read a legal data pattern from the disk, but because no write buffers correspond to the pattern, the data must be considered corrupt.
3	`Read data does not match write buffer.` Explanation: DILX compared the read and write data and discovered that they did not correspond.
4	`Compare host data should have reported a compare error but did not.` Explanation: A compare host data compare was issued in a way that DILX expected to receive a compare error, but no error was received.

Tape Inline Exerciser (TILX)

Use TILX to check the data-transfer capability of tape devices.

Checking for Tape Device Problems

TILX generates intense read/write loads to the tape device while monitoring tape performance and status. Run TILX on as many tape devices as desired, but since this utility creates substantial I/O loads on the controller, Compaq recommends stopping host-based I/O activity during the test.

Finding a Tape Device in the Subsystem

Use the following steps to find a tape device in the subsystem:

1. Connect a PC or a terminal to the controller maintenance port.
2. Show the tapes that are configured on the controller with the following command:

   SHOW TAPES

3. Find the specific tape device in the enclosure with the following command:

   LOCATE *unit-number*

   This command causes the device LED to blink continuously.

4. Enter the following command to turn off the LED:

   LOCATE CANCEL

Testing the Read Capability of a Tape Device

Use the following steps to test the read capability of a tape device:

1. From a host console, dismount the logical unit that contains the tape device being tested.
2. Connect a terminal to the controller maintenance port that accesses the tape device being tested.
3. Run TILX with the following command:

   RUN TILX

4. Enter **Y**(es) to accept the default test settings.

5. Enter the unit number of the specific tape device to test.

   For example: to test T107, enter the number 107.

6. Enter **Y**(es) after making sure a tape cartridge is loaded in the tape device being tested.

7. To test more than one tape device, enter the appropriate unit numbers when prompted. Otherwise, enter **N**(o) to start the test.

   NOTE: Use the control sequences listed in Table 2–16 to control TILX during the test.
   TILX will run for 10 minutes and then display the results of the testing.

Testing the Read and Write Capabilities of a Tape Device

Run a TILX basic function test to test the read and write capability of a tape device. During the basic function test, TILX runs the following tests.

Specific patterns of data are written to the tape during the write pass (see Table 2–19). The write pass executes in two phases:

- Data intensive — The first one third of the specified number of records are written as 16 KB records. With this high byte count and the default queue depth, this phase should test the streaming capability (if supported) of the tape unit.
- Random — The remaining two thirds of the records are written in random byte counts. The command sequence is *write*, *reposition back one record*, *read*, and is repeated three times. Tape mark is intermixed in the test.

The read pass consists of three phases:

- Data intensive — Read operations of fixed record sizes with a byte count equal to the expected tape record size. Forward position commands are issued when tape marks are encountered.
- Random — Begins at the point where random-sized records were written to the tape. Most read operations are issued with a byte count equal to the expected tape record byte count. Occasionally, read operations are intermixed with a byte count less than or greater than the expected record byte count. Forward position commands are issued when tape marks are encountered.
- Position intensive — Begins halfway down from the start of the area where random-sized records are located. Read operations and position commands are intermixed so that the test gradually proceeds toward the end-of-tape (EOT). Forward position commands are issued when tape marks are encountered.

In all phases, if EOT is detected, the tape is rewound to the beginning-of-tape (BOT) and the write pass starts again.

Table 2–19 Data Patterns for Write Pass

Pattern	Pattern in Hexadecimal Numbers
1	0000
2	8B8B
3	3333
4	3091
5	0001, 0003, 0007, 000F, 001F, 003F, 007F, 00FF, 01FF, 03FF, 07FF, 0FFF, 1FFF, 3FFF, 7FFF
6	FIE, FFFC, FFFC, FFFC, FFE0, FFE0, FFE0, FFE0, FE00, FC00, F800, F000, F000, C000, 8000, 0000
7	0000, 0000, 0000, FFFF, FFFF, FFFF, 0000, 0000, FFFF, FFFF, 0000, FFFF, 0000, FFFF, 0000, FFFF
8	B6D9
9	5555, 5555, 5555, AAAA, AAAA, AAAA, 5555, 5555, AAAA, AAAA, 5555, AAAA, 5555, AAAA, 5555, AAAA, 5555
10	DB6C
11	2D2D, 2D2D, 2D2D, D2D2, D2D2, D2D2, 2D2D, 2D2D, D2D2, D2D2, 2D2D, D2D2, 2D2D, D2D2, 2D2D, D2D2
12	DB6D, B6DB, 6DB6, DB6D, B6DB, 6DB6, DB6D, B6DB, 6DB6, DB6D, B6DB, 6DB6, DB6D
13, ripple 1	0001, 0002, 0004, 0008, 0010, 0020, 0040, 0080, 0100, 0200, 0400, 0800, 1000, 2000, 4000, 8000
14, ripple 0	FIE, FFFD, FFFB, FFF7, FFEF, FFDF, FFBF, FF7F, FEFF, FDFF, FBFF, F7FF, EFFF, BFFF, DFFF, 7FFF
15	DB6D, B6DB, 6DB6, DB6D, B6DB, 6DB6, DB6D, B6DB, 6DB6, DB6D, B6DB, 6DB6, DB6D
16	3333, 3333, 3333, 1999, 9999, 9999, B6D9, B6D9, B6D9, B6D9, FFFF, FFFF, 0000, 0000, DB6C, DB6C
17	9999, 1999, 699C, E99C, 9921, 9921, 1921, 699C, 699C, 0747, 0747, 0747, 699C, E99C, 9999, 9999
18	FFFF

Use the following steps to test the read and write capabilities of a specific tape device:

CAUTION: Running this test on the tape drive will erase all data on the tape. Make sure that the tape drives used do not contain customer data.

1. From a host console, dismount the logical unit that contains the tape device that needs testing.
2. Connect a terminal to the controller maintenance port that accesses the tape device being tested.
3. Run TILX with the following command:

```
RUN TILX
```

4. Enter **N**(o) to decline the default settings.

   NOTE: To ensure that TILX accesses the entire tape space, enter 120 minutes or more in the next step. The default setting is 10 minutes.

5. Enter the number of minutes desired for running the test.
6. Enter the number of minutes between the display of performance summaries.
7. Enter **Y**(es) to include performance statistics in the summary.
8. Enter **Y**(es) to display both hard and soft errors.
9. Enter **Y**(es) to display the hex dump.
10. Press **Enter**/**Return** to accept the hard-error limit default.
11. Press **Enter**/**Return** to accept the soft-error limit default.
12. Press **Enter**/**Return** to accept the default for maximum number of outstanding I/Os for each unit.
13. Enter **N**(o) to suppress caching.
14. Enter **1** to run the basic function test option.
15. Enter **0** to select ALL for the data patterns that TILX issues for write requests.
16. Press **Enter**/**Return** to accept the default for the number of records to be written/read during the test.
17. Enter **Y**(es) to allow TILX to compare the read and write data.
18. Press **Enter**/**Return** to accept the default percentage of reads and writes that TILX compares.
19. Enter the unit number of the specific tape device to be tested.

    For example: to test T107, enter the number 107.

20. Enter **Y**(es) after making sure a tape cartridge is loaded in the tape device being tested.
21. To test more than one tape device, enter the appropriate unit numbers when prompted. Otherwise, enter **N**(o) to start the test.

    NOTE: Use the control sequences listed in Table 2–16 to control the test.

TILX Error Codes

Table 2–20 explains the error codes that TILX might display during and after testing.

Table 2–20 TILX Error Codes

Error Code	Message and Explanation
1	`Illegal Data Pattern Number found in data pattern header.` TILX read data from the tape and discovered that the data did not conform to the pattern that TILX had previously written.
2	`No write buffers correspond to data pattern.` Explanation: TILX read a legal data pattern from the tape, but because no write buffers correspond to the pattern, the data must be considered corrupt.
3	`Read data does not match write buffer.` Explanation: TILX compared the read and write data and discovered that they did not correspond.
4	`TILX/TAPE record size mismatch.` Explanation: The size of the record that TILX read from the tape did not match the size of the record that was written on the previous write pass.
5	`A tape mark was detected in a place where it was not expected.` Explanation: TILX encountered a tape mark where a mark was not expected. The tape device might not be able to accurately position the tape.
6	`Record data truncated but not received.` Explanation: TILX issued a read with a byte count less than what was written to the current tape record and expects to receive a Record Data Truncated status. If TILX does not receive the Record Data Truncated status when expected, an error is reported. This error can only be detected on a read pass.
7	`EOT encountered in unexpected position.` Explanation: The end-of-tape (EOT) was reached before expected by TILX. The tape device might not be able to accurately position the tape.

Format and Device Code Load Utility (HSUTIL)

Use the HSUTIL utility to upgrade the firmware on disk drives and tape drives in the subsystem and to format disk drives. While formatting disk drives or installing new firmware, HSUTIL might produce one or more of the messages shown in Table 2–21 (many of the self-explanatory messages have been omitted from the table).

Table 2–21 HSUTIL Messages and Inquiries

Message	Description
Insufficient resources.	HSUTIL cannot find or perform the operation because internal controller resources are not available.
Unable to change operation mode to maintenance for unit.	HSUTIL was unable to put the source single-disk drive unit into maintenance mode to enable formatting or code load.
Unit successfully allocated.	HSUTIL has allocated the single-disk drive unit for code load operation. At this point, the unit and the associated device are not available for other subsystem operations.
Unable to allocate unit.	HSUTIL could not allocate the single-disk drive unit. An accompanying message explains the reason.
Unit is owned by another sysop.	Device cannot be allocated because the device is being used by another subsystem function or local program.
Unit is in maintenance mode.	Device cannot be formatted or code loaded because the device is being used by another subsystem function or local program.
Exclusive access is declared for unit.	Another subsystem function has reserved the unit shown.
The other controller has exclusive access declared for unit.	The companion controller has locked out this controller from accessing the unit shown.
The RUNSTOP_SWITCH is set to RUN_DISABLED for unit.	The RUN\NORUN unit indicator for the unit shown is set to NORUN; the disk cannot spin up.
What BUFFER SIZE (in BYTES), does the drive require (2048, 4096, 8192) [8192]?	HSUTIL detects that an unsupported device has been selected as the target device and the firmware image requires multiple SCSI Write Buffer commands. Specify the number of bytes to be sent in each Write Buffer command. The default buffer size is 8192 bytes. A firmware image of 256 K, for example, can be code loaded in 32 Write Buffer commands, each transferring 8192 bytes.
What is the TOTAL SIZE of the code image in BYTES [*device default*]?	HSUTIL detects that an unsupported device has been selected as the target device. Enter the total number of bytes of data to be sent in the code load operation.

Table 2–21 HSUTIL Messages and Inquiries (Continued)

Message	Description
Does the target device support only the download microcode and save?	HSUTIL detects that an unsupported device has been selected as the target device. Specify whether the device supports the SCSI Write Buffer command download and save function.
Should the code be downloaded with a single write buffer command?	HSUTIL detects that an unsupported device has been selected as the target device. Indicate whether to download the firmware image to the device in one or more contiguous blocks, each corresponding to one SCSI Write Buffer command.

Configuration (CONFIG) Utility

Use the CONFIG utility to add one or more storage devices to the subsystem. This utility checks the device ports for new disk drives or tape drives, adds them to the controller configuration, and automatically names them. Refer to the controller installation and configuration guide for more information about using the CONFIG utility.

NOTE: Do not run the CONFIG utility during a tape backup or copy operation.

Code Load and Code Patch (CLCP) Utility

Use the CLCP utility to upgrade the controller software. Also use CLCP to patch the controller software. To successfully install a new controller, the correct (or current) software version and patch numbers must be available. See the controller maintenance and service guide for more information about using this utility during a replacement or upgrade process.

Clone (CLONE) Utility

Use the CLONE utility to duplicate the data on any unpartitioned single-disk unit, stripeset, mirrorset, or striped mirrorset. Back up the cloned data while the actual storageset remains online. When the cloning operation is done, back up the clones rather than the storageset or single-disk unit, which can continue to service the I/O load. When cloning a mirrorset, the CLONE utility does not need to create a temporary mirrorset. Instead, the CLONE utility adds a temporary member to the mirrorset and copies the data onto this new member.

The CLONE utility creates a temporary, two-member mirrorset for each member in a single-disk unit or stripeset. Each temporary mirrorset contains one disk drive from the unit being cloned and one disk drive onto which the CLONE utility copies the data. During the copy operation, the unit remains online and active so the clones contain the most up-to-date data.

After the CLONE utility copies the data from the members to the clones, the CLONE utility restores the unit to the original configuration and creates a clone unit for backup purposes.

Field Replacement Utility (FRUTIL)

Use FRUTIL to replace a failed controller, cache module, or ECB, in a dual-redundant controller configuration, without shutting down the subsystem. See the controller maintenance and service guide for a more detailed explanation on how FRUTIL is used during the replacement process.

Change Volume Serial Number (CHVSN) Utility

The CHVSN utility generates a new volume serial number (called VSN) for the specified device and writes the VSN on the media. The CHVSN utility is used to eliminate duplicate volume serial numbers and to rename duplicates with different volume serial numbers.

NOTE: Only Compaq authorized service providers can use this utility.

Chapter 3

Event Reporting Templates

This chapter describes the event codes that the fault management software provides for spontaneous events and last failure events.

The HSJ80 controller uses various codes to report different types of events, and these codes are presented in template displays. Instance codes are unique codes that identify events, additional sense code (ASC) and additional sense code qualifier (ASCQ) codes explain the cause of the events, and last failure codes describe unrecoverable conditions that might occur with the controller.

> **NOTE:** The error log messages in this chapter are used for all Compaq StorageWorks controller devices; therefore, some of the events reported in this chapter might not be applicable to the HSJ80 controller.

The HSJ80 controller reports events that occur during normal operation in specific mass storage control protocol (MSCP) and/or tape mass storage control protocol (TMSCP) error log message formats.

The following is a list of events that are reported in the error log message formats:

- Controller errors
- Memory errors
- Disk transfer errors
- Bad block replacement attempts
- Tape errors
- Media loader errors
- Disk copy data correlation

Implementation-Dependent Areas of Event Logs

All of the error log message formats (except Disk Copy Data Correlation Error Log message format) provide an implementation-dependent information area positioned at the end of the error log message.

The HSJ80 controller implementation-dependent information area is shown in Table 3–1 and the various fields are described in Table 3–2.

Table 3–1 Implementation-Dependent Information Format

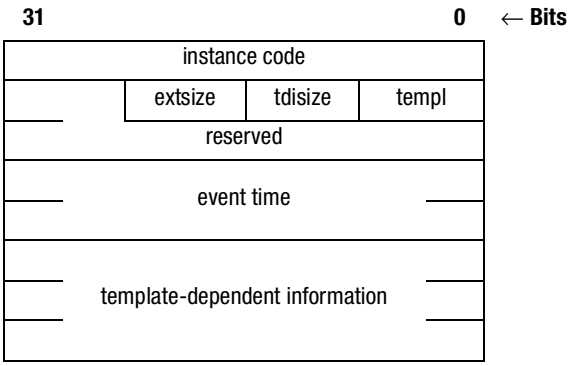


Table 3–2 Implementation-Dependent Format Description

Field	Description
instance code	A number that uniquely identifies the event being reported. See Chapter 5 for the field format and a complete list of Instance Codes.
templ	A two-digit number that uniquely describes the format of the template-dependent information field. These templates are described later in this chapter.
tdisize	The number of bytes contained in the template-dependent information field.
extsize	The number of bytes contained in any extension to the template-dependent information field. This field is only defined for those template formats that define an extension to the template-dependent information field. For all other template formats, this field is shown as “reserved.”
reserved	Reserved for future use; currently set to zero.

Table 3–2 Implementation-Dependent Format Description (Continued)

Field	Description
event time	The time the event occurred according to the power-on time value maintained by the controller operational software. The time expended during controller restarts, power-on diagnostics, and system initialization is not accounted for by this value.
template-dependent information	Information specific to the type of event being reported. Size and format are specific to the template specified by the templ field.

Common Event Log Fields

Several of the software components listed in the Component ID Codes table (see Chapter 4) share common event log fields. The following sections list the software components and the common fields each shares.

Host Interconnect Services Common Fields

Fields common to certain event logs generated by the Host Interconnect Services (HIS) are shown in Table 3–3.

Table 3–3 HIS Common Fields (Sheet 1 of 4)

Field	Description		
HIS status	HIS status code		
	00000000	=	Request succeeded.
	00000001	=	The remote sent a message over a connection that has been invalidated.
	00000002	=	The remote sent a message for which no receive credit is available.
	00000003	=	Received a message from the remote while in an invalid or illegal connection state.
	00000004	=	Pending work exists but connection state is invalid or illegal.
	00000009	=	Request failed, no additional information available.
	00000032	=	A port to port dirver (PPD) message was received from the remote but the Virtual Circuit is in an invalid or illegal state.
	00000033	=	A PPD START was received from the remote but the Virtual Circuit state indicates that the Virual Circuit is already OPEN.
	00000034	=	A PPD NODE_STOP was received from the remote.

Table 3–3 HIS Common Fields (Sheet 2 of 4)

Field			Description
	00000035	=	The “PPD START send without receiving a PPD START in response” limit has been reached; the remote node is acknowledging the packets but not responding to them.
	00000036	=	The “PPD STACK send without receiving a PPD ACK in response” limit has been reached; the remote node is acknowledging the packets but not responding to them.
	00000064	=	The “CI IDREQ send without receiving a CI ID in response” limit has been reached on Path A and Path B; the remote node is acknowledging the packets but not responding to them.
	00000065	=	A CI ID or CI CNF packet (transmitted by the thread on behalf of Host Interconnect Services) could not be successfully transmitted.
	00010009	=	Virtual circuit (VC) closed due to CI ID request failure.
	00020009	=	VC closed due to unexpected SCS state.
	00030009	=	VC closed due to CI START failure.
	00040009	=	VC closed due to CI STACK failure.
	00050009	=	VC closed due to PPD ACK failure.
	00060009	=	PPD START NODE_STOP or PPD START message received.
	00070009	=	VC closed due to NAK ADP retry CI ID transmit failure.
	00080009	=	VC closed due to NAK ADP retry transmit failure.
	00090009	=	VC closed due to NOR DDL retry transmit failure on Path A.
	000A0009	=	VC closed due to NOR DDL retry transmit failure on Path B.
	000B0009	=	VC closed due to NOR ADP retry CI ID transmit failure.
	000C0009	=	VC closed due to NOR ADP retry transmit failure.
	000D0009	=	VC closed due to NAK DDL retry transmit failure on Path A.
	000E0009	=	VC closed due to NAK DDL retry transmit failure on Path B.
	000F0009	=	VC closed due to arbitration timeout on Path A.
	00100009	=	VC closed due to arbitration timeout on Path B.
	00110009	=	VC closed due to Path A off.
	00120009	=	VC closed due to Path B off.
	00130009	=	VC closed due to dual receive.
	00140009	=	VC closed due to invalid receive data structure state.
	00150009	=	VC closed due to no path.
	00160009	=	VC closed due to message transmit closed.
	00170009	=	VC closed due to data transmit closed.

Table 3–3 HIS Common Fields (Sheet 3 of 4)

Field	Description		
	00180009	=	VC closed due to message scan.
	00190009	=	VC closed due to data scan.
	001A0009	=	VC closed due to data timeout.
	001B0009	=	VC closed due to unrecognized packet.
	001C0009	=	VC closed due to data transmit failure.
	001D0009	=	VC closed due to CI ID complete failure.
	001E0009	=	VC closed due to lost command.
	001F0009	=	Not implemented in CI environment.
	00200009	=	VC closed due to sequence number mismatch.
	00210009	=	VC closed due to receipt of a message with no receive credit.
	00220009	=	VC closed due to receipt of a message with no receive credit.
	00230009	=	VC closed due to an invalid connection state.
	00240009	=	VC closed due to an invalid connection state.
	00250009	=	VC closed due to a mismatched connection identifier.
	00260009	=	VC closed due to a parity error receiving a packet.
	00270009	=	VC closed due to receiving a PPD START packet.
	00280009	=	VC closed due to receiving a PPD STOP packet.
	00290009	=	VC close while recovering from a hardware overrun error.
	002A0009	=	VC close while recovering from a hardware overrun error.
error id	The address of the HIS routine that detected the event.		
src	CI source node address		
dst	CI destination node address		

Table 3–3 HIS Common Fields (Sheet 4 of 4)

Field	Description					
intopcd	CI message operation code					
	00	=	Reserved	0A	=	DATREQ2
	01	=	DG	0B	=	ID
	02	=	MSG	0C	=	PSREQ
	03	=	CNF	0D	=	LB
	04	=	MCNF	0E	=	MDATREQ
	05	=	IDREQ	0F	=	RETPS
	06	=	RST	10	=	SNTDAT
	07	=	STRT	11	=	RETDAT
	08	=	DATREQ0	12	=	SNTMDAT
	09	=	DATREQ1	13	=	RETMDAT
vcstate	VC state code. The setting of bit 7 in this field indicates the state of ID polling for the virtual circuit. If bit 7 is set, ID polling is complete. Otherwise, ID polling is incomplete.					
	01	=	VC_CLOSED	04	=	VC_OPEN
	02	=	START_SENT	05	=	VC_CLOSING
	03	=	START_REC			
ppd opcode	Port/port driver layer operation oode					
	0000	=	START	0004	=	SCS_MSG
	0001	=	STACK	0005	=	ERROR_LOG
	0002	=	ACK	0006	=	NODE_STOP
	0003	=	SCS_DG			
scs opcode	System communication services layer operation code					
	0000	=	CONNECT_REQ	0006	=	DISCONNECT_REQ
	0001	=	CONNECT_RSP	0007	=	DISCONNECT_RSP
	0002	=	ACCEPT_REQ	0008	=	CREDIT_REQ
	0003	=	ACCEPT_RSP	0009	=	CREDIT_RSP
	0004	=	REJECT_REQ	000A	=	APPL_MSG
	0005	=	REJECT_RSP	000B	=	APPL_DG

Disk/Tape MSCP Server, CI Host Interconnect, Device and Value-Added Services Common Fields

These services share the common Host/Server Connection Common fields, which include:

- connection id—Identifies the host/server connection associated with the event being reported. A zero value indicates the host/server connection was invalidated before the event could be reported.
- remote node name—An 6-byte ASCII string representing the node name associated with the host/server connection identified in the "connection id" field. A zero value indicates the content of this field is undefined.

Device and Value Added Services Common Fields

These services share the common Byte Count/Logical Block Number common fields as shown in Table 3–4.

Table 3–4 Device and Value Added Services Common Fields

Field	Description		
Byte Count/Logical Block Number	Common fields include:		
	byte count	Number of bytes of the HSJ80 controller software component initiated transfer successfully transferred.	
	logical block number	Starting logical block number of the HSJ80 controller software component initiated transfer.	
Device Location/Identification	Common fields include:		
	device locator	The location within the HSJ80 controller subsystem of the target device involved in the event being reported. A value of FF in any of these fields indicates that the information is not available. This field has the format of Port-Target-LUN:	
		Port	The SCSI bus number to which the target device is connected.
		Target	The SCSI target number on the port to which the target device is connected.
		LUN	The logical unit number on the target by which the target device is logically addressed.

Table 3–4 Device and Value Added Services Common Fields (Continued)

Field		Description	
	devtype	The SCSI device type of the device. If the device type information is unavailable or not applicable, this field contains the value 1F or FF. Supported SCSI device type codes include:	
		00	Direct-Access devices, such as magnetic disks.
		01	Sequential-Access devices, such as magnetic tapes.
		05	CD-ROM devices.
		07	Optical Memory devices, such as some optical disks.
		08	Medium Changer devices, such as jukeboxes.
		0C	Controller pass-through devices, which are actually not defined by the SCSI specification.
	device identification	Contains 16 bytes of ASCII data as defined by the device vendor in the Product Identification field of the SCSI INQUIRY command data. The most significant character of the product identification data appears in the low-order byte of the first longword of this field. The least significant character appears in the high-order byte of the last long word of this field. For unknown or inapplicable product information, this field is filled with ASCII spaces.	
	device serial number	Contains eight bytes of data as defined by the device vendor in the Product Serial Number field of the SCSI Unit Serial Number Page data. The most significant character of the serial number data appears in the low-order byte of the first longword of this field. The least significant character appears in the high-order byte of the last long word of this field. The number of characters of serial number data supplied varies from vendor-to-vendor and from device-to-device. If the serial number data is:	
		Less than eight characters—The field is filled with ASCII spaces from the low-order byte containing a serial number character through the high-order byte of the last longword.	
		Greater than eight characters—The serial number data is truncated at eight bytes so that the least-significant character(s) of the serial number data are lost.	
		Unavailable or inapplicable—This field is filled with ASCII spaces.	

Device Services and Value Added Services Common Fields

The Device Services and Value Added Services software components also share common SCSI Device Sense Data fields (see Table 3–5).

Table 3–5 Device Service and Value Added Services Common Fields

Field	Description
cmdopcd	This field is supplied by the HSJ80 controller to provide qualifying information required to interpret the other SCSI Sense Data Common fields in the report. The operation code of the SCSI command issued to the target device. SCSI command operation codes vary according to device type, so the content of this field depends on the content of the devtype field.
sdqual	This field is supplied by the HSJ80 controller to provide qualifying information required to interpret the other SCSI Sense Data Common fields in the report. The field contains information necessary to determine whether the Sense Data contained in the ercdval through keyspec fields is either supplied by an attached device or generated by the controller, and to qualify the content of the info field.
ercdval, segment, snsflgs, info, addsnsl, cmdspec, asc, ascq, frucode, and keyspec	These fields are part of the template-dependent information field and contain the Standard Sense Data; the first 18 bytes of the SCSI REQUEST SENSE command response.
frucode	Depending on the information in the other fields, this field identifies the field replacable unit that has failed.
additional sense bytes	This field is an extension of the template-dependent information field and varies in size depending on the device and/or the event being reported. This field contains the additional Sense Bytes field of the SCSI REQUEST SENSE command response only if the device supplies that information.

Specific Event Log Formats

This section contains examples of specific event log formats. Theses formats are described in this guide as "templates." Within these template examples are fields that contain codes which help you to determine the condition that was detected by the software or hardware.

The 15 event logs (14 templates) described in this section, to include:

- Template 01—Last Failure Event Log Format, Table 3–6 on page 3–12
- Template 05—Failover Event Log Format, Table 3–8 on page 3–15
- Template 11—Nonvolatile Parameter Memory Component Event Log Format, Table 3–10 on page 3–17
- Template 12—Backup Battery Failure Event Log Format, Table 3–12 on page 3–19
- Template 13—Subsystem Built-In Self Test Failure Event Log Format, Table 3–14 on page 3–22
- Template 14—Memory System Failure Event Log Format, Table 3–16 on page 3–24
- Template 32—CI Port/Port Driver Event Log Format, Table 3–18 on page 3–28
- Template 33—CI System Communication Services Event Log Format, Table 3–20 on page 3–31
- Template 34—CI HSJ80 Host Port Error Log Format, Table 3–23 on page 3–34
- Template 41—Device Services Non-Transfer Error Event Log Format, Table 3–25 on page 3–36
- Template 51—Disk Transfer Error Event Log Format, Table 3–27 on page 3–38
- Template 57—Disk Bad Block Replacement Attempt Event Log Format, Table 3–29 on page 3–44
- Template 61—Tape Transfer Error Event Log Format, Table 3–31 on page 3–46
- Template 71—Media Loader Error Event Log Format, Table 3–33 on page 3–50
- Disk Copy Data Correlation Event Log on page 3–54

These templates contain three basic code types:

- ASC and ASCQ Codes—codes that explain the cause of the event (see Chapter 4).
- Instance Codes—codes that identify events (see Chapter 5).
- Last Failure Codes—codes detailing unrecoverable conditions that might occur with the controller (see Chapter 6).

Last Failure Event Logs (Template 01)

Unrecoverable conditions (detected by either software or hardware) and certain operator-initiated conditions that result in the termination of HSJ80 array controller operation. In most cases, following such a termination, the controller attempts to restart with hardware components and software data structures initialized to the states necessary to perform normal operations. If the restart was successful and communications were re-established with the host systems and “Miscellaneous” error logging was enabled by one or more host systems, the controller sends a Last Failure Event Log that describes the condition that caused the controller operation to halt. This log is sent to all hosts that enabled “Miscellaneous” error logging on connections established with the controller Disk and/or Tape MSCP Server. The Last Failure Event Log is reported via the TMSCP/MSCP Controller Errors error log message format.

Template 01 is shown in Table 3–6 and template formats are described in Table 3–7.

Table 3–6 Template 01—Last Failure Event Log Format

31		0	← Bit / ↓ Offset
command reference number			0
sequence number	reserved		4
event code	flags	format	8
controller identifier			0C
			10
reserved	chvrsn	csvrsn	14
instance code			18
	tdisize	templ	1C
reserved			20
event time			24
			28
last failure code			2C
last failure parameters			30
			34
			38
			3C
			40
			44
			48
			4C

Table 3–7 Template 01—Selected Last Failure Event Log Field Descriptions

Field	Description
reserved	Offsets 16 and 1E. These fields contain the value 0.
event code	This field contains an MSCP code and instance code for this event log.
format	This field contains the value 00, which is the TMSCP/MSCP Controller Errors error log format code.
instance code	See Chapter 5 for a description of the Instance Codes.
tdisize	The number of bytes contained in the template-dependent information field. For this event log the value is 24.
templ	A number that uniquely describes the format of the template-dependent information field. For this (last failure) event log the value is 01.
event time	The time the event occurred according to the power-on time value maintained by the controller operational software. The time expended during controller restarts, power-on diagnostics, and system initialization is not accounted for by this value.
last failure code	See Chapter 6 for a description of the Last Failure Codes.
last failure parameters	This field contains supplemental information specific to the failure being reported.

Failover Event Log (Template 05)

The controller Failover Control software component reports errors and other conditions encountered during redundant controller communications and failover operations via the Failover Event Log. This log is sent to all hosts that enabled “Miscellaneous” error logging on connections established with the controller Disk and/or Tape MSCP Server. The Failover Event log is reported via the TMSCP/MSCP Controller Errors error log message format. The format is identical to the Last Failure Event log format but the values in the fields are different.

Template 05 is shown in Table 3–8 and template formats are described in Table 3–9.

Table 3–8 Template 05—Failover Event Log Format

31		0	← Bit / ↓ Offset
command reference number			0
sequence number	reserved		4
event code	flags	format	8
controller identifier			0C
			10
reserved	chvrsn	csvrsn	14
instance code			18
	tdisize	templ	1C
reserved			20
event time			24
			28
last failure code			2C
last failure parameters			30
			34
			38
			3C
			40
			44
			48
			4C

Table 3–9 Template 05—Selected Failover Event Log Field Descriptions

Field	Description
format	This field contains the value 00, which is the TMSCP/MSCP Controller Errors error log format code.
event code	This field contains an MSCP code and instance code for this event log.
reserved	Offsets 16 and 1E. These fields contain the value 0.
instance code	See Chapter 5 for a description of the Instance Codes.
templ	A number that uniquely describes the format of the template-dependent information field. For this event log the value is 05.
tdisize	The number of bytes contained in the template-dependent information field. For this event log the value is 24.
event time	The time the event occurred according to the power-on time value maintained by the controller operational software. The time expended during controller restarts, power-on diagnostics, and system initialization is not accounted for by this value.
last failure code and last failure parameters	These fields contain the last failure information supplied in the last gasp message sent by the other HSJ80 controller in a dual-redundant configuration as a normal part of terminating controller operation. See Chapter 6 for a description of the Last Failure Codes.

NOTE: The content of certain fields in Template 05 might be undefined depending on the value supplied in the “instance code” field. Refer to Chapter 5 to see what fields are left undefined for certain Instance Codes.

Nonvolatile Parameter Memory Component Event Log (Template 11)

The controller Executive software component reports errors detected while accessing a Nonvolatile Parameter Memory Component via the Nonvolatile Parameter Memory Component Event Log. This log is sent to all hosts that enabled "Miscellaneous" error logging on connections established with the controller Disk and/or Tape MSCP Server. The Nonvolatile Parameter Memory Component Event log is reported via the TMSCP/MSCP Controller Errors error log message format.

Template 11 is shown in Table 3–10 and template formats are described in Table 3–11.

Table 3–10 Template 11—Nonvolatile Parameter Memory Component Event Log Format

31 — 0	← Bit / ↓ Offset
command reference number	0
sequence number / reserved	4
event code / flags / format	8
controller identifier	0C
	10
reserved / chvrsn / csvrsn	14
memory address	18
instance code	1C
tdisize / templ	20
reserved	24
event time	28
	2C
byte count	30
undef / number of times written	34

Table 3–11 Template 11—Selected Nonvolatile Parameter Memory Component Event Log Field Descriptions

Field	Description
format	This field contains the value 01, which is the TMSCP/MSCP Memory Errors error log format code.
event code	This field contains an MSCP code and instance code for this event log.
memory address	The physical address of the beginning of the affected Nonvolatile Parameter Memory component area.
instance code	See Chapter 5 for a description of the Instance Codes.
templ	A number that uniquely describes the format of the template-dependent information field. For this event log the value is 11.
tdisize	The number of bytes contained in the template-dependent information field. For this event log the value is 08.
reserved	Offset 22. This field contains the value 0.
event time	The time the event occurred according to the power-on time value maintained by the controller operational software. The time expended during controller restarts, power-on diagnostics, and system initialization is not accounted for by this value.
byte count	The number of bytes contained in the affected Nonvolatile Parameter Memory component area. That is, the area bounded by “memory address” through “memory address” + “byte count”- 1.
number of times written	The number of times the Nonvolatile Parameter Memory component area has been written.
undef	This field is only present to provide longword alignment. Content is undefined.

Backup Battery Failure Event Log (Template 12)

The controller Value Added Services software component reports backup battery failure conditions for hardware components that use a battery to maintain state during power failures. This is accomplished with the Backup Battery Failure Event Log. This log is sent to all hosts that enabled “Miscellaneous” error logging on connections established with the controller Disk and/or Tape MSCP Server. The Backup Battery Failure Event Log is reported via the TMSCP/MSCP Memory Errors error log message format.

Template 12 is shown in Table 3–12 and template formats are described in Table 3–13.

Table 3–12 Template 12—Backup Battery Failure Event Log Format

31		0	← Bit / ↓ Offset
command reference number			0
sequence number	reserved		4
event code	flags	format	8
controller identifier			0C
			10
reserved	chvrsn	csvrsn	14
memory address			18
instance code			1C
	tdisize	templ	20
reserved			24
event time			28
			2C

Table 3–13 Template 12—Selected Backup Battery Failure Event Log Field Descriptions

Code	Description
format	This field contains the value of 01, which is the TMSCP/MSCP Memory Errors error log format code.
event code	This field contains an MSCP code and instance code for this specific event log.
memory address	The contents of this field depend on the value in the instance code field.
instance code	See Chapter 5 for instance code values.
templ	A number that uniquely describes the format of the template-dependent information field. For this event log the value is 12.
tdisize	The number of bytes contained in the template-dependent information field. For this event log the value is 00.
reserved	Offset 22. This field contains the value 0.
event time	The time the event occurred according to the power-on time value maintained by the controller operational software. The time expended during controller restarts, power-on diagnostics, and system initialization is not accounted for by this value.

Subsystem Built-In Self Test Failure Event Log (Template13)

The controller Subsystem Built-In Self Test software component reports errors detected during test execution via the Subsystem Built-In Self Test Failure Event Log. This log is sent to all hosts that enabled “Miscellaneous” error logging on connections established with the controller Disk and/or Tape MSCP Server. The Subsystem Built-In Self Test Failure Event log is reported via the TMSCP/MSCP Controller Errors error log message format.

Template 13 is shown in Table 3–14 and template formats are described in Table 3–15.

Table 3–14 Template 13—Subsystem Built-In Self Test Failure Event Log Format

31			0	← Bit / ↓ Offset
command reference number				0
sequence number		reserved		4
event code		flags	format	8
controller identifier				0C
				10
reserved		chvrsn	csvrsn	14
instance code				18
		tdisize	templ	1C
reserved				20
event time				24
				28
hdrflgs	hdrtype	undefined		2C
tflags	tcmd	tnum	te	30
return code		error code		34
address of error				38
expected error data				3C
actual error data				40
extra status 1				44
extra status 2				48
extra status 3				4C

Table 3–15 Template 13—Selected Subsystem Built-In Self Test Failure Event Log Field Descriptions

Field	Description
format	This field contains the value 00, which is the TMSCP/MSCP Controller Errors error log format code.
event code	This field contains an MSCP code and instance code for this event log.
reserved	Offsets 16 and 1E. These fields contain the value 0.
instance code	See Chapter 5 for a description of the Instance Codes.
templ	A number that uniquely describes the format of the template-dependent information field. For this event log the value is 13.
tdisize	The number of bytes contained in the template-dependent information field. For this event log the value is 24.
event time	The time the event occurred according to the power-on time value maintained by the controller operational software. The time expended during controller restarts, power-on diagnostics, and system initialization is not accounted for by this value.
undefined	This field is only present to provide longword alignment. Content is undefined.

The content of the remaining fields in the Subsystem Built-In Self Test Failure Event Log, shown in the following list, vary depending on which controller Subsystem Built-In Self Test detected the error condition and the error condition detected.

- hdrtype
- hdrflgs
- te
- tnum
- tcmd
- tflags
- error code
- return code
- address to error
- expected error data
- actual error data
- extra status 1
- extra status 2
- extra status 3

Memory System Failure Event Log (Template 14)

The controller Memory Controller Event Analyzer software component and the Cache Manager (part of the Value Added software component), report occurrences of memory errors via the Memory System Failure Event Log. This log is sent to all hosts that enabled "Miscellaneous" error logging on connections established with the controller Disk and/or Tape MSCP Server. The Memory System Failure Event log is reported via the TMSCP/MSCP Memory Errors error log message format.

Template 14 is shown in Table 3–16 and template formats are described in Table 3–17.

Table 3–16 Template 14—Memory System Failure Event Log Format

31		0	← Bit / ↓ Offset
command reference number			0
sequence number	reserved		4
event code	flags	format	8
controller identifier			0C
			10
reserved	chvrsn	csvrsn	14
memory address			18
instance code			1C
	tdisize	templ	20
reserved			24
event time			28
			2C
byte count			30
psr			34
csr			38
ear			3C
edr1			40
edr0			44
icr			48
imr			4C
dmr1			50

Table 3–16 Template 14—Memory System Failure Event Log Format (Continued)

31 0	← Bit / ↓ Offset
dmr0	54
did	58
psp	5C
cfw	60
rrr	64
rdr0	68
rdr1	6C
rdr2	70
wdr0	74
wdr1	78
rdear	7C
fxpscr	80
fxcsr	84
fxccsr	88
fxpaec	8C
fxcaec	90
fxpaep	94
fxcaep	98

Table 3–17 Template 14—Memory System Failure Event Log Field Descriptions

Field	Description
format	This field contains the value of 01, which is the TMSCP/MSCP Memory Errors error log format code.
event code	This field contains an MSCP code and instance code for this specific event log.
memory address	The contents of this field depend upon the value in the instance code field.
instance code	See Chapter 5 for instance code values.
templ	A number that uniquely describes the format of the template-dependent information field. For this event log the value is 14.
tdisize	The number of bytes contained in the template-dependent information field. For this event log the value is 6C.
reserved	Offset 22. This field contains the value 0.
event time	The time the event occurred according to the power-on time value maintained by the controller operational software. The time expended during controller restarts, power-on diagnostics, and system initialization is not accounted for by this value.
byte count	The number of bytes contained in the bad memory area. That area is bounded by: “memory address” through “memory address” + “byte count”- 1.

PCI Register Value Fields

The following fields of the Memory System Failure Event Log contain PCI register values for the PCI register that detected the memory failure.

- psr
- csr
- ear
- edr1
- edr0
- icr
- imr
- dmr1
- dmr0
- did
- psp
- cfw
- rrr

Read/Write Diagnostic Register Value Fields

The following fields of the Memory System Failure Event Log contain HSJ80 Read and Write Diagnostic values that are contained in the Read and Write Diagnostic registers.

- rdr0
- rdr1
- rdr2
- wdr0
- wdr1
- rdear

FX Register Value Fields

The following fields of the Memory System Failure Event Log contain FX register values for when the memory failure was detected.

- fxpscr
- fxcsr
- fxccsr
- fxpaec
- fxcaec
- fxpaep
- fxcaep

NOTE: The content of certain fields in Template 14 might be undefined depending on the value supplied in the "instance code" field. Refer to Chapter 5 to see what fields are left undefined for certain Instance Codes.

CI Port/Port Driver Event Log (Template 32)

The controller Host Interconnect Services software component reports errors detected while performing work related to the CI Port/Port Driver (PPD) communication layer via the CI Port/Port Driver Event Log. This log is sent to all hosts that enabled "Miscellaneous" error logging on connections established with the controller Disk and/or Tape MSCP Server. The CI Port/Port Driver Event log is reported via the TMSCP/MSCP Controller Errors error log message format.

Template 32 is shown in Table 3–18 and template formats are described in Table 3–19.

Table 3–18 Template 32—CI Port/Port Driver Event Log Format

31 ← Bit / ↓ Offset 0				
command reference number				0
sequence number	reserved			4
event code	flags	format		8
controller identifier				0C
				10
reserved	chvrsn	csvrsn		14
instance code				18
	tdisize	templ		1C
reserved				20
event time				24
				28
his status				2C
error id				30
vcstate	intopcd	dst	src	34
undefined		ppd opcode		38

Table 3–19 Template 32—Selected CI Port/Port Driver Event Log Field Descriptions

Field	Description
format	This field contains the value 00, which is the TMSCP/MSCP Controller Errors error log format code.
event code	This field contains an MSCP code and instance code for this event log.
reserved	Offsets 16 and 1E. These fields contain the value 0.
instance code	See Chapter 5 for a description of the Instance Codes.
templ	A number that uniquely describes the format of the template-dependent information field. For this event log the value is 32.
tdisize	The number of bytes contained in the template-dependent information field. For this event log the value is 10.
event time	The time the event occurred according to the power-on time value maintained by the controller operational software. The time expended during controller restarts, power-on diagnostics, and system initialization is not accounted for by this value.
undefined	This field is only present to provide longword alignment. Content is undefined.

The following fields in the CI Port/Port Driver Event Log are described in Host Interconnect Services Common Fields, Table 3–3 on page 3–3.

- his status
- error id
- src
- dst
- intopcd
- vcstate
- ppd opcode

NOTE: The content of certain fields in Template 32 might be undefined depending on the value supplied in the “instance code” field. Refer to Chapter 5 to see what fields are left undefined for certain Instance Codes.

CI System Communication Services Event Log (Template 33)

The controller Host Interconnect Services software component reports errors detected while performing work related to the CI System Communication Services (SCS) communication layer. These errors are reported by way of the CI System Communication Services Event Log. This log is sent to all hosts that enabled “Miscellaneous” error logging on connections established with the controller Disk and/or Tape MSCP Server. The CI System Communication Services Event Log is reported via the TMSCP/MSCP Controller Errors error log message format.

Template 33 is shown in Table 3–20 and template formats are described in Table 3–21.

Table 3–20 Template 33—CI System Communication Services Event Log Format

31			0 ← Bit / ↓ Offset
command reference number			0
sequence number	reserved		4
event code	flags	format	8
controller identifier			0C
			10
reserved	chvrsn	csvrsn	14
instance code			18
	tdisize	templ	1C
reserved			20
event time			24
			28
his status			2C
error id			30
vcstate	intopcd	dst	src	34
scs opcode	ppd opcode		38
connection id			3C
remote node name			40
			44
remote connection id			48
received connection id			4C
send connection id			50
undefined	connection state		54

Table 3–21 Template 33—Selected CI System Communication Services Event Log Field Descriptions

Field	Description
format	This field contains the value 00, which is the TMSCP/MSCP Controller Errors error log format code.
event code	This field contains an MSCP code and instance code for this event log.
reserved	Offsets 16 and 1E. These fields contain the value 0.
instance code	See Chapter 5 for a description of the Instance Codes.
templ	A number that uniquely describes the format of the template-dependent information field. For this event log the value is 33.
tdisize	The number of bytes contained in the template-dependent information field. For this event log the value is 2C.
event time	The time the event occurred according to the power-on time value maintained by the controller operational software. The time expended during controller restarts, power-on diagnostics, and system initialization is not accounted for by this value.
remote connection id	A connection identifier supplied by the host node.
received connection id	Connection identifier of the System Application (SYSAP) that is receiving the message contained in the Host Transaction Block.
send connection id	Connection identifier of the System Application (SYSAP) that is sending the message contained in the Host Transaction Block.
connection state	Connection state code as defined in Table 3–22.
undefined	This field is only present to provide longword alignment. Content is undefined.

The following fields in the CI System Communication Services Event Log are described in Host Interconnect Services Common Fields, Table 3–3 on page 3–3.

- his status
- error id
- src
- dst
- intopcd
- vcstate
- ppd opcode

The “connection id” and “remote node name” fields in the CI Communication Services Event Log are described under Common Event Log Fields on page 3–3.

Table 3–22 CI Connection State Codes

Code	Description
0000	CLOSED
0001	LISTENING
0002	CONNECT_SENT
0003	CONNECT_ACK
0004	CONNECT_REC
0005	ACCEPT_SENT
0006	REJECT_SENT
0007	OPEN
0008	DISCONNECT_SENT
0009	DISCONNECT_REC
000A	DISCONNECT_ACK
000B	DISCONNECT_MATCH

NOTE: The content of certain fields in Template 33 might be undefined depending on the value supplied in the “instance code” field. Refer to Chapter 5 to see what fields are left undefined for certain Instance Codes.

CI HSJ80 Host Port Error Event Log (Template 34)

The controller Host Interconnect Services software component reports errors detected while performing work related to the CI Port communication layer. These errors are reported by way of the CI HSJ80 Host Port Error Event Log (also called the CI Port Event Log). This log is sent to all hosts that enabled "Miscellaneous" error logging on connections established with the controller Disk and/or Tape MSCP Server. The CI HSJ80 Host Port Error Event Log is reported via the TMSCP/MSCP Controller Errors error log message format.

Template 34 is shown in Table 3–23 and template formats are described in Table 3–24.

Table 3–23 Template 34—CI HSJ80 Host Port Error Log Format

31			0	← Bit / ↓ Offset
command reference number				0
sequence number	reserved			4
event code		flags	format	8
controller identifier				0C
				10
reserved		chvrsn	csvrsn	14
instance code				18
		tdisize	templ	1C
reserved				20
event time				24
				28
his status				2C
error id				30
port	intopcd	dst	src	34
PCICI Receive Status Port 1				38
PCICI Transmit Status Port 1				3C
PCICI Receive Status Port 2				40
PCICI Transmit Status Port 2				44

Table 3–24 Template 34—Selected CI HSJ80 Host Port Error Event Log Field Descriptions

Field	Description
format	This field contains the value 00, which is the TMSCP/MSCP Controller Errors error log format code.
event code	This field contains an MSCP code and instance code for this event log.
reserved	Offsets 16 and 1E. These fields contain the value 0.
instance code	See Chapter 5 for a description of the Instance Codes.
templ	A number that uniquely describes the format of the template-dependent information field. For this event log the value is 34.
tdisize	The number of bytes contained in the template-dependent information field. For this event log the value is 1D.
event time	The time the event occurred according to the power-on time value maintained by the controller operational software. The time expended during controller restarts, power-on diagnostics, and system initialization is not accounted for by this value.

The following fields in the CI HSJ80 Host Port Error Event Log are described in Host Interconnect Services Common Fields, Table 3–3 on page 3–3.

- his status
- error id
- src
- dst
- intopcd

The last four fields of the CI HSJ80 Host Port Error Event Log are hardware registers that contain a single 32-bit hexidecimal value. These fields include:

- Receive status register Port 1
- Transmit status register Port 1
- Receive status register Port 2
- Transmit status register Port 2

Device Services Non-Transfer Error Event Log (Template 41)

The controller Device Services software component reports errors detected while performing non-transfer work related to disk, tape, or media loader device operations. These errors are reported via the Device Services Non-Transfer Error Event Log.

If the detected error is associated with a command issued by a host system, the Device Services Non-Transfer Error Event Log is sent to the host system that issued the command. The log is sent over the same connection on which the command was received, if "This Host" error logging is enabled on that connection, and to all host systems that enabled "Other Host" error logging on connections established with the controller Disk and/or Tape MSCP Server.

If the error is associated with a command issued by a controller software component, the Device Services Non-Transfer Error Event Log is sent to all host systems that enabled "Miscellaneous" error logging on a connection established with the controller Disk and/or Tape MSCP Server. The Device Services Non-Transfer Error Event Log is reported via the TMSCP/MSCP Controller Errors error log message format.

Template 41 is shown in Table 3–25 and the template formats are described in Table 3–26.

Table 3–25 Template 41—Device Services Non-Transfer Error Event Log Format

31			0	← Bit / ↓ Offset
command reference number				0
sequence number		reserved		4
event code		flags	format	8
controller identifier				0C
				10
reserved		chvrsn	csvrsn	14
instance code				18
		tdisize	templ	1C
reserved				20
event time				24
				28
ascq	asc	target	port	2C

Table 3–26 Template 41—Selected Device Services Non-Transfer Error Event Log Field Descriptions

Field	Description
format	This field contains the value 00, which is the TMSCP/MSCP Controller Errors error log format code.
event code	This field contains an MSCP code and instance code for this event log.
reserved	Offsets 16 and 1E. These fields contain the value 0.
instance code	See Chapter 5 for a description of the Instance Codes.
templ	A number that uniquely describes the format of the template-dependent information field. For this event log the value is 41.
tdisize	The number of bytes contained in the template-dependent information field. For this event log the value is 04.
event time	The time the event occurred according to the power-on time value maintained by the controller operational software. The time expended during controller restarts, power-on diagnostics, and system initialization is not accounted for by this value.
port	The SCSI bus number affected by the error being reported.
target	The SCSI target number on the “port” affected by the error being reported.
asc and ascq	These fields contain the values supplied in byte 0C (Additional Sense Code) and byte 0D (Additional Sense Code Qualifier) fields, respectively, of the Sense Data returned in the response of a SCSI REQUEST SENSE command issued to the target device. The description of the value supplied in the instance code field describes the Sense Key value supplied in the Sense Data returned. Chapter 4 lists all the ASC and ASCQ codes and Chapter 5 lists all the Instance Codes available for all templates.

NOTE: The content of certain fields in Template 41 might be undefined depending on the value supplied in the “instance code” field. Refer to Chapter 5 to see what fields are left undefined for certain Instance Codes.

Disk Transfer Error Event Log (Template 51)

The controller Device Services and Value Added Services software components report errors detected while performing work related to disk unit transfer operations. These errors are reported by way of the Disk Transfer Error Event Log.

If the detected error is associated with a command issued by a host system, the Disk Transfer Error Event Log is sent to the host system that issued the command. This log is sent over the same connection on which the command was received, if "This Host" error logging is enabled on that connection, and to all host systems that enabled "Other Host" error logging on connections established with the controller Disk and/or Tape MSCP Server.

If the error is associated with a command issued by a controller software component, the Disk Transfer Error Event Log is sent to all host systems that enabled "Miscellaneous" error logging on a connection established with the controller Disk MSCP Server. The Disk Transfer Error Event Log is reported via the MSCP Disk Transfer Errors error log message format.

Template 51 is shown in Table 3–27 and template formats are described in Table 3–28.

Table 3–27 Template 51—Disk Transfer Error Event Log Format

31 ← Bit / ↓ Offset 0				
command reference number				0
sequence number	unit number			4
event code	flags	format		8
controller identifier				0C
				10
multiunit code	chvrsn	csvrsn		14
unit identifier				18
				1C
retry	level	uhvrsn	usvrsn	20
volume serial number				24
header code				28
instance code				2C

Table 3–27 Template 51—Disk Transfer Error Event Log Format (Continued)

31			0	← Bit / ↓ Offset
	extsize	tdisize	templ	30
reserved				34
event time				38
				3C
ancillary information				40
				44
				48
devtype	device loader			4C
device identification				50
				54
				58
				5C
device serial number				60
				64
segment	ercdval	sdqual	cmdopcd	68
info			snsflgs	6C
cmdspec		addsnsl	info	70
ascq	asc	cmdspec		74
keyspec			frucode	78
additional sense bytes (device/event dependent length; 1 to 237 bytes)				7C ↓ 168

Table 3–28 Template 51—Selected Disk Transfer Error Event Log Field Descriptions

Field	Description
format	This field contains the value 02, which is the MSCP Disk Transfer Errors error log format code.
event code	This field contains an MSCP code and instance code for this event log.
instance code	See Chapter 5 for a description of the Instance Codes.
templ	A number that uniquely describes the format of the template-dependent information field. For this event log the value is 51.
tdisize	The number of bytes contained in the template-dependent information field. For this event log the value is 3C.
extsize	The number of bytes contained in any extension to the template-dependent information field. The value supplied in this field varies. See the descriptions of the “addsnsl” and “additional sense bytes” fields for more detail.
reserved	Offset 33. This field contains the value 0.
event time	The time the event occurred according to the power-on time value maintained by the controller operational software. The time expended during controller restarts, power-on diagnostics, and system initialization is not accounted for by this value.

Table 3–28 Template 51—Selected Disk Transfer Error Event Log Field Descriptions (Continued)

Field	Description
ancillary information	The format of this field is dependent on whether the event reported is associated with a command issued by a host system or a command issued by a controller software component: ■ If the event being reported is associated with a command issued by the host system, the format of this field is as follows: connection id remote node name See Disk/Tape MSCP Server, CI Host Interconnect, Device and Value-Added Services Common Fields on page 3–7 for a description of these two fields. ■ If the event being reported is associated with a controller software component, the format of this field is as follows: byte count logical block number reserved See Device and Value Added Services Common Fields, Table 3–4 on page 3–7 for a description of the first two fields. The reserved field contains the value 0.

The following fields in the Disk Transfer Error Event Log are described in Device and Value Added Services Common Fields, Table 3–4 on page 3–7.

- device locator
- devtype
- device information
- device serial number

The following fields in the Disk Transfer Error Event Log are described in Device Services and Value Added Services Common Fields, Table 3–5 on page 3–9.

- cmdopcd
- ercdval
- segment
- snsflgs
- info
- addsnsl
- cmdspec
- asc
- ascq
- frucode
- keyspec
- additional sense bytes

NOTE: The content of certain fields in Template 51 might be undefined depending on the value supplied in the “instance code” field. Also, the size of this event log varies depending on the amount of information supplied in the “additional sense bytes” field, if any. Refer to Chapter 5 to see what fields are left undefined for certain Instance Codes.

Disk Bad Block Replacement Attempt Event Log (Template 57)

The controller Value Added software component reports disk unit bad block replacement attempt results. These results are reported via the Disk Bad Block Replacement Attempt Event Log.

If the replacement is associated with a command issued by a host system, the Disk Bad Block Replacement Attempt Event Log is sent to the host system that issued the command. The log is sent over the same connection on which the command was received, if “This Host” error logging is enabled on that connection, and to all host systems that enabled “Other Host” error logging on connections established with the controller Disk and/or Tape MSCP Server.

If the replacement is associated with a command issued by a controller software component, the Disk Bad Block Replacement Attempt Event Log is sent to all host systems that enabled “Miscellaneous” error logging on a connection established with the controller Disk MSCP Server. The Disk Bad Block Replacement Attempt Event Log is reported via the MSCP Bad Block Replacement Attempt error log message format.

Template 57 is shown in Table 3–29 and template formats are described in Table 3–30.

Table 3–29 Template 57—Disk Bad Block Replacement Attempt Event Log Format

31 ← Bit / ↓ Offset 0	
command reference number	0
sequence number / unit number	4
event code / flags / format	8
controller identifier	0C–10
multiunit code / chvrsn / csvrsn	14
unit identifier	18–1C
replace flags / uhvrsn / usvrsn	20
volume serial number	24
Bad LBN	28
Old RBN	2C
New RBN	30
reserved / cause	34
instance code	38
tdisize / templ	3C
reserved	40
event time	44–48
devtype / device locator	4C
device identification	50–5C
device serial number	60–64

Table 3–30 Template 57—Selected Disk Bad Block Replacement Attempt Event Log Field Descriptions

Field	Description
format	This field contains the value 09, which is the MSCP Bad Block Replacement Attempt error log format code.
event code	This field contains an MSCP code and instance code for this event log.
reserved	Offsets 36 and 3E. These fields contain the value 0.
instance code	See Chapter 5 for a description of the Instance Codes.
templ	A number that uniquely describes the format of the template-dependent information field. For this event log the value is 57.
tdisize	The number of bytes contained in the template-dependent information field. For this event log the value is 1C.
event time	The time the event occurred according to the power-on time value maintained by the controller operational software. The time expended during controller restarts, power-on diagnostics, and system initialization is not accounted for by this value.

The following fields in the Disk Bad Block Replacement Attempt Event Log are described in Device and Value Added Services Common Fields, Table 3–4 on page 3–7.

- device locator
- devtype
- device information
- device serial number

NOTE: The content of certain fields in Template 57 might be undefined depending on the value supplied in the "instance code" field. Refer to Chapter 5 to see what fields are left undefined for certain Instance Codes.

Tape Transfer Error Event Log (Template 61)

The controller Device Services and Value Added Services software components report errors detected while performing work related to tape unit transfer operations. These errors are reported via the Tape Transfer Error Event Log.

If the error is associated with a command issued by a host system, the Tape Transfer Error Event Log is sent to the host that issued the command. The log is sent over the same connection on which the command was received, if "This Host" error logging is enabled on that connection, and to all host systems that enabled "Other Host" error logging on a connection or connections established with the controller Disk and/or Tape MSCP Server.

If the error is associated with a command issued by a controller software component, the Tape Transfer Error Event Log is sent to all host systems that enabled "Miscellaneous" error logging on a connection established with the controller Tape TMSCP/MSCP Server. The Tape Transfer Error Event Log is reported via the TMSCP Tape Errors error log message format.

Template 61 is shown in Table 3–31 and template formats are described in Table 3–32.

Table 3–31 Template 61—Tape Transfer Error Event Log Format

31			0	← Bit / ↓ Offset
command reference number				0
sequence number		unit number		4
event code		flags	format	8
controller identifier				0C 10
multiunit code		chvrsn	csvrsn	14
unit identifier				18 1C
retry	level	uhvrsn	usvrsn	20
position (object count)				24
reserved		fhvrsn	fsvrsn	28
instance code				2C
	extsize	tdisize	templ	30
reserved				34

Table 3–31 Template 61—Tape Transfer Error Event Log Format (Continued)

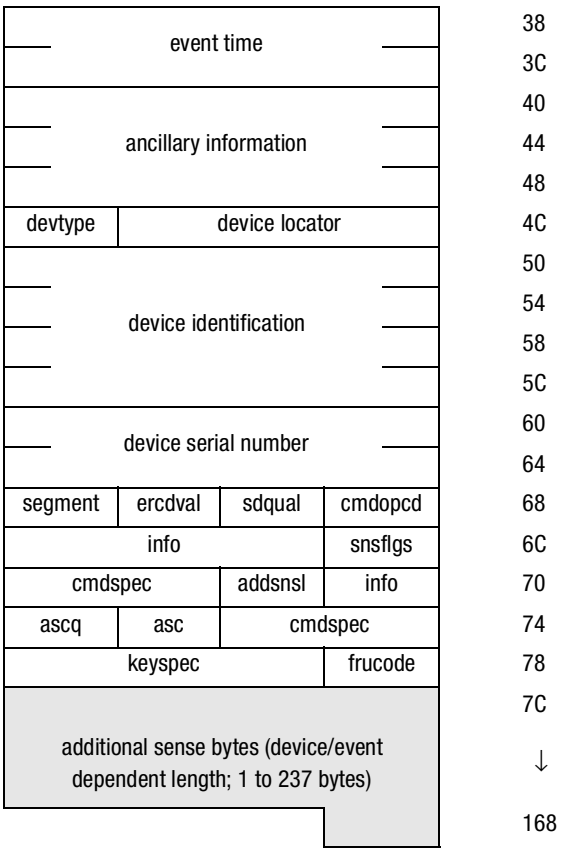


Table 3–32 Template 61—Selected Tape Transfer Error Event Log Field Descriptions

Code	Description
format	This field contains the value 05, which is the TMSCP Tape Errors error log format code.
event code	This field contains an MSCP code and instance code for this event log.
instance code	See Chapter 5 for a description of the Instance Codes.
templ	A number that uniquely describes the format of the template-dependent information field. For this event log the value is 61.
tdisize	The number of bytes contained in the template-dependent information field. For this event log the value is 3C.
extsize	The number of bytes contained in any extension to the template-dependent information field. The value supplied in this field varies. See the descriptions of the "addsnsl" and "additional sense bytes" fields for more detail.
reserved	Offset 33. This field contains the value 0.
event time	The time the event occurred according to the power-on time value maintained by the controller operational software. The time expended during controller restarts, power-on diagnostics, and system initialization is not accounted for by this value.
ancillary information	The format of this field is dependent on whether the event reported is associated with a command issued by a host system or a command issued by an HSJ80 controller software component: ■ If the event being reported is associated with a command issued by the host system, the format for this field is as follows: connection id remote node name See Disk/Tape MSCP Server, CI Host Interconnect, Device and Value-Added Services Common Fields on page 3–7 for a description of these two fields. ■ If the event being reported is associated with a controller software component, the format for this field is considered "reserved" and contains the value 0.

The following fields in the Tape Transfer Error Event Log are described in Device and Value Added Services Common Fields, Table 3–4 on page 3–7.

- device locator
- devtype
- device information
- device serial number

The following fields in the Tape Transfer Error Event Log are described in Device Services and Value Added Services Common Fields, Table 3–5 on page 3–9.

- cmdopcd
- ercdval
- segment
- snsflgs
- info
- addsnsl
- cmdspec
- asc
- ascq
- frucode
- keyspec
- additional sense bytes

NOTE: The content of certain fields in Template 61 might be undefined depending on the value supplied in the “instance code” field. Also, the size of this event log varies depending on the amount of information supplied in the “additional sense bytes” field, if any. Refer to Chapter 5 to see what fields are left undefined for certain Instance Codes.

Media Loader Error Event Log (Template 71)

The controller Device Services software component reports errors detected while performing work related to media loader operations. These errors are reported via the Media Loader Error Event Log.

If the error is associated with a command issued by a host system, the Media Loader Error Event Log is sent to the host that issued the command. The log is sent over the same connection on which the command was received, if "This Host" error logging is enabled on that connection, and to all host systems that enabled "Other Host" error logging on connections established with the controller Disk and/or Tape MSCP Server.

If the error is associated with a command issued by a controller software component, the Media Loader Error Event Log is sent to all host systems that enabled "Miscellaneous" error logging on a connection established with the controller Tape MSCP Server. The Media Loader Error Event Log is reported via the TMSCP/MSCP Media Loader Errors error log message format.

Template 71 is shown in Table 3–33 and template formats are described in Table 3–34.

Table 3–33 Template 71—Media Loader Error Event Log Format

31		0	← Bit / ↓ Offset
command reference number			0
sequence number	unit number		4
event code	flags	format	8
controller identifier			0C 10
multiunit code	chvrsn	csvrsn	14
unit identifier			18 1C
reserved	uhvrsn	usvrsn	20
media loader identifier			24 28
mi unit number	mihvrsn	misvrsn	2C
instance code			30

Table 3–33 Template 71—Media Loader Error Event Log Format (Continued)

31			0	← Bit / ↓ Offset
	extsize	tdisize	templ	34
reserved				38
event time				3C
				40
ancillary information				44
				48
				4C
devtype	device locator			50
device identification				54
				58
				5C
				60
device serial number				64
				68
segment	ercdval	sdqual	cmdopcd	6C
info			snsflgs	70
cmdspec		addsnsl	info	74
ascq	asc	cmdspec		78
keyspec			frucode	7C
additional sense bytes (device/event dependent length; 1 to 237 bytes)				80 ↓ 168

Table 3–34 Template 71—Selected Media Loader Error Event Log Field Descriptions

Code	Description
format	This field contains the value 0A, which is the TMSCP/MSCP Media Loader Errors error log format code.
event code	This field contains an MSCP code and instance code for this event log.
instance code	See Chapter 5 for a description of the Instance Codes.
templ	A number that uniquely describes the format of the template-dependent information field. For this event log the value is 71.
tdisize	The number of bytes contained in the template-dependent information field. For this event log the value is 3C.
extsize	The number of bytes contained in any extension to the template-dependent information field. The value supplied in this field varies. See the descriptions of the "addsnsl" and "additional sense bytes" fields for more detail.
reserved	Offset 37. This field contains the value 0.
event time	The time the event occurred according to the power-on time value maintained by the controller operational software. The time expended during controller restarts, power-on diagnostics, and system initialization is not accounted for by this value.
ancillary information	The format of this field is dependent on whether the event reported is associated with a command issued by a host system or a command issued by a controller software component: ■ If the event being reported is associated with a command issued by the host system, the format for this field is as follows: connection id remote node name ■ If the event being reported is associated with a controller software component, the format for this field is considered "reserved" and contains the value 0.

The following fields in the Media Loader Error Event Log are described in Device and Value Added Services Common Fields, Table 3–4 on page 3–7.

- device locator
- devtype
- device information
- device serial number

The following fields in the Media Loader Error Event Log are described in Device Services and Value Added Services Common Fields, Table 3–5 on page 3–9.

- cmdopcd
- ercdval
- segment
- snsflgs
- info
- addsnsl
- cmdspec
- asc
- ascq
- frucode
- keyspec
- additional sense bytes

NOTE: The content of certain fields in Template 71 might be undefined depending on the value supplied in the "instance code" field. Refer to Chapter 5 to see what fields are left undefined for certain Instance Codes.

Disk Copy Data Correlation Event Log

The controller Disk MSCP Server software component reports errors detected while performing Disk Copy Data commands. These errors reported via the Disk Copy Data Correlation Event Log.

The format of the Disk Copy Data Correlation Event Logs is identical to the format of the MSCP Disk Copy Data Correlation error log message. The controller generates Disk Copy Data Correlation Event Logs in accordance with the MSCP specification.

If a controller error with one of the two subcodes listed below is detected, the controller stores one of the values listed in Table 3–35 in the first longword of the "event dependent information" field of the MSCP Disk Copy Data Correlation error log to identify the resource that is lacking.

Controller error subcodes:

- Local Connection Request Failed, Insufficient Resources to Request Local Connection
- Remote Connection Request Failed, Insufficient Resources to Request Remote Connection

Table 3–35 Disk Copy Data Correlation Event Log— "Event Dependent Information" Values

Value	Description
00000001	Unable to allocate a sufficient number of DCD Context Blocks to support this host.
00000002	Unable to find an inactive Unit Path Block.
00000003	Unable to find an inactive Source Unit Block.
00000004	Insufficient resources returned by HIS$CONNECT.

Chapter 4

ASC/ASCQ, Repair Action, and Component Identifier Codes

This chapter lists and describes the ASC/ASCQ codes, recommended Repair Action codes, and Component Identifier (ID) codes called out in the various templates.

Vendor Specific SCSI ASC/ASCQ Codes

Table 4–1 lists HSJ80 controller vendor-specific SCSI ASC and ASCQ codes. These codes are also template-specific.

NOTE: Additional codes that are common to all SCSI devices can be found in the *Small Computer System Interface-2 (SCSI-2)* specification.

Table 4–1 ASC and ASCQ Code Descriptions (Sheet 1 of 9)

ASC Code	ASCQ Code	Description
00	00	No additional sense information.
00	01	Filemark detected.
00	02	End-of-partition/medium detected.
00	03	Setmark detected.
00	04	Beginning-of-partition/medium detected.
00	05	End-of-data detected.
00	06	I/O process stopped.
00	11	Audio play operation in progress.

Table 4–1 ASC and ASCQ Code Descriptions (Sheet 2 of 9)

ASC Code	ASCQ Code	Description
00	12	Audio play operation paused.
00	13	Audio play operation successfully completed.
00	14	Audio play operation stopped due to error.
00	15	No current audio status to return.
01	00	No index/sector signal.
02	00	No seek complete.
03	00	Peripheral device write fault.
03	01	No write current.
03	02	Excessive write errors.
04	00	Logical unit not ready, cause not reportable.
04	01	Logical unit is in process of becoming ready.
04	02	Logical unit not ready, initializing command required.
04	03	Logical unit not ready, manual intervention required.
04	04	Logical unit not ready, format in progress.
04	80	Logical unit is disaster tolerant failsafe locked (inoperative).
06	00	No reference position found.
07	00	Multiple peripheral devices selected.
08	00	Logical unit communication failure.
08	01	Logical unit communication time-out.
08	02	Logical unit communication parity error.
09	00	Track following error.
09	01	Tracking servo failure.
09	02	Focus servo failure.
09	03	Spindle servo failure.
0A	00	Error log overflow.
0C	00	Write error.
0C	01	Write error recovered with auto reallocation.
0C	02	Write error - auto reallocation failed.
10	00	Id crc or ecc error.
11	00	Unrecovered read error.
11	01	Read retries exhausted.

Table 4–1 ASC and ASCQ Code Descriptions (Sheet 3 of 9)

ASC Code	ASCQ Code	Description
11	02	Error too long to correct.
11	03	Multiple read errors.
11	04	Unrecovered read error - auto reallocate failed.
11	05	L-ec uncorrectable error.
11	06	Circ unrecovered error.
11	07	Data synchronization error.
11	08	Incomplete block read.
11	09	No gap found.
11	0A	Miscorrected error.
11	0B	Unrecovered read error - recommend reassignment.
11	0C	Unrecovered read error - recommend rewrite the data.
12	00	Address mark not found for id field.
13	00	Address mark not found for data field.
14	00	Recorded entity not found.
14	01	Record not found.
14	02	Filemark or setmark not found.
14	03	End-of-data not found.
14	04	Block sequence error.
15	00	Random positioning error.
15	01	Mechanical positioning error.
15	02	Positioning error detected by read of medium.
16	00	Data synchronization mark error.
17	00	Recovered data with no error correction applied.
17	01	Recovered data with retries.
17	02	Recovered data with positive head offset.
17	03	Recovered data with negative head offset.
17	04	Recovered data with retries and/or circ applied.
17	05	Recovered data with previous sector id.
17	06	Recovered data without ecc - data auto-reallocated.
17	07	Recovered data without ecc - recommend reassignment.
17	08	Recovered data without ecc - recommend rewrite.

Table 4–1 ASC and ASCQ Code Descriptions (Sheet 4 of 9)

ASC Code	ASCQ Code	Description
18	00	Recovered data with error correction applied.
18	01	Recovered data with error correction and retried applied.
18	02	Recovered data - data auto-reallocated.
18	03	Recovered data with circ.
18	04	Recovered data with lec.
18	05	Recovered data - recommend reassignment.
18	06	Recovered data - recommend rewrite.
19	00	Defect list error.
19	01	Defect list not available.
19	02	Defect list error in primary list.
19	03	Defect list error in grown list.
1A	00	Parameter list length error.
1B	00	Synchronous data transfer error.
1C	00	Defect list not found.
1C	01	Primary defect list not found.
1C	02	Grown defect list not found.
1D	00	Miscompare during verify operation.
1E	00	Recovered id with ecc correction.
20	00	Invalid command operation code.
21	00	Logical block address out of range.
21	01	Invalid element address.
22	00	Illegal function (should use 20 00, 24 00, or 26 00)
24	00	Invalid field in cdb.
25	00	Logical unit not supported.
26	00	Invalid field in parameter field.
26	01	Parameter not supported.
26	02	Parameter value invalid.
26	03	Threshold parameters not supported.
27	00	Write protected.
28	00	Not ready to ready transition, medium may have changed.
28	01	Import or export element accessed.

Table 4–1 ASC and ASCQ Code Descriptions (Sheet 5 of 9)

ASC Code	ASCQ Code	Description
29	00	Power on, reset, or bus device reset occurred.
29	01	Power on occurred.
29	02	SCSI bus reset occurred.
29	03	Bus device reset occurred.
2A	00	Parameters changed.
2A	01	Mode parameters changed.
2A	02	Log parameters changed.
2A	03	Reservations Preempted.
2B	00	Copy cannot execute since host cannot disconnect.
2C	00	Command sequence error.
2D	00	Overwrite error on update in place.
2F	00	Commands cleared by another initiator.
30	00	Incompatible medium installed.
30	01	Cannot read medium - unknown format.
30	02	Cannot read medium - incompatible format.
30	03	Cleaning cartridge installed.
31	00	Medium format corrupted.
31	01	Format command failed.
32	00	No defect spare location available.
32	01	Defect list update failure.
33	00	Tape length error.
37	00	Rounded parameter.
39	00	Saving parameters not supported.
3A	00	Medium not present.
3B	00	Invalid bits in identify message.
3B	01	Tape position error at beginning-of-medium.
3B	02	Tape position error at end-of-medium.
3B	08	Reposition error.
3B	0D	Medium destination element full.
3B	0E	Medium source element empty.
3D	00	Invalid bits in identify message.

Table 4–1 ASC and ASCQ Code Descriptions (Sheet 6 of 9)

ASC Code	ASCQ Code	Description
3E	00	Logical unit has not self-configured yet.
3F	00	Target operating conditions have changed.
3F	01	Microcode has been changed.
3F	02	Changed operating definition.
3F	03	Inquiry data has changed.
3F	85	Test Unit Ready or Read Capacity Command failed.
3F	87	Drive failed by a Host Mode Select command.
3F	88	Drive failed due to a deferred error reported by drive.
3F	90	Unrecovered Read/Write error.
3F	C0	No response from one or more drives.
3F	C2	NV memory and drive metadata indicate conflicting drive configurations.
3F	D2	Synchronous Transfer Value differences between drives.
40	nn	Diagnostic failure detected on component nn: where nn identifies a specific target device component (nn range 90 through FF). Refer to documentation provide dby the vendor of the target device for a description of the component identified by nn.
40	00	Ram failure (should use 40 80 through 40 FF).
41	00	Data path failure (should use 40 80 through 40 FF).
42	00	Power-on or self-test failure (should use 40 80 through 40 FF).
43	00	Message error.
44	00	Internal target failure.
45	00	Select or reselect failure.
46	00	Unsuccessful soft reset.
47	00	SCSI parity error.
48	00	Initiator detected error message received.
49	00	Invalid message error.
4A	00	Command phase error.
4B	00	Data phase error.
4C	00	Logical unit failed self-configuration.
4E	00	Overlapped commands attempted.
50	00	Write append error.

Table 4–1 ASC and ASCQ Code Descriptions (Sheet 7 of 9)

ASC Code	ASCQ Code	Description
50	01	Write append position error.
50	02	Position error related to timing.
51	00	Erase failure.
52	00	Cartridge fault.
53	00	Media load or eject failed.
53	01	Unload tape failure.
53	02	Medium removal prevented.
57	00	Unable to recover table-of-contents.
58	00	Generation does not exist.
59	00	Updated block read.
5A	00	Operator request or state change input (unspecified).
5A	01	Operator medium removal request.
5A	02	Operator selected write protect.
5A	03	Operator selected write permit.
5B	00	Log exception.
5B	01	Threshold condition met.
5B	02	Log counter at maximum.
5B	03	Log list codes exhausted.
5C	00	Rpl status changed.
5C	01	Spindles synchronized.
5C	02	Spindles not synchronized.
63	00	End of user area encountered on this track.
64	00	Illegal mode for this track.
82	01	No Command control structures available.
84	04	Command failed - SCSI ID verification failed.
85	05	Data returned from drive is invalid.
89	00	Request Sense command to drive failed.
8A	00	Illegal command for passthrough mode.
8C	04	Data transfer request error.
8F	00	Premature completion of a drive command.
93	00	Drive returned vendor-unique sense data.

Table 4–1 ASC and ASCQ Code Descriptions (Sheet 8 of 9)

ASC Code	ASCQ Code	Description
A0	00	Last failure event report.
A0	01	Nonvolatile parameter memory component event report.
A0	02	Backup battery failure event report.
A0	03	Subsystem built-in self test failure event report.
A0	04	Memory system failure event report.
A0	05	Failover event report.
A0	07	RAID membership event report.
A0	0A	Disaster Tolerance failsafe error mode can now be enabled.
A1	00	Shelf OK is not properly asserted.
A1	01	Unable to clear SWAP interrupt. Interrupt disabled.
A1	02	Swap interrupt re-enabled.
A1	03	Asynchronous SWAP detected.
A1	04	Controller shelf OK is not properly asserted.
A1	0A	EMU fault: Power Supplies not OK.
A1	0B	EMU fault: Fans not OK.
A1	0C	EMU fault: Temperature not OK.
A1	0D	EMU fault: External Air Sense not OK.
A1	10	Power supply fault is now fixed.
A1	11	Fans fault is now fixed.
A1	12	Temperature fault is now fixed.
A1	13	External Air Sense fault is now fixed.
A1	14	EMU and cabinet now available.
A1	15	EMU and cabinet now unavailable.
B0	00	Command timeout.
B0	01	Watchdog timer timeout.
D0	01	Disconnect timeout.
D0	02	Chip command timeout.
D0	03	Byte transfer timeout.
D1	00	Bus errors.
D1	02	Unexpected bus phase.
D1	03	Disconnect expected.

Table 4–1 ASC and ASCQ Code Descriptions (Sheet 9 of 9)

ASC Code	ASCQ Code	Description
D1	04	ID Message not sent.
D1	05	Synchronous negotiation error.
D1	07	Unexpected disconnect.
D1	08	Unexpected message.
D1	09	Unexpected Tag message.
D1	0A	Channel busy.
D1	0B	Device initialization failure. Device sense data available.
D2	00	Miscellaneous SCSI driver error.
D2	03	Device services had to reset the bus.
D3	00	Drive SCSI chip reported gross error.
D4	00	Non-SCSI bus parity error.
D5	02	Message Reject received on a valid message.
D7	00	Source driver programming error.
E0	03	Fault Manager detected an unknown error code.
E0	06	Maximum number of errors for this I/O exceeded.
E0	07	Drive reported recovered error without transferring all data.

Recommended Repair Action Codes

Recommended Repair Action codes are embedded in Instance and Last Failure Codes. See Chapter 5 and Chapter 6, respectively, for a more detailed description of the relationship between these codes.

Table 4–2 contains the Repair Action codes assigned to each significant event in the system.

Table 4–2 Recommended Repair Action Codes (Sheet 1 of 5)

Code	Description
00	No action necessary.
01	An unrecoverable hardware detected fault occurred or an unrecoverable software inconsistency was detected. Proceed with controller support avenues.
03	Follow the recommended Repair Action contained as indicated in the Last Failure Code.
04	Two possible problem sources are indicated: ■ In the case of a shelf with dual power supplies, one of the power supplies has failed. Follow Repair Action 07 for the power supply with the Power LED out. ■ One of the shelf fans has failed. Follow Repair Action 06.
05	Four possible problem sources are indicated: ■ Total power supply failure on a shelf. Follow Repair Action 09. ■ A device inserted into a shelf that has a broken internal SBB connector. Follow Repair Action 0A. ■ A standalone device is connected to the controller with an incorrect cable. Follow Repair Action 08. ■ A controller hardware failure. Follow Repair Action 20.
06	Determine which fan has failed and replace the fan.
07	Replace power supply.
08	Replace the cable. Refer to the specific device documentation.
09	Determine power failure cause.
0A	Determine which SBB has a failed connector and replace the SBB.
0B	The other controller in a dual-redundant configuration has been reset with the “Kill” line by the controller that reported the event. To restart the “Killed” controller enter the CLI command RESTART OTHER on the “Surviving” controller and then depress the (//) RESET button on the “Killed” controller. If the other controller is repeatedly being “Killed” for the same or a similar reason, follow Repair Action 20.

Table 4–2 Recommended Repair Action Codes (Sheet 2 of 5)

Code	Description
0C	Both controllers in a dual-redundant configuration are attempting to use the same SCSI ID (either 6 or 7 as indicated in the event report). The other controller of the dual-redundant pair has been reset with the "Kill" line by the controller that reported the event. Two possible problem sources are indicated: ■ A controller hardware failure. ■ A controller backplane failure. First, follow Repair Action 20 for the "Killed" controller. If the problem persists follow Repair Action 20 for the "Surviving" controller. If the problem still persists replace the controller backplane.
0D	The Environmental Monitoring Unit has detected an elevated temperature condition. Check the shelf and its components for the cause of the fault.
0E	The Environmental Monitoring Unit has detected an external air-sense fault. Check components outside of the shelf for the cause of the fault.
0F	An environmental fault previously detected by the Environmental Monitoring Unit is now fixed. This event report is notification that the repair was successful.
10	Restore on-disk configuration information to original state.
11	The Uninterruptable Power Supply (UPS) signaled a 2 minute warning (TMW) before signaling an AC line failure. UPS signals will be ignored until this condition clears. ■ Repair or replace the UPS. ■ The communication cable between the UPS and PVA is missing or damaged. Replace the cable.
20	Replace the controller module.
22	Replace the indicated cache module or the appropriate memory DIMMs on the indicated cache module.
23	Replace the indicated write cache battery. **WARNING:** Battery replacement might cause injury. Follow the directions that come with the new battery.
24	Check for the following invalid write cache configurations: ■ If the wrong write cache module is installed, replace with the matching module or clear the invalid cache error via the CLI. Refer to controller CLI reference guide for more information. ■ If the write cache module is missing, reseat the cache module if the cache module is actually present, or add the missing cache module, or clear the invalid cache error via the CLI. Refer to controller CLI reference guide for more details. ■ If in a dual-redundant configuration and one of the write cache modules is missing, match write cache boards with both controllers.

Table 4–2 Recommended Repair Action Codes (Sheet 3 of 5)

Code	Description
25	An unrecoverable Memory System failure occurred. Upon restart the controller will generate one or more Memory System Failure Event Sense Data Responses; follow the Repair Actions contained therein.
37	The Memory System Failure translator could not determine the failure cause. Follow Repair Action 01.
38	Replace the indicated cache memory DIMM.
39	Check that the cache memory DIMMs are properly configured.
3A	This error applies to this controller mirrored cache. Since the mirrored cache is physically located on the other controller cache module, replace the other controller's cache module, or the appropriate memory DIMMs on the other controller cache module.
3C	This error applies to this controller mirrored cache. Since the mirrored cache is physically located on the other controller cache module, replace the indicated cache memory DIMM on the other controller cache module.
3D	Either the primary cache or the mirrored cache has inconsistent data. Check for the following conditions to determine appropriate means to restore mirrored copies. ■ If the mirrored cache is reported as inconsistent and a previous FRU Utility warmswap of the mirrored cache module was unsuccessful, retry the procedure via the FRU Utility, by removing the module and re-inserting the same or a new module. ■ Otherwise, enter the CLI command SHUTDOWN THIS to clear the inconsistency upon restart.
3E	Replace the indicated cache module.
3F	No action necessary; cache diagnostics will determine whether the indicated cache module is faulty.
40	If the Sense Data FRU field is non-zero, follow Repair Action 41. Otherwise, replace the appropriate FRU associated with the device's SCSI interface or the entire device.
41	Consult the device maintenance manual for guidance on replacing the indicated device FRU.
43	Update the configuration data to correct the problem.
44	Replace the SCSI cable for the failing SCSI bus. If the problem persists, replace the controller backplane, drive backplane, or controller module.
45	Interpreting the device-supplied Sense Data is beyond the scope of the controller software. Refer to the device service manual to determine the appropriate Repair Action, if any.

Table 4–2 Recommended Repair Action Codes (Sheet 4 of 5)

Code	Description
50	The RAIDset is inoperative for one of the following reasons: ■ More than one member malfunctioned. Perform Repair Action 55. ■ More than one member is missing. Perform Repair Action 58. ■ Before reconstruction of a previously replaced member completes, another member becomes missing or malfunctions. Perform Repair Action 59. ■ The members have been moved around and the consistency checks show mismatched members. Perform Repair Action 58.
51	The mirrorset is inoperative for one of the following reasons: ■ The last NORMAL member has malfunctioned. Perform repair actions 55 and 59. ■ The last NORMAL member is missing. Perform Repair Action 58. ■ The members have been moved around and the consistency checks show mismatched members. Perform Repair Action 58.
52	The indicated storageset member was removed for one of the following reasons: ■ The member malfunctioned. Perform Repair Action 56. ■ By operator command. Perform Repair Action 57.
53	The storageset may be in a state that prevents adding a replacement member. Check the state of the storageset and its associated UNIT and resolve the problems found before adding the replacement member.
54	The device may be in a state that prevents adding the device as a replacement member or may not be large enough for the storageset. Use another device for the ADD action and perform Repair Action 57 for the device that failed to be added.
55	Perform the repair actions indicated in any and all event reports found for the devices that are members of the storageset.
56	Perform the repair actions indicated in any and all event reports found for the member device that was removed from the storageset. Then perform Repair Action 57.
57	Delete the device from the failedset and redeploy, perhaps by adding the device to the spareset so the device will be available to be used to replace another failing device.
58	Install the physical devices that are members of the storageset in the proper Port, Target, and LUN locations.
59	Delete the storageset, recreate the storageset with the appropriate ADD, INITIALIZE, and ADD UNIT commands and reload the storageset contents from backup storage.
5A	Restore the mirrorset data from backup storage.

Table 4–2 Recommended Repair Action Codes (Sheet 5 of 5)

Code	Description
5B	The mirrorset is inoperative due to a disaster tolerance failsafe locked condition, as a result of the loss of all local or remote NORMAL/NORMALIZING members while ERROR_MODE=FAILSAFE was enabled. To clear the failsafe locked condition, enter the CLI command SET unit-number ERROR_MODE=NORMAL.
5C	The mirrorset has at least one local NORMAL/NORMALIZING member and one remote NORMAL/NORMALIZING member. Failsafe error mode can now be enabled by entering the CLI command SET unit-number ERROR_MODE=FAILSAFE.
60	Swap the transmit and receive cables for the indicated path.
61	Check indicated path cables for proper installation.
63	Check the CI adapter on the host system identified in the “remote node name” field for proper operation.
64	Excessive VC closures are occurring. Perform repair action 61 on both sets of path cables. If the problem persists, perform repair action 63.
66	Number of hosts forming virtual circuits with the controller exceeds the current user specified maximum. Increase the maximum number of hosts allowed value.
80	An EMU fault has occurred.
81	The EMU reported terminator power out of range. Replace the indicated I/O module(s).
83	An EMU has become unavailable. ■ This EMU (and associated cabinet) may have been removed from the subsystem; no action is required. ■ The cabinet has lost power; restore power to the cabinet. ■ The EMU-to-EMU communications bus cable has been disconnected or broken; replace or reconnect the cable to reestablish communications. ■ The specified EMU is broken; replace the EMU module. ■ The EMU in cabinet 0 is broken; replace the EMU module.

Component ID Codes

Component ID codes are embedded in Instance and Last Failure Codes. See Chapter 5 and Chapter 6, respectively, for a more detailed description of the relationship between these codes.

Table 4–3 lists the Component Identifier codes.

Table 4–3 Component ID Codes

Code	Description
01	Executive Services
02	Value Added Services
03	Device Services
04	Fault Manager
05	Common Library Routines
06	Dual Universal Asynchronous Receiver/Transmitter Services
07	Failover Control
08	Nonvolatile Parameter Memory Failover Control
09	Facility Lock Manager
0A	Integrated Logging Facility
0B	Configuration Manager Process
0C	Memory Controller Event Analyzer
0D	Poweroff Process
12	Value Added Services (extended)
20	Command Line Interpreter (CLI)
40	Host Interconnect Services (HIS)
42	Host Interconnect Port Services
60	Disk and Tape MSCP Server
61	Diagnostics and Utilities Protocol Server
62	System Communication Services Directory Service
80	Disk Inline Exercise (DILX)
81	Tape Inline Exerciser (TILX)
82	Subsystem Built-In Self Tests (BIST)
83	Device Configuration Utilities (CONFIG/CFMENU)

Table 4–3 Component ID Codes (Continued)

Code	Description
84	Clone Unit Utility (CLONE)
85	Format and Device Code Load Utility (HSUTIL)
86	Code Load/Code Patch Utility (CLCP)
8A	Field Replacement Utility (FRUTIL)
8B	Periodic Diagnostics (PDIAG)

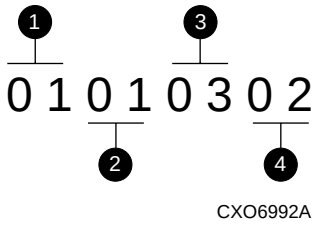
Chapter 5

Instance Codes

An Instance Code is a number that uniquely identifies an event being reported.

Instance Code Structure

Figure 5–1 shows the structure of an Instance Code. By fully understanding this structure, each code can be translated without using the FMU.



❶ Component ID number
❷ Event Number
❸ Repair Action
❹ Notification/Recovery (NR) threshold

Figure 5–1. Structure of an Instance Code

Instance Codes and FMU

The format of an Instance Code as displayed in Sense Data Responses is shown in Table 5–1.

Table 5–1 Instance Code Format

31 24	23 16	15 8	7 0	← Bit Position
Component ID	Event Number	Repair Action	NR Threshold	

Notification/Recovery Threshold

Located at bit position 0–7 is the notification/recovery (NR) threshold assigned to the event. This two-digit value is used during Symptom-Directed Diagnosis procedures to determine when to take notification/recovery action. For a description of event NR threshold classifications, see Table 5–2.

Table 5–2 Event Notification/Recovery (NR) Threshold Classifications

Threshold Value	Classification	Description
01	IMMEDIATE	Indicates either a failure or potential failure of a component critical to proper controller operation; immediate attention is required.
02	HARD	Indicates either a failure of a component that affects controller performance or inability to access a device connected to the controller.
0A	SOFT	Indicates either an unexpected condition detected by a controller software component (for example, protocol violations, host buffer access errors, internal inconsistencies, uninterpreted device errors, etc.) or an intentional restart or shutdown of controller operation.
64	INFORMATIONAL	Indicates an event having little or no effect on proper controller or device operation.

Repair Action

The Repair Action code found at bit position 8–15 indicates the *recommended Repair Action code* assigned to the event. This value is used during Symptom-Directed Diagnosis procedures to determine what notification/recovery (recommended repair) action to take upon reaching the NR Threshold. For details about recommended Repair Action codes, see Chapter 4.

Event Number

The Event Number is located at bit position 16–23. Combining this number with the Component ID field value uniquely identifies the reported event.

Component ID

A Component ID is located at bit position 24–31. This number uniquely identifies the software component that detected the event. For details about components ID numbers, see Chapter 4.

Table 5–3 contains the numerous Instance Codes, *in ascending order*, that might be issued by the controller fault management software.

Table 5–3 Instance Codes and Repair Action Codes (Sheet 1 of 25)

Instance Code	Description	Template	Repair Action Code
01010302	An unrecoverable hardware detected fault occurred.	01	03
0102030A	An unrecoverable software inconsistency was detected or an intentional restart or shutdown of controller operation was requested.	01	03
01032002	Nonvolatile parameter memory component error detection code (EDC) check failed; content of the component reset to default settings.	11	20
02020064	Disk Bad Block Replacement attempt completed for a write within the user data area of the disk. Note that due to the way Bad Block Replacement is performed on SCSI disk drives, information on the actual replacement blocks is not available to the controller and is therefore not included in the event report.	51	00

Table 5–3 Instance Codes and Repair Action Codes (Sheet 2 of 25)

Instance Code	Description	Template	Repair Action Code
02032001	Journal static random access memory (SRAM) backup battery failure; detected during *system restart*. The Memory Address field contains the starting physical address of the Journal SRAM.	12	20
02042001	Changes to *periodic check*.		
02052301	A processor interrupt was generated by the CACHEA0 Memory Controller with an indication that the CACHE backup battery has failed or is low (needs charging). The Memory Address field contains the starting physical address of the CACHEA0 memory.	12	23
02072201	The *CACHEA0* Memory Controller failed testing performed by the Cache Diagnostics. The Memory Address field contains the starting physical address of the *CACHEA0* memory.	14	22
02082201	Changes to *CACHEA1*.		
02090064	A data compare error was detected during the execution of a compare modified READ or WRITE command.	51	00
020A0064	A data compare error was detected during the execution of a compare modified READ and WRITE command.	61	00
020B2201	Failed read test of a write-back metadata page residing in cache. Dirty write-back cached data exists and cannot be flushed to media. The dirty data is lost. The Memory Address field contains the starting physical address of the CACHEA0 memory.	14	22
020C2201	Cache Diagnostics have declared the cache bad during testing. The Memory Address field contains the starting physical address of the CACHEA0 memory.	14	22
020D2401	The wrong write cache module is configured. The serial numbers do not match. Either the existing or the expected cache contains dirty write-back cached data. Note that in this instance, the Memory Address, Byte Count, exclusive OR (XOR) engine (FX) Chip Register, Memory Controller register, and Diagnostic register fields are undefined.	14	24
020E2401	The write cache module is missing. A cache is expected to be configured and contains dirty write-back cached data. Note that in this instance, the Memory Address, Byte Count, FX Chip Register, Memory Controller register, and Diagnostic register fields are undefined.	14	24

Table 5–3 Instance Codes and Repair Action Codes (Sheet 3 of 25)

Instance Code	Description	Template	Repair Action Code
02102401	The write cache modules are not configured properly for a dual-redundant configuration. One of the cache modules is not the same size to perform cache failover of dirty write-back cached data. Note that in this instance, the Memory Address, Byte Count, FX Chip Register, Memory Controller register, and Diagnostic register fields are undefined.	14	24
02110064	Disk Bad Block Replacement attempt completed for a read within the user data area of the disk. Note that due to the way Bad Block Replacement is performed on SCSI disk drives, information on the actual replacement blocks is not available to the controller and is therefore not included in the event report.	51	00
021A0064	Disk Bad Block Replacement attempt completed for a write of controller metadata to a location outside the user data area of the disk. Note that due to the way Bad Block Replacement is performed on SCSI disk drives, information on the actual replacement blocks is not available to the controller and is therefore not included in the event report.	41	00
021B0064	Disk Bad Block Replacement attempt completed for a read of controller metadata from a location outside the user data area of the disk. Note that due to the way Bad Block Replacement is performed on SCSI disk drives, information on the actual replacement blocks is not available to the controller and is therefore not included in the event report.	41	00
021D0064	Unable to lock the “other controller” cache in a write-cache failover attempt. Either a latent error could not be cleared on the cache or the “other controller” did not release the “other controller” cache. Note that in this instance, the Memory Address, Byte Count, FX Chip register, Memory Controller register, and Diagnostic register fields are undefined.	14	00
021E0064	The device specified in the Device Locator field has been added to the RAIDset associated with the logical unit. The RAIDset is now in Reconstructing state.	51	00
02280064	The device specified in the Device Locator field has been added to the mirrorset associated with the logical unit. The new mirrorset member is now in Copying state.	51	00
022C0064	The device specified in the Device Locator has transitioned from Copying or Normalizing state to Normal state.	51	00

Table 5–3 Instance Codes and Repair Action Codes (Sheet 4 of 25)

Instance Code	Description	Template	Repair Action Code
022E0064	The device specified in the Device Locator field has been converted to a mirrorset associated with the logical unit.	51	00
022F0064	The mirrored device specified in the Device Locator field has been converted to a single device associated with the logical unit.	51	00
02383A01	The CACHEB0 Memory Controller, which resides on the other cache module, failed testing performed by the Cache Diagnostics. This is the mirrored cache Memory Controller. The Memory Address field contains the starting physical address of the CACHEB0 memory.	14	3A
02392201	Both the CACHEB0 Memory Controller and CACHEB1 Memory Controller, which resides on the other cache module, failed testing performed by the Cache Diagnostics. Data cannot be accessed in the primary cache or the mirror cache. The Memory Address field contains the starting physical address of the CACHEA0 memory.	14	22
023E2401	Metadata residing in the controller and on the two cache modules disagree as to the mirror node. Note that in this instance, the Memory Address, Byte Count, FX Chip register, Memory Controller register, and Diagnostic register fields are undefined.	14	24
023F2301	The cache backup battery covering the mirror cache is insufficiently charged. The Memory Address field contains the starting physical address of the CACHEB1 memory.	12	23
02402301	The cache backup battery covering the mirror cache has been declared bad. Either the battery failed testing performed by the Cache Diagnostics during system startup or the battery was low (insufficiently charged) for longer than the expected duration. The Memory Address field contains the starting physical address of the CACHEB1 memory.	12	23
02412401	Mirrored cache writes have been disabled. Either the primary or the mirror cache has been declared bad or data invalid and will not be used. Note that in this instance, the Memory Address, Byte Count, FX Chip register, Memory Controller register, and Diagnostic register fields are undefined.	14	24
02422464	Cache failover attempt failed because the other cache was illegally configured with DIMMs. Note that in this instance, the Memory Address, Byte Count, FX Chip register, Memory Controller register, and Diagnostic register fields are undefined.	14	24

Table 5–3 Instance Codes and Repair Action Codes (Sheet 5 of 25)

Instance Code	Description	Template	Repair Action Code
02460064	A Write Append Position Error occurred during a tape write but no recovery was attempted because the attempted transfer did not meet the parameters for a recoverable Write Append Position Error.	61	00
02470064	When attempting to recover a Write Append Position Error on a tape unit, the recovery failed to start because resources required for the recovery were not available.	61	00
02480064	When attempting to recover a Write Append Position Error on a tape unit, an error occurred during the recovery.	61	00
02492401	The write cache module, which is the mirror for the primary cache, is unexpectedly not present (missing). A cache is expected to be configured and the cache may contain dirty write cached data. Note that in this instance, the Memory Address, Byte Count, FX Chip register, Memory Controller register, and Diagnostic register fields are undefined.	14	24
024A2401	Mirroring is enabled and the primary write cache module is unexpectedly not present (missing). A cache is expected to be configured and the cache may contain dirty write cached data. Note that in this instance, the Memory Address, Byte Count, FX Chip register, Memory Controller register, and Diagnostic register fields are undefined.	14	24
024B2401	Write-back caching has been disabled either due to a cache or battery-related problem. The exact nature of the problem is reported by other Instance Codes. Note that in this instance, the Memory Address, Byte Count, FX Chip register, Memory Controller register, and Diagnostic register fields are undefined.	14	24
024F2401	This cache module is populated with DIMMs incorrectly. Cache metadata resident in the cache module indicates that unflushed write cache data exists for a cache size different than what is found present. Note that in this instance, the Memory Address, Byte Count, FX Chip register, Memory Controller register, and Diagnostic register fields are undefined.	14	24

Table 5–3 Instance Codes and Repair Action Codes (Sheet 6 of 25)

Instance Code	Description	Template	Repair Action Code
025F2201	Memory diagnostics performed during controller initialization detected an excessive number (512 pages or more) of memory errors on the *primary cache memory*. Diagnostics have not declared the cache failed, due to the isolated bad memory regions, but this is a warning to replace the cache as soon as possible in case of further degradation. The software performed the necessary error recovery as appropriate. Note that in this instance, the Memory Address and Byte Count fields are undefined.	14	22
02603A01	Applies to *mirrored cache memory*.		3A
02613801	Memory diagnostics performed during controller initialization detected that the DIMM in *location 1* failed on the cache module. Note that in this instance, the Byte Count field in undefined.	14	38
02623801	Applies to *location 2*.		
02633801	Applies to *location 3*.		
02643801	Applies to *location 4*.		
02653C01	Memory diagnostics performed during controller initialization detected that the DIMM in *location 3* on the other controller's cache module (on mirrored cache) failed. Mirroring has been disabled. Note that in this instance, the Byte Count field is undefined.	14	3C
02663C01	Applies to *location 4*.		
02675201	The device specified in the Device Locator field has been removed from the RAIDset associated with the logical unit. The removed device is now in the failedset. The RAIDset is now in Reduced state.	51	52
0268530A	The device specified in the Device Locator field failed to be added to the RAIDset associated with the logical unit. The device will remain in the spareset.	51	53
02695401	The device specified in the Device Locator field failed to be added to the RAIDset associated with the logical unit. The failed device has been moved to the failedset.	51	54
026A5001	The RAIDset associated with the logical unit has become inoperative.	51	50
026B0064	The RAIDset associated with the logical unit has transitioned from *Normal state to Reconstructing state*.	51	00
026C0064	Applies to *Reconstructing state to Normal state*.		

Table 5–3 Instance Codes and Repair Action Codes (Sheet 7 of 25)

Instance Code	Description	Template	Repair Action Code
026D5201	The device specified in the Device Locator field has been removed from the mirrorset associated with the logical unit. The removed device is now in the failedset.	51	52
026E0001	The device specified in the Device Locator field has been reduced from the mirrorset associated with the logical unit. The nominal number of members in the mirrorset has been decreased by one. The reduced device is now available for use.	51	00
026F530A	The device specified in the Device Locator field failed to be added to the mirrorset associated with the logical unit. The device will remain in the spareset.	51	53
02705401	The device specified in the Device Locator field failed to be added to the mirrorset associated with the logical unit. The failed device has been moved to the failedset.	51	54
02710064	The mirrorset associated with the logical unit has had the mirrorset nominal membership changed. The new nominal number of members for the mirrorset is specified in the Device Sense Data Information field.	51	00
02725101	The mirrorset associated with the logical unit has become inoperative.	51	51
02730001	The device specified in the Device Locator field had a read error which has been repaired with data from another mirrorset member.	51	00
02745A0A	The device specified in the Device Locator field had a read error. Attempts to repair the error with data from another mirrorset member failed due to lack of an alternate error-free data source.	51	5A
02755601	The device specified in the Device Locator field had a read error. Attempts to repair the error with data from another mirrorset member failed due to a write error on the original device. The original device will be removed from the mirrorset.	51	56
02773D01	The mirrored cache is not being used because the data in the mirrored cache is inconsistent with the data in the primary cache. The primary cache contains valid data, so the controller is caching solely from the primary cache. The mirrored cache is declared “failed”, but this is not due to a hardware fault, only inconsistent data. Mirrored writes have been disabled until this condition is cleared. Note that in this instance, the Memory Address, Byte Count, FX Chip register, Memory Controller register, and Diagnostic register fields are undefined.	14	3D

Table 5–3 Instance Codes and Repair Action Codes (Sheet 8 of 25)

Instance Code	Description	Template	Repair Action Code
02782301	The cache backup battery is not present. The Memory Address field contains the starting physical address of the CACHEA0 memory.	12	23
02792301	The cache backup battery covering the mirror cache is not present. The Memory Address field contains the starting physical address of the CACHEB1 memory.	12	23
027A2201	The *CACHEB0* Memory Controller failed Cache Diagnostics testing performed on the other cache during a cache failover attempt. The Memory Address field contains the starting physical address of the *CACHEB0* memory.	14	22
027B2201	Applies to *CACHEB1*.		
027C2201	The CACHEB0 and CACHEB1 Memory Controllers failed Cache Diagnostics testing performed on the other cache during a cache failover attempt. The Memory Address field contains the starting physical address of the CACHEB0 memory.	14	22
027D5B01	The mirrorset associated with the logical unit has become inoperative due to a disaster tolerance failsafe locked condition.	51	5B
027F2301	The CACHE backup battery has been declared bad. The battery did not become fully charged within the expected duration. The Memory Address field contains the starting physical address of the CACHEA0 memory.	12	23
02825C64	The mirrorset associated with the logical unit has just had a membership change such that disaster tolerance failsafe error mode can now be enabled if desired.	51	5C
02864002	The controller has set the specified unit Data Safety Write Protected due to an unrecoverable device failure which prevents writing cached data.	51	40
02872301	The CACHE backup battery has exceeded the maximum number allowed for deep discharges. Battery capacity may be below specified values. The Memory Address field contains the starting physical address of the CACHEA0 memory.	12	23
02882301	The CACHE backup battery covering the mirror cache has exceeded the maximum number allowed for deep discharges. Battery capacity may be below specified values. The Memory Address field contains the starting physical address of the CACHEB1 memory.	12	23

Table 5–3 Instance Codes and Repair Action Codes (Sheet 9 of 25)

Instance Code	Description	Template	Repair Action Code
02892301	The CACHE backup battery is near end of life. The Memory Address field contains the starting physical address of the CACHEA0 memory.	12	23
028A2301	The CACHE backup battery covering the mirror cache is near end of life. The Memory Address field contains the starting physical address of the CACHEB1 memory.	12	23
028B3801	Memory diagnostics performed during controller initialization detected that the DIMM in *location 1* failed on the cache module. The failed DIMM should be replaced as soon as possible. Control Structures have been moved to secondary memory and are now unprotected against additional memory failures. Note that in this instance, the Byte Count field is undefined.	14	38
028C3801	Applies to *location 2*.		
028D0064	The device specified in the Device Locator field has been removed from the spareset into the failedset. The new nominal number of members for the spareset is specified in the Device Sense Data Information field.	51	00
02925D01	The device specified in the Device Locator field has been removed from the spareset into the failedset; there are no devices left in the spareset. The new nominal number of members for the spareset is specified in the Device Sense Data Information field.	51	5D
03010101	No command control structures available for disk operation. Note that in this instance, the Associated ASC and Associated ASCQ fields are undefined.	41	01
03022002	SCSI interface chip command timeout during disk operation. Note that in this instance, the Associated ASC and Associated ASCQ fields are undefined.	41	20
03034002	Byte transfer timeout during disk operation. Note that in this instance, the Associated ASC and Associated ASCQ fields are undefined.	41	40
03044402	SCSI bus errors during disk operation. Note that in this instance, the Associated ASC and Associated ASCQ fields are undefined.	41	44
03052002	Device port SCSI chip reported gross error during disk operation. Note that in this instance, the Associated ASC and Associated ASCQ fields are undefined.	41	20
03062002	Non-SCSI bus parity error during disk operation. Note that in this instance, the Associated ASC and Associated ASCQ fields are undefined.	41	20
03070101	Source driver programming error encountered during disk operation. Note that in this instance, the Associated ASC and Associated ASCQ fields are undefined.	41	01

Table 5–3 Instance Codes and Repair Action Codes (Sheet 10 of 25)

Instance Code	Description	Template	Repair Action Code
03080101	Miscellaneous SCSI Port Driver coding error detected during disk operation. Note that in this instance, the Associated ASC and Associated ASCQ fields are undefined.	41	01
03094002	An unrecoverable disk drive error was encountered while performing work related to disk unit operations.	51	40
030C4002	A drive failed because a Test Unit Ready command or a Read Capacity command failed.	51	40
030D000A	Drive was failed by a Mode Select command received from the host.	51	00
030E4002	Drive failed due to a deferred error reported by drive.	51	40
030F4002	Unrecovered Read or Write error.	51	40
03104002	No response from one or more drives.	51	40
0311430A	Nonvolatile memory and drive metadata indicate conflicting drive configurations.	51	43
0312430A	The Synchronous Transfer Value differs between drives in the same storageset.	51	43
03134002	Maximum number of errors for this data transfer operation exceeded.	51	40
03144002	Drive reported recovered error without transferring all data.	51	40
03154002	Data returned from drive is invalid.	51	40
03164002	Request Sense command to drive failed.	51	40
03170064	Illegal command for passthrough mode.	51	00
03180064	Data transfer request error.	51	00
03194002	Premature completion of a drive command.	51	40
031A4002	Command timeout.	51	40
031B0101	Watchdog timer timeout.	51	01
031C4002	Disconnect timeout.	51	40
031D4002	Unexpected bus phase.	51	40
031E4002	Disconnect expected.	51	40
031F4002	ID Message not sent by drive.	51	40
03204002	Synchronous negotiation error.	51	40
03214002	The drive unexpectedly disconnected from the SCSI bus.	51	40

Table 5–3 Instance Codes and Repair Action Codes (Sheet 11 of 25)

Instance Code	Description	Template	Repair Action Code
03224002	Unexpected message.	51	40
03234002	Unexpected Tag message.	51	40
03244002	Channel busy.	51	40
03254002	Message Reject received on a valid message.	51	40
0326450A	The disk device reported Vendor Unique SCSI Sense Data.	51	45
03270101	A disk related error code was reported which was unknown to the Fault Management software. Note that in this instance, the Associated ASC and Associated ASCQ fields are undefined.	41	01
0328450A	The disk device reported standard SCSI Sense Data.	51	45
03644002	An unrecoverable tape drive error was encountered while performing work related to tape unit operation.	61	40
03664002	An unrecoverable tape drive error was encountered while performing work related to tape unit operations.	61	40
03674002	A drive failed because a Test Unit Ready command or a Read Capacity command failed.	61	40
0368000A	A drive was failed by a Mode Select command received from the host.	61	00
03694002	A drive failed due to a deferred error reported by a drive.	61	40
036A4002	Unrecoverable Read or Write error.	61	40
036B4002	No response from one or more drives.	61	40
036C430A	Nonvolatile memory and drive metadata indicate conflicting drive configurations.	61	43
036D430A	The Synchronous Transfer Value differs between drives in the same storageset.	61	43
036E4002	Maximum number of errors for this data transfer operation exceeded.	61	40
036F4002	Drive reported recovered error without transferring all data.	61	40
03704002	Data returned from drive is invalid.	61	40
03714002	Request Sense command to drive failed.	61	40
03720064	Illegal command for passthrough mode.	61	00
03730064	Data transfer request error.	61	00
03744002	Premature completion of a drive command.	61	40

Table 5–3 Instance Codes and Repair Action Codes (Sheet 12 of 25)

Instance Code	Description	Template	Repair Action Code
03754002	Command timeout.	61	40
03760101	Watchdog timer timeout.	61	01
03774002	Disconnect timeout.	61	40
03784002	Unexpected bus phase.	61	40
03794002	Disconnect expected.	61	40
037A4002	ID Message not sent by drive.	61	40
037B4002	Synchronous negotiation error.	61	40
037C4002	The drive unexpectedly disconnected from the SCSI bus.	61	40
037D4002	Unexpected message.	61	40
037E4002	Unexpected Tag message.	61	40
037F4002	Channel busy.	61	40
03804002	Message Reject received on a valid message.	61	40
0381450A	The tape device reported Vendor Unique SCSI Sense Data.	61	45
03820101	No command control structures available for tape operation. In this case, the ASC and ASCQ fields are undefined.	41	01
03832002	SCSI interface chip command timeout during tape operation. In this case, the ASC and ASCQ fields are undefined.	41	20
03844002	Byte transfer timeout during tape operation. In this case, the ASC and ASCQ fields are undefined.	41	40
03854402	SCSI bus errors during tape operation. In this case, the ASC and ASCQ fields are undefined.	41	44
03862002	Device port SCSI chip reported gross error during tape operation. In this case, the ASC and ASCQ fields are undefined.	41	20
03872002	Non-SCSI bus parity error during tape operation. In this case, the ASC and ASCQ fields are undefined.	41	20
03880101	Source driver programming error encountered during tape operation. In this case, the ASC and ASCQ fields are undefined.	41	01
03890101	Miscellaneous SCSI Port Driver coding error detected during a tape operation. In this case, the ASC and ASCQ fields are undefined.	41	01
038A0101	A tape related error code was reported which was unknown to the Fault Management software. In this case, the ASC and ASCQ fields are undefined.	41	01

Table 5–3 Instance Codes and Repair Action Codes (Sheet 13 of 25)

Instance Code	Description	Template	Repair Action Code
038B450A	The tape device reported standard SCSI sense data.	61	45
03964002	An unrecoverable media loader error was encountered while performing work related to media loader operations.	71	40
03994002	A drive failed because a Test Unit Ready command or a Read Capacity command failed.	71	40
039A000A	A drive was failed by a Mode Select command received from the host.	71	00
039B4002	A drive failed due to a deferred error reported by the drive.	71	40
039C4002	Unrecoverable Read or Write error.	71	40
039D4002	No response from one or more drives.	71	40
039E430A	Nonvolatile memory and drive metadata indicate conflicting drive configurations.	71	43
039F430A	The Synchronous Transfer Value differs between drives in the same storageset.	71	43
03A04002	Maximum number of errors for this data transfer operation exceeded.	71	40
03A14002	A drive reported a recovered error without transferring all data.	71	40
03A24002	Data returned from drive is invalid.	71	40
03A34002	Request Sense command to drive failed.	71	40
03A40064	Illegal command for passthrough mode.	71	00
03A50064	Data transfer request error.	71	00
03A64002	Premature completion of a drive command.	71	40
03A74002	Command timeout.	71	40
03A80101	Watchdog timer timeout.	71	01
03A94002	Disconnect timeout.	71	40
03AA4002	Unexpected bus phase.	71	40
03AB4002	Disconnect expected.	71	40
03AC4002	ID Message not sent by drive.	71	40
03AD4002	Synchronous negotiation error.	71	40
03AE4002	The drive unexpectedly disconnected from the SCSI bus.	71	40
03AF4002	Unexpected message.	71	40
03B04002	Unexpected Tag message.	71	40

Table 5–3 Instance Codes and Repair Action Codes (Sheet 14 of 25)

Instance Code	Description	Template	Repair Action Code
03B14002	Channel busy.	71	40
03B24002	Message Reject received on a valid message.	71	40
03B3450A	The media changer device reported Vendor Unique SCSI Sense Data.	71	45
03B40101	No command control structures available for media loader operation. In this case, the ASC and ASCQ fields are undefined.	41	01
03B52002	SCSI interface chip command timeout during media loader operation. In this case, the ASC and ASCQ fields are undefined.	41	20
03B64002	Byte transfer timeout during media loader operation. In this case, the ASC and ASCQ fields are undefined.	41	40
03B74402	SCSI bus errors during media loader operation. In this case, the ASC and ASCQ fields are undefined.	41	44
03B82002	Device port SCSI chip reported gross error during media loader operation. In this case, the ASC and ASCQ fields are undefined.	41	20
03B92002	Non-SCSI bus parity error during media loader operation. In this case, the ASC and ASCQ fields are undefined.	41	20
03BA0101	Source driver programming error encountered during media loader operation. In this case, the ASC and ASCQ fields are undefined.	41	01
03BB0101	Miscellaneous SCSI Port Driver coding error detected during a media loader operation. In this case, the ASC and ASCQ fields are undefined.	41	01
03BC0101	A media loader related error code was reported which was unknown to the Fault Management software. In this case, the ASC and ASCQ fields are undefined.	41	01
03BD450A	The media changer device reported standard SCSI Sense Data.	71	45
03BE0701	The EMU for the cabinet indicated by the Associated Port field has powered down the cabinet because there are less than four working power supplies present. Note that in this instance, the Associated Target, Associated ASC, and Associated ASCQ fields are undefined.	41	07
03BF0D01	The EMU for the cabinet indicated by the Associated Port field has powered down the cabinet because the temperature has reached the allowable maximum. Note that in this instance, the Associated Target, Associated ASC, and Associated ASCQ fields are undefined.	41	0D

Table 5–3 Instance Codes and Repair Action Codes (Sheet 15 of 25)

Instance Code	Description	Template	Repair Action Code
03C00601	The EMU for the cabinet indicated by the Associated Port field has powered down the cabinet because a fan has been missing for more than 8 minutes. Note that in this instance, the Associated Target, Associated ASC, and Associated ASCQ fields are undefined.	41	06
03C10F64	The EMU for the cabinet indicated by the Associated Port field has allowed the cabinet to receive power because the number of power supplies is greater than or equal to four. Note that in this instance, the Associated Target, Associated ASC, and Associated ASCQ fields are undefined.	41	0F
03C20F64	The EMU for the cabinet indicated by the Associated Port field has allowed the cabinet to receive power because the high temperature problem has been fixed. Note that in this instance, the Associated Target, Associated ASC, and Associated ASCQ fields are undefined.	41	0F
03C30F64	The EMU for the cabinet indicated by the Associated Port field has allowed the cabinet to receive power because the fan that was missing has been replaced. Note that in this instance, the Associated Target, Associated ASC, and Associated ASCQ fields are undefined.	41	0F
03C80101	No command control structures available for operation to a device which is unknown to the controller. Note that in this instance, the Associated ASC and Associated ASCQ fields are undefined.	41	01
03C92002	SCSI interface chip command timeout during operation to a device which is unknown to the controller. Note that in this instance, the Associated ASC and Associated ASCQ fields are undefined.	41	20
03CA4002	Byte transfer timeout during operation to a device which is unknown to the controller. Note that in this instance, the Associated ASC and Associated ASCQ fields are undefined.	41	40
03CB0101	Miscellaneous SCSI Port Driver coding error detected during operation to a device which is unknown to the controller. Note that in this instance, the Associated ASC and Associated ASCQ fields are undefined.	41	01
03CC0101	An error code was reported which was unknown to the Fault Management software. Note that in this instance, the Associated ASC and Associated ASCQ fields are undefined.	41	01
03CD2002	Device port SCSI chip reported gross error during operation to a device which is unknown to the controller. Note that in this instance, the Associated ASC and Associated ASCQ fields are undefined.	41	20

Table 5–3 Instance Codes and Repair Action Codes (Sheet 16 of 25)

Instance Code	Description	Template	Repair Action Code
03CE2002	Non-SCSI bus parity error during operation to a device which is unknown to the controller. Note that in this instance, the Associated ASC and Associated ASCQ fields are undefined.	41	20
03CF0101	Source driver programming error encountered during operation to a device which is unknown to the controller. Note that in this instance, the Associated ASC and Associated ASCQ fields are undefined.	41	01
03D04002	A failure occurred while attempting a SCSI Test Unit Ready or Read Capacity command to a device. The device type is unknown to the controller. Note that in this instance, the Associated ASC and Associated ASCQ fields are undefined.	41	40
03D14002	The identification of a device does not match the configuration information. The actual device type is unknown to the controller. Note that in this instance, the Associated ASC, and Associated ASCQ fields are undefined.	41	40
03D24402	SCSI bus errors during device operation. The device type is unknown to the controller. Note that in this instance, the Associated ASC and Associated ASCQ fields are undefined.	41	44
03D3450A	During device initialization, the device reported the SCSI Sense Key NO SENSE. This indicates that there is no specific sense key information to be reported for the designated logical unit. This would be the case for a successful command or a command that received CHECK CONDITION or COMMAND TERMINATED status because one of the FM, EOM, or ILI bits is set to one in the sense data flags field.	41	45
03D4450A	During device initialization, the device reported the SCSI Sense Key RECOVERED ERROR. This indicates the last command completed successfully with some recovery action performed by the target.	41	45
03D5450A	During device initialization, the device reported the SCSI Sense Key NOT READY. This indicates that the logical unit addressed cannot be accessed. Operator intervention may be required to correct this condition.	41	45
03D6450A	During device initialization, the device reported the SCSI Sense Key MEDIUM ERROR. This indicates that the command stopped with a non-recovered error condition that was probably caused by a flaw in the medium or an error in the recorded data. This sense key may also be returned if the target is unable to distinguish between a flaw in the medium and a specific hardware failure (HARDWARE ERROR sense key).	41	45

Table 5–3 Instance Codes and Repair Action Codes (Sheet 17 of 25)

Instance Code	Description	Template	Repair Action Code
03D7450A	During device initialization, the device reported the SCSI Sense Key HARDWARE ERROR. This indicates that the target detected a non-recoverable hardware failure (for example, controller failure, device failure, parity error, etc.) while performing the command or during a self test.	41	45
03D8450A	During device initialization, the device reported the SCSI Sense Key ILLEGAL REQUEST. This indicates that there was an illegal parameter in the command descriptor block or in the additional parameters supplied as data for some commands (FORMAT UNIT, SEARCH DATA, etc.). If the target detects an invalid parameter in the command descriptor block, then the target will stop the command without altering the medium. If the target detects an invalid parameter in the additional parameters supplied as data, then the target may have already altered the medium. This sense key may also indicate that an invalid IDENTIFY message was received.	41	45
03D9450A	During device initialization, the device reported the SCSI Sense Key UNIT ATTENTION. This indicates that the removable medium may have been changed or the target has been reset.	41	45
03DA450A	During device initialization, the device reported the SCSI Sense Key DATA PROTECT. This indicates that a command that reads or writes the medium was attempted on a block that is protected from this operation. The read or write operation is not performed.	41	45
03DB450A	During device initialization, the device reported the SCSI Sense Key BLANK CHECK. This indicates that a write-once device encountered blank medium or format-defined end-of-data indication while reading or a write-once device encountered a non-blank medium while writing.	41	45
03DC450A	During device initialization, the device reported a SCSI Vendor Specific Sense Key. This sense key is available for reporting vendor specific conditions.	41	45
03DD450A	During device initialization, the device reported the SCSI Sense Key COPY ABORTED. This indicates a COPY, COMPARE, or COPY AND VERIFY command was aborted due to an error condition on the source device, the destination device, or both.	41	45
03DE450A	During device initialization, the device reported the SCSI Sense Key ABORTED COMMAND. This indicates the target aborted the command. The initiator may be able to recover by trying the command again.	41	45

Table 5–3 Instance Codes and Repair Action Codes (Sheet 18 of 25)

Instance Code	Description	Template	Repair Action Code
03DF450A	During device initialization, the device reported the SCSI Sense Key EQUAL. This indicates a SEARCH DATA command has satisfied an equal comparison.	41	45
03E0450A	During device initialization, the device reported the SCSI Sense Key VOLUME OVERFLOW. This indicates a buffered peripheral device has reached the end-of-partition and data may remain in the buffer that has not been written to the medium. A RECOVER BUFFERED DATA command(s) may be issued to read the unwritten data from the buffer.	41	45
03E1450A	During device initialization, the device reported the SCSI Sense Key MISCOMPARE. This indicates the source data did not match the data read from the medium.	41	45
03E2450A	During device initialization, the device reported a reserved SCSI Sense Key.	41	45
03E40F64	The EMU has indicated that Termination Power is good on all ports. Note that in this instance, the Associated Target, Associated ASC, and Associated ASCQ fields are undefined.	41	0F
03E58002	The EMU has detected bad Termination Power on the indicated port. Note that in this instance, the Associated Target, Associated ASC, and Associated ASCQ fields are undefined.	41	80
03EE0064	The EMU for the cabinet indicated by the Associated Port field has become *available*. Note that in this instance, the Associated Target, Associated Additional Sense Code, and the Associated Additional Sense Code Qualifier fields are undefined.	41	00
03EF8301	Changes to *unavailable*.		83
03F10502	The SWAP interrupt from the device port indicated by the Associated Port field cannot be cleared. All SWAP interrupts from all ports will be disabled until corrective action is taken. When SWAP interrupts are disabled, both controller front panel button presses and removal/insertion of devices are not detected by the controller. Note that in this instance, the Associated Target, Associated ASC, and Associated ASCQ fields are undefined.	41	05
03F20064	The SWAP interrupts have been cleared and re-enabled for all device ports. Note that in this instance, the Associated Port, Associated Target, Associated ASC, and Associated ASCQ fields are undefined.	41	00

Table 5–3 Instance Codes and Repair Action Codes (Sheet 19 of 25)

Instance Code	Description	Template	Repair Action Code
03F30064	An asynchronous SWAP interrupt was detected by the controller for the device port indicated by the Associated Port field. Possible reasons for this occurrence include: ■ device insertion or removal ■ shelf power failure ■ SWAP interrupts reenabled Note that in this instance, the Associated Target, Associated ASC, and Associated ASCQ fields are undefined.	41	00
03F40064	Device services had to reset the port to clear a bad condition. Note that in this instance, the Associated Target, Associated ASC, and Associated ASCQ fields are undefined.	41	00
03F60402	The controller shelf is reporting a problem. This could mean one or both of the following: ■ If the shelf is using dual power supplies, one power supply has failed. ■ One of the shelf cooling fans has failed. Note that in this instance, the Associated Target, Associated ASC, and Associated ASCQ fields are undefined.	41	04
03F70401	The shelf indicated by the Associated Port field is reporting a problem. This could mean one or both of the following: ■ If the shelf is using dual power supplies, one power supply has failed. ■ One of the shelf cooling fans has failed. Note that in this instance, the Associated Target, Associated ASC, and Associated ASCQ fields are undefined.	41	04
03F80701	The EMU has detected one or more bad power supplies. Note that in this instance, the Associated Target, Associated ASC, and Associated ASCQ fields are undefined.	41	07
03F90601	The EMU has detected one or more bad fans. Note that in this instance, the Associated Target, Associated ASC, and Associated ASCQ fields are undefined.	41	06

Table 5–3 Instance Codes and Repair Action Codes (Sheet 20 of 25)

Instance Code	Description	Template	Repair Action Code
03FA0D01	The EMU has detected an elevated temperature condition. Note that in this instance, the Associated Target, Associated ASC, and Associated ASCQ fields are undefined.	41	0D
03FB0E01	The EMU has detected an external air sense fault. Note that in this instance, the Associated Target, Associated ASC, and Associated ASCQ fields are undefined.	41	0E
03FC0F01	The EMU-detected power supply fault is now fixed. Note that in this instance, the Associated Target, Associated ASC, and Associated ASCQ fields are undefined.	41	0F
03FD0F01	The EMU-detected bad-fan fault is now fixed. Note that in this instance, the Associated Target, Associated ASC, and Associated ASCQ fields are undefined.	41	0F
03FE0F01	The EMU-detected elevated temperature fault is now fixed. Note that in this instance, the Associated Target, Associated ASC, and Associated ASCQ fields are undefined.	41	0F
03FF0F01	The EMU-detected external air sense fault is now fixed. Note that in this instance, the Associated Target, Associated ASC, and Associated ASCQ fields are undefined.	41	0F
07030B0A	Failover Control detected a receive packet sequence number mismatch. The controllers are out of synchronization with each other and are unable to communicate. Note that in this instance, the Last Failure Code and Last Failure Parameters fields are undefined.	05	0B
07040B0A	Failover Control detected a transmit packet sequence number mismatch. The controllers are out of synchronization with each other and are unable to communicate. Note that in this instance, the Last Failure Code and Last Failure Parameters fields are undefined.	05	0B
07050064	Failover Control received a Last Gasp message from the other controller. The other controller is expected to restart within a given time period. If the other controller does not, the other controller will be held reset with the “Kill” line.	05	00

Table 5–3 Instance Codes and Repair Action Codes (Sheet 21 of 25)

Instance Code	Description	Template	Repair Action Code
07060C01	Failover Control detected that both controllers are acting as *SCSI ID 6*. Since IDs are determined by hardware, it is unknown which controller is the real *SCSI ID 6*. Note that in this instance, the Last Failure Code and Last Failure Parameters fields are undefined.	05	0C
07070C01	Changes to *SCSI ID 7*.		
07080B0A	Failover Control was unable to send "keepalive" communication to the other controller. It is assumed that the other controller is hung or not started. Note that in this instance, the Last Failure Code and Last Failure Parameters fields are undefined.	05	0B
07090064	Failover Control received a Code Load message from the other controller indicating that a new program image is being written onto the other controller program (PCMCIA) card. During this process, "keepalive" communication between controllers will not occur. This controller will not "kill" the other controller for lack of "keepalive" communication.	05	00
0C00370A	Memory System Error Analysis is indicated in the information preserved during a previous last failure but no error conditions are indicated in the available Memory Controller registers. The Quadrant 0 Memory Controller (CACHEA0) registers content is supplied.	14	37
0C103E02	The Quadrant 0 Memory Controller (CACHEA0) detected an Address Parity error.	14	3E
0C113E02	The Quadrant 1 Memory Controller (CACHEA1) detected an Address Parity error.	14	3E
0C123E02	The Quadrant 2 Memory Controller (CACHEB0) detected an Address Parity error.	14	3E
0C133E02	The Quadrant 3 Memory Controller (CACHEB1) detected an Address Parity error.	14	3E
0C203E02	The Quadrant 0 Memory Controller (CACHEA0) detected a Data Parity error.	14	3E
0C213E02	The Quadrant 1 Memory Controller (CACHEA1) detected a Data Parity error.	14	3E
0C223E02	The Quadrant 2 Memory Controller (CACHEB0) detected a Data Parity error.	14	3E
0C233E02	The Quadrant 3 Memory Controller (CACHEB1) detected a Data Parity error.	14	3E
0C303F02	The Quadrant 0 Memory Controller (CACHEA0) detected a Multibit ECC error.	14	3F
0C313F02	The Quadrant 1 Memory Controller (CACHEA1) detected a Multibit ECC error.	14	3F

Table 5–3 Instance Codes and Repair Action Codes (Sheet 22 of 25)

Instance Code	Description	Template	Repair Action Code
0C323F02	The Quadrant 2 Memory Controller (CACHEB0) detected a Multibit ECC error.	14	3F
0C333F02	The Quadrant 3 Memory Controller (CACHEB1) detected a Multibit ECC error.	14	3F
0C403E02	The Quadrant 0 Memory Controller (CACHEA0) detected a Firewall error.	14	3E
0C413E02	The Quadrant 1 Memory Controller (CACHEA1) detected a Firewall error.	14	3E
0C423E02	The Quadrant 2 Memory Controller (CACHEB0) detected a Firewall error.	14	3E
0C433E02	The Quadrant 3 Memory Controller (CACHEB1) detected a Firewall error.	14	3E
40016001	CI A/B transmit cables are crossed.	34	60
40026001	CI A/B receive cables are crossed.	34	60
4004020A	Host Interconnect Services detected a protocol error upon validating a received packet.	32	02
400F640A	Host Interconnect Services detected a packet sequence number mismatch.	34	64
40102001	Host Port detected a parity error while receiving a packet. The port has been reset, all virtual circuits on this port have been closed and will be restarted.	34	20
40112001	Host Port detected a parity error while transmitting a packet. The transmit attempt will be retried.	34	20
40120064	A Path that was unknown or could not be used is now in a good state.	34	00
40136001	Path has changed from good to bad.	34	60
40142001	Host Port received a packet with an invalid or unsupported packet opcode. This may be a CI Host Port error. All Virtual Circuits have been closed and will be restarted.	34	20
40162001	Host Port received a packet with an invalid or unsupported port-port datagram (PPD) code.	34	20
40176401	Host Port has been requested to reset (Host Reset). All Virtual Circuits have been closed and will be restarted.	34	64
40186401	As part of the Host Port error recovery for reception of an invalid packet opcode, this Virtual Circuit was closed and will be restarted.	34	64
4019020A	Host system reported a seven tick time slot (not a supported cluster configuration).	34	02
401A020A	Host system reported a different cluster size (not a supported cluster configuration).	34	02
401B2001	The Host Port detected a hardware overrun condition while receiving.	34	20

Table 5–3 Instance Codes and Repair Action Codes (Sheet 23 of 25)

Instance Code	Description	Template	Repair Action Code
401C6401	As part of the Host Port error recovery for receive overrun, Virtual Circuits were closed and will be restarted.	34	64
401D2001	Host Port has detected an arbitration timeout. This may be a remote system problem or a peripheral component interface (PCI) chip interface (PCICI) problem.	34	20
403F020A	Received a PPD START but the virtual circuit state was already VC_OPEN.	34	02
402B010A	Illegal connection state. Not in CLOSED connection state when a serial communication service (SCS) CONNECT_REQ is pending.	33	01
402C010A	Illegal connection state. Not in OPEN or DISCONNECT_REC connection state when an SCS DISCONNECT_REQ is pending.	33	01
403D020A	Received packet with an unrecognized PPD opcode. Note that the content of the "vcstate" field is undefined in this instance.	32	02
403F020A	Received a PPD START but the virtual circuit state was already VC_OPEN.	34	02
40440064	Received a PPD NODE_STOP and closed virtual circuit.	34	00
40450064	The virtual circuit was closed due to Negative Acknowledgment (NAK) retry failure.	34	00
40460064	The virtual circuit was closed due to No Response (NOR) retry failure.	34	00
40470064	The virtual circuit was closed due to a received parity error.	34	00
4051020A	Received SCS CONNECT_RSP when not in the CONNECT_SENT connection state.	33	02
4052020A	Received SCS CONNECT_RSP on a connection that is no longer valid.	33	02
4053020A	Received SCS ACCEPT_REQ when not in the CONNECT_ACK connection state.	33	02
4054020A	Received SCS ACCEPT_RSP when not in the ACCEPT_SENT connection state.	33	02
4055020A	Received SCS REJECT_REQ when not in the CONNECT_ACK connection state.	33	02
4056020A	Received SCS REJECT_RSP when not in the REJECT_SENT connection state.	33	02
4057020A	Received SCS DISCONNECT_REQ when not in the OPEN, DISCONNECT_SENT or DISCONNECT_ACK connection state.	33	02
4058020A	Received SCS DISCONNECT_RSP when not in the DISCONNECT_SENT or DISCONNECT_MATCH connection state.	33	02

Table 5–3 Instance Codes and Repair Action Codes (Sheet 24 of 25)

Instance Code	Description	Template	Repair Action Code
4059020A	Received SCS CREDIT_REQ when in the DISCONNECT_REC or DISCONNECT_MATCH connection state.	33	02
405A020A	Received SCS APPL_MSG when in the DISCONNECT_SENT or DISCONNECT_ACK connection state.	33	02
405B020A	Received SCS ACCEPT_REQ on a connection that is no longer valid. In this case if the "connection id" field is zero, the content of the "vcstate," "remote node name," "remote connection id," and "connection state" fields are undefined.	33	02
405C020A	Received SCS ACCEPT_RSP on a connection that is no longer valid. In this case if the "connection id" field is zero, the content of the "vcstate," "remote node name," "remote connection id," and "connection state" fields are undefined.	33	02
405D020A	Received SCS REJECT_RWQ on a connection that is no longer valid. In this case if the "connection id" field is zero, the content of the "vcstate," "remote node name," "remote connection id," and "connection state" fields are undefined.	33	02
405E020A	Received SCS REJECT_RSP on a connection that is no longer valid. In this case if the "connection id" field is zero, the content of the "vcstate," "remote node name," "remote connection id," and "connection state" fields are undefined.	33	02
405F020A	Received SCS DISCONNECT_REQ on a connection that is no longer valid. In this case if the "connection id" field is zero, the content of the "vcstate," "remote node name," "remote connection id," and "connection state" fields are undefined.	33	02
4060020A	Received SCS DISCONNECT_RSP on a connection that is no longer valid. In this case if the "connection id" field is zero, the content of the "vcstate," "remote node name," "remote connection id," and "connection state" fields are undefined.	33	02
4061020A	Received SCS CREDIT_REQ on a connection that is no longer valid. In this case if the "connection id" field is zero, the content of the "vcstate," "remote node name," "remote connection id," and "connection state" fields are undefined.	33	02

Table 5–3 Instance Codes and Repair Action Codes (Sheet 25 of 25)

Instance Code	Description	Template	Repair Action Code
4062020A	Received SCS CREDIT_RSP on a connection that is no longer valid. In this case if the “connection id” field is zero, the content of the “vcstate,” “remote node name,” “remote connection id,” and “connection state” fields are undefined.	33	02
4063020A	Received SCS APPL_MSG on a connection that is no longer valid. In this case if the “connection id” field is zero, the content of the “vcstate,” “remote node name,” “remote connection id,” and “connection state” fields are undefined.	33	02
4064020A	Received an unrecognized SCS message. In this case if the “connection id” field is zero, the content of the “vcstate,” “remote node name,” “remote connection id,” and “connection state” fields are undefined.	33	02
4065020A	Received SCS CONNECT_RSP with an unrecognized status. Connection is broken by Host Interconnect Services.	33	02
4066020A	Received SCS REJECT_REQ with no receive credit available.	33	02
4067020A	Received SCS APPL_MSG with no receive credit available.	33	02
82042002	A spurious interrupt was detected during the execution of a Subsystem Built-In Self Test.	13	20
82052002	An unrecoverable error was detected during execution of the HOST PORT Subsystem Test. The system will not be able to communicate with the host.	13	20
82062002	An unrecoverable error was detected during execution of the UART/DUART Subsystem Test. This will cause the console to be unusable. This will cause failover communications to fail.	13	20
82072002	An unrecoverable error was detected during execution of the FX Subsystem Test.	13	20
820A2002	An unrecoverable error was detected during execution of the PCI9060ES Test.	13	20
820B2002	An unrecoverable error was detected during execution of the Device Port Subsystem Built-In Self Test. One or more of the device ports on the controller module has failed; some or all of the attached storage is no longer accessible using this controller.	13	20

Chapter 6

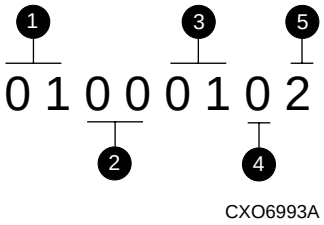
Last Failure Codes

A Last Failure Code is a number that uniquely describes an unrecoverable condition. The Last Failure Code is found at byte offset 104 to 107 and only appears in two templates:

- Template 01—Last Failure Event Log Format (see Chapter 3)
- Template 05—Failover Event Log Format (see Chapter 3)

Last Failure Code Structure

Figure 6–1 shows the structure of a Last Failure Code. By fully understanding this structure, each code can be translated without using the FMU.



❶ Component ID code
❷ Error Number
❸ Repair Action
❹ Restart Code and HW flag
❺ Parameter Count

Figure 6–1. Structure of a Last Failure Code

Last Failure Codes and FMU

The format of a Last Failure Code is shown in Table 6–1.

Table 6–1 Last Failure Code Format

31 24	23 16	15 9	8 7	6 4	3 0	← Bit Position
Component ID	Error Number	Repair Action	HW	Restart Code	Parameter Count	

NOTE: Do not confuse the Last Failure Code with that of an Instance Code (see Chapter 5). Both codes are similar in format, but convey different information.

Parameter Count

The Parameter Count is located at bit position 0–3 and indicates the number of Last Failure Parameters containing supplemental information supplied.

Restart Code

Located at bit position 4–6, the Restart Code describes the actions taken to restart the controller after the unrecoverable condition was detected. See Table 6–2 for available Restart Codes.

Table 6–2 Controller Restart Codes

Restart Code	Description
0	Full software restart
1	No restart
2	Automatic hardware restart

Hardware/Software Flag

The hardware/software (HW) flag is located at bit position 7–8. If this flag is a 1, the unrecoverable condition is due to a hardware detected fault. If this flag is a 0, the unrecoverable condition is due to an inconsistency with the software, or a requested restart or shutdown of the controller.

Repair Action

The Repair Action code at bit position 9–15 indicates the *recommended Repair Action code* assigned to the failure. This value is used during Symptom-Directed Diagnosis procedures to determine what notification/recovery action to take. For details about recommended Repair Action codes, see Chapter 4.

Error Number

The Error Number is located at bit position 16–23. Combining this number with the Component ID field value uniquely identifies the reported failure.

Component ID Code

The Component ID code is located at bit position 24–31. This code uniquely identifies the software component that reported the failure. For details about component ID codes, see Chapter 4.

Table 6–3 contains the numerous Last Failure Codes, *in ascending order*, that might be issued by the controller.

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 1 of 42)

Last Failure Code	Description	Repair Action Code
01000100	Memory allocation failure during executive initialization.	01
01010100	An interrupt without any handler was triggered.	01
01020100	Entry on timer queue was not of type associated queue (AQ) or blocking queue (BQ).	01
01030100	Memory allocation for a facility lock failed.	01
01040100	Memory initialization called with invalid memory type.	01
01082004	The core diagnostics reported a fault. ■ Last Failure Parameter [0] contains the error code value (same as blinking OCP LEDs error code). ■ Last Failure Parameter [1] contains the address of the fault. ■ Last Failure Parameter [2] contains the actual data value. ■ Last Failure Parameter [3] contains the expected data value.	20

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 2 of 42)

Last Failure Code	Description	Repair Action Code
01090105	A nonmaskable interrupt (NMI) occurred during EXEC$BUGCHECK processing. ■ Last Failure Parameter [0] contains the executive flags value. ■ Last Failure Parameter [1] contains the return instruction pointer (RIP) from the NMI stack. ■ Last Failure Parameter [2] contains the read diagnostic register 0 value. ■ Last Failure Parameter [3] contains the FX Chip Control and Status Register (CSR) value. ■ Last Failure Parameter [4] contains the System Information Page (SIP) Last Failure Code value.	01
010D0110	The System Information structure within the SIP has been reset to default settings. The only known cause for this event is an i960 processor hang caused by a reference to a memory region that is not implemented. When such a hang occurs, controller modules equipped with inactivity watchdog timer circuitry will spontaneously reboot after the watchdog timer expires (within seconds of the hang). Controller modules not so equipped will hang as indicated by the green LED on the OCP remaining in a steady state.	01
010E0110	All structures contained in the SIP and the Last Failure entries have been reset to their default settings. This is a normal occurrence for the first boot following manufacture of the controller module and during the transition from one software version to another if and only if the format of the SIP is different between the two versions. If this event is reported at any other time, follow the recommended Repair Action associated with this Last Failure Code.	01
010F0110	All structures contained in the SIP and the Last Failure entries have been reset to their default settings as the result of certain controller manufacturing configuration activities. If this event is reported at any other time, follow the recommended Repair Action associated with this Last Failure Code.	01
01100100	Non-maskable interrupt entered but no Non-maskable interrupt pending. This is typically caused by an indirect call to address 0.	01
01110106	A bugcheck occurred during EXEC$BUGCHECK processing. ■ Last Failure Parameter [0] contains the executive flags value. ■ Last Failure Parameter [1] contains the RIP from the bugcheck call stack. ■ Last Failure Parameter [2] contains the first SIP last failure parameter value. ■ Last Failure Parameter [3] contains the second SIP last failure parameter value. ■ Last Failure Parameter [4] contains the SIP Last Failure Code value. ■ Last Failure Parameter [5] contains the EXEC$BUGCHECK call Last Failure Code value.	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 3 of 42)

Last Failure Code	Description	Repair Action Code
01150106	A bugcheck occurred before subsystem initialization completed. ■ Last Failure Parameter [0] contains the executive flags value. ■ Last Failure Parameter [1] contains the RIP from the bugcheck call stack. ■ Last Failure Parameter [2] contains the first SIP last failure parameter value. ■ Last Failure Parameter [3] contains the second SIP last failure parameter value. ■ Last Failure Parameter [4] contains the SIP Last Failure Code value. ■ Last Failure Parameter [5] contains the EXEC$BUGCHECK call Last Failure Code value.	01
01170108	The i960 processor reported a machine fault (parity error) while an NMI was being processed. ■ Last Failure Parameter [0] contains the RESERVED value. ■ Last Failure Parameter [1] contains the access type value. ■ Last Failure Parameter [2] contains the access address value. ■ Last Failure Parameter [3] contains the number of faults value. ■ Last Failure Parameter [4] contains the process controls register (PC) value. ■ Last Failure Parameter [5] contains the arithmetic controls register (AC) value. ■ Last Failure Parameter [6] contains the fault type and subtype values. ■ Last Failure Parameter [7] contains the RIP value.	01
01180105	A machine fault (parity error) occurred during EXEC$BUGCHECK processing. ■ Last Failure Parameter [0] contains the executive flags value. ■ Last Failure Parameter [1] contains the RIP from the machine fault stack. ■ Last Failure Parameter [2] contains the read diagnostic register 0 value. ■ Last Failure Parameter [3] contains the FX Chip CSR value. ■ Last Failure Parameter [4] contains the SIP Last Failure Code value.	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 4 of 42)

Last Failure Code	Description	Repair Action Code
011B0108	The i960 processor reported a machine fault (nonparity error). ■ Last Failure Parameter [0] contains the Fault Data (2) value. ■ Last Failure Parameter [1] contains the Fault Data (1) value. ■ Last Failure Parameter [2] contains the Fault Data (0) value. ■ Last Failure Parameter [3] contains the Number of Faults value. ■ Last Failure Parameter [4] contains the PC value. ■ Last Failure Parameter [5] contains the AC value. ■ Last Failure Parameter [6] contains the Fault Flags, Type and Subtype values. ■ Last Failure Parameter [7] contains the RIP value (actual).	01
011C0011	Controller execution stopped via display of solid fault code in OCP LEDs. Note that upon receipt of this Last Failure in a last gasp message the other controller in a dual controller configuration will inhibit assertion of the KILL line. ■ Last Failure Parameter [0] contains the OCP LED solid fault code value.	00
011D0100	Relocated zero (for example, C0000000) entered via call or branch.	01
018000A0	A powerfail interrupt occurred.	00
018600A0	A processor interrupt was generated with an indication that the other controller in a dual controller configuration asserted the KILL line to disable this controller.	00
018700A0	A processor interrupt was generated with an indication that the (//) RESET button on the controller module was depressed.	00
018800A0	A processor interrupt was generated with an indication that the program card was removed.	00
018900A0	A processor interrupt was generated with an indication that the controller inactivity watchdog timer expired.	00

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 5 of 42)

Last Failure Code	Description	Repair Action Code
018F2087	A NMI interrupt was generated with an indication that a controller system problem occurred. ■ Last Failure Parameter [0] contains the value of read diagnostic register 0. ■ Last Failure Parameter [1] contains the value of read diagnostic register 1. ■ Last Failure Parameter [2] contains PCI status. Bits 31::24 hold PCI FX engine (PCFX) PCI status command register (PSCR) status and bits 15::08 hold PLX (bridge chip) PSCR status. ■ Last Failure Parameter [3] contains the PCFX PCI data/address line (PDAL) control/status register. ■ Last Failure Parameter [4] contains the Intel bus (IBUS) address of error register. ■ Last Failure Parameter [5] contains the previous PDAL address of error register. ■ Last Failure Parameter [6] contains the current PDAL address of error register.	20
01902086	The PCI bus on the controller will not allow a master to initiate a transfer. Unable to provide further diagnosis of the problem. ■ Last Failure Parameter [0] contains the value of read diagnostic register 0. ■ Last Failure Parameter [1] contains the value of read diagnostic register 1. ■ Last Failure Parameter [2] contains the value of read diagnostic register 2. ■ Last Failure Parameter [3] contains the value of write diagnostic register 0. ■ Last Failure Parameter [4] contains the value of write diagnostic register 1. ■ Last Failure Parameter [5] contains the IBUS address of error register.	20
01910084	A Cache Module was inserted or removed. ■ Last Failure Parameter [0] contains the value of actual Cache Module A exists state. ■ Last Failure Parameter [1] contains the value of actual Cache Module B exists state. ■ Last Failure Parameter [2] contains the value of expected Cache Module A exists state. ■ Last Failure Parameter [3] contains the value of expected Cache Module B exists state.	00

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 6 of 42)

Last Failure Code	Description	Repair Action Code
01920186	Unable to read the FX because a Device Port or a Host Port locked the PDAL bus. ■ Last Failure Parameter [0] contains the value of read diagnostic register 0. ■ Last Failure Parameter [1] contains the value of read diagnostic register 1. ■ Last Failure Parameter [2] contains the value of read diagnostic register 2. ■ Last Failure Parameter [3] contains the value of write diagnostic register 0. ■ Last Failure Parameter [4] contains the value of write diagnostic register 1. ■ Last Failure Parameter [5] contains the IBUS address of error register.	01
01932588	An error has occurred on the *cache data/address line (CDAL)*. ■ Last Failure Parameter [0] contains the value of read diagnostic register 0. ■ Last Failure Parameter [1] contains the value of read diagnostic register 1. ■ Last Failure Parameter [2] contains the value of write diagnostic register 0. ■ Last Failure Parameter [3] contains the value of write diagnostic register 1. ■ Last Failure Parameter [4] contains the IBUS address of error register. ■ Last Failure Parameter [5] contains the PCFX *CDAL* control / status register. ■ Last Failure Parameter [6] contains the previous *CDAL* address of error register. ■ Last Failure Parameter [7] contains the current *CDAL* address of error register.	25
01942088	Changes to *PDAL*.	20
01950188	An error has occurred that caused the FX to be reset, when not permissible. ■ Last Failure Parameter [0] contains the value of read diagnostic register 0. ■ Last Failure Parameter [1] contains the value of read diagnostic register 1. ■ Last Failure Parameter [2] contains the value of write diagnostic register 0. ■ Last Failure Parameter [3] contains the value of write diagnostic register 1. ■ Last Failure Parameter [4] contains the IBUS address of error register. ■ Last Failure Parameter [5] contains the PCFX PDAL control / status register. ■ Last Failure Parameter [6] contains the PCFX CDAL control / status register. ■ Last Failure Parameter [7] contains the current PDAL address of error register.	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 7 of 42)

Last Failure Code	Description	Repair Action Code
01960186	The IBUS is inaccessible. ■ Last Failure Parameter [0] contains the value of read diagnostic register 0. ■ Last Failure Parameter [1] contains the value of read diagnostic register 1. ■ Last Failure Parameter [2] contains the value of read diagnostic register 2. ■ Last Failure Parameter [3] contains the value of write diagnostic register 0. ■ Last Failure Parameter [4] contains the value of write diagnostic register 1. ■ Last Failure Parameter [5] contains the IBUS address of error register.	01
01970188	Software indicates all NMI causes cleared, but some remain. ■ Last Failure Parameter [0] contains the value of read diagnostic register 0. ■ Last Failure Parameter [1] contains the value of read diagnostic register 1. ■ Last Failure Parameter [2] contains the value of read diagnostic register 2. ■ Last Failure Parameter [3] contains the value of write diagnostic register 0. ■ Last Failure Parameter [4] contains the value of write diagnostic register 1. ■ Last Failure Parameter [5] contains the IBUS address of error register. ■ Last Failure Parameter [6] contains the PCFX PDAL control / status register. ■ Last Failure Parameter [7] contains the PCFX CDAL control / status register.	01
01982087	The IBUS encountered a parity error. ■ Last Failure Parameter [0] contains the value of read diagnostic register 0. ■ Last Failure Parameter [1] contains the value of read diagnostic register 1. ■ Last Failure Parameter [2] contains the value of read diagnostic register 2. ■ Last Failure Parameter [3] contains the value of write diagnostic register 0. ■ Last Failure Parameter [4] contains the value of write diagnostic register 1. ■ Last Failure Parameter [5] contains the IBUS address of error register. ■ Last Failure Parameter [6] contains the RIP.	20

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 8 of 42)

Last Failure Code	Description	Repair Action Code
01992088	An error was detected by the PLX. ■ Last Failure Parameter [0] contains the value of read diagnostic register 0. ■ Last Failure Parameter [1] contains the value of read diagnostic register 1. ■ Last Failure Parameter [2] contains the value of write diagnostic register 0. ■ Last Failure Parameter [3] contains the value of write diagnostic register 1. ■ Last Failure Parameter [4] contains the IBUS address of error register. ■ Last Failure Parameter [5] contains the PLX status register. ■ Last Failure Parameter [6] contains the previous PDAL address of error register. ■ Last Failure Parameter [7] contains the RIP.	20
02010100	Initialization code was unable to allocate enough memory to set up the send data descriptors.	01
02040100	Unable to allocate memory necessary for data buffers.	01
02050100	Unable to allocate memory for the Free Buffer Array.	01
02080100	A call to EXEC$ALLOCATE_MEM_ZEROED failed to return memory when populating the *disk read* Device Work Descriptor (DWD) stack.	01
02090100	Changes to *disk write*.	
020A0100	Changes to *tape read*.	
020B0100	Changes to *tape write*.	
020C0100	Changes to *miscellaneous*.	
02100100	A call to EXEC$ALLOCATE_MEM_ZEROED failed to return memory when creating the device services state table.	01
02170100	Unable to allocate memory for the Free Node Array.	01
021D0100	Unable to allocate memory for the Free Buffer Array.	01
021F0100	Unable to allocate memory for write algorithm request packets (WARPs) and RAID member data (RMDs).	01
02210100	Invalid parameters in CACHE$OFFER_META call.	01
02220100	No buffer found for CACHE$MARK_META_DIRTY call.	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 9 of 42)

Last Failure Code	Description	Repair Action Code
02270104	A callback from device services (DS) on a transfer request has returned a bad or illegal DWD status. ■ Last Failure Parameter [0] contains the DWD Status. ■ Last Failure Parameter [1] contains the DWD address. ■ Last Failure Parameter [2] contains the Physical Unit Block (PUB) address. ■ Last Failure Parameter [3] contains the Device Port.	01
02360101	Unrecognized state supplied to FOC$SEND callback routine VA_DAP_SND_CMD_COMPLETE. Last Failure Parameter [0] contains the unrecognizable value.	01
02370102	Unsupported return from HIS$GET_CONN_INFO routine. ■ Last Failure Parameter [0] contains the device descriptor (DD) Address. ■ Last Failure Parameter [1] contains the invalid status.	01
02380102	An invalid status was returned from CACHE$LOCK_READ( ). ■ Last Failure Parameter [0] contains the DD address. ■ Last Failure Parameter [1] contains the invalid status.	01
023A2084	A processor interrupt was generated by the controller FX, indicating an unrecoverable error condition. ■ Last Failure Parameter [0] contains the FX CSR. ■ Last Failure Parameter [1] contains the FX direct memory access (DMA) Indirect List Pointer register (DILP). ■ Last Failure Parameter [2] contains the FX DMA Page Address register (DADDR). ■ Last Failure Parameter [3] contains the FX DMA Command and Control register (DCMD).	20
02440100	The logical unit mapping type was detected invalid in VA_SET_DISK_GEOMETRY( ).	01
02530102 02560102	An invalid status was returned from CACHE$LOOKUP_LOCK( ). ■ Last Failure Parameter [0] contains the DD address. ■ Last Failure Parameter [1] contains the invalid status.	01
02570102	An invalid status was returned from VA$XFER( ) during an operation. ■ Last Failure Parameter [0] contains the DD address. ■ Last Failure Parameter [1] contains the invalid status.	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 10 of 42)

Last Failure Code	Description	Repair Action Code
025A0102	An invalid status was returned from CACHE$LOOKUP_LOCK( ). ■ Last Failure Parameter [0] contains the DD address. ■ Last Failure Parameter [1] contains the invalid status.	01
02690102	An invalid status was returned from CACHE$OFFER_WRITE_DATA( ). ■ Last Failure Parameter [0] contains the DD address. ■ Last Failure Parameter [1] contains the invalid status.	01
027B0102	An invalid status was returned from VA$XFER( ) in a complex ACCESS operation. ■ Last Failure Parameter [0] contains the DD address. ■ Last Failure Parameter [1] contains the invalid status.	01
027D0100 027E0100 027F0100 02800100	Unable to allocate memory for a Failover Control Block.	01
02840100	Unable to allocate memory for the XNode Array.	01
02860100	Unable to allocate memory for the Fault Management Event Information Packet used by the Cache Manager in generating error logs to the host.	01
02880100	Invalid failover control (FOC) Message in CMFOC_SND_CMD.	01
028A0100 028B0100	Invalid return status from DIAG$CACHE_MEMORY_TEST.	01
028C0100	Invalid error status given to CACHE_FAIL.	01
028E0100	Invalid device correlation array (DCA) state detected in INIT_CRASHOVER.	01
02910100	Invalid metadata combination detected in BUILD_RAID_NODE.	01
02920100	Unable to handle that many bad dirty pages (exceeded MAX_BAD_DIRTY). Cache memory is bad.	01
02930100	There was no free or freeable buffer to convert bad metadata or to borrow a buffer during failover of bad dirty data.	01
02940100	A free Device Correlation Array entry could not be found during write-back cache failover.	01
02950100	Invalid DCA state detected in START_CRASHOVER.	01
02960100	Invalid DCA state detected in START_FAILOVER.	01
02970100	Invalid DCA state detected in INIT_FAILOVER.	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 11 of 42)

Last Failure Code	Description	Repair Action Code
02990100	A free RAID Correlation Array entry could not be found during write-back cache failover.	01
029A0100	Invalid cache buffer metadata detected while scanning the Buffer Metadata Array. Found a page containing dirty data but the corresponding Device Correlation Array entry does exist.	01
029D0100	Invalid metadata combination detected in BUILD_BAD_RAID_NODE.	01
029F0100	The Cache Manager software has insufficient resources to handle a buffer request pending.	01
02A00100	Value added (VA) change state is trying to change device affinity and the cache has data for this device.	01
02A10100 02A20100	Pubs not one when transportable.	01
02A30100	No available data buffers. If the cache module exists then this is true after testing the whole cache. Otherwise there were no buffers allocated from BUFFER memory on the controller module.	01
02A40100	A call to EXEC$ALLOCATE_MEM_ZEROED failed to return memory when allocating *VA transfer descriptors (VAXDs)*.	01
02A50100	Changes to *DILPs*.	
02A60100	A call to EXEC$ALLOCATE_MEM_ZEROED failed to return memory when allocating *Change State Work Items*.	01
02A70100	Changes to *VA Request Items*.	
02A90100	Too many pending FOC$SEND requests by the Cache Manager. Code is not designed to handle more than one FOC$SEND pending because there is no reason to expect more than one pending.	01
02AA0100	An invalid call was made to CACHE$DEALLOCATE_CLD. Either that device had dirty data or it was bound to a RAIDset.	01
02AB0100	An invalid call was made to CACHE$DEALLOCATE_SLD. A RAIDset member either had dirty data or write-back already turned on.	01
02AC0100	An invalid call was made to CACHE$DEALLOCATE_SLD. The RAIDset still has data (strip nodes).	01
02AE0100	The mirrorset member count and individual member states are inconsistent. Discovered during a mirrorset write or erase.	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 12 of 42)

Last Failure Code	Description	Repair Action Code
02AF0102	An invalid status was returned from VA$XFER( ) in a *write* operation. ■ Last Failure Parameter [0] contains the DD address. ■ Last Failure Parameter [1] contains the invalid status.	01
02B00102	Changes to *erase*.	
02B10100	A mirrorset read operation was received and the round robin selection algorithm found no normal members in the mirrorset. Internal inconsistency.	01
02B20102	An invalid status was returned from CACHE$LOCK_READ during a mirror copy operation. ■ Last Failure Parameter [0] contains the DD address. ■ Last Failure Parameter [1] contains the invalid status.	01
02B30100	CACHE$CHANGE_MIRROR_MODE invoked illegally (cache bad, dirty data still resident in the cache.)	01
02B90100	Invalid code loop count attempting to find the Cache ID Blocks.	01
02BD0100	A mirrorset metadata online operation found no normal members in the mirrorset. Internal inconsistency.	01
02BE0100	No free pages in the other cache. In performing mirror cache failover, a bad page was found, and an attempt was made to recover the data from the good copy (primary/mirror), but no free good page was found on the other cache to copy the data to.	01
02BF0100	REPORT_ERROR routine encountered an unexpected failure status returned from DIAG$LOCK_AND_TEST_CACHE_B.	01
02C00100	COPY_BUFF_ON_THIS routine expected the given page to be marked bad and it was not.	01
02C10100	COPY_BUFF_ON_OTHER routine expected the given page to be marked bad and it was not.	01
02C30100	CACHE$CREATE_MIRROR was invoked by C_SWAP under unexpected conditions (e.g., other controller not dead, bad lock state).	01
02C60100	Mirroring transfer found cache list descriptor (CLD) with writeback state OFF.	01
02C70100	Bad BBR offsets for active shadowset, detected on *write*.	01
02C80100	Changes to *read*.	
02C90100	Illegal call made to CACHE$PURGE_META when the storageset was not quiesced.	01
02CA0100	Illegal call made to VA$RAID5_META_READ when another read (of metadata) is already in progress on the same strip.	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 13 of 42)

Last Failure Code	Description	Repair Action Code
02CB0000	A restore of the configuration has been done. This cleans up and restarts with the new configuration.	00
02CC0100	On an attempt to allocate a cache node, which is not allowed to fail, no freeable cache node was found.	01
02D00100	Not all ALTER_DEVICE requests from VA_SAVE_CONFIG completed within the timeout interval.	01
02D30100	The controller has insufficient memory to allocate enough data structures used to manage metadata operations.	01
02D60100	An invalid storage set type was specified for metadata initialization.	01
02D90100	Bad CLD pointer passed setwb routine.	01
02DA0100	A fatal logic error occurred while trying to restart a stalled data transfer stream.	01
02DB0100	A call to EXEC$ALLOCATE_MEM_ZEROED failed to return memory when populating the *disk read* PCI XOR engine (PCX) DWD stack.	01
02DC0100	Changes to *disk write*.	
02DD0101	The VA state change deadman timer expired, and at least one VA state information (VSI) was still interlocked. ■ Last Failure Parameter [0] contains the NV_INDEX.	01
02DE0100	An attempt to allocate memory for a null PUB failed to get the memory.	01
02DF0101	License identified in Last Failure Parameter [0] was not forced valid.	01
02E00180	Mirror functionality is broken.	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 14 of 42)

Last Failure Code	Description	Repair Action Code
02E11016	While attempting to restore saved configuration information, data for two unrelated controllers was found. The restore code is unable to determine which disk contains the correct information. The Port/Target/LUN information for the two disks is contained in the parameter list. Remove the disk containing the incorrect information, reboot the controller, and issue the SET THIS_CONTROLLER INITIAL_CONFIGURATION command. When the controller restarts, the proper configuration will be loaded. ■ Last Failure Parameter [0] contains the first disk port. ■ Last Failure Parameter [1] contains the first disk target. ■ Last Failure Parameter [2] contains the first disk LUN. ■ Last Failure Parameter [3] contains the second disk port. ■ Last Failure Parameter [4] contains the second disk target. ■ Last Failure Parameter [5] contains the second disk LUN.	10
02E20100	An attempt to allocate a VA_CS_WORK item from the S_VA_FREE_CS_WORK_QUEUE failed.	01
02E30100 02E40100 02E50100 02E60100 02E70100 02E80100 02E90100 02EA0100	An attempt to allocate a free VA request (VAR) failed.	01
02EB0100	An attempt to allocate a free metadata WARP failed.	01
02EC0101	An online request was received for a unit when both controllers had dirty data for the unit. The crash allows the surviving controller to copy over all of the dirty data. ■ Last Failure Parameter [0] contains the NV_INDEX of the unit.	01
02ED0100	On an attempt to allocate a buffer descriptor block (BDB), which is not allowed to fail, no freeable BDB was found.	01
02EE0102	A CLD is already allocated when it should be free. ■ Last Failure Parameter [0] contains the requesting entity. ■ Last Failure Parameter [1] contains the CLD index.	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 15 of 42)

Last Failure Code	Description	Repair Action Code
02EF0102	A CLD is free when it should be allocated. ■ Last Failure Parameter [0] contains the requesting entity. ■ Last Failure Parameter [1] contains the CLD index.	01
02F00100	The controller has insufficient free resources for the configuration restore process to obtain a facility lock.	01
02F10102	The configuration restore process encountered an unexpected non-volatile parameter store format. The process cannot restore from this version. ■ Last Failure Parameter [0] contains the version found. ■ Last Failure Parameter [1] contains the expected version.	01
02F20100	The controller has insufficient free resources for the configuration restore process to release a facility lock.	01
02F34083	A device read operation failed during the configuration restore operation. The controller is crashed to prevent possible loss of saved configuration information on other functioning devices. ■ Last Failure Parameter [0] contains the disk port. ■ Last Failure Parameter [1] contains the disk target. ■ Last Failure Parameter [2] contains the disk LUN.	40
02F44083	The calculated error detection code on the saved configuration information is bad. The controller is crashed to prevent destruction of other copies of the saved configuration information. Remove the device with the bad information and retry the operation. ■ Last Failure Parameter [0] contains the disk port. ■ Last Failure Parameter [1] contains the disk target. ■ Last Failure Parameter [2] contains the disk LUN.	40
02F54083	The device saved configuration information selected for the restore process is from an unsupported controller type. Remove the device with the unsupported information and retry the operation. ■ Last Failure Parameter [0] contains the disk port. ■ Last Failure Parameter [1] contains the disk target. ■ Last Failure Parameter [2] contains the disk LUN.	40

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 16 of 42)

Last Failure Code	Description	Repair Action Code
02F60103	An invalid modification to the NO_INTERLOCK VSI flag was attempted. ■ Last Failure Parameter [0] contains the NV_INDEX of the config on which the problem was found. ■ Last Failure Parameter [1] contains the modification flag. ■ Last Failure Parameter [2] contains the current value of the NO_INTERLOCK flag. If the modification flag is 1, then an attempt was being made to set the NO_INTERLOCK flag, and the NO_INTERLOCK flag was not clear at the time. If the modification flag is 0, then an attempt was being made to clear the NO_INTERLOCK flag, and the NO_INTERLOCK flag was not set (== 1) at the time.	01
02F70100	During boot testing, one or more device ports (SCSI) were found to be bad. Due to a problem in the SYM53C770 chip, the diagnostic may occasionally fail the port even though the hardware is OKAY. A reboot should clear up the problem. If the port is actually broken, logic to detect a loop that repeatedly causes the same bugcheck will cause a halt.	01
02F80103	An attempt was made to bring a unit online when the cache manager says that a member CLD was not in the appropriate state. ■ Last Failure Parameter [0] contains the NV_INDEX of the config on which the problem was found. ■ Last Failure Parameter [1] contains the map type of that config. ■ Last Failure Parameter [2] contains the value from CACHE$CHECK_CID that was not acceptable.	01
02F90100	A call to EXEC$ALLOCATE_MEM_ZEROED failed to return memory when allocating structures for read ahead caching.	01
02FA0100	A read ahead data descriptor (RADD) is inconsistent.	01
02FB2084	A processor interrupt was generated by the controller FX, indicating an unrecoverable error condition. ■ Last Failure Parameter [0] contains the FX CSR. ■ Last Failure Parameter [1] contains the FX DILP. ■ Last Failure Parameter [2] contains the FX DADDR. ■ Last Failure Parameter [3] contains the FX DCMD.	20
02FC0180	The FX detected a compare error for data that was identical. This error has always previously occurred due to a hardware problem.	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 17 of 42)

Last Failure Code	Description	Repair Action Code
02FD0100	The controller has insufficient free memory to restore saved configuration information from disk.	01
02FE0105	A field in the VSI was not cleared when an attempt was made to clear the interlock. ■ Last Failure Parameter [0] contains the nonvolatile (NV) index of the VSI on which the problem was found. ■ Last Failure Parameter [1] contains the contents of the ENABLE_CHANGE field of the VSI, which should be zero. ■ Last Failure Parameter [2] contains the contents of the DESIRED_STATE field of the VSI, which should be zero. ■ Last Failure Parameter [3] contains the contents of the COMPLETION_ROUTINE field of the VSI, which should be zero. ■ Last Failure Parameter [4] contains the contents of the OPEN_REQUESTS field of the VSI, which should be zero.	01
03010100	Failed request for port-specific scripts memory allocation.	01
03020101	Invalid SCSI direct-access device opcode in miscellaneous command DWD. ■ Last Failure Parameter [0] contains the SCSI command opcode.	01
03030101	Invalid SCSI sequential-access device opcode in miscellaneous command DWD. ■ Last Failure Parameter [0] contains the SCSI command opcode.	01
03040101	Invalid SCSI CDROM device opcode in miscellaneous command DWD. ■ Last Failure Parameter [0] contains the SCSI command opcode.	01
03050101	Invalid SCSI medium changer device opcode in miscellaneous command DWD. ■ Last Failure Parameter [0] contains the SCSI command opcode.	01
03060101	Invalid SCSI device type in PUB. ■ Last Failure Parameter [0] contains the SCSI device type.	01
03070101	Invalid command description block (CDB) Group Code detected during create of miscellaneous command DWD. ■ Last Failure Parameter [0] contains the SCSI command opcode.	01
03080101	Invalid SCSI OPTICAL MEMORY device opcode in miscellaneous command DWD. ■ Last Failure Parameter [0] contains the SCSI command opcode.	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 18 of 42)

Last Failure Code	Description	Repair Action Code
03090101	Failed request for allocation of PCI miscellaneous block. ■ Last Failure Parameter [0] contains the failed DWD command class.	01
030A0100	Error DWD not found in port IN_PROC_Q.	01
030B0188	A dip error was detected when PCB_BUSY was set. ■ Last Failure Parameter [0] contains the process controls block (PCB) PORT_PTR value. ■ Last Failure Parameter [1] contains the new info NULL-SSTAT0-DSTAT-ISTAT. ■ Last Failure Parameter [2] contains the PCB copy of the device port DMA byte counter (DBC) register. ■ Last Failure Parameter [3] contains the PCB copy of the device port DMA next address data (DNAD) register. ■ Last Failure Parameter [4] contains the PCB copy of the device port DMA SCRIPTS™ pointer (DSP) register. ■ Last Failure Parameter [5] contains the PCB copy of the device port DMA SCRIPTS pointer saved (DSPS) register. ■ Last Failure Parameter [6] contains the PCB copies of the device port SSTAT2/SSTAT1/SSTAT0/DSTAT registers. ■ Last Failure Parameter [7] contains the PCB copies of the device port LCRC/RESERVED/ISTAT/DFIFO registers.	01
031E0100	Cannot find IN_ERROR DWD on in-process queue.	01
031F0100	Either DWD_PTR is null or bad value in dsps.	01
03280100	SCSI CDB contains an invalid group code for a transfer command.	01
03290100	The required Event Information Packet (EIP) or DWD were not supplied to the Device Services error logging code.	01
032A0100	HIS$GET_CONN_INFO( ) returned an unexpected completion code.	01
032B0100	A DWD was supplied with a NULL PUB pointer.	01
03320101	An invalid code was passed to the error recovery thread in the ERROR_STAT field of the PCB. ■ Last Failure Parameter [0] contains the PCB ERROR_STAT code.	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 19 of 42)

Last Failure Code	Description	Repair Action Code
03330188	A parity error was detected by a device port while sending data out onto the SCSI bus. ■ Last Failure Parameter [0] contains the PCB PORT_PTR value. ■ Last Failure Parameter [1] contains the PCB copy of the device port TEMP register. ■ Last Failure Parameter [2] contains the PCB copy of the device port DBC register. ■ Last Failure Parameter [3] contains the PCB copy of the device port DNAD register. ■ Last Failure Parameter [4] contains the PCB copy of the device port DSP register. ■ Last Failure Parameter [5] contains the PCB copy of the device port DSPS register. ■ Last Failure Parameter [6] contains the PCB copies of the device port SSTAT2/SSTAT1/SSTAT0/DSTAT registers. ■ Last Failure Parameter [7] contains the PCB copies of the device port LCRC/RESERVED/ISTAT/DFIFO registers.	01
03370108	A device port detected an illegal script instruction. ■ Last Failure Parameter [0] contains the PCB PORT_PTR value. ■ Last Failure Parameter [1] contains the PCB copy of the device port TEMP register. ■ Last Failure Parameter [2] contains the PCB copy of the device port DBC register. ■ Last Failure Parameter [3] contains the PCB copy of the device port DNAD register. ■ Last Failure Parameter [4] contains the PCB copy of the device port DSP register. ■ Last Failure Parameter [5] contains the PCB copy of the device port DSPS register. ■ Last Failure Parameter [6] contains the PCB copies of the device port SSTAT2/SSTAT1/SSTAT0/DSTAT registers. ■ Last Failure Parameter [7] contains the PCB copies of the device port LCRC/RESERVED/ISTAT/DFIFO registers.	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 20 of 42)

Last Failure Code	Description	Repair Action Code
03380188	A device port device statistics (DSTAT) register contains multiple asserted bits, or an invalidly asserted bit, or both. ■ Last Failure Parameter [0] contains the PCB PORT_PTR value. ■ Last Failure Parameter [1] contains the PCB copy of the device port TEMP register. ■ Last Failure Parameter [2] contains the PCB copy of the device port DBC register. ■ Last Failure Parameter [3] contains the PCB copy of the device port DNAD register. ■ Last Failure Parameter [4] contains the PCB copy of the device port DSP register. ■ Last Failure Parameter [5] contains the PCB copy of the device port DSPS register. ■ Last Failure Parameter [6] contains the PCB copies of the device port SSTAT2/SSTAT1/SSTAT0/DSTAT registers. ■ Last Failure Parameter [7] contains the PCB copies of the device port LCRC/RESERVED/ISTAT/DFIFO registers.	01
03390108	An unknown interrupt code was found in a device port DSPS register. ■ Last Failure Parameter [0] contains the PCB PORT_PTR value. ■ Last Failure Parameter [1] contains the PCB copy of the device port TEMP register. ■ Last Failure Parameter [2] contains the PCB copy of the device port DBC register. ■ Last Failure Parameter [3] contains the PCB copy of the device port DNAD register. ■ Last Failure Parameter [4] contains the PCB copy of the device port DSP register. ■ Last Failure Parameter [5] contains the PCB copy of the device port DSPS register. ■ Last Failure Parameter [6] contains the PCB copies of the device port SSTAT2/SSTAT1/SSTAT0/DSTAT registers. Last Failure Parameter [7] contains the PCB copies of the device port LCRC/RESERVED/ISTAT/DFIFO registers.	01
033C0101	An invalid code was seen by the error recovery thread in the ER_FUNCT_STEP field of the PCB. ■ Last Failure Parameter [0] contains the PCB ER_FUNCT_STEP code.	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 21 of 42)

Last Failure Code	Description	Repair Action Code
033E0108	An attempt was made to restart a device port at the save data pointer (SDP) data buffer descriptor (DBD). ■ Last Failure Parameter [0] contains the PCB PORT_PTR value. ■ Last Failure Parameter [1] contains the PCB copy of the device port TEMP register. ■ Last Failure Parameter [2] contains the PCB copy of the device port DBC register. ■ Last Failure Parameter [3] contains the PCB copy of the device port DNAD register. ■ Last Failure Parameter [4] contains the PCB copy of the device port DSP register. ■ Last Failure Parameter [5] contains the PCB copy of the device port DSPS register. ■ Last Failure Parameter [6] contains the PCB copies of the device port SSTAT2/SSTAT1/SSTAT0/DSTAT registers. ■ Last Failure Parameter [7] contains the PCB copies of the device port LCRC/RESERVED/ISTAT/DFIFO registers.	01
033F0108	An EDC error was detected on a read of a soft-sectored device path not yet implemented. ■ Last Failure Parameter [0] contains the PCB PORT_PTR value. ■ Last Failure Parameter [1] contains the PCB copy of the device port TEMP register. ■ Last Failure Parameter [2] contains the PCB copy of the device port DBC register. ■ Last Failure Parameter [3] contains the PCB copy of the device port DNAD register. ■ Last Failure Parameter [4] contains the PCB copy of the device port DSP register. ■ Last Failure Parameter [5] contains the PCB copy of the device port DSPS register. ■ Last Failure Parameter [6] contains the PCB copies of the device port SSTAT2/SSTAT1/SSTAT0/DSTAT registers. ■ Last Failure Parameter [7] contains the PCB copies of the device port LCRC/RESERVED/ISTAT/DFIFO registers.	01
03410101	Invalid SCSI device type in PUB. ■ Last Failure Parameter [0] contains the PUB SCSI device type.	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 22 of 42)

Last Failure Code	Description	Repair Action Code
03450188	A Master Data Parity Error was detected by a port. ■ Last Failure Parameter [0] contains the PCB PORT_PTR value. ■ Last Failure Parameter [1] contains the PCB copies of the device port DCMD/DBC registers. ■ Last Failure Parameter [2] contains the PCB copy of the device port DNAD register. ■ Last Failure Parameter [3] contains the PCB copy of the device port DSP register. ■ Last Failure Parameter [4] contains the PCB copy of the device port DSPS register. ■ Last Failure Parameter [5] contains the PCB copies of the device port DSTAT/SSTAT0/SSTAT1/SSTAT2 registers. ■ Last Failure Parameter [6] contains the PCB copies of the device port DFIFO/ISTAT/SBCL/RESERVED registers. ■ Last Failure Parameter [7] contains the PCB copies of the device port SIST0/SIST1/SXFER/SCNTL3 registers.	01
03470100	Insufficient memory available for target block allocation.	01
03480100	Insufficient memory available for device port info block allocation.	01
03490100	Insufficient memory available for autoconfig buffer allocation.	01
034A0100	Insufficient memory available for PUB allocation.	01
034B0100	Insufficient memory available for DS init buffer allocation.	01
034C0100	Insufficient memory available for static structure allocation.	01
034D0100	DS init DWDs exhausted.	01
034E2080	Diagnostics report all device ports are broken.	20
034F0100	Insufficient memory available for reselect target block allocation.	01
03500100	Insufficient memory available for command disk allocation.	01
03520100	A failure resulted when an attempt was made to allocate a DWD for use by DS command data interface (CDI).	01
03530102	A DWD with an illegal address has been found. ■ Last Failure Parameter [0] contains the bad DWD pointer. ■ Last Failure Parameter [1] contains the corresponding PCB pointer.	01
03640100	Processing RUN_SWITCH disabled for LOGDISK associated with the other controller.	01
03650100	Processing PUB unblock for LOGDISK associated with the other controller.	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 23 of 42)

Last Failure Code	Description	Repair Action Code
03660100	No memory available to allocate PUB to tell the other controller of *reset* to one if its LUNs.	01
03670100	Changes to *a bad block replacement (BDR)*.	
036F0101	Either SEND_SDTR or SEND_WDTR flag set in a non-miscellaneous DWD. ■ Last Failure Parameter [0] contains the invalid command class type.	01
03780181	In DS_GET_RESUME_ADDR, the buffer address is non-longword aligned for FX access. ■ Last Failure Parameter [0] contains the re-entry dbd address value.	01
03790188	A PCI bus fault was detected by a device port. ■ Last Failure Parameter [0] contains the PCB PORT_PTR value. ■ Last Failure Parameter [1] contains the PCB copy of the device port TEMP register. ■ Last Failure Parameter [2] contains the PCB copy of the device port DBC register. ■ Last Failure Parameter [3] contains the PCB copy of the device port DNAD register. ■ Last Failure Parameter [4] contains the PCB copy of the device port DSP register. ■ Last Failure Parameter [5] contains the PCB copy of the device port DSPS register. ■ Last Failure Parameter [6] contains the PCB copies of the device port SSTAT2/SSTAT1/SSTAT0/DSTAT registers. ■ Last Failure Parameter [7] contains the PCB copies of the device port LCRC/RESERVED/ISTAT/DFIFO registers.	01
03820100	Failed request for mapping table memory allocation.	01
03830100	Failed request for SYM53C875 PCI block memory allocation.	01
03850101	DS_ALLOC_MEM called with invalid memory type. ■ Last Failure Parameter [0] contains the invalid memory type.	01
03860100	DS_ALLOC_MEM was unable to get requested memory allocated: NULL pointer returned.	01
038C0100	Insufficient memory available for completion of DWD array allocation.	01
03980100	Failed to allocate expandable EMU static work structures.	01
03990100	Failed to allocate expandable EMU work entry.	01
039A0100	Failed to allocate expandable EMU FOC work entry.	01
039B0100	EMU request work queue corrupted.	01
039C0100	EMU response work queue corrupted.	01
039D0100	EMU work queue corrupted.	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 24 of 42)

Last Failure Code	Description	Repair Action Code
039E0100	EMU FOC request work queue corrupted.	01
039F0100	EMU FOC response work queue corrupted.	01
03A08093	A configuration or hardware error was reported by the EMU. ■ Last Failure Parameter [0] contains the solid OCP pattern which identifies the type of problem encountered. ■ Last Failure Parameter [1] contains the cabinet ID reporting the problem. ■ Last Failure Parameter [2] contains the SCSI Port number where the problem exists (if port-specific).	80
03A28193	The EMU reported Terminator Power out of range. ■ Last Failure Parameter [0] contains a bit mask indicating which SCSI Port number(s) where the problem exists for cabinet 0. Bit 0 set indicates SCSI Port 1, Bit 1 set indicates SCSI port 2, etc. ■ Last Failure Parameter [1] contains a bit mask indicating which SCSI Port number(s) where the problem exists for cabinet 2. ■ Last Failure Parameter [2] contains a bit mask indicating which SCSI Port number(s) where the problem exists for cabinet 3.	81
03A30790	The EMU in cabinet 0 is performing an emergency shutdown because there are less than four functioning power supplies.	07
03A40D90	The EMU in cabinet 0 is performing an emergency shutdown because it has determined that the temperature is above the maximum limit.	0D
03A50690	The EMU in cabinet 0 is performing an emergency shutdown because a fan has been missing for more than 8 minutes.	06
04010101	The requester ID component of the Instance Code passed to FM$REPORT_EVENT is larger than the maximum allowed for this environment. ■ Last Failure Parameter [0] contains the Instance Code value.	01
04020102	The requester error table index passed to FM$REPORT_EVENT is larger than the maximum allowed for this requester. ■ Last Failure Parameter [0] contains the Instance Code value. ■ Last Failure Parameter [1] contains the requester error table index value.	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 25 of 42)

Last Failure Code	Description	Repair Action Code
04030102	The unit state block (USB) index supplied in the EIP is larger than the maximum number of USBs. ■ Last Failure Parameter [0] contains the Instance Code value. ■ Last Failure Parameter [1] contains the USB index value.	01
04040103	The event log format found in V_FM_TEMPLATE_TABLE is not supported by the Fault Manager. The bad format was discovered while trying to fill in a supplied EIP. ■ Last Failure Parameter [0] contains the Instance Code value. ■ Last Failure Parameter [1] contains the format code value. ■ Last Failure Parameter [2] contains the requester error table index value.	01
04050100	The Fault Manager could not allocate memory for its EIP buffers.	01
04060100	The Fault Manager could not allocate a Datagram host transaction block (HTB) in its initialization routine.	01
04070103	There is more EIP information than fits into a datagram. The requester specific size is probably too large. ■ Last Failure Parameter [0] contains the instance code value. ■ Last Failure Parameter [1] contains the format code value. ■ Last Failure Parameter [2] contains the requester error table index value.	01
04080102	The event log format found in the already built EIP is not supported by the Fault Manager. The bad format was discovered while trying to copy the EIP information into a datagram HTB. ■ Last Failure Parameter [0] contains the format code value. ■ Last Failure Parameter [1] contains the instance code value.	01
04090100	The caller of FM$CANCEL_EVENT_NOTIFICATION passed an address of an event notification routine which does not match the address of any routines for which event notification was enabled.	01
040D0100	FM$ENABLE_EVENT_NOTIFICATION was called to enable EIP notification but the specified routine was already enabled to receive EIP notification.	01
040F0102	The EIP->GENERIC.MSCP1.FLGS field of the EIP passed to FM$REPORT_EVENT contains an invalid flag. ■ Last Failure Parameter [0] contains the Instance Code value. ■ Last Failure Parameter [1] contains the value supplied in the EIP->GENERIC.MSCP1.FLGS field.	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 26 of 42)

Last Failure Code	Description	Repair Action Code
04100101	Unexpected template type found during FMU_DISPLAY_ERRLOG processing. ■ Last Failure Parameter [0] contains the unexpected template value.	01
04110101	Unexpected Instance Code found during FMU_MEMERR_REPORT processing. ■ Last Failure Parameter [0] contains the unexpected Instance Code value.	01
04120101	CLIB$SDD_FAO call failed. ■ Last Failure Parameter [0] contains the failure status code value.	01
05010100	In RECURSIVE_NONCONFLICT could not get enough memory for scanning the keyword tables for configuration name conflicts.	01
06010100	The DUART was unable to allocate enough memory to establish a connection to the CLI.	01
06020100	A port other than terminal port A was referred to by a set terminal characteristics command. This is illegal.	01
06030100	A diagnostic utility protocol (DUP) question or default question message type was passed to the DUART driver, but the pointer to the input area to receive the response to the question was NULL.	01
06040100	Attempted to detach unattached maintenance terminal.	01
06050100	Attempted output to unattached maintenance terminal.	01
06060100	Attempted input from output only maintenance terminal service.	01
06070100	The DUART was unable to allocate enough memory for its input buffers	01
06080000	Controller was forced to restart due to entry of a CONTROL-K character on the maintenance terminal.	00
07010100	All available slots in the FOC notify table are filled.	01
07020100	FOC$CANCEL_NOTIFY( ) was called to disable notification for a return that did not have notification enabled.	01
07030100	Unable to start the Failover Control Timer before main loop.	01
07040100	Unable to restart the Failover Control Timer.	01
07050100	Unable to allocate flush buffer.	01
07060100	Unable to allocate active receive failover control block (FCB).	01
07070100	The other controller killed this, but could not assert the kill line because nindy on or in debug. So it “killed” this now.	01
07080000	The other controller crashed, so this one must crash too.	00

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 27 of 42)

Last Failure Code	Description	Repair Action Code
07090100	A call to EXEC$ALLOCATE_MEM_ZEROED failed to return memory when allocating VA Request Items.	01
08010101	A remote state change was received from the FOC thread that nonvolatile FOC (NVFOC) does not recognize. ■ Last Failure Parameter [0] contains the unrecognized state value.	01
08020100	No memory could be allocated for a NVFOC information packet.	01
08030101	Work received on the S_NVFOC_BQUE did not have a NVFOC work ID. ■ Last Failure Parameter [0] contains the ID type value that was received on the NVFOC work queue.	01
08040101	Unknown work value received by the S_NVFOC_BQUE. ■ Last Failure Parameter [0] contains the unknown work value.	01
08060100	A write command was received when the NV memory was not locked.	01
08070100	A write to NV memory was received while not locked.	01
08080000	The other controller requested this controller to restart.	00
08090010	The other controller requested this controller to shut down.	00
080A0000	The other controller requested this controller to self test.	00
080B0100	Could not get enough memory to build a FCB to send to the remote routines on the other controller.	01
080C0100	Could not get enough memory for FCBs to receive information from the other controller.	01
080D0100	Could not get enough memory to build a FCB to reply to a request from the other controller.	01
080E0101	An out-of-range receiver ID was received by the NVFOC communication utility (master send to slave send ACK). ■ Last Failure Parameter [0] contains the bad ID value.	01
080F0101	An out-of-range receiver ID was received by the NVFOC communication utility (received by master). ■ Last Failure Parameter [0] contains the bad ID value.	01
08100101	A call to NVFOC$TRANSACTION had a from field (ID) that was out of range for the NVFOC communication utility. ■ Last Failure Parameter [0] contains the bad ID value.	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 28 of 42)

Last Failure Code	Description	Repair Action Code
08110101	NVFOC tried to defer more than one FOC send. ■ Last Failure Parameter [0] contains the master ID of the connection that had the multiple delays.	01
08140100	Could not allocate memory to build a workblock to queue to the NVFOC thread.	01
08160100	A request to clear the remote configuration was received but the memory was not locked.	01
08170100	A request to read the next configuration was received but the memory was not locked.	01
08180100	Could not get enough memory for firmware licensing system (FLS) FCBs to receive information from the other controller.	01
08190100	An unlock command was received when the NV memory was not locked.	01
081A0100	Unable to allocate memory for remote work.	01
081B0101	Bad remote work received on remote work queue. ■ Last Failure Parameter [0] contains the ID type value that was received on the NVFOC remote work queue.	01
081C0101	Bad member management work received. ■ Last Failure Parameter [0] contains the bad member management value that was detected.	01
081D0000	In order to go into *mirrored* cache mode, the controllers must be restarted.	00
081E0000	Changes to *nonmirrored*.	
081F0000	An FLM$INSUFFICIENT_RESOURCES error was returned from a facility lock manager (FLM) lock or unlock call.	00
08200000	Expected restart so the WRITE_INSTANCE may recover from a configuration mismatch.	00
08210100	Unable to allocate memory to setup NVFOC lock/unlock notification routines.	01
09010100	Unable to acquire memory to initialize the FLM structures.	01
09640101	Work that was not FLM work was found on the FLM queue. Bad format is detected or the formatted string overflows the output buffer. ■ Last Failure Parameter [0] contains the work found.	01
09650101	Work that was not FLM work was found on the FLM queue. ■ Last Failure Parameter [0] contains the structure found.	01
09670101	Local FLM detected an invalid facility to act upon. ■ Last Failure Parameter [0] contains the faciltiy found.	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 29 of 42)

Last Failure Code	Description	Repair Action Code
09680101	Remote FLM detected an error and requested the local controller to restart. ■ Last Failure Parameter [0] contains the reason for the request.	01
09C80101	Remote FLM detected an invalid facility to act upon. ■ Last Failure Parameter [0] contains the facility found.	01
09C90101 09CA0101	Remote FLM detected an invalid work type. ■ Last Failure Parameter [0] contains the work type found.	01
09CB0012	Remote FLM detected that the other controller has a facility lock manager at an incompatible revision level with this controller. ■ Last Failure Parameter [0] contains the this controller FLM revision. ■ Last Failure Parameter [1] contains the other controller FLM revision.	00
0A020100	ILF$CACHE_READY unable to allocate necessary DWDs.	01
0A030100	ILF$CACHE_READY BUFFERS_OBTAINED > non-zero stack entry count.	01
0A040100	ILF$CACHE_READY DWD overrun.	01
0A050100	ILF$CACHE_READY DWD underrun.	01
0A060100	ILF$CACHE_READY found buffer marked for other controller.	01
0A070100	CACHE$FIND_LOG_BUFFERS returned continuation handle > 0.	01
0A080100	Not processing a bugcheck.	01
0A090100	No active DWD.	01
0A0A0100	Current entry pointer is not properly aligned.	01
0A0B0100	Next entry pointer is not properly aligned.	01
0A0E0100	Active DWD is not a DISK WRITE DWD as expected.	01
0A0F0100	New active DWD is not a DISK WRITE DWD as expected.	01
0A100100 0A120100 0A130100	Data buffer pointer is not properly aligned.	01
0A140100	New entry pointer is not properly aligned.	01
0A150100	New entry record type is out of range.	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 30 of 42)

Last Failure Code	Description	Repair Action Code
0A190102	ILF_DEPOPULATE_DWD_TO_CACHE first page guard check failed. ■ Last Failure Parameter [0] contains the DWD address value. ■ Last Failure Parameter [1] contains the buffer address value.	01
0A1C0102 0A1D0102 0A1E0102	ILF$LOG_ENTRY page guard check failed. ■ Last Failure Parameter [0] contains the DWD address value. ■ Last Failure Parameter [1] contains the buffer address value.	01
0A1F0100	ILF_REBIND_CACHE_BUFFS_TO_DWDS found duplicate buffer for current DWD.	01
0A200101	Unknown bugcheck code passed to ILF_CACHE_INTERFACE_CRASH. ■ Last Failure Parameter [0] contains the unknown bugcheck code value.	01
0A210100	ILF_REBIND_CACHE_BUFFS_TO_DWDS found buffer type not IDX_ILF.	01
0A220100	ILF_REBIND_CACHE_BUFFS_TO_DWDS found buffer DBD index too big.	01
0A240100	ILF_CHECK_HANDLE_ARRAY_EDC found ihiea EDC bad.	01
0A250100	ILF_GET_NEXT_HANDLE found no free ihiea entry.	01
0A260100	ILF_REMOVE_HANDLE could not find specified handle.	01
0A270100	ILF_DEPOPULATE_DWD_TO_CACHE could not find handle for first buffer.	01
0A280100	ILF_DEPOPULATE_DWD_TO_CACHE buffer handle does not match current handle.	01
0A290100	ILF_REBIND_CACHE_BUFFS_TO_DWDS could not find handle for DWD being rebound.	01
0A2B0100	ILF$CACHE_READY cache manager did not return multiple of DWD DBDs worth of buffers.	01
0A2C0100	ILF_REBIND_CACHE_BUFFS_TO_DWDS page guard check failed.	01
0A2D0100	ILF_POPULATE_DWD_FROM_CACHE buffer stack entry zero or not page aligned.	01
0A2E0100	ILF_POPULATE_DWD_FROM_CACHE returned buffer type not IDX_ILF.	01
0A2F0100	ILF_REBIND_CACHE_BUFFS_TO_DWDS buffer stack entry not page aligned.	01
0A300100	ILF_DEPOPULATE_DWD_TO_CACHE buffer stack entry zero or not page aligned.	01
0A310100	ILF_DISTRIBUTE_CACHE_DWDS active handle count not as expected.	01
0A320102	ILF$LOG_ENTRY, page guard check failed. ■ Last Failure Parameter [0] contains the DWD address value. ■ Last Failure Parameter [1] contains the buffer address value.	01
0A330100	ILF_OUPUT_ERROR, MESSAGE_KEEPER_ARRAY full.	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 31 of 42)

Last Failure Code	Description	Repair Action Code
0A340101	ILF_OUTPUT_ERROR, no memory for message display. ■ Last Failure Parameter [0] contains the message address value.	01
0A360100	Duplicate entry found in ILF_POPULATE_DWD_FROM_CACHE buffer stack.	01
0A370100	Duplicate entry found in ILF_REBIND_CACHE_BUFFS_TO_DWDS buffer stack.	01
0A380108	Next entry was partially loaded. ■ Last Failure Parameter [0] contains the next entry address. ■ Last Failure Parameter [1] contains the next entry record type. ■ Last Failure Parameter [2] contains the next entry time of day (TOD) flag. ■ Last Failure Parameter [3] contains the next entry interrupt (INT) flag. ■ Last Failure Parameter [4] contains the next entry byte count. ■ Last Failure Parameter [5] contains the next entry TOD ticks. ■ Last Failure Parameter [6] contains the next entry TOD days. ■ Last Failure Parameter [7] contains the next entry data start.	01
0B010010	Due to an operator request, the controller non-volatile configuration information has been reset to its initial state.	00
0B020100	The controller has insufficient free memory to allocate a Configuration Manager work item needed to perform the requested configuration *reset*.	01
0B030100	Changes to *restore*.	
0B0A0100	Unable to find any unused partition group. With 127 available, we should be able to find at least one.	01
0D000011	The EMU firmware returned a bad status when told to power off. ■ Last Failure Parameter [0] contains the value of the bad status.	00
12000103	Two values found *not equal*. ■ Last Failure Parameter [0] contains the ASSUME instance address. ■ Last Failure Parameter [1] contains the first variable value. ■ Last Failure Parameter [2] contains the second variable value.	01
12010103	Changes to *equal*.	

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 32 of 42)

Last Failure Code	Description	Repair Action Code
12020103	First value found *bigger or equal*. ■ Last Failure Parameter [0] contains the ASSUME instance address. ■ Last Failure Parameter [1] contains the first variable value. ■ Last Failure Parameter [2] contains the second variable value.	01
12030103	Changes to *bigger*.	
12040103	Changes to *smaller or equal*.	
12050103	Changes to *smaller*.	
12060102	VSI_PTR->NO_INTERLOCK not set. ■ Last Failure Parameter [0] contains the ASSUME instance address. ■ Last Failure Parameter [1] contains NV_INDEX value.	01
12070102	VSI_PTR->ALLOCATED_THIS not set. ■ Last Failure Parameter [0] contains the ASSUME instance address. ■ Last Failure Parameter [1] contains NV_INDEX value.	01
12080102	VSI_PTR->CS_INTERLOCKED not set. ■ Last Failure Parameter [0] contains the ASSUME instance address. ■ Last Failure Parameter [1] contains NV_INDEX value.	01
12090102	Unhandled switch case. ■ Last Failure Parameter [0] contains the ASSUME instance address. ■ Last Failure Parameter [1] contains NV_INDEX value.	01
120A0103	WARP expand point value does not match blocks. ■ Last Failure Parameter [0] contains the warp address. ■ Last Failure Parameter [1] contains the warp expand point value. ■ Last Failure Parameter [2] contains the warp blocks value.	01
120B2380	Forced restart of the controller upon a cache battery failure. This is only done under conditions which require the restart for error recovery.	23
20010100	The action for work on the CLI queue should be CLI_CONNECT, CLI_COMMAND_IN or CLI_PROMPT. If it is not one of these three, this bugcheck will result.	01
20020100	The formatted ASCII output (FAO) returned a non-successful response. This will only happen if a bad format is detected or the formatted string overflows the output buffer.	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 33 of 42)

Last Failure Code	Description	Repair Action Code
20030100	The type of work received on the CLI work queue was not of type CLI.	01
20070100	A work item of an unknown type was placed on the CLI DUP Virtual Terminal thread work queue by the CLI.	01
20080000	This controller requested this controller to *restart*.	00
20090010	Changes to *shut down*.	
200A0000	Changes to *self test*.	
200B0100	Could not get enough memory for FCBs to receive information from the other controller.	01
200D0101	After many calls to DS$PORT_BLOCKED, we never got a FALSE status back (which signals that nothing is blocked). ■ Last Failure Parameter [0] contains the port number (1 - n) that we were waiting on to be unblocked.	01
200E0101	While traversing the structure of a unit, a CONFIG_INFO node was discovered with an unrecognized structure type. ■ Last Failure Parameter [0] contains the structure type number that was unrecognized.	01
200F0101	A CONFIG_INFO node was discovered with an unrecognized structure type. ■ Last Failure Parameter [0] contains the structure type number that was unrecognized.	01
20100101	A CONFIG_NODE of type VA_MA_DEVICE had an unrecognized SCSI device type. ■ Last Failure Parameter [0] contains the SCSI device type number that was unrecognized.	01
20110100	An attempt to allocate memory, so the CLI prompt messages could be deleted, failed.	01
20120101	While traversing the structure of a unit, a CONFIG_INFO node was discovered with an unrecognized structure type. ■ Last Failure Parameter [0] contains the structure type number that was unrecognized.	01
20130101	While traversing the structure of a unit, the device was of an unrecognized type. ■ Last Failure Parameter [0] contains the SCSI device type that was unrecognized.	01
20160000	In order to go into mirrored cache mode, the controllers must be restarted.	00
20160100	Unable to allocate resources needed for the CLI local program.	01
20170000	In order to go into nonmirrored cache mode, the controllers must be restarted.	00
20190010	A cache state of a unit remains WRITE_CACHE_UNWRITTEN_DATA. The unit is not ONLINE, thus this state would only be valid for a very short period of time.	00
201A0100	An attempt to allocate memory so a CLI prompt message could be reformatted failed.	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 34 of 42)

Last Failure Code	Description	Repair Action Code
201B0100	Insufficient resources to get memory to *lock* CLI.	01
201C0100	Changes to *unlock*.	
20200100	CLI$ALLOCATE_STRUCT( ) could not obtain memory for a new NVFOC_RW_REMOTE_NVMEM structure.	01
20220020	This controller requested this subsystem to power off.	00
20260000	With “set failover copy=other”, the controller to which the configuration is copied will automatically be restarted by this bugcheck.	00
20640000	Nindy was turned *on*.	00
20650000	Changes to *off*.	
20692010	To enter dual-redundant mode, both controllers must be of the same type.	20
206A0000	Controller restart forced by DEBUG CRASH REBOOT command.	00
206B0010	Changes to DEBUG CRASH NOREBOOT.	
206C0020	Controller was forced to restart in order for new controller code image to take effect.	00
206D0000	Controller code load was not completed because the controller could not rundown all units.	00
206E0000	A restart of both controllers is required when entering multibus failover and the last failover mode of the source controller was transparent, or when entering transparent failover and the last failover mode of the source controller was multibus.	00
40000101	An unrecognized CI opcode was received by HIS. These CI opcode packets are recognized by the port but not by HIS. ■ Last Failure Parameter [0] contains the CI opcode value.	01
40150100	LOCAL VC Timer is in an unexpected state.	01
402A0100	Failed to allocate ID member template.	01
402C0100	Failed to allocate message HTBs.	01
402D0101	S_MAX_NODE greater than MAX_VC_ENTRIES. ■ Last Failure Parameter [0] contains the S_CI_MAX_NODES value.	01
402E0101	S_MAX_NODE not set to valid value. Valid values are 8,16, 32, 64, 128, and 256. ■ Last Failure Parameter [0] contains the S_CI_MAX_NODES value.	01
402F0100	Failure to allocate a HIS EIP structure.	01
40300100	Failure in memory allocation.	01
40560100	Failed to find a VC entry for connection block (CB) during HIS_CLOSE_CONNECTION routine.	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 35 of 42)

Last Failure Code	Description	Repair Action Code
407B0100	SCS command timeout unexpectedly inactive during SCS Accept Request.	01
407C0100	SCS command timeout unexpectedly inactive during SCS Reject Request.	01
408E0100	Message receive queue count disagrees with the number of HTBs on the queue.	01
408F0100	Unrecognized HTB ID type.	01
40900100	HTB_ID type not datagram (DG) when attempting to transmit DG HTB.	01
40930100	Message receive queue count disagrees with the number of HTBs on the queue.	01
40B40101	Invalid queue in MAX_NODES field of SE_PARAMS structure. ■ Last Failure Parameter [0] contains the MAX_NODES field value.	01
42000100	CMPL_MAIN routine found an invalid port xmt status.	01
42140101	Could not allocate critical HTB. ■ Last Failure Parameter [0] contains failure location.	01
42280100	Host port ISR failed to allocate an error logging block.	01
422D6611	Host port found that the controller has exceeded the maximum number of user specified host VCs. ■ Last Failure Parameter [0] is a 32-bit MASK of OPEN VCs to host nodes.	66
424B0001	CI_ISR found Host Reset on Path A. ■ Last Failure Parameter [0] contains the node number of the resetting node.	00
424C0001	CI_ISR found Host Reset on Path B. ■ Last Failure Parameter [0] contains the node number of the resetting node.	00
42522082	CI host port detected a receive parity error. ■ Last Failure Parameter [0] contains the port number. ■ Last Failure Parameter [1] contains the path number.	20
42532082	CI host port detected a transmit parity error. ■ Last Failure Parameter [0] contains the port number. ■ Last Failure Parameter [1] contains the path number.	20
60020102	The unit index supplied in a call to SYSAP$CHANGE_STATE does not correspond to a real unit. ■ Last Failure Parameter [0] contains the unit index. ■ Last Failure Parameter [1] contains the callback routine address.	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 36 of 42)

Last Failure Code	Description	Repair Action Code
60030100	Unable to find free DCD_CMDCORL_BLOCK.	01
60050100	Invalid return value from routine HIS$CONNECT while disk copy data (DCD) was attempting to establish a connection to a remote subsystem.	01
60090100	Invalid return value from routine HIS$DISCONNECT while DMSCP_DCD_COMM_PATH_EVENT attempted to disconnect a remote source connection.	01
600C0100	Invalid return value from routine RESMGR$ALLOCATE_DATA_SEGMENT.	01
600D0100	Opcode field in command being aborted is invalid.	01
60120100	Opcode of TMSCP command to be aborted is invalid.	01
60130100	TMSCP_CLEAR_SEX_CDL_CMPL_RTN detected an unexpected opcode.	01
60140100	TMSCP_CLEAR_SEX_CDL_CMPL_RTN detected an unexpected opcode.	01
60150100	VA$CHANGE_STATE failed to change the software (SW) Write protect when requested to do so as part of the Disk Set Unit Characteristics command.	01
60160100	VA$CHANGE_STATE failed to change the SW Write protect when requested to do so as part of the Tape Set Unit Characteristics command.	01
60170100	Invalid type in entry of long work interval queue.	01
60180100	MSCP_SHORT_INTERVAL found an Invalid type in entry of longword interval work queue.	01
60190100	DMSCP_DCD_SEND_CMD found that the short interval work item (SIWI) code supplied is unrecognized or invalid in this context during DCD inhibited processing.	01
601B0100	Invalid EVENT_CODE parameter in call to DMSCP_CONNECTION_EVENT.	01
601C0100	Invalid EVENT_CODE parameter in call to TMSCP_CONNECTION_EVENT.	01
601D0100	Invalid EVENT_CODE parameter in call to DMSCP_DCD_COMM_PATH_EVENT.	01
601E0100	Invalid EVENT_CODE parameter in call to DMSCP_DCD_COMM_PATH_EVENT.	01
60250100	An attempt was about to be made to return the invalid progress indicator 0xFFFFFFFF to the host, which is the only invalid progress indicator.	01
60260100	A WH_DAF command was requested to be performed by the wrong process.	01
60270100	A non-immediate WHM operation was passed to the DMSCP_EXEC_WHM_IMMMEDIATE routine.	01
60280100	This routine found an invalid XFER_STATE so the routine cannot continue.	01
60290100	HIS did not allocate an HTB when there should have been one reserved for this connection as determined by MSCP_RCV_LISTEN.	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 37 of 42)

Last Failure Code	Description	Repair Action Code
602A0100	HIS did not allocate an HTB when there should have been one reserved for this connection as determined by DMSCP_DCD_SRC_GCS_SEND.	01
602B0100	HIS did not allocate an HTB when there should have been one reserved for this connection as determined by DMSCP_DCD_COMM_PATH_EVENT.	01
602C0100	An attempt was made to place the extra send-HTB on the connections SEND_HTB_LIST when one already existed on the queue.	01
602D0100	The VA$CHANGE_STATE service did not set the software write protect as requested for disk.	01
602E0100	The VA$CHANGE_STATE service did not set the software write protect as requested for tape.	01
603B0100	Initial HIS$LISTEN call for MSCP$DISK was unsuccessful.	01
603C0100	Initial HIS$LISTEN call for MSCP$TAPE was unsuccessful.	01
60400100	An unrecognized or invalid return value in this context from routine RESMGR$ALLOCATE_DATA_SEGMENT, while DMSCP_DCD_ALLOCATE_DSEG attempted to allocate a data segment.	01
60410100	An unrecognized or invalid return value in this context from routine RESMGR$ALLOCATE_DATA_BUFFERS while DMSCP_DCD_ALLOCATE_DBUF attempted to allocate a data buffer.	01
60440100	DMSCP_DCD_SRC_GCS_CMPL found the command being command get statused (GCSed) is no longer at the head of the remote connections queue.	01
60450100	DMSCP_DCD_ERRLOG_RVC found that an error log is not associated with a command. The internal miscellaneous error logs are assumed to not be associated with a connection and remote miscellaneous error logs generation was not requested.	01
60460100	DMSCP_DCD_ELRT_SCC_SEND was entered to issue a remote source connection set control characteristic (SCC) but was unable to locate a viable HTB on the connection HTB_LIST. With no active DCDs, the connection should always have HTBs available.	01
60480100	TMSCP_SUC_AVL_CMPL_RTN found the unit in the unavailable state.	01
60490100	TMSCP_CLEAR_SEX_CDL_CMPL_RTN found the state change failed.	01
604A0100	TMSCP_CLEAR_SEX_CDL_CMPL_RTN found the state change failed.	01
604B0100	The subroutine PROCESS_EVENT returned a value to DMSCP_DCD_COMM_PATH_EVENT indicating that an internal disconnect request occurred while processing an immediate communications event.	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 38 of 42)

Last Failure Code	Description	Repair Action Code
604D0100	The subroutine PROCESS_EVENT returned a value to DMSCP_DCD_COMM_PATH_EVENT indicating that a connection established event occurred while no DCD commands were active.	01
604F0100	TMSCP_SET_SEX_CMPL_RTN found the state change failed.	01
60500100	DMSCP_DCD_OP_CMPL found an unrecognized P_STS value in a DCD HTB status field.	01
60550100	MSCP_INITIALIZE was unable to obtain LOCAL STATIC memory from exec for use as a local connection internal transaction block (ITB).	01
60560100	MSCP_INITIALIZE was unable to obtain LOCAL STATIC memory from exec for use as an AVAILABLE ITB.	01
605D0100	TMSCP_ONL_CLEANUP_RTN detected a failure in enabling variable speed mode suppression.	01
605E0100	TMSCP_SUC_CMPL_RTN detected a failure in enabling variable speed mode suppression.	01
605F0100	TMSCP_SUC_CMPL_RTN detected a failure in enabling variable speed mode suppression.	01
60610100	MSCP_INITIALIZE was unable to obtain BUFFER STATIC memory from exec for use as Write History Logs.	01
60620100	MSCP_INITIALIZE was unable to obtain LOCAL_STATIC memory from exec for use as Write History Log Allocation Failure Lists.	01
60640100	Invalid condition when no unused Write History Log Entries are available.	01
60650100	Attempting to block incoming requests for the tape or loader when it was unexpectedly found already blocked.	01
60660100	Loader boundary block request to stall incoming requests to the tape or loader unit was not set up as expected.	01
60670100	The controller has insufficient memory available for allocating context blocks needed for Disk Copy Data commands	01
60680100	VA$ENALE_NOTIFICATION failed with insufficient resources at init time.	01
606B0100	MSCP_FOC_RECEIVE_CMD detected that the message sent from the other controller had an illegal USB index.	01
606C0100	MSCP_FOC_RECEIVE_CMD detected that the message sent from the other controller had an illegal exclusive access state.	01
606D0100	FOC provided MSCP_FOC_SEND_CMPL_RTN with an invalid status for the FOC$SEND transmit command completion.	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 39 of 42)

Last Failure Code	Description	Repair Action Code
606E0100	FOC provided MSCP_FOC_SEND_RSP_DONE with an invalid status for the FOC$SEND transmit response completion.	01
61020100	HIS$LISTEN call failed with INSUFFICIENT_RESOURCES.	01
61090100	LISTEN_CONNECTION_ESTABLISHED event from HIS specified a connection ID for a connection already known to exist.	01
610C0100	HIS reported a connection event that is not allowed.	01
62000100	HIS$LISTEN call failed with INSUFFICIENT_RESOURCES.	01
62020100	Failure to allocate an associated timer queue.	01
62030100	Failure to allocate a connection ID timer.	01
80010100	An HTB was not available to issue an I/O when it should have been.	01
80020100	A unit could not be dropped from testing because an available command failed.	01
80030100	DILX tried to release a facility that was not reserved by DILX.	01
80040100	DILX tried to change the unit state from MAINTENANCE_MODE to NORMAL but was rejected because of insufficient resources.	01
80050100	DILX tried to change the USB unit state from MAINTENANCE_MODE to NORMAL but DILX never received notification of a successful state change.	01
80060100	DILX tried to switch the unit state from MAINTENANCE_MODE to NORMAL but was not successful.	01
80070100	DILX aborted all commands via VA$D_ABORT( ) but the HTBs have not been returned.	01
80080100	While DILX was deallocating its EIP buffers, at least one could not be found.	01
80090100	DILX received an end message which corresponds to an op code not supported by DILX.	01
800A0100	DILX was not able to restart HIS timer.	01
800B0100	DILX tried to issue an I/O for an opcode not supported.	01
800C0100	DILX tried to issue a oneshot I/O for an opcode not supported.	01
800D0100	A DILX device control block contains an unsupported UNIT_STATE.	01
800E0100	While trying to print an Event Information Packet, DILX discovered an unsupported MSCP error log format.	01
80100100	DILX could not compare buffers because no memory was available from EXEC$ALLOCATE_MEM_ZEROED.	01
80120100	DILX expected an EIP to be on the receive EIP queue but no EIPs were there.	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 40 of 42)

Last Failure Code	Description	Repair Action Code
80130100	DILX was asked to fill a data buffer with an unsupported data pattern.	01
80140100	DILX could not process an unsupported answer in DX$REUSE_PARAMS( ).	01
81010100	An HTB was not available to issue an I/O when it should have been.	01
81020100	A unit could not be dropped from testing because an available command failed.	01
81030100	TILX tried to release a facility that was not reserved by TILX.	01
81040100	TILX tried to change the unit state from MAINTENANCE_MODE to NORMAL but was rejected because of insufficient resources.	01
81050100	TILX tried to change the USB unit state from MAINTENANCE_MODE to NORMAL but TILX never received notification of a successful state change.	01
81060100	TILX tried to switch the unit state from MAINTENANCE_MODE to NORMAL but was unsuccessful.	01
81070100	TILX aborted all commands via VA$D_ABORT( ) but the HTBs have not been returned.	01
81080100	At least one EIP buffer could not be found when TILX attempted to deallocate its EIP buffers.	01
81090100	TILX received an end message which corresponds to an opcode not supported by TILX.	01
810A0100	TILX was unable to restart its timer.	01
810B0100	TILX attempted to issue an I/O for an unsupported opcode.	01
810C0100	TILX attempted to issue a oneshot I/O for an unsupported opcode.	01
810D0100	A TILX device control block contains an unsupported UNIT_STATE.	01
810E0100	TILX received an unsupported Value Added status in a Value added completion message.	01
810F0100	TILX found an unsupported device control block substate while trying to build a command for the Basic Function test.	01
81100100	TILX found an unsupported device control block substate while trying to build a command for the Read Only test.	01
81110100	TILX found an unsupported device control block substate while trying to build a command for the User Defined test.	01
81120100	TILX received an end-of-tape (EOT) encountered while in a substate where EOT should not occur.	01
81130100	TILX calculated an illegal position type value while trying to generate a command for the position intensive phase of the Basic Function test.	01
81140100	TILX discovered an unsupported MSCP error log format when trying to print an Event Information Packet.	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 41 of 42)

Last Failure Code	Description	Repair Action Code
811A0100	TILX expected a deferred error to be on the receive deferred error queue but no deferred errors were found.	01
811B0100	TILX was asked to fill a data buffer with an unsupported data pattern.	01
811C0100	TILX could not process an unsupported answer in TX$REUSE_PARAMS( ).	01
83020100	An unsupported message type or terminal request was received by the CONFIG virtual terminal code from the CLI.	01
83030100	Not all ALTER_DEVICE requests from the CONFIG utility completed within the timeout interval.	01
84010100	An unsupported message type or terminal request was received by the CLONE virtual terminal code from the CLI.	01
85010100	HSUTIL tried to release a facility that was not reserved by HSUTIL.	01
85020100	HSUTIL tried to change the unit state from MAINTENANCE_MODE to NORMAL but was rejected because of insufficient resources.	01
85030100	HSUTIL tried to change the USB unit state from MAINTENANCE_MODE to NORMAL but HSUTIL never received notification of a successful state change.	01
85040100	HSUTIL tried to switch the unit state from MAINTENANCE_MODE to NORMAL but was not successful.	01
86000020	Controller was forced to restart in order for new code load or patch to take effect.	00
86010010	The controller code load function is about to update the program card. This requires controller activity to cease. This code is used to inform the other controller this controller will stop responding to inter-controller communications during card update. An automatic restart of the controller at the end of the program card update will cause normal controller activity to resume.	00
86020011	The EMU firmware returned a bad status when told to prepare for a code load. ■ Last Failure Parameter [0] contains the value of the bad status.	00
8A040080	New cache module failed diagnostics. The controller has been reset to clear the error.	00
8A050080	Could not initialize new cache module. The controller has been reset to clear the error.	00

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 42 of 42)

Last Failure Code	Description	Repair Action Code
8B000186	An single bit error was found by software scrubbing. ■ Last Failure Parameter [0] contains the address of the first single bit error correction code (ECC) error found. ■ Last Failure Parameter [1] contains the count of single bit ECC errors found in the same region below this address. ■ Last Failure Parameter [2] contains the lower 32 bits of the actual data read at the Parameter [0] address. ■ Last Failure Parameter [3] contains the higher 32 bits of the actual data read at the Parameter [0] address. ■ Last Failure Parameter [4] contains the lower 32 bits of the expected data at the Parameter [0] address. ■ Last Failure Parameter [5] contains the higher 32 bits of the expected data at the Parameter [0] address.	01

Glossary

This glossary defines terms pertaining to the HSJ80 array controller troubleshooting resources guide. This glossary is not a comprehensive glossary of computer terms.

ACS Array controller software. Software contained on a removable program card that provides the operating system for the array controller.

adapter A device that converts the protocol and hardware interface of one bus type into another without changing the function of the bus.

ANSI American National Standards Institute. An organization that develops standards used voluntarily by many manufacturers within the USA. ANSI is not a government agency.

array controller *See* controller.

array controller software *See* ACS.

asynchronous Pertaining to events that are scheduled as the result of a signal asking for the event; pertaining to that which is without any specified time relation.

See also synchronous.

autospare A controller feature that automatically replaces a failed disk drive. To aid the controller in automatically replacing failed disk drives, enable the AUTOSPARE switch for the failedset—causing physically replaced disk drives to be automatically placed into the spareset. Also called "autonewspare."

backplane The electronic printed circuit board into which subsystem devices are plugged—for example, the SBB or power supply.

bad block A data block that contains a physical defect.

bad block replacement *See* BBR.

BBR Bad block replacement. A replacement routine that substitutes defect-free disk blocks for those found to have defects. This process takes place in the controller, transparent to the host.

BIST Built-in self-test. A diagnostic test performed by the array controller software on the controller policy processor.

bit A single binary digit having a value of either 0 or 1. A bit is the smallest unit of data a computer can process.

block The smallest collection of consecutive bytes addressable on a disk drive. In integrated storage elements, a block contains 512 bytes of data, error codes, flags, and the block address header. Also called a sector.

bootstrapping A method used to bring a system or device into a defined state by means of its own action. For example, a machine routine whose first few instructions are enough to bring the rest of the routine into the computer from an input device.

built-in self-test *See* BIST.

byte A binary character string made up of 8 bits operated on as a unit.

cache memory A portion of memory used to accelerate read and write operations.

cache module A fast storage buffer.

CCITT Consultive Committee International Telephone and Telegraph. An international association that sets worldwide communication standards, recently renamed International Telecommunications Union (ITU).

CDU Cable distribution unit. The power entry device for StorageWorks racks (cabinets). The CDU provides the connections necessary to distribute power to the enclosures and fans.

channel An interface which allows high speed transfer of large amounts of data. Another term for a SCSI bus.

See also SCSI.

chunk A block of data written by the host.

chunk size The number of data blocks, assigned by a system administrator, written to the primary RAIDset or stripeset member before the remaining data blocks are written to the next RAIDset or stripeset member.

CI bus A term expressing the Computer Interconnect (CI) bus used to connect the nodes in a clustered subsystem. The CI bus uses two serial paths, each with a data transfer rate of 70 Mb/s (8.75 MB/s).

CLCP Code-load code-patch utility.

CLI Command line interpreter. The configuration interface to operate the controller software.

coax *See* coaxial cable.

coaxial cable A two-conductor wire in which one conductor completely wraps the other with the two separated by insulation.

cold swap A method of device replacement that requires the entire subsystem to be turned off before the device can be replaced.

See also hot swap and warm swap.

command line interpreter *See* CLI.

configuration file A file that contains a representation of a storage subsystem configuration.

container 1) Any entity that is capable of storing data, whether the container is a physical device or a group of physical devices, or (2) a virtual, internal controller structure representing either a single disk or a group of disk drives linked as a storageset. Stripesets and mirrorsets are examples of storageset containers the controller uses to create units.

controller A hardware device that, with proprietary software, facilitates communications between a host and one or more devices organized in an array. HS family controllers are examples of array controllers.

copying A state in which data to be copied to the mirrorset is inconsistent with other members of the mirrorset.

See also normalizing.

copying member Any member that joins the mirrorset after the mirrorset is created is regarded as a copying member. Once all the data from the normal member (or members) is copied to a normalizing or copying member, the copying member then becomes a normal member.

See also normalizing member.

CSR Control and status register.

DAEMON Pronounced “demon.” A program usually associated with a UNIX system that performs a utility (housekeeping or maintenance) function without being requested or even known of by the user. A daemon is a diagnostic and execution monitor.

data center cabinet A generic reference to large Compaq subsystem cabinets (racks), such as the SW600-series and SW800-series racks in which StorageWorks components can be mounted.

data striping The process of segmenting logically sequential data, such as a single file, so that segments can be written to multiple physical devices (usually disk drives) in a round-robin fashion. This technique is useful if the processor is capable of reading or writing data faster than a single disk can supply or accept the data. While data is being transferred from the first disk, the second disk can locate the next segment.

DDL Dual data link. The ability to operate on the CI bus using both paths simultaneously to the same remote node.

device *See* node and peripheral device.

differential I/O module A 16-bit I/O module with SCSI bus converter circuitry for extending a differential SCSI bus.

See also I/O module.

differential SCSI bus A bus in which a signal level is determined by the potential difference between two wires. A differential bus is more robust and less subject to electrical noise than is a single-ended bus.

DILX Disk inline exerciser. The controller diagnostic software used to test the data transfer capabilities of disk drives in a way that simulates a high level of user activity.

DIMM Dual inline memory module.

dirty data The write-back cached data that has not been written to storage media, even though the host operation processing the data has completed.

DMA Direct memory access.

driver A hardware device or a program that controls or regulates another device. For example, a device driver is a driver developed for a specific device that allows a computer to operate with the device, such as a printer or a disk drive.

dual-redundant configuration A controller configuration consisting of two active controllers operating as a single controller. If one controller fails, the other controller assumes control of the failing controller devices.

dual-simplex A communications protocol that allows simultaneous transmission in both directions in a link, usually with no flow control.

DUART Dual universal asynchronous receiver and transmitter. An integrated circuit containing two serial, asynchronous transceiver circuits.

ECB External cache battery. The unit that supplies backup power to the cache module in the event the primary power source fails or is interrupted.

ECC Error correction code.

EDC Error detection code.

EIA Electronic Industries Association. EIA is a standards organization specializing in the electrical and functional characteristics of interface equipment.

EMU Environmental monitoring unit. A unit that provides increased protection against catastrophic failures. Some subsystem enclosures include an EMU which works with the controller to detect conditions such as failed power supplies, failed blowers, elevated temperatures, and external air sense faults. The EMU also controls certain rack hardware including alarms and fan speeds.

ESD Electrostatic discharge. The discharge of potentially harmful static electrical voltage as a result of improper grounding.

extended subsystem A subsystem in which two expansion subsystems are connected to the primary subsystem.

external cache battery *See* ECB.

failback The process of restoring data access to the newly-restored controller in a dual-redundant controller configuration.

See also failover.

failedset A group of failed mirrorset or RAIDset devices automatically created by the controller.

failover The process that takes place when one controller in a dual-redundant configuration assumes the workload of a failed companion controller. Failover continues until the failed controller is repaired or replaced.

FCC Federal Communications Commission. The federal agency responsible for establishing standards and approving electronic devices within the United States.

FCC Class A This certification label appears on electronic devices that can only be used in a commercial environment within the United States.

FCC Class B This certification label appears on electronic devices that can be used in either a home or a commercial environment within the United States.

FD SCSI The fast, narrow, differential SCSI bus with an 8-bit data transfer rate of 10 MB/s.

See also FWD SCSI and SCSI.

flush The act of writing dirty data from cache to a storage media.

FMU Fault management utility.

forced errors A data bit indicating a corresponding logical data block contains unrecoverable data.

FRU Field replaceable unit. A hardware component that can be replaced at the customer location by Compaq authorized service providers.

FRUTIL Field replacement utility.

full duplex (adj) Pertaining to a communications method in which data can be transmitted and received at the same time.

full duplex (n) A communications system in which there is a capability for 2-way transmission and acceptance between two sites at the same time.

FWD SCSI A fast, wide, differential SCSI bus with a maximum 16-bit data transfer rate of 20 MB/s.

See also SCSI and FD SCSI.

giga A prefix indicating a billion (10^9) units.

gigabaud An encoded bit transmission rate of one billion (10^9) bits per second.

gigabyte A value normally associated with a disk drives storage capacity, meaning a billion (10^9) bytes. The decimal value 1024 is usually used for one thousand.

half-duplex (adj) Pertaining to a communications system in which data can be either transmitted or received but only in one direction at one time.

HBVS Host-based volume shadowing. Also known as Phase 2 volume shadowing.

host The primary or controlling computer to which a storage subsystem is attached.

host adapter A device that connects a host system to a SCSI bus. The host adapter usually performs the lowest layers of the SCSI protocol. This function may be logically and physically integrated into the host system.

hot disks A disk containing multiple hot spots. Hot disks occur when the workload is poorly distributed across storage devices. This prevents optimum subsystem performance.

See also hot spots.

hot pluggable *See* hot swap.

hot spots A portion of a disk drive frequently accessed by the host. Because the data being accessed is concentrated in one area, rather than spread across an array of disks providing parallel access, I/O performance is significantly reduced.

See also hot disks.

hot swap A method of device replacement that allows normal I/O activity on a device bus to continue during device removal and insertion. The device being removed or inserted is the only device that cannot perform operations during this process. Also known as hot pluggable.

See also cold swap and warm swap.

HSUTIL Format and device code load utility.

I/O Refers to input and output functions.

I/O driver The set of code in the kernel that handles the physical I/O to a device. This is implemented as a fork process. Same as driver.

I/O interface *See* interface.

I/O module A device that integrates an enclosure with either an 8-bit single-ended, 16-bit single-ended, or 16-bit differential SCSI bus.

I/O operation The process of requesting a transfer of data from a peripheral device to memory (or vice versa), the actual transfer of the data, and the processing and overlaying activity to make both of those happen.

IBR Initial boot record.

ILF Illegal function.

INIT Initialize input and output.

initiator A SCSI device that requests an I/O process to be performed by another SCSI device, namely, the SCSI target. The controller is the initiator on the device bus. The host is the initiator on the host bus.

instance code A four-byte value displayed in most text error messages and issued by the controller when a subsystem error occurs. The instance code indicates when during software processing the error was detected.

interface A set of protocols used between components, such as cables, connectors, and signal levels.

IPI Intelligent peripheral interface. An ANSI standard for controlling peripheral devices by a host computer.

IPI-3 Disk Intelligent peripheral interface level 3 for disk.

IPI-3 Tape Intelligent peripheral interface level 3 for tape.

JBOD Just a bunch of disks. A term used to describe a group of single-device logical units.

kernel The most privileged processor access mode.

LBN Logical block number. The logical address for a block of data.

LED Light emitting diode.

local connection A connection to the subsystem using either a controller serial maintenance port or the host SCSI bus. A local connection enables the connection to a subsystem controller within the physical range of the serial or host SCSI cable.

local terminal A terminal plugged into the EIA-423 maintenance port located on the front bezel of the controller.

See also maintenance terminal.

logical block number *See* LBN.

logical bus A single-ended bus connected to a differential bus by a SCSI bus signal converter.

logical unit A physical or virtual device addressable through a target identification (ID) number. LUNs use their target bus connection to communicate on the SCSI bus.

logical unit number A value that identifies a specific logical unit belonging to a SCSI target ID number. A number associated with a physical device unit during task I/O operations. Each task in the system must establish correspondence between logical unit numbers and physical devices.

logon A procedure whereby a participant, either a person or network connection, is identified as being an authorized network participant. Also called login.

LRU Least recently used. A cache term used to describe the block replacement policy for read cache.

maintenance terminal An EIA-423-compatible terminal used with the controller. This terminal is used to identify the controller, enable host paths, enter configuration information, and check the controller status. The maintenance terminal is not required for normal operations.

See also local terminal.

Mbps Approximately one million (10^6) bits per second—that is, megabits per second.

MBps Approximately one million (10^6) bytes per second—that is, megabytes per second.

MSCP	Mass storage control protocol. The protocol by which blocks of information are transferred between the host and the controller over the CI bus.
member	A container that is a storage element in a RAID array.
metadata	The data written to a disk for the purposes of controller administration. Metadata improves error detection and media defect management for the disk drive. Metadata is also used to support storageset configuration and partitioning. Nontransportable disks also contain metadata to indicate they are uniquely configured for StorageWorks environments. Metadata can be thought of as "data about data."
mirrored write-back caching	A method of caching data that maintains two copies of the cached data. The copy is available if either cache module fails.
mirroring	The act of creating an exact copy or image of data.
mirrorset	*See* RAID level 1.
MIST	Module integrity self-test.
network	In data communication, a configuration in which two or more terminals or devices are connected to enable information transfer.
node	In data communications, the point at which one or more functional units connect transmission lines.
nominal membership	The desired number of mirrorset members when the mirrorset is fully populated with active devices. If a member is removed from a mirrorset, the actual number of members may fall below the "nominal" membership.
nonredundant controller configuration	(1) A single controller configuration, or (2) a controller configuration that does not include a second controller.
normal member	A mirrorset member that, block-for-block, contains the same data as other normal members within the mirrorset. Read requests from the host are always satisfied by normal members.
normalizing	Normalizing is a state in which, block-for-block, data written by the host to a mirrorset member is consistent with the data on other normal and normalizing members. The normalizing state exists only after a mirrorset is initialized. Therefore, no customer data is on the mirrorset.

normalizing member A mirrorset member whose contents are the same as all other normal and normalizing members, for data that has been written since the mirrorset was created or lost cache data was cleared. A normalizing member is created by a normal member when either all of the normal members fail or all of the normal members are removed from the mirrorset.

See also copying member.

NVM Non-volatile memory. A type of memory where the contents survive power loss. Also sometimes referred to as NVMEM.

OCP Operator control panel. The control and indicator panel associated with an array controller. The OCP is mounted on the controller and is accessible to the operator.

offset A relative address referenced from the base element address. Event Sense Data Response Templates use offsets to identify various information contained within one byte of memory (bits 0 through 7).

other controller The controller in a dual-redundant pair that is connected to the controller serving the current CLI session.

See also this controller.

parallel data transmission A data communication technique in which more than one code element (for example, bit) of each byte is sent or received simultaneously.

parity A method of checking if binary numbers or characters are correct by counting the ONE bits. In odd parity, the total number of ONE bits must be odd; in even parity, the total number of ONE bits must be even. Parity information can be used to correct corrupted data. RAIDsets use parity to improve the availability of data.

parity bit A binary digit added to a group of bits that checks to see if errors exist in the transmission.

parity check A method of detecting errors when data is sent over a communications line. With even parity, the number of ones in a set of binary data should be even. With odd parity, the number of ones should be odd.

parity RAID *See* RAIDset.

partition A logical division of a container, represented to the host as a logical unit.

PCM Polycenter console manager.

PCMCIA Personal Computer Memory Card Industry Association. An international association formed to promote a common standard for PC card-based peripherals to be plugged into notebook computers. The card, commonly known as a PCMCIA card or program card, is about the size of a credit card.

See also program card.

peripheral device Any unit, distinct from the CPU and physical memory, that can provide the system with input or accept any output from the unit. Terminals, printers, tape drives, and disks are peripheral devices.

pluggable *See* warm swap.

port (1) In general terms, a logical channel in a communications system, or (2) the hardware and software used to connect a host controller to a communications bus, such as a SCSI bus or serial bus.

Regarding the controller, the port is (1) the logical route for data in and out of a controller that can contain one or more channels, all of which contain the same type of data, or (2) the hardware and software that connects a controller to a SCSI device.

primary enclosure The master enclosure that contains the controllers, cache modules, and external cache batteries.

program card The PCMCIA card containing the controller operating software.

See also PCMCIA.

protocol The conventions or rules for the format and timing of messages sent and received.

PTL Port-target-LUN. The controller method of locating a device on the controller device bus.

quiesce The act of rendering bus activity inactive or dormant. For example, “quiesce the SCSI bus operations during a device warm swap.”

RAID Redundant array of independent disks. Represents multiple levels of storage access developed to improve performance or availability or both.

RAID level 0 A RAID storageset that stripes data across an array of disk drives. A single logical disk spans multiple physical disks, allowing parallel data processing for increased I/O performance. While the performance characteristics of RAID level 0 is excellent, this RAID level is the only one that does not provide redundancy. Raid level 0 storagesets are sometimes referred to as stripesets.

RAID level 0+1 A RAID storageset that stripes data across an array of disks (RAID level 0) and mirrors the striped data (RAID level 1) to provide high I/O performance and high availability. Raid level 0+1 storagesets are sometimes referred to as striped mirrorsets.

RAID level 1 A RAID storageset of two or more physical disks that maintains a complete and independent copy of the entire virtual disk's data. This type of storageset has the advantage of being highly reliable and extremely tolerant of device failure. Raid level 1 storagesets are sometimes referred to as mirrorsets.

RAID level 3 A RAID storageset that transfers data parallel across the array disk drives a byte at a time, causing individual blocks of data to be spread over several disks serving as one enormous virtual disk. A separate redundant check disk for the entire array stores parity on a dedicated disk drive within the storageset.

See also RAID level 5.

RAID level 3/5 A Compaq-developed RAID storageset that stripes data and parity across three or more members in a disk array. Raid level 3/5 storagesets are sometimes referred to as RAIDsets. A RAIDset combines the best characteristics of RAID level 3 and RAID level 5. A RAIDset is the best choice for most applications with small to medium I/O requests, unless the application is write-intensive. A RAIDset is sometimes called parity RAID.

RAID level 5 A RAID storageset that, unlike RAID level 3, stores the parity information across all of the disk drives within the storageset.

See also RAID level 3.

RAIDset *See* RAID level 3/5.

RAM Random access memory.

read ahead caching A caching technique for improving performance of synchronous sequential reads by prefetching data from disk.

read caching A cache management method used to decrease the subsystem response time to a read request by allowing the controller to satisfy the request from the cache memory rather than from the disk drives.

reconstruction The process of regenerating the contents of a failed member's data. The reconstruction process writes the data to a spareset disk and then incorporates the spareset disk into the mirrorset, striped mirrorset, or RAIDset from which the failed member came.

See also regeneration.

reduced Indicates that a mirrorset or RAIDset is missing one member because the member has failed or has been physically removed.

redundancy The provision of multiple interchangeable components to perform a single function in order to cope with failures and errors. A RAIDset is considered to be redundant when user data is recorded directly to one member and all of the other members include associated parity information.

regeneration (1) The process of calculating missing data from redundant data, or (2) the process of recreating a portion of the data from a failing or failed drive using the data and parity information from the other members within the storageset. The regeneration of an entire RAIDset member is called reconstruction.

See also reconstruction.

replacement policy The policy specified by a switch with the SET FAILEDSET command indicating whether a failed disk from a mirrorset or RAIDset is to be automatically replaced with a disk from the spareset. The two switch choices are AUTOSPARE and NOAUTOSPARE.

request rate The rate at which requests are arriving at a servicing entity.

RFI Radio frequency interference. The disturbance of a signal by an unwanted radio signal or frequency.

SBB StorageWorks building block. (1) A modular carrier plus the interface required to mount the carrier into a standard StorageWorks enclosure, or (2) any device conforming to enclosure mechanical and electrical standards installed in a 3.5-inch or 5.25-inch carrier (typically a storage device or power supply).

See also StorageWorks.

SCSI Small computer system interface. (1) An ANSI interface standard defining the physical and electrical parameters of a parallel I/O bus used to connect initiators to devices, or (2) a processor-independent standard protocol for system-level interfacing between a computer and intelligent devices including hard drives, floppy disks, CD-ROMs, printers, scanners, and others.

SCSI bus signal converter Sometimes referred to as an adapter. (1) A device used to interface between the subsystem and a peripheral device unable to be mounted directly into a subsystem, (2) a device used to connect a differential SCSI bus to a single-ended SCSI bus, or (3) a device used to extend the length of a differential or single-ended SCSI bus.

See also I/O module.

SCSI device (1) A host computer adapter, a peripheral controller, or an intelligent peripheral that can be attached to the SCSI bus, or (2) any physical unit that can communicate on a SCSI bus.

SCSI device ID number A bit-significant representation of the SCSI address referring to one of the signal lines, numbered 0 through 7 for an 8-bit bus, or 0 through 15 for a 16-bit bus.

See also target ID number.

SCSI ID number The representation of the SCSI address that refers to one of the signal lines numbered 0 through 15.

SCSI port (1) Software: The channel controlling communications to and from a specific SCSI bus in the system, or (2) Hardware: The name of the logical socket at the back of the system unit to which a SCSI device is connected.

See also port.

SCSI-A cable A 50-conductor (25 twisted-pair) cable generally used for single-ended, SCSI-bus connections.

SCSI-P cable A 68-conductor (34 twisted-pair) cable generally used for differential bus connections.

serial transmission A method transmission in which each bit of information is sent sequentially on a single channel rather than simultaneously as in parallel transmission.

signal converter *See* SCSI bus signal converter.

SIMM Single inline memory module.

single-ended I/O module A 16-bit I/O module.

See also I/O module.

single-ended SCSI bus An electrical connection where one wire carries the signal and another wire or shield is connected to electrical ground. Each signal logic level is determined by the voltage of a single wire in relation to ground. This is in contrast to a differential connection where the second wire carries an inverted signal.

spareset A collection of disk drives made ready by the controller to replace failed members of a storageset.

star coupler The physical hub of the CI cluster subsystem cabling. The star coupler is a rack containing cable connections and transformers through which the nodes of a cluster connect to one another via the CI bus.

storage array An integrated set of storage devices.

storage array subsystem *See* storage subsystem.

storage subsystem The controllers, storage devices, enclosures, cables, and power supplies used to form a mass storage subsystem.

storage unit The general term that refers to storagesets, single-disk units, and all other storage devices that are installed in the subsystem and accessed by the host. A storage unit can be any entity that is capable of storing data, whether the storage unit is a physical device or a group of physical devices.

storageset (1) A group of devices configured with RAID techniques to operate as a single container, or (2) any collection of containers, such as stripesets, mirrorsets, striped mirrorsets, and RAIDsets.

StorageWorks A family of Compaq modular data storage products that allow customers to design and configure their own storage subsystems. Components include power, packaging, cabling, devices, controllers, and software. Customers can integrate devices and array controllers in StorageWorks enclosures to form storage subsystems.

StorageWorks systems include integrated Storageworks building blocks (devices) and array controllers to form storage subsystems. System-level enclosures to house the enclosure chassis and standard mounting devices for these building blocks are also included.

See also SBB.

stripe The data divided into blocks and written across two or more member disks in an array.

stripe size The stripe capacity as determined by *n*–1 times the chunksize, where *n* is the number of RAIDset members.

striped mirrorset *See* RAID level 0+1.

stripeset *See* RAID level 0.

striping The technique used to divide data into segments, also called chunks. The segments are striped, or distributed, across members of the stripeset. This technique helps to distribute hot spots across the array of physical devices to prevent hot spots and hot disks.

Each stripeset member receives an equal share of the I/O request load, improving performance.

surviving controller The controller in a dual-redundant configuration pair that serves companion devices when the companion controller fails.

switch A method that controls the flow of functions and operations in software.

synchronous Pertaining to a method of data transmission which allows each event to operate in relation to a timing signal.

See also asynchronous.

tape A storage device supporting sequential access to variable sized data records.

target (1) A SCSI device that performs an operation requested by an initiator, or (2) designates the target ID number of the device.

target ID number The address a bus initiator uses to connect with a bus target. Each bus target is assigned a unique target address.

See also SCSI device ID number.

this controller The controller that is serving a current CLI session through a local or remote terminal.

See also other controller.

TILX Tape inline exerciser. The controller diagnostic software to test the data transfer capabilities of tape drives in a way that simulates a high level of user activity.

TMSCP Tape mass storage control protocol. The protocol by which blocks of information are transferred between the host and a CI controller on the CI Bus using tape devices.

transfer rate The speed at which data may be exchanged with the central processor, expressed in thousands of bytes per second.

Ultra SCSI bus A wide, Fast-20 SCSI bus.

unit A container made accessible to a host. A unit may be created from a single disk drive or tape drive. A unit may also be created from a more complex container such as a RAIDset. The controller supports a maximum of eight units on each target.

See also target.

unwritten cached data Sometimes called unflushed data.

See dirty data.

UPS Uninterruptible power supply. A battery-powered power supply guaranteed to provide power to an electrical device in the event of an unexpected interruption to the primary power supply. Uninterruptible power supplies are usually rated by the amount of voltage supplied and the length of time the voltage is supplied.

VHDCI Very high-density-cable interface. A 68-pin interface. Required for Ultra SCSI connections.

virtual terminal A software path from an operator terminal on the host to the controller CLI interface, sometimes called a host console. The path can be established via the host port on the controller or via the maintenance port through an intermediary host.

See also maintenance terminal.

VTDPY Virtual terminal display. A utility that allows viewing of specific informational displays using CLI commands.

warm swap A device replacement method that allows the complete system to remain online during device removal or insertion. The system bus may be halted, or quiesced, for a brief period of time during the warm swap procedure. Also known as pluggable.

See also cold swap and hot swap.

write hole The period of time in a RAID level 1 or RAID level 5 write operation when an opportunity emerges for undetectable RAIDset data corruption. Write holes occur under conditions such as power outages, where the writing of multiple members can be abruptly interrupted. A battery backed-up cache design eliminates the write hole because data is preserved in cache and unsuccessful write operations can be retried.

write-back cache *See* cache module.

write-back caching A cache management method used to decrease the subsystem response time to write requests by allowing the controller to declare the write operation "complete" as soon as the data reaches the controller cache memory. The controller performs the slower operation of writing the data to the disk drives at a later time.

write-through cache A cache management technique for retaining host write requests in read cache. When the host requests a write operation, the controller writes data directly to the storage device. This technique allows the controller to complete some read requests from the cache, greatly improving the response time to retrieve data. The operation is complete only after the data to be written is received by the target storage device.

This cache management method may update, invalidate, or delete data from the cache memory accordingly, to ensure that the cache contains the most current data.

write-through caching A cache management method used to decrease the subsystem response time to a read. This method allows the controller to satisfy the request from the cache memory rather than from the disk drives.

Index

D

G

H

I

S

T

U

V

W