Compaq StorageWorks

HSG80 Array Controller
ACS Version 8.6

Troubleshooting Reference Guide

First Edition (June 2001)
Part Number: EK-G80TR-SA. A01
Compaq Computer Corporation

Printed in the U.S.A.

HSG80 Array Controller ACS Version 8.6
Troubleshooting Reference Guide
First Edition (June 2001)
Part Number: EK-G80TR-SA. A01

Contents

Chapter 2

Utilities and Exercisers

Chapter 6

Last Failure Codes

Glossary

Index

Figures

Tables

About This Guide

This guide is a troubleshooting resource for HSG80 array controllers running array controller software (ACS) versions 8.6F, 8.6G, 8.6P, and 8.6S. It contains information on various utilities, software templates, and event reporting codes.

Text Conventions

This document uses the following conventions to distinguish elements of text:

Keys	Keys appear in boldface. A plus sign (+) between two keys indicates that they should be pressed simultaneously.
USER INPUT	User input appears in a different typeface and in uppercase
FILENAMES	File names appear in uppercase italics.
Menu Options, Command Names, Dialog Box Names	These elements appear in initial capital letters.
COMMANDS, DIRECTORY NAMES, and DRIVE NAMES	These elements appear in upper case. **NOTE:** UNIX commands are case sensitive and will not appear in uppercase.
Type	When you are instructed to *type* information, type the information **without** pressing the **Enter** key.
Enter	When you are instructed to enter information, type the information and then press the **Enter** key.

"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.

Symbols in Text

These symbols may be found in the text of this guide. They have the following meanings.

WARNING: Text set off in this manner indicates that failure to follow directions in the warning could result in bodily harm or loss of life.

CAUTION: Text set off in this manner indicates that failure to follow directions could result in damage to equipment or loss of information.

IMPORTANT: Text set off in this manner presents clarifying information or specific instructions.

NOTE: Text set off in this manner presents commentary, sidelights, or interesting points of information.

Symbols on Equipment

These icons may be located on equipment in areas where hazardous conditions may exist.

Any surface or area of the equipment marked with these symbols indicates the presence of electrical shock hazards. The enclosed area contains no operator serviceable parts.

WARNING: To reduce the risk of injury from electrical shock hazards, do not open this enclosure.

Any RJ-45 receptacle marked with these symbols indicates a Network Interface Connection.

WARNING: To reduce the risk of electrical shock, fire, or damage to the equipment, do not plug telephone or telecommunications connectors into this receptacle.

Any surface or area of the equipment marked with these symbols indicates the presence of a hot surface or hot component. If this surface is contacted, the potential for injury exists.

WARNING: To reduce the risk of injury from a hot component, allow the surface to cool before touching.

Power Supplies or Systems marked with these symbols indicate the equipment is supplied by multiple sources of power.

WARNING: To reduce the risk of injury from electrical shock, remove all power cords to completely disconnect power from the system.

Any product or assembly marked with these symbols indicates that the component exceeds the recommended weight for one individual to handle safely.

WARNING: To reduce the risk of personal injury or damage to the equipment, observe local occupational health and safety requirements and guidelines for manual material handling.

Rack Stability

WARNING: To reduce the risk of personal injury or damage to the equipment, be sure that:

- The leveling jacks are extended to the floor.
- The full weight of the rack rests on the leveling jacks.
- The stabilizing feet are attached to the rack if it is a single rack installation.
- The racks are coupled together in multiple rack installations.
- A rack may become unstable if more than one component is extended for any reason. Extend only one component at a time.

Getting Help

If you have a problem and have exhausted the information in this guide, you can get further information and other help in the locations listed in this section.

Compaq Technical Support

You are entitled to free hardware technical telephone support for your product for as long you own the product. A technical support specialist will help diagnose the problem or guide you to the next step in the warranty process.

In North America, call the Compaq Technical Phone Support Center at 1-800-OK-COMPAQ. This service is available 24 hours a day, 7 days a week.

NOTE: For continuous quality improvement, calls may be recorded or monitored.

Outside North America, call the nearest Compaq Technical Support Phone Center. Telephone numbers for world wide Technical Support Centers are listed on the Compaq website. Access the Compaq website by logging on to the Internet at http://www.compaq.com.

Be sure to have the following information available before you call Compaq:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages

- Add-on boards or hardware
- Third-party hardware or software
- Operating system type and revision level
- Detailed, specific questions

Compaq Website

The Compaq website has latest information on this product as well as the latest drivers. You can access the Compaq website by logging on to the Internet at http://www.compaq.com/storage.

Compaq Authorized Reseller

For the name of your nearest Compaq Authorized Reseller:

- In the United States, call 1-800-345-1518.
- In Canada, call 1-800-263-5868.
- Elsewhere, see the Compaq website for locations and telephone numbers.

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 BA370 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” on page 1–11, and “Solid OCP Pattern Display Reporting” on page 1–13, 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. Use the fault management utility (FMU) to 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 Guidelines (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 (BA370 enclosure only) AC input box.
		BA370 enclosure only: Make sure that all cooling fans are installed. If one or more fans are missing or all are inoperative for more than 8 minutes, the EMU shuts down the subsystem.	Turn off power switch on AC input box. Replace cooling fan. Restore power to subsystem.
		BA370 enclosure only: Determine if the standby power switch on the PVA was pressed for more than 5 seconds.	Press the alarm control switch on the EMU.
	Failed controller.	If the previous remedies fail to resolve the problem, 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 FLASHING; other LEDs also lit.	Device in error or failedset on corresponding device port with other LEDs lit.	SHOW *device* FULL.	Follow repair action using Table 1–3.

Table 1–1 Troubleshooting Guidelines (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 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 previous remedies fail to resolve the problem, check for OCP LED codes.	Follow repair action using Table 1–2 or Table 1–3.
	Node ID is all zeros.	SHOW_THIS to see if node ID is all zeros.	Set node ID using the node ID (bar code) that is located on the frame in which the controller sits. See SET THIS_CONTROLLER NODE_ID in the controller CLI reference guide. Also, be sure to copy in the right direction. If cabled to the new controller, use SET FAILOVER COPY= OTHER_CONTROLLER. If cabled to old controller, use SET FAILOVER COPY=THIS_CONTROLLER.

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

Symptom	Possible Cause	Investigation	Remedy
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 previous remedy fails to resolve the problem, 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 previous remedy fails to resolve the problem, 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 previous remedy fails to resolve the problem, check for OCP LED codes.	Replace DIMM in "other controller" cache module.
Mirrored cache: controller reports battery not present.	Memory module was installed before the cache module was connected to an ECB.	BA370 enclosure: ECB cable not connected to cache module. Model 2200 enclosure: ECB not installed or seated properly in backplane.	BA370 enclosure: Connect ECB cable to cache module, then restart both controllers by pushing their reset buttons simultaneously. Model 2200 enclosure: 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 cache contents to synchronize the primary and mirrored data.) Restart the controllers that were shut down.

Table 1–1 Troubleshooting Guidelines (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 Guidelines (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 previous remedies fail to resolve the problem, 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 uninterruptible power supply (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.

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

Symptom	Possible Cause	Investigation	Remedy
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.
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 installation and configuration guide that accompanied the software release.
	Invalid Cache	See the description for the invalid cache symptom on page 1–7.	See the description for the invalid cache symptom.
	Units have lost data.	Issue the SHOW UNITS FULL command.	Clear these units with: 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 the 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, such as the "dd" utility for a TRU64 UNIX host.	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 the bus that corresponds to the LED 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 bus.

Flashing OCP Pattern Display Reporting

Certain events can cause a FLASHING display of the OCP LEDs. Each event and the resulting pattern are 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.
■○●○●○○	14	Controller Module memory controller timer has failed.	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
■○●●○○●	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	An unnecessary interrupt pending.	Replace controller.
■●●●●○○	3C	An unexpected fault during initialization.	Replace controller.
■●●●●○●	3D	An unexpected maskable interrupt during initialization.	Replace controller.
■●●●●●○	3E	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 the OCP LEDs to display ON or SOLID. Each event and the resulting pattern are 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:

```
%FLL--HSG> --13-MAY-2001 04:39:45 (time not set)-- OCP Code: 38
Controller operation terminated.

%FLL--HSG> --13-MAY-2001 04:32:26 (time not set)-- OCP Code: 26
Memory module is missing.
```

Table 1–3 Solid OCP Pattern Displays and Repair Actions (Sheet 1 of 5)

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 actions 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).

Legend:

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

Table 1–3 Solid OCP Pattern Displays and Repair Actions (Sheet 2 of 5)

Pattern	OCP Code	Error	Repair Action
■●❍❍●●●	27	Memory module has insufficient usable memory.	Replace indicated DIMMs. This indication is only provided when Fault LED logging is enabled.
■●❍●❍❍❍	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 no jumpers are installed. 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.

Legend:

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

Table 1–3 Solid OCP Pattern Displays and Repair Actions (Sheet 3 of 5)

Pattern	OCP Code	Error	Repair Action
■●❍●●❍●	2D	Master enclosure SCSI buses are not all set to ID 0.	Set the PVA ID to 0 for the enclosure with the controllers. If the problem persists, try the following repair actions: 1. Replace the PVA module. 2. Replace the EMU. 3. Remove all devices. 4. Replace the enclosure.
■●❍●●●❍	2E	Multiple enclosures have the same SCSI ID. More than one enclosure have the same SCSI ID.	Reconfigure the PVA ID to uniquely identify each enclosure in the subsystem. The enclosure with the controllers must be set to PVA ID 0; additional enclosures must use PVA IDs 2 and 3. If the error continues after PVA settings are unique, replace each PVA module one at a time. Check the enclosure if the problem remains.
■●❍●●●●	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.
■●●❍❍❍●	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.

Legend:

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

Table 1–3 Solid OCP Pattern Displays and Repair Actions (Sheet 4 of 5)

Pattern	OCP Code	Error	Repair Action
■●●❍❍●●	33	Nonvolatile program memory (NVPM) structure revision too low. NVPM structure revision number is lower than 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 and failed.	Replace controller.
■●●❍●●●	37	Software-induced controller reset expected and 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.
■●●●❍●❍	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.

Legend:

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

Table 1–3 Solid OCP Pattern Displays and Repair Actions (Sheet 5 of 5)

Pattern	OCP Code	Error	Repair Action
■●●●●❍●	3D	NVPM structure revision higher than image. NVPM structure revision number is higher 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 shows a Last Failure report:

```
%LFL--HSG> --13-MAY-2001 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: HSG80
Serial Number: AA12345678 Hardware Version: 0000(00)
Software Version: V086P(FF)
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--HSG> --13-OCT-2000 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: HSG80
Serial Number: AA12345678 Hardware Version: 0000(00)
Software Version: V086P(FF)
Informational Report
Instance Code: 0102030A
Last Failure Code: 011C0011
Last Failure Parameter[0.] 0000003F

%EVL--HSG> --13-OCT-2000 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: HSG80
Serial Number: AA12345678 Hardware Version: 0000(00)
Software Version: V086P(FF)
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
HSG>
```

Spontaneous event logs are reported to the host error log using SCSI Sense Data Templates 01, 04, 05, 11, 12, 13, 14, 41, 51, and 90. See Chapter 3 for a more detailed explanation of templates.

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--HSG> --13-OCT-2000 04:32:20 (time not set)-- Previous controller-
operation stopped with display of solid fault code, OCP Code: 3F
HSG>
```

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 occur 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 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 low.

The 4-minute polling continues for the maximum allowable time to recharge the battery—up to 10 hours for a BA370 enclosure, or 3.5 hours for a Model 2200 enclosure. If the battery does not charge sufficiently after the allotted 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 downtime did not drain more than 50 percent of 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.

ECB battery capacity depends on the size of the cache module memory configuration as shown in Table 1–4. For example, when the batteries are fully charged, an ECB can preserve 512 MB of cache memory for 24 hours (1 day).

Table 1–4 ECB Capacity Based On Memory Size

Size	DIMM Combinations	Capacity in Hours (Days)
128 MB	Four, 32 MB each	48 (4)
128 MB	One, 128 MB each	96 (4)
256 MB	Two, 128 MB each	48 (2)
512 MB	Four, 128 MB each	24 (1)

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

NOTE: If a 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. Read caching is enabled by default 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. Read-ahead caching is enabled by default 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

Write-back caching is enabled by default 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
or
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

The controller provides write-back caching for storage units as long as the controller cache memory is connected to a nonvolatile backup power source, such as an ECB. The cache module must be nonvolatile to preserve unwritten cache data during a power failure. If the cache memory is not connected to a backup power supply, this unwritten data will be lost during a power failure.

NOTE: Disaster-tolerant mirrorsets are not subject to this requirement.

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:

- For BA370 enclosures 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 1–5 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 1–5 are the same for Cache B failures.

Table 1–6 on page 1–26 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 1–6 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 1–5 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 lost write-back data from the mirrored copy on Cache B. Cache policy: Both controllers support write-back caching. Failover: None

Table 1–5 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 *unit-number* 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 memory on Cache A is repaired or replaced.	Data loss: Controller A recovers all of 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 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 1–6 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 fail over 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 1–6 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 fail over 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, fail over 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, 128 MB, 256 MB, or 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)

  BA370 enclosure only: SET *controller* UPS=NODE_ONLY (a 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)
- 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 nonvolatile 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, or the repair action.
- Display the Instance Codes that identify and accompany significant events that do not cause the controller to halt operation.
- Display the Last Failure Codes that identify and accompany failure events that 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” on 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 nonvolatile 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-OCT-2000 at 15:29:28
Power On Time: 0. Years, 14. Days, 19. Hours, 51. Minutes, 31. Seconds
Controller Model: HSG80
Serial Number: AA12345678 Hardware Version: 0000(00)
Software Version: V086P(FF)
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 alphanumeric 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 1–18). 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 1–17). 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" on 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 1–19). 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 HSG80 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
- Local and remote controller activity in a Data Replication Manager 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**: CLEAR DISPLAY CACHE DISPLAY DEFAULT DISPLAY DEVICE DISPLAY HOST DISPLAY REMOTE (ACS version 8.6P only) DISPLAY RESOURCE 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/W	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 REMOTE - Use 132 column controller status display
DISPLAY RESOURCE - Use 132 column controller status display
DISPLAY STATUS - Use 132 column controller status display
CLEAR - Clears the host port event counters
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
- Resource Statistics Screen
- Remote Status Screen

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

```
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 (the display for ACS version 8.6P differs slightly), consists of the following sections and subsections:

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

```
VTDPY> DISPLAY DEFAULT

HSG80             S/N: ZG92712820  SW: V86P-0  HW: E-01
                  0.0% Idle          0 KB/S           0 Rq/S               Up: 0 22:10.03
Pr Name    Stk/Max Typ  Sta   CPU% Target             Unit   ASWC  KB/S  Rd%   Wr% Cm% Ht%
0  NULL      0/  0     Rn     0.0             111111 D0001  x  a    0     0     0   0   0
                                  0123456789012345 D0002  o^ a    0     0     0   0   0
                                 P1DDDD  hHDDDDDDDD D0003  o^ a    0     0     0   0   0
                                 o2DDDD  hHDDDDDDDD D0004  o^ a    0   100     0   0   0
                                 r3DDDD  hHDDDDDDDD D0005  o^ a    0   100     0   0   0
                                 t4DDDD  hH DDDDD D D0006  x  a    0     0     0   0   0
                                  5 DDD  hHDDDDDDDD D0081  x  a    0     0     0   0   0
                                  6DDDD  hHDDDDDDDD D0082  x  a    0     0     0   0   0
```

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 uptime
- 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

HSG80      S/N: ZG92712934 SW: V86P-0 HW: E-01
   0.0% Idle    18093 KB/S    3165 Rq/S                    Up: 19  5:02:22
Pr Name    Stk/Max Typ Sta  CPU%        Unit  ASWC KB/S    Unit  ASWC KB/S
0  NULL      0/  0    Rn  100.0        D0000 o^ a  658    D0112 x  a    0
                                       D0001 o^ a  683    D0113 x  a    0
                                       D0002 o^ a  237    D0114 x  a    0
                                       D0006 o^ a  237    D0115 x  a    0
                                       D0007 o^ a  696    D0116 x  a    0
                                       D0008 o^ a 2993    D0117 x  a    0
                                       D0009 o^ a 2351
                                       D0010 o^ a 2830
                                       D0011 o^ a 2031
                                       D0012 o^ a 2793
                                       D0013 o^ a 2579
```

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 uptime
- Unit status
- Unit I/O activity

```
VTDPY>DISPLAY CACHE

HSG80              S/N: ZG92712820   SW: V86P-0   HW: E-01
     58.1% Idle     878 KB/S      787 Rq/S                  Up: 0  22:10:28
Unit  ASWC        KB/S  Rd%  Wr%  Cm%  Ht%  Ph%  MS%  Purge  BlChd  BlHit
P0300 o              0    0    0    0    0    0    0      0      0      0
D0303 o^ b           0    0    0    0    0    0    0      0      0      0
D0304                0    0    0    0    0    0    0      0      0      0
P0400                0    0    0    0    0    0    0      0      0      0
P0401                0    0    0    0    0    0    0      0      0      0
D0402 x^ b           0    0    0    0    0    0    0      0      0      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 uptime
- Device port configuration (upper left)
- Device performance (upper right)
- Device port performance (lower left)

```
VTDPY>DISPLAY DEVICE

HSG80                  S/N: ZG92712820  SW: V86P-0  HW: E-01
                       99.9% Idle      0 KB/S      0 Rq/S      Up: 0 22:08:21
        Target                  P TL   ASWF   Rq/S RdKB/S WrKB/S Que Tg BR ER
            111111             P1120   A^        0      0      0   0  0  0  0
  0123456789012345             D1130   A^        0      0      0   0  0  0  0
P1      hH    PDD              D1140   A^        0      0      0   0  0  0  0
o2      hH    DDD              D2120   A^        0      0      0   0  0  0  0
r3  ????hH                     D2130   A^        0      0      0   0  0  0  0
t4      hH DDD                 D2140   a^        0      0      0   0  0  0  0
 5   P  hH                     ?3020    ^ F      0      0      0   0  0  0  0
 6D     hH                     ?3030    ^ F      0      0      0   0  0  0  0
                               ?3040    ^ F      0      0      0   0  0  0  0
                               ?3050    ^ F      0      0      0   0  0  0  0
                               D4090   A^        0      0      0   0  0  0  0
                               D4100   A^        0      0      0   0  0  0  0
                               D4110   A^        0      0      0   0  0  0  0
                               P5030   A^        0      0      0   0  0  0  0
                               D6010   A^        0      0      0   0  0  0  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     0      0      0   0   0   0
  5     0      0      0   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 uptime
- Known hosts
- Host port 1 configuration and link error counters
- Host port 2 configuration and link error counters

NOTE: Figure 2–6 applies to "this controller" only. To see "other controller" connections, run VTDPY again on the "other controller."

```
VTDPY>DISPLAY HOST

                          FIBRE CHANNEL HOST STATUS DISPLAY
 ********* KNOWN HOSTS **********   ******* PORT 1 *******     ******* PORT 2 *******
## NAME      BB FrSz ID/ALPA P  S  Topology          :FABRIC  Topology          :FABRIC
00 BONK2P2   7  2048 210113  2  N  Current Status    :FABRIC  Current Status    :FABRIC
10 !NEWCON35 7  2048 210213  2  N  Current ID/ALPA   :210313  Current ID/ALPA   :210413
11 DADRA11   7  2048 210213  1  N  Tachyon Status    :    ff  Tachyon Status    :    ff
12 BONK1P1   7  2048 210113  1  N  Queue Depth       :     6  Queue Depth       :     0
                                   Busy/QFull Rsp    :     0  Busy/QFull Rsp    :     0
                                      LINK ERROR COUNTERS        LINK ERROR COUNTERS
                                   Link Downs        :     1  Link Downs        :     1
                                   Soft Inits        :     0  Soft Inits        :     0
                                   Hard Inits        :     0  Hard Inits        :     0
                                   Loss of Signals   :     0  Loss of Signals   :     0
                                   Bad Rx Chars      :     3  Bad Rx Chars      :     3
                                   Loss of Syncs     :     0  Loss of Syncs     :     0
                                   Link Fails        :     0  Link Fails        :     0
                                   Received EOFa     :     0  Received EOFa     :     0
                                   Generated EOFa    :     0  Generated EOFa    :     0
                                   Bad CRCs          :     0  Bad CRCs          :     0
                                   Protocol Errors   :     0  Protocol Errors   :     0
                                   Elastic Errors    :     0  Elastic Errors    :     1
```

Figure 2–6. Sample of the VTDPY host screen

Resource Statistics Screen

The RESOURCE screen, shown in Figure 2–7, consists of the following sections:

- Screen header, which includes:
  - Controller ID data
  - Subsystem performance
  - Controller uptime
- Physical resource name fields
- Cache memory requirement fields (Free, Need, and Wait)
- Full unit performance
- Resource status fields (Wait Flush, wait FX, Nodes, Dirty, and Flush)

```
VTDPY>DISPLAY RESOURCE

HSG80        S/N: ZG92712934 SW: V86P-0   HW:  E-01
             0.0% Idle   18574 KB/S    3276 Rq/S           Up:  19  5:01:43
Resource Name    Free   Need Wait            Unit  ASWC KB/S  Rd% Wr% Cm% HT%
-------------   ------ ---- ----            D0000 o^ a  614  50  49   0 100
Buffers         307739    0    0            D0001 o^ a  609  50  50   0 100
VAXDs              302    0    0            D0002 o^ a  259   0 100   0   0
WARPs               68    0    0            D0006 o^ a  743 100   0   0  99
RMDs               180    0    0            D0007 o^ a  613  50  49   0 100
XBUFs              306    0    0            D0008 o^ a 2924   0 100   0   0
ZBUFs              106    0    0            D0009 o^ a 2551   0 100   0   0
Disk Read DWDs     291    0    0            D0010 o^ a 2709   0 100   0   0
Disk Write DWDs    196    0    0            D0011 o^ a 2463   0 100   0   0
DPCX Read DWDs     144    0    0            D0012 o^ a 2665   0 100   0   0
DPCX Write DWDs    138    0    0            D0013 o^ a 2420   0 100   0   0
DDs                243    0    0            D0100 x  a    0   0   0   0   0
Wait Flush:      0 (DDs)        0 (blocks)
Wait FX:         0 (wait)       1 (queue)
Nodes:           0 (cache)      0 (strip)
Dirty:       12295 (blocks) 23721 (nodes)
Flush:       77328 (blocks)   610 (nodes)
```

Figure 2–7. Sample of the VTDPY resource screen

Remote Status Screen

The REMOTE screen (ACS version 8.6P only), shown in Figure 2–8, consists of the following sections:

- Remote copy set name
- Runtime status

```
VTDPY>DISPLAY REMOTE

COPY SET TARGET       C  INIT U   Kb/S  ASSOC SET  LOG  U Kb/S   LS   %LOG %MRG %CPY
======================  ==== =   ====  =========  ==== = =====  ==   ==== ==== ====
RCS2     G213_TAR/D52 D  D2   o    920  ASC1       D98  o *****  LG    67%   0% 100%
RCS3     G213_TAR/D0  D  D3   x  *****  ASC2       D99  x *****  **   ***% ***% ***%
RCS4     G213_TAR/D0  D  D4   x  *****  ASC3       D97  x *****  **   ***% ***% ***%
RCS5     NO TARGETS   *  D5   x  *****  *********  **** x *****  **   ***% ***% ***%
RCS7     G213_TAR/D57 D  D7   o    714  ASC4       D96  o   336  LG    49%   0% 100%
RCS8     G213_TAR/D0  D  D8   x  *****  ASC2       D99  x *****  **   ***% ***% ***%
```

Figure 2–8. Sample of the VTDPY remote status screen (ACS version 8.6P only)

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 VTDPY screens display information in the following screen subsections:

- Screen Header
- Common Data Fields
- Unit Performance Data Fields
- Device Performance Data Fields
- Device Port Performance Data Fields
- Host Port Configuration
- TACHYON Chip Status
- Runtime Status of Remote Copy Sets
- Device Port Configuration
- Controller/Processor Utilization
-

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 HSG80 storage subsystem and is further divided into the following four subsections:

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

The controller ID data appears as follows:

```
HSG80    S/N: xxxxxxxxxxxx    SW: xxxxxxx    HW: xx-xx
```

where:

- HSG80: string represents the controller model name and number.

- S/N: depicts an alphanumeric 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 uptime.
- KB/S displays cumulative data transfer rate in kilobytes per second.
- RQ/S displays cumulative unit request rate in requests per second.

The controller uptime data shows the uptime of the HSG80 controller in days, hours and minutes in the following format:

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

Common Data Fields

Some VTDPY displays contain common data fields, such as the DEFAULT, STATUS, and DEVICE screens. Table 2–4 provides a description of common data fields on DEFAULT and STATUS 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
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 VTDPY data fields in the DEFAULT and DEVICE screens are described in Table 2–5.

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

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

Unit Performance Data Fields

VTDPY displays virtual storage unit performance information in a block of tabular data in the DEFAULT, STATUS, CACHE, and RESOURCE 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).
- RESOURCE screen also uses a brief format (see Figure 2–7).

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:		
	D	=	disk drive or CD-ROM drive
	I	=	invisible device
	P	=	passthrough device
	?	=	unknown device type
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”
	z	=	currently not accessible to host due to a remote copy condition (ACS version 8.6P only)
	space	=	unknown availability
S	State of a virtual storage unit:		
	^	=	disk device spinning at correct speed
	>	=	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

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

Column	Contents		
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
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.		

Device Performance Data Fields

VTDPY displays up to 42 devices in the device performance region (see Figure 2–5, upper right) 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	State of the device:		
	^	=	disk device spinning at correct speed
	>	=	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 32 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.		

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

Column	Contents
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.
BR	Number of SCSI bus resets that occurred since VTDPY was started.
ER	Number of SCSI errors received. If the device is swapped or deleted, then the value clears and resets to 0.

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 32 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 HOST screen only. The data is displayed for both host Port 1 and host Port 2 independently, although the format is the same for both.

Use the VTDPY>CLEAR command to clear the host display link error counters.

Table 2–9 outlines the "Known Hosts" portion of the Fibre Channel Host Status Display. For a more detailed explanation of certain field labels and their definitions, consult *The Fibre Channel Physical and Signaling Interface Standard* (also known as the FC-PH specification).

Table 2–9 Fibre Channel Host Status Display—Known Host Connections

Field Label	Description
##	Internal ID
NAME	Refer to the SHOW *CONNECTIONS* command in controller CLI reference guide.
BB	Buffer-to-buffer credit
FrSz	Frame size
ID/ALPA	Host ID
P	Port number (1 or 2)
S	Status:
	N = online
	F = offline

The following tables detail the remaining portions of the Fibre Channel Host Status Display. Table 2–10 includes the labels that report the status of ports one and two, and Table 2–11 describes the Link Error Counters.

Table 2–10 Fibre Channel Host Status Display—Port Status

Field Label	Description
Topology	FABRIC, LOOP, or OFFLNE
Current Status	FABRIC, LOOP, DOWN, STNDBY, or OFFLNE
Current ID/ ALPA	Controller ID
TACHYON Status	This denotes the current state of the TACHYON or Fibre Channel control chip. See "TACHYON Chip Status" on page 2–28 for more detail.

Table 2–10 Fibre Channel Host Status Display—Port Status (Continued)

Field Label	Description
Queue Depth	Queue depth shows the instantaneous number of commands at the controller port.
Busy/QFull Rsp	This field represents the total number of QFull/Busy responses sent by the port.

Table 2–11 Fibre Channel Host Status Display—Link Error Counters

Field Label	Description
Link Downs	This field refers to the total number of link down/up transitions.
Soft Inits	Soft initializations are the number of loop initialization caused by this port.
Hard Inits	Hard initializations indicate the number of TACHYON chip resets.
Loss of Signals	Loss of signals show the number of times the Frame Manager detected a low-to-high transition on the lnk_unuse signal.
Bad Rx Chars	This field represents the number of times the 8B/10B decode detected an invalid 10-bit code. FC-PH denotes this value as “Invalid Transmission Word during frame reception.” This field may be non-zero after initialization. After initialization, the host should read this value to determine the correct starting value for this error count.
Loss of Syncs	Loss of Sync denotes the number of times the loss of sync is greater than RT_TOV.
Link Fails	This field indicates the number of times the Frame Manager detected a NOS or other initialization protocol failure that caused a transition to the Link Failure state.
Received EOFa	Received EOFa refers to the number of frames containing an EOFa delimiter that the TACHYON chip has received.
Generated EOFa	This field reveals the number of problem frames that the TACHYON chip has received that caused the Frame Manager to attach an EOFa delimiter. Frames that the TACHYON chip discarded due to internal FIFO overflow are not included in this or any other statistic.
Bad CRCs	Bad CRCs denotes the number of bad CRC frames that the TACHYON chip has received.
Protocol Errors	This field indicates the number of protocol errors that the Frame Manager has detected.
Elastic Errors	Elastic errors reveal the timing difference between the receive and transmit clocks and usually indicate cable pulls.

TACHYON Chip Status

The number that appears in the TACHYON Status field represents the current state of the TACHYON or Fibre Channel control chip. It consists of a two-digit hexadecimal number, the first of which is explained in Table 2–12. The second digit is outlined in Table 2–13. Refer to the Hewlett-Packard TACHYON user manual for a more detailed explanation of the TACHYON chip definitions.

Table 2–12 First Digit on the TACHYON Chip

State	Definition	State	Definition
0	MONITORING	8	INITIALIZING
1	ARBITRATING	9	O_I INIT FINISH
2	ARBITRATION WON	a	O_I PROTOCOL
3	OPEN	b	O_I LIP RECEIVED
4	OPENED	c	HOST CONTROL
5	XMITTED CLOSE	d	LOOP FAIL
6	RECEIVED CLOSE	f	OLD PORT
7	TRANSFER		

Table 2–13 Second Digit on the TACHYON Chip

State	Definition	State	Definition
0	OFFLINE	6	LR2
1	OL1	7	LR3
2	OL2	9	LF1
3	OL3	a	LF2
5	LR1	f	ACTI VE

Runtime Status of Remote Copy Sets

Use the REMOTE screen to check the runtime status of all remote copy sets. Table 2–14 provides a description of the REMOTE screen column headings and possible entries under each column.

NOTE: This feature is only supported in ACS version 8.6P.

Table 2–14 Remote Display Column Definitions— ACS Version 8.6P Only

Column	Contents
COPY SET	Remote copy set name
TARGET	Target connection name and target unit number
C	Connection status:
	U = connection Up (online)
	D = connection Down (offline)
INIT	Initiator unit number
U	Availability of the unit:
	a = available to “other controller”
	d = disabled for servicing, offline
	e = mounted for exclusive access by a user
	f = media format error
	i = inoperative
	m = maintenance mode for diagnostic purposes
	o = online. Host can access this unit through “this controller”.
	r = rundown with the SET NORUN command
	v = no volume mounted due to lack of media
	x = online. Host can access this unit through “other controller”.
	z = currently not accessible to host due to a remote copy condition
	= (space) unknown availability
Kb/S	Total initiator unit bandwidth in Kb per second
ASSOC SET	Association set name
LOG	Write history log unit number
U	Log unit status: uses the same codes as “U - Availability of the unit”
Kb/S	Total log unit bandwidth in Kb per second

Table 2–14 Remote Display Column Definitions— ACS Version 8.6P Only (Continued)

Column	Contents		
LS	Log State:		
	LG	=	logging
	MG	=	merging
	CP	=	copying
	NR	=	normal
	NZ	=	normalizing
%LOG	Percent of the write history log unit available for use / remaining		
%MRG	Percent of merge process completed		
%CPY	Percent of copy process completed		

Device Port Configuration

VTDPY displays device port configuration information in a block of tabular data in the DEFAULT and DEVICE 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. Field information is explained Table 2–15.

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

Table 2–15 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 2–16 and Table 2–17.

Table 2–16 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.

Table 2–16 Controller/Processor Utilization Definitions (Continued)

Column	Contents		
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 2–17 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.

Table 2–17 VTDPY Thread Descriptions (Continued)

Thread	Description
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.
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.

Resource Performance Statistics

VTDPY displays resource performance statistics using a block of tabular data in the RESOURCE screen only. Resource name and statistical data is located along the left side of the screen (see Figure 2–7). Table 2–18 defines the resource name and statistical fields.

Table 2–18 Resource Performance Statistics Definitions

Column	Contents
Resource Name	Name of the physical resource
Free	Current resources not being used
Need	Number of resources required for the specific transaction
Wait	Number of transactions waiting to be accomplished
Buffers	Number of cache data buffers available for holding data
VAXDs	Number of value-added transfer descriptors that manage the actual device I/O operations within the controller
WARPs	Number of write algorithm request packets that manage data for RAID level 5 writes
RMDs	Number of RAID member data descriptors that manage data for RAID level 5 writes
XBUFs	Number of XOR buffers used by the FX chip for XOR operations
ZBUFs	Number of zeroed XBUFs used by the FX chip for XOR operations

Table 2–18 Resource Performance Statistics Definitions (Continued)

Column	Contents
Disk Read DWDs	Number of device work descriptors that process work requests for disk reads
Disk Write DWDs	Number of device work descriptors that process work requests for disk writes
DPCX Read DWDs	Number of device work descriptors that process work requests for tape reads
DPCX Write DWDs	Number of device work descriptors that process work requests for tape writes
DDs	Number of device work descriptors that maintain context for transfers between the host and controller
Wait Flush	Number of host write data queued for caching, pending the flushing of dirty data already cached
Wait FX	Number of transactions waiting for the FX chip to be available
Nodes	Number of cache nodes that are available for use
Dirty	Amount of data buffers in cache memory that needs to be written
Flush	Number of dirty data buffers pending flush or currently flushing from cache memory

Disk Inline Exerciser (DILX)

Use DILX to check the data transfer capability of a unit (which may be composed of one or more disk drives).

Checking for Unit Problems

DILX generates intense read/write loads to the unit while monitoring drive performance and status. Run DILX on as many units 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.

IMPORTANT: DILX cannot be run on snapshot units (ACS versions 8.6S and 8.6P) or remote copy sets (ACS version 8.6P only).

Finding a Unit in the Subsystem

Use the following steps to find a unit 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 fault LED to FLASH continuously.
4. Enter the following command to turn off the LED:

   LOCATE CANCEL

Testing the Read Capability of a Unit

Use the following steps to test the read capability of a unit:

1. From a host console, dismount the logical unit that contains the unit being tested.
2. Connect a terminal to the controller maintenance port that accesses the unit 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 unit in the subsystem.

4. Enter **N**(o) to decline the auto-configure option and to allow testing of a specific unit.
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 unit to test.

   For example: to test D107, enter the number 107.

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

   NOTE: Use the control sequences listed in Table 2–19 to control DILX during the test.

Table 2–19 DILX 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.

Testing the Read and Write Capabilities of a Unit

Run a DILX basic function test to test the read and write capability of a unit. 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 2-38 expires.

- **Write test.** Writes specific patterns of data to the unit (see Table 2–20). 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 unit 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 2–20 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 unit:

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

1. From a host console, dismount the logical unit that contains the unit that needs testing.
2. Connect a terminal to the controller maintenance port that accesses the unit 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 unit in the subsystem.

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

   NOTE: To ensure that DILX accesses the entire unit 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 unit to be tested.

    For example: to test D107, enter the number 107.

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

    NOTE: Use the command sequences shown in Table 2–19 to control the test.

DILX Error Codes

Table 2–21 explains the error codes that DILX might display during and after testing.

Table 2–21 DILX Error Codes

Error Code	Message and Explanation
1	`Illegal Data Pattern Number found in data pattern header.` Explanation: DILX read data from the unit 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 unit, 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.

Format and Device Code Load Utility (HSUTIL)

Use the HSUTIL utility to upgrade the firmware on disk 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 2–22 (many of the self-explanatory messages have been omitted from the table).

Table 2–22 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 2–22 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 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.

Code Load and Code Patch (CLCP) Utility

Use the CLCP utility to upgrade the controller software and the EMU 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.

NOTE: Only Compaq authorized service providers are allowed to upload EMU microcode updates. Contact the Customer Service Center (CSC) for directions to obtain the appropriate EMU microcode and installation guide.

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 of how FRUTIL is used during the replacement process.

IMPORTANT: FRUTIL cannot run in remote copy set environments while I/O is in progress to the target side, due to host write and normalization (ACS version 8.6P only).

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 HSG80 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 codes (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 HSG80 controller.

Passthrough Device Reset Event Sense Data Response

Events reported by passthrough devices during host/device operations are conveyed directly to the host system without intervention or interpretation by the HSG80 controller, with the exception of device sense data that is truncated to 160 bytes when it exceeds 160 bytes.

Events which are related to passthrough device recognition, initialization, and SCSI bus communication events, result in a reset of a passthrough device by the HSG80 controller. These events are reported using standard SCSI Sense Data (see Table 3–1). For all other events, refer to the templates contained within this section.

- ASC and ASCQ codes (byte offsets 12 and 13) are detailed in Chapter 4.
- Instance codes (byte offsets 8–11) are detailed in Chapter 5.

Table 3–1 Passthrough Device Reset Event Sense Data Response Format

↓offset	bit →	7	6	5	4	3	2	1	0
0		Valid	Error Code						
1		Segment							
2		FM	EOM	ILI	Reserved	Sense Key			
3–6		Information							
7		Additional Sense Length							
8–11		Instance Code							
12		Additional Sense Code (ASC)							
13		Additional Sense Code Qualifier (ASCQ)							
14		Field Replaceable Unit Code							
15		SKSV	Sense Key Specific						
16		Sense Key Specific							
17		Sense Key Specific							

Last Failure Event Sense Data Response (Template 01)

Unrecoverable conditions, detected by either software or hardware, and certain operator-initiated conditions, terminate 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 (see Table 3–2). Following a successful restart, the condition that caused controller operation to terminate is signaled to all host systems on all logical units.

> **NOTE:** For ACS version 8.6P configurations, last failure events generated by the target will not be signaled to any host unless the host has a direct connection to the target—which is not through the initiator. In addition, these events might not appear on the initiator.

- ASC and ASCQ codes (byte offsets 12 and 13) are detailed in the Chapter 4.
- Instance codes (byte offsets 32–35) are detailed in the Chapter 5.
- Last failure codes (byte offsets 104–107) are detailed in Chapter 6.

Table 3–2 Template 01—Last Failure Event Sense Data Response Format

↓offset	bit →	7	6	5	4	3	2	1	0
0		Unused	Error Code						
1		Unused							
2		Unused				Sense Key			
3–6		Unused							
7		Additional Sense Length							
8–11		Unused							
12		Additional Sense Code (ASC)							
13		Additional Sense Code Qualifier (ASCQ)							
14		Unused							
15–17		Unused							
18–31		Reserved							
32–35		Instance Code							
36		Template							
37		Template Flags							
38–53		Reserved							
54–69		Controller Board Serial Number							
70–73		Controller Software Revision Level							
74		Reserved or Patch Version (TM2)							
75		Reserved							
76		LUN Status							
77–103		Reserved							
104–107		Last Failure Code							
108–111		Last Failure Parameter [0]							
112–115		Last Failure Parameter [1]							
116–119		Last Failure Parameter [2]							
120–123		Last Failure Parameter [3]							
124–127		Last Failure Parameter [4]							
128–131		Last Failure Parameter [5]							
132–135		Last Failure Parameter [6]							
136–139		Last Failure Parameter [7]							
140–159		Reserved							

Multiple-Bus Failover Event Sense Data Response (Template 04)

The controller SCSI Host Interconnect Services software component reports Multiple-Bus Failover events via the Multiple Bus Failover Event Sense Data Response (see Table 3–3). The error or condition is signaled to all host systems on all logical units.

- ASC and ASCQ codes (byte offsets 12 and 13) are detailed in Chapter 4.
- Instance codes (byte offsets 32–35) are detailed in Chapter 5.

Table 3–3 Template 04—Multiple-Bus Failover Event Sense Data Response Format

↓offset	bit → 7	6	5	4	3	2	1	0
0	Unused	Error Code						
1	Unused							
2	Unused				Sense Key			
3–6	Unused							
7	Additional Sense Length							
8–11	Unused							
12	Additional Sense Code (ASC)							
13	Additional Sense Code Qualifier (ASCQ)							
14	Unused							
15–17	Unused							
18–26	Reserved							
27	Failed Controller Target Number							
28–31	Affected LUNs							
32–35	Instance Code							
36	Template							
37	Template Flags							
38–53	Other Controller Board Serial Number							
54–69	Controller Board Serial Number							
70–73	Controller Software Revision Level							
74	Reserved or Patch Version (TM2)							
75	Reserved							
76	LUN Status							
77–103	Reserved							
104–131	Affected LUNs Extension (TM0)							
132–159	Reserved							

Failover Event Sense Data Response (Template 05)

The controller Failover Control software component reports errors and other conditions encountered during redundant controller communications and failover operation via the Failover Event Sense Data Response (see Table 3–4). The error or condition is signaled to all host systems on all logical units.

- ASC and ASCQ codes (byte offsets 12 and 13) are detailed in Chapter 4.
- Instance codes (byte offsets 32–35) are detailed in Chapter 5.
- Last failure codes (byte offsets 104–107) are detailed in Chapter 6.

Table 3–4 Template 05—Failover Event Sense Data Response Format

↓offset	bit →	7	6	5	4	3	2	1	0
0		Unused	Error Code						
1		Unused							
2		Unused				Sense Key			
3–6		Unused							
7		Additional Sense Length							
8–11		Unused							
12		Additional Sense Code (ASC)							
13		Additional Sense Code Qualifier (ASCQ)							
14		Unused							
15–17		Unused							
18–31		Reserved							
32–35		Instance Code							
36		Template							
37		Template Flags							
38–53		Reserved							
54–69		Controller Board Serial Number							
70–73		Controller Software Revision Level							
74		Reserved or Patch Version (TM2)							
75		Reserved							
76		LUN Status							
77–103		Reserved							
104–107		Last Failure Code							
108–111		Last Failure Parameter [0]							
112–115		Last Failure Parameter [1]							
116–119		Last Failure Parameter [2]							
120–123		Last Failure Parameter [3]							
124–127		Last Failure Parameter [4]							
128–131		Last Failure Parameter [5]							
132–135		Last Failure Parameter [6]							
136–139		Last Failure Parameter [7]							
140–159		Reserved							

Nonvolatile Parameter Memory Component Event Sense Data Response (Template 11)

The controller executive software component reports errors detected while accessing a nonvolatile parameter memory component via the Nonvolatile Parameter Memory Component Event Sense Data Response (see Table 3–5). Errors are signaled to all host systems on all logical units.

- ASC and ASCQ codes (byte offsets 12 and 13) are detailed in Chapter 4.
- Instance codes (byte offsets 32–35) are detailed in Chapter 5.

Table 3–5 Template 11—Nonvolatile Parameter Memory Component Event Sense Data Response Format

↓offset	bit →	7	6	5	4	3	2	1	0
0		Unused	Error Code						
1		Unused							
2		Unused				Sense Key			
3–6		Unused							
7		Additional Sense Length							
8–11		Unused							
12		Additional Sense Code (ASC)							
13		Additional Sense Code Qualifier (ASCQ)							
14		Unused							
15–17		Unused							
18–31		Reserved							
32–35		Instance Code							
36		Template							
37		Template Flags							
38–53		Reserved							
54–69		Controller Board Serial Number							
70–73		Controller Software Revision Level							
74		Reserved or Patch Version (TM2)							
75		Reserved							
76		LUN Status							
77–103		Reserved							
104–107		Memory Address							
108–111		Byte Count							
112–114		Number of Times Written							
115		Undefined							
116–159		Reserved							

Backup Battery Failure Event Sense Data Response (Template 12)

The controller Value Added Services software component reports backup battery failure conditions for the various hardware components that use a battery to maintain state during power failures via the Backup Battery Failure Event Sense Data Response (see Table 3–6). The failure condition is signaled to all host systems on all logical units.

- ASC and ASCQ codes (byte offsets 12 and 13) are detailed in Chapter 4.
- Instance codes (byte offsets 32–35) are detailed in Chapter 5.

Table 3–6 Template 12—Backup Battery Failure Event Sense Data Response Format

↓offset	bit →	7	6	5	4	3	2	1	0
0		Unused	Error Code						
1		Unused							
2		Unused				Sense Key			
3–6		Unused							
7		Additional Sense Length							
8–11		Unused							
12		Additional Sense Code (ASC)							
13		Additional Sense Code Qualifier (ASCQ)							
14		Unused							
15–17		Unused							
18–31		Reserved							
32–35		Instance Code							
36		Template							
37		Template Flags							
38–53		Reserved							
54–69		Controller Board Serial Number							
70–73		Controller Software Revision Level							
74		Reserved or Patch Version (TM2)							
75		Reserved							
76		LUN Status							
77–103		Reserved							
104–107		Memory Address							
108–159		Reserved							

Subsystem Built-In Self Test Failure Event Sense Data Response (Template 13)

The controller Subsystem Built-In Self-Test software component reports errors detected during test execution via the Subsystem Built-In Self-Test Failure Event Sense Data Response (see Table 3–7). Errors are signaled to all host systems on all logical units.

- ASC and ASCQ codes (byte offsets 12 and 13) are detailed in Chapter 4.
- Instance codes (byte offsets 32–35) are detailed in Chapter 5.

Table 3–7 Template 13—Subsystem Built-In Self Test Failure Event Sense Data Response Format

↓offset	bit →	7	6	5	4	3	2	1	0
0		Unused	Error Code						
1		Unused							
2		Unused				Sense Key			
3–6		Unused							
7		Additional Sense Length							
8–11		Unused							
12		Additional Sense Code (ASC)							
13		Additional Sense Code Qualifier (ASCQ)							
14		Unused							
15–17		Unused							
18–31		Reserved							
32–35		Instance Code							
36		Template							
37		Template Flags							
38–53		Reserved							
54–69		Controller Board Serial Number							
70–73		Controller Software Revision Level							
74		Reserved or Patch Version (TM2)							
75		Reserved							
76		LUN Status							
77–103		Reserved							
104–105		Undefined							
106		Header Type							
107		Header Flags							
108		TE							

Table 3–7 Template 13—Subsystem Built-In Self Test Failure Event Sense Data Response Format (Continued)

↓offset	bit →	7	6	5	4	3	2	1	0
109					Test Number				
110					Test Command				
111					Test Flags				
112–113					Error Code				
114–115					Return Code				
116–119					Address of Error				
120–123					Expected Error Data				
124–127					Actual Error Data				
128–131					Extra Status 1				
132–135					Extra Status 2				
136–139					Extra Status 3				
140–159					Reserved				

Memory System Failure Event Sense Data Response (Template 14)

The controller Memory Controller Event Analyzer software component and the Cache Manager, part of the Value Added software component, report the occurrence of memory errors via the Memory System Failure Event Sense Data Response (see Table 3–8). Errors are signaled to all host systems on all logical units.

- ASC and ASCQ codes (byte offsets 12 and 13) are detailed in Chapter 4.
- Instance codes (byte offsets 32–35) are detailed in Chapter 5.

Table 3–8 Template 14—Memory System Failure Event Sense Data Response Format

↓offset	bit →	7	6	5	4	3	2	1	0
0		Unused	Error Code						
1		Unused							
2		Unused				Sense Key			
3–6		Unused							
7		Additional Sense Length							
8–11		Unused							
12		Additional Sense Code (ASC)							
13		Additional Sense Code Qualifier (ASCQ)							
14		Unused							
15–17		Unused							
18–19		Reserved							
20–23		Reserved or RDR2 (TM1)							
24–27		Reserved or RDEAR (TM1)							
28–31		Reserved							
32–35		Instance Code							
36		Template							
37		Template Flags							
38–39		Reserved							
40–43		Reserved or FXPSCR (TM1)							
44–47		Reserved or FXCSR (TM1)							
48–51		Reserved or FXCCSR (TM1)							
52–53		Reserved							
54–69		Controller Board Serial Number							
70–73		Controller Software Revision Level							

Table 3–8 Template 14—Memory System Failure Event Sense Data Response Format (Continued)

↓offset	bit →	7	6	5	4	3	2	1	0
74	Reserved or Patch Version (TM2)								
75	Reserved								
76	LUN Status								
77–79	Reserved								
80–83	Reserved or FXPAEC (TM1)								
84–87	Reserved or FXCAEC (TM1)								
88–91	Reserved or FXPAEP (TM1)								
92–95	Reserved or CHC (TM0) or FXCAEP (TM1)								
96–99	Reserved or CMC (TM0) or CFW (TM1)								
100–103	Reserved or DSR2 (TM0) or RRR (TM1)								
104–107	Memory Address								
108–111	Byte Count								
112–115	DSR or PSR (TM1)								
116–119	CSR or CSR (TM1)								
120–123	DCSR or EAR (TM1)								
124–127	DER or EDR1 (TM1)								
128–131	EAR or EDR0 (TM1)								
132–135	EDR or ICR (TM1)								
136–139	ERR or IMR (TM1)								
140–143	RSR or DID (TM1)								
144–147	RDR0								
148–151	RDR1								
152–155	WDR0								
156–159	WDR1								

Device Services Nontransfer Error Event Sense Data Response (Template 41)

The controller Device Services software component reports errors detected while performing nontransfer work related to disk (including CD-ROM and optical memory) device operations via the Device Services Nontransfer Event Sense Data Response (see Table 3–9). If an error occurred during the execution of a command issued by an HSG80 controller software component, it is signaled to all host systems on all logical units.

- ASC and ASCQ codes (byte offsets 12 and 13) are detailed in Chapter 4.
- Instance codes (byte offsets 32–35) are detailed in Chapter 5.

Table 3–9 Template 41—Device Services Non-Transfer Error Event Sense Data Response Format

↓offset	bit →	7	6	5	4	3	2	1	0
0		Unused	Error Code						
1		Unused							
2		Unused				Sense Key			
3–6		Unused							
7		Additional Sense Length							
8–11		Unused							
12		Additional Sense Code (ASC)							
13		Additional Sense Code Qualifier (ASCQ)							
14		Unused							
15–17		Unused							
18–31		Reserved							
32–35		Instance Code							
36		Template							
37		Template Flags							
38–53		Reserved							
54–69		Controller Board Serial Number							
70–73		Controller Software Revision Level							
74		Reserved or Patch Version (TM2)							
75		Reserved							
76		LUN Status							
77–103		Reserved							
104		Associated Port							
105		Associated Target							
106		Associated Additional Sense Code							
107		Associated Additional Sense Code Qualifier							
108–159		Reserved							

Disk Transfer Error Event Sense Data Response (Template 51)

The controller Device Services and Value Added Services software components report errors detected while performing work related to disk (including CD-ROM and optical memory) device transfer operations via the Disk Transfer Error Event Sense Data Response (see Table 3–10). If an error occurred during the execution of a command issued by an HSG80 controller software component, the error is signaled to all host systems on the logical unit associated with the physical unit that reported the error.

- ASC and ASCQ codes (byte offsets 12 and 13) are part of the Standard Sense Data and detailed in Chapter 4.
- Instance codes (byte offsets 32–35) are detailed in Chapter 5.

Table 3–10 Template 51—Disk Transfer Error Event Sense Data Response Format

↓offset	bit →	7	6	5	4	3	2	1	0
0–17	Standard Sense Data								
18–19	Reserved								
20	Total Number of Errors								
21	Total Retry Count								
22–25	ASC/ASCQ Stack								
26–28	Device Locator								
29–31	Reserved								
32–35	Instance Code								
36	Template								
37	Template Flags								
38	Reserved								
39	Command OpCode								
40	Sense Data Qualifier								
41–50	Original CDB								
51	Host ID								
52–53	Reserved								
54–69	Controller Board Serial Number								
70–73	Controller Software Revision Level								
74	Reserved or Patch Version (TM2)								
75	Reserved								
76	LUN Status								
77–78	Reserved								
79–82	Device Firmware Revision Level								
83–98	Device Product ID								
99–100	Reserved								
101	Device Type								
102–103	Reserved								
104–121	Device Sense Data								
122–159	Reserved								

Data Replication Manager Services Event Sense Response (Template 90)

This section only applies to ACS version 8.6P. The controller Data Replication Manager Services software component reports events via the Data Replication Manager Services Event Sense Data Response.

With Data Replication Manager, fault management events are reported using Template 90, shown in Table 3–11. The error is signaled to all host systems on the logical unit associated with the initiator unit that reported the error.

- ASC and ASCQ codes (byte offsets 12 and 13) are detailed in Chapter 4.
- Instance codes (byte offsets 32–35) are detailed in Chapter 5.

Table 3–11 Template 90—Data Replication Manager Services Event Sense Data Response Format (ACS Version 8.6P Only)

↓offset	bit →	7	6	5	4	3	2	1	0
0		Unused	Error Code						
1		Unused							
2		Unused				Sense Key			
3–6		Unused							
7		Additional Sense Length							
8–11		Unused							
12		Additional Sense Code (ASC)							
13		Additional Sense Code Qualifier (ASCQ)							
14		Unused							
15–17		Unused							
18–27		Reserved							
28–31		Reserved or Log Unit Number (TM0)							
32–35		Instance Code							
36		Template							
37		Template Flags							
38–53		Target Controller Board Serial Number							
54–69		Controller Board Serial Number							
70–73		Controller Software Revision Level							
74		Reserved or Patch Version (TM2)							
75		Reserved							
76		LUN Status							
77–79		Reserved							
80–95		Initiator WWLID							
96–103		Initiator Node Name							
104–107		Initiator Unit Number							
108–123		Target WWLID							
124–131		Target Node Name							
132–135		Target Unit Number							
136–139		Number of Targets							
140–148		Remote Copy Set Name							
149–157		Reserved or Association Set Name (TM0)							
158–159		Reserved							

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 HSG80 controller vendor-specific SCSI ASC and ASCQ codes. These codes are also template-specific and appear at byte offsets 12 and 13.

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 3)

ASC Code	ASCQ Code	Description
04	80	Logical unit is disaster tolerant failsafe locked (inoperative).
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	CE	UPS TMW before AC_FAIL.
3F	D2	Synchronous Transfer Value differences between drives.
80	00	Forced error on Read.
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.
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.

Table 4–1 ASC and ASCQ Code Descriptions (Sheet 2 of 3)

ASC Code	ASCQ Code	Description
A0	08	Multiple Bus failover event.
A0	09	Multiple Bus failback event.
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.
A2	00	Data Replication Manager connection event.
A2	01	Remote Copy Set membership event.
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.
D1	04	ID Message not sent.
D1	05	Synchronous negotiation error.
D1	07	Unexpected disconnect.

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

ASC Code	ASCQ Code	Description
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.
F0	01	Device Nickname has been freed.
F0	02	New Device Nickname.
F0	03	Device Nickname changed.

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 6)

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. Contact a Compaq authorized service provider.
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 6)

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 EMU has detected an elevated temperature condition. Check the shelf and its components for the cause of the fault.
0E	The EMU 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 EMU is now fixed. This event report is notification that the repair was successful.
10	Restore on-disk configuration information to original state.
11	The 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 the 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 6)

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 the mirrored cache for this controller. Since the mirrored cache is physically located on the other controller cache module, replace the other controller 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 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 6)

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 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 6)

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.
5D	The last member of the SPARESET has been removed. Add new drives to the SPARESET.
69	An unrecoverable fault occurred at the host port. There may be more than one entity attempting to use the same SCSI ID, or some other bus configuration error, such as improper termination, may exist. If no host bus configuration problems are found, follow Repair Action 01.
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.
88	The remote copy set has an online initiator unit and at least one remote NORMAL/NORMALIZING target member. Failsafe error mode can now be enabled by entering the CLI command SET *remote-copy-set-name* ERROR_MODE=FAILSAFE.
89	The remote copy set is inoperative due to a disaster tolerance failsafe locked condition, as a result of the loss of the local initiator unit or remote NORMAL/NORMALIZING target members while ERROR_MODE=FAILSAFE was enabled. To clear the failsafe locked condition, enter the CLI command SET *remote-copy-set-name* ERROR_MODE=NORMAL.
8A	The indicated remote copy set target member was removed for one of the following reasons: ■ By operator command. ■ The member malfunctioned. Perform the repair actions indicated in any and all event reports found for that target member.

Table 4–2 Recommended Repair Action Codes (Sheet 6 of 6)

Code	Description
8B	Unable to communicate to the target member of the remote copy set for one of the following reasons: ■ The target malfunctioned. Perform the repair actions indicated in any and all event reports found for that target unit. ■ The target controller malfunctioned. Perform the repair actions indicated in any and all event reports found for that target controller. ■ Malfunction that occurred in the Fibre Channel fabric between the peer controllers.
8C	Unable to communicate to an initiator unit of the remote copy set because the unit malfunctioned. Perform the repair actions indicated in any and all event reports found for that initiator unit.
8D	Not safe to present the WWLID to the host because a site failover may have taken place, but cannot confirm with the remote controller. Perform one of the following repair actions: ■ Follow Repair Action 8B. ■ If a site failover took place, and you do not plan to perform a future site failback, then delete the remote copy set on this controller.
8E	Not safe to present the WWLID to the host because a site failover has taken place. Perform one of the following repair actions: ■ Perform a site failback. ■ Delete the remote copy set on this controller.
8F	Unable to communicate to a log unit because the unit malfunctioned. Perform the repair actions indicated in any and all event reports found for that log unit.

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	Power off Process
0E	Data Replication Manager Services (ACS version 8.6P only)
12	Value Added Services (extended)
20	Command Line Interpreter (CLI)
43	Host Port Protocol Layer
44	Host Port Transport Layer
64	SCSI Host Value Added Services
80	Disk Inline Exercise (DILX)
82	Subsystem Built-In Self Tests (BIST)
83	Device Configuration Utilities (CONFIG)
84	Clone Unit Utility (CLONE)
85	Format and Device Code Load Utility (HSUTIL)
86	Code Load/Code Patch Utility (CLCP)

Table 4–3 Component ID Codes (Continued)

Code	Description
8A	Field Replacement Utility (FRUTIL)
8B	Periodic Diagnostics (PDIAG)

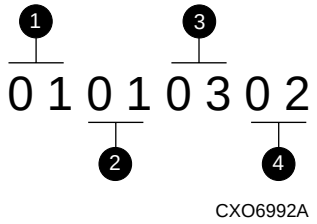
Chapter 5

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

offset	bit →	7	6	5	4	3	2	1	0
{8}32		NR Threshold							
{9}33		Repair Action							
{10}34		Event Number							
{11}35		Component ID							

NOTE: The offset values enclosed in braces ({ }) apply only to the passthrough device reset event sense data response format (see Chapter 3, Table 3–1).

The nonbraced offset values apply only to the logical device event sense data response formats shown in the templates provided in Chapter 3.

Notification/Recovery Threshold

Located at byte offset {8}32 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 byte offset {9}33 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 byte offset {10}34. Combining this number with the Component ID field value uniquely identifies the reported event.

Component ID

A Component ID is located at byte offset {11}35. This number uniquely identifies the software component that detected the event. For details about component 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 22)

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
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
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

Table 5–3 Instance Codes and Repair Action Codes (Sheet 2 of 22)

Instance Code	Description	Template	Repair Action Code
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
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

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

Instance Code	Description	Template	Repair Action Code
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
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

Table 5–3 Instance Codes and Repair Action Codes (Sheet 4 of 22)

Instance Code	Description	Template	Repair Action Code
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
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
0251000A	This command failed because the target unit is not online to the controller. The Information field of the Device Sense Data contains the block number of the first block in error.	51	00
0253000A	The data supplied from the host for a data compare operation differs from the data on the disk in the specified block. The Information field of the Device Sense Data contains the block number of the first block in error.	51	00

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

Instance Code	Description	Template	Repair Action Code
0254000A	The command failed due to a host data transfer failure. The Information field of the Device Sense Data contains the block number of the first block in error.	51	00
0255000A	The controller was unable to successfully transfer data to the target unit. The Information field of the Device Sense Data contains the block number of the first block in error.	51	00
0256000A	The write operation failed because the unit is Data Safety Write Protected. The Information field of the Device Sense Data contains the block number of the first block in error.	51	00
0257000A	An attempt to reassign a bad disk block failed. The contents of the disk block are lost. The Information field of the Device Sense Data contains the block number of the first block in error.	51	00
0258000A	This command was aborted prior to completion. The Information field of the Device Sense Data contains the block number of the first block in error.	51	00
0259000A	The write operation failed because the unit is hardware write protected. The Information field of the Device Sense Data contains the block number of the first block in error.	51	00
025A000A	The command failed because the unit became inoperative prior to command completion. The Information field of the Device Sense Data contains the block number of the first block in error.	51	00
025B000A	The command failed because the unit became unknown to the controller prior to command completion. The Information field of the Device Sense Data contains the block number of the first block in error.	51	00
025C000A	The command failed because of a unit media format error. The Information field of the Device Sense Data contains the block number of the first block in error.	51	00
025D000A	The command failed for an unknown reason. The Information field of the Device Sense Data contains the block number of the first block in error.	51	00

Table 5–3 Instance Codes and Repair Action Codes (Sheet 6 of 22)

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 22)

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 22)

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 fully charge 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 of deep discharges allowed. 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 22)

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
028F8901 02908901 02918901	The host command failed because the remote copy set went failsafe locked prior to command completion. The remote copy set is specified by the Remote Copy Name field. The Information field of the Device Sense Data contains the block number of the first block in error.	51	89
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
02931101	The UPS signaled a 2-minute warning (TMW) before signaling an AC line failure. UPS signals will be ignored until this condition clears.	12	11
0294000A	A requested block of data contains a forced error. A forced error occurs when a disk block is successfully reassigned, but the data in that block is lost. Re-writing the disk block will clear the forced error condition. The Information field of the Device Sense Data contains the block number of the first block in error.	51	00
0295000A	The snapshot unit indicated by the Unit Number field has been disabled. Reads to the unit will fail. Reasons for disabling the snapshot are a failure to copy to the temporary storageset, or no room on the temporary storageset to properly fail over the snapshot.	51	00

Table 5–3 Instance Codes and Repair Action Codes (Sheet 10 of 22)

Instance Code	Description	Template	Repair Action Code
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
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

Table 5–3 Instance Codes and Repair Action Codes (Sheet 11 of 22)

Instance Code	Description	Template	Repair Action Code
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
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
03324002	SCSI bus selection timeout.	Passthrough	40
03330002	Device power on reset.	Passthrough	00
03344002	Target assertion of REQ after WAIT DISCONNECT.	Passthrough	40
03354002	During device initialization a Test Unit Ready command or a Read Capacity command to the device failed.	Passthrough	40
03364002	During device initialization the device reported a deferred error.	Passthrough	40
03374002	During device initialization the maximum number of errors for a data transfer operation was exceeded.	Passthrough	40

Table 5–3 Instance Codes and Repair Action Codes (Sheet 12 of 22)

Instance Code	Description	Template	Repair Action Code
03384002	Request Sense command to the device failed.	Passthrough	40
03394002	Command timeout.	Passthrough	40
033A4002	Disconnect timeout.	Passthrough	40
033B4002	Unexpected bus phase.	Passthrough	40
033C4002	The device unexpectedly disconnected from the SCSI bus.	Passthrough	40
033D4002	Unexpected message.	Passthrough	40
033E4002	Message Reject received on a valid message.	Passthrough	40
033F0101	No command control structures available for passthrough device operation.	Passthrough	01
03402002	Device port SCSI chip reported gross error.	Passthrough	20
03410101	Miscellaneous SCSI Port Driver coding error.	Passthrough	01
03420101	A passthrough device related internal error code was reported that is not recognized by the Fault Management software.	Passthrough	01
03434002	During device initialization the device reported unexpected standard SCSI Sense Data.	Passthrough	40
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
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

Table 5–3 Instance Codes and Repair Action Codes (Sheet 13 of 22)

Instance Code	Description	Template	Repair Action Code
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
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

Table 5–3 Instance Codes and Repair Action Codes (Sheet 14 of 22)

Instance Code	Description	Template	Repair Action Code
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
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

Table 5–3 Instance Codes and Repair Action Codes (Sheet 15 of 22)

Instance Code	Description	Template	Repair Action Code
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
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

Table 5–3 Instance Codes and Repair Action Codes (Sheet 16 of 22)

Instance Code	Description	Template	Repair Action Code
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, neither controller front panel button presses nor removal/insertion of devices are 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 17 of 22)

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 18 of 22)

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 19 of 22)

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 20 of 22)

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
0E010064	A remote copy set has been created specified by the Remote Copy Set Name field. The initiator unit of the Remote Copy Set is specified by the Initiator WWLID field.	90	00
0E020064	The remote copy set specified by the Remote Copy Set Name field has been deleted by the operator.	90	00
0E030064	The logical unit specified by the Target WWLID has transitioned from the normalizing or copying state to the normal state.	90	00
0E050064	The logical unit specified by the Target WWLID has been added to the remote copy set specified by the Remote Copy Set Name field. The new target member is now in the normalizing state.	90	00
0E068A01	The logical unit specified by the Target WWLID has been removed from the remote copy set specified by the Remote Copy Set Name field.	90	8A
0E078A01	The logical unit specified by the Target WWLID has been removed from the remote copy set specified by the Remote Copy Set Name field. The target was removed by the operator.	90	8A
0E088864	The remote copy set specified by the Remote Copy Set Name field has just had a membership change such that disaster tolerance failsafe error mode can now be enabled if desired.	90	88
0E098901	The remote copy set specified by the Remote Copy Set Name field has gone inoperative due to a disaster tolerance failsafe locked condition.	90	89
0E0A8D01	The unit is not made available to the host for the remote copy set specified in the Remote Copy Set Name field. This controller cannot verify a site failover did not occur; hence, it is not safe to present the WWLID.	90	8D
0E0B8E01	The unit is not made available to the host for the remote copy set specified in the Remote Copy Set Name field. This controller discovered a site failover occurred; hence, this controller cannot present the WWLID.	90	8E

Table 5–3 Instance Codes and Repair Action Codes (Sheet 21 of 22)

Instance Code	Description	Template	Repair Action Code
0E0C8C01	The copy was terminated due to a *read failure on the initiator unit*. The initiator unit is specified by the Initiator WWLID field.	90	8C
0E0E8B01	Changes to *write failure on the target unit*.		8B
0E0F8B01	The copy was terminated due to a write failure on the target unit. The write failure was due to the links being down (target inaccessible). The copy will restart when at least one link is restored. The initiator unit is specified by the Initiator WWLID field.	90	8B
0E100064	A link (connection) to a target controller was just restored.	90	00
0E110064	The logical unit specified by the Target WWLID has transitioned from the merging state to the normal state.	90	00
0E120064	A link (connection) to a target controller was just restored.	90	00
0E1A8B01	Write history log merge has encountered a write error on the remote target unit.	90	8B
0E1D8B01	Write history log merge detected the target unit has failed.	90	8B
0E1E8C01	The asynchronous merge was terminated due to a read failure on the initiator unit.	90	8C
0E1F8B01	The asynchronous merge was terminated due to a write failure on the target unit.	90	8B
0E210064	The logical unit specified by the Target WWLID field has transitioned from the normal state to the write history logging state due to a remote connection event (the target controllers are no longer accessible) or CLI SUSPEND command.	90	00
0E220064	The logical unit specified by the Target WWLID field has transitioned from the logging state to the merging state due to a remote connection event (the target controllers are no longer accessible) or CLI RESUME command.	90	00
0E238F01	The logical unit specified by the Log Unit Number field has failed.	90	8F
0E258F01	Write history logging encountered a write error on the log unit.	90	8F
0E260064	There is no more space left at the end of the log unit for write history logging.	90	00
0E278F01	Write history log merge has encountered a read error on the log unit.	90	8F
0E288F01	The log unit has failed with a Media Format Error.	90	8F

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

Instance Code	Description	Template	Repair Action Code
0E290064	The log unit has been reset because the specified target member has been marked invalid. For instance, a site failover has been detected or a full member copy has started.	90	00
0E2A8F01	The logical unit specified by the Log Unit Number field is unknown or inoperative.	90	8F
0E2B0064	The log unit has been reset due to loss of cached data for the write history log. The specified target member has been marked for a full copy.	90	00
0E2C0064	A target member is being removed while write history logging is active.	90	00
43010064	Host Port Protocol component has detected that the other controller has failed and that this controller has taken over the units specified in the extended sense data.	04	00
43020064	Host Port Protocol component has detected that this controller has taken over (failed back) the units specified in the extended sense data.	04	00
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

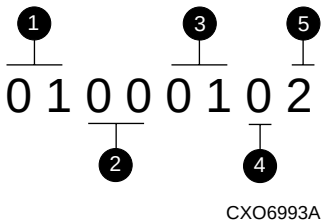
Last Failure Codes

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 Sense Data Response Format (see Chapter 3)
- Template 05—Failover Event Sense Data Response 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

offset	bit →	7	6	5	4	3	2	1	0
104		HW	Restart Code			Parameter Count			
105		Repair Action							
106		Error Number							
107		Component ID							

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 byte offset 104, bits 0–3 and indicates the number of Last Failure Parameters containing supplemental information supplied.

Restart Code

Located at byte offset 104, bits 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 byte offset 104, bit 7. 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 byte offset 105 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 byte offset 106. Combining this number with the Component ID field value uniquely identifies the reported failure.

Component ID Code

The Component ID code is located at byte offset 107. 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 43)

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 flashing 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
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 power on 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

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 2 of 43)

Last Failure Code	Description	Repair Action Code
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
01140102	DEBUG, ASSUME, or ASSUME_LE macro executed. ■ Last Failure Parameter [0] contains the address of the module name where the macro is located. ■ Last Failure Parameter [1] contains the line number within the module where the macro is located. The high order byte of this value identifies the macro type: 0 = DEBUG, 1 = ASSUME, 2 = ASSUME_LE.	01
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

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 3 of 43)

Last Failure Code	Description	Repair Action Code
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
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

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 4 of 43)

Last Failure Code	Description	Repair Action Code
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
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

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 5 of 43)

Last Failure Code	Description	Repair Action Code
01910084	A Cache Module was inserted or removed. ■ Last Failure Parameter [0] contains the value of the actual Cache Module A exists state. ■ Last Failure Parameter [1] contains the value of the actual Cache Module B exists state. ■ Last Failure Parameter [2] contains the value of the expected Cache Module A exists state. ■ Last Failure Parameter [3] contains the value of the expected Cache Module B exists state.	00
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 the error register. ■ Last Failure Parameter [5] contains the PCFX *CDAL* control / status register. ■ Last Failure Parameter [6] contains the previous *CDAL* address of the error register. ■ Last Failure Parameter [7] contains the current *CDAL* address of the error register.	25
01942088	Changes to *PDAL*.	20

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 6 of 43)

Last Failure Code	Description	Repair Action Code
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 the 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 the error register.	01
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 the 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 the 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

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 7 of 43)

Last Failure Code	Description	Repair Action Code
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 the error register. ■ Last Failure Parameter [6] contains the RIP.	20
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 the error register. ■ Last Failure Parameter [5] contains the PLX status register. ■ Last Failure Parameter [6] contains the previous PDAL address of the error register. ■ Last Failure Parameter [7] contains the RIP.	20
019A2093	Hardware Port Hardware failure - TACHYON. ■ Last Failure Parameter [0] contains failed port number. ■ Last Failure Parameter [1] contains gluon status. ■ Last Failure Parameter [2] contains TACHYON status.	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*.	
020C0100	Changes to *miscellaneous*.	

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 8 of 43)

Last Failure Code	Description	Repair Action Code
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$MARK_META_DIRTY call.	01
02270104	A callback from device services (DS) on a transfer request has returned a bad or illegal DWD status. ■ Last Failure Parameter [0] contains the DWD Status. ■ Last Failure Parameter [1] contains the DWD address. ■ Last Failure Parameter [2] contains the Physical Unit Block (PUB) address. ■ Last Failure Parameter [3] contains the Device Port.	01
022C0100	A *READ_LONG* operation was requested for a Local Buffer Transfer. *READ_LONG* is not supported for Local Buffer Transfers.	01
022D0100	Changes to *WRITE_LONG*.	
02380102	An invalid status was returned from CACHE$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

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 9 of 43)

Last Failure Code	Description	Repair Action Code
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
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

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 10 of 43)

Last Failure Code	Description	Repair Action Code
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
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 02A50100	A call to EXEC$ALLOCATE_MEM_ZEROED failed to return memory when allocating *VA transfer descriptors (VAXDs)*. Changes to *DILPs*.	01
02A60100 02A70100	A call to EXEC$ALLOCATE_MEM_ZEROED failed to return memory when allocating *Change State Work Items*. Changes to *VA Request Items*.	01
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

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 11 of 43)

Last Failure Code	Description	Repair Action Code
02AC0100	An invalid call was made to CACHE$DEALLOCATE_SLD. The RAIDset still has data (strip nodes).	01
02AE0100	The mirrorset member count and individual member states are inconsistent. Discovered during a mirrorset write or erase.	01
02AF0102	An invalid status was returned from VA$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 (for example, 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*.	

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 12 of 43)

Last Failure Code	Description	Repair Action Code
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
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 13 of 43)

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 14 of 43)

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 nonvolatile 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 15 of 43)

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 power on 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 power on 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 16 of 43)

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
03040101	Invalid SCSI CDROM 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
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

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 17 of 43)

Last Failure Code	Description	Repair Action Code
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
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 18 of 43)

Last Failure Code	Description	Repair Action Code
03330188	A parity error was detected by a device port while sending data 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 19 of 43)

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

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 20 of 43)

Last Failure Code	Description	Repair Action Code
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
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

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 21 of 43)

Last Failure Code	Description	Repair Action Code
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 43)

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 automatic configuration buffer allocation.	01
034A0100	Insufficient memory available for PUB allocation.	01
034B0100	Insufficient memory available for DS initialization 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

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 23 of 43)

Last Failure Code	Description	Repair Action Code
035A0100	Invalid SCSI message byte passed to DS.	01
035B0100	Insufficient DWD resources available for SCSI message passthrough.	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
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

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 24 of 43)

Last Failure Code	Description	Repair Action Code
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
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 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 SCSI Port number(s) where the problem exists for cabinet 2. ■ Last Failure Parameter [2] contains a bit mask indicating 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

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 25 of 43)

Last Failure Code	Description	Repair Action Code
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
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
040A0100	The caller of FM$CANCEL_SCSI_DE_NOTIFICATION passed an address of a deferred error notification routine which does not match the address of any routines for which deferred error notification is enabled.	01
040E0100	FM$ENABLE_DE_NOTIFICATION was called to enable deferred error notification but the specified routine was already enabled to receive deferred error 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
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

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 26 of 43)

Last Failure Code	Description	Repair Action Code
04120101	CLIB$SDD_FAO call failed. Last Failure Parameter [0] contains the failure status code value.	01
04140103	The template value found in the EIP is not supported by the Fault Manager. The bad template value was discovered while trying to build an ESD. ■ Last Failure Parameter [0] contains the Instance Code value. ■ Last Failure Parameter [1] contains the template code value. ■ Last Failure Parameter [2] contains the requester error table index value.	01
04170102	The template value found in the ESD is not supported by the Fault Manager. The bad template value was discovered while trying to translate an ESD into an EIP. ■ Last Failure Parameter [0] contains the Instance Code value. ■ Last Failure Parameter [1] contains the template code value.	01
04180103	The COMMON$MEM_FAIL_TEMPLATE template found in the ESD is not supported by the Fault Manager. The bad template was discovered while trying to translate an ESD into an EIP. ■ Last Failure Parameter [0] contains the Instance Code value. ■ Last Failure Parameter [1] contains the template code value. ■ Last Failure Parameter [2] contains the template flags value.	01
04190100	A NULL pointer was found for the target_ctx, or the target_ctx has an invalid type.	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

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 27 of 43)

Last Failure Code	Description	Repair Action Code
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$CANCEL_NOTIFY( ) was called to disable notification for a return that did not have notification enabled.	01
07030100	Unable to start the Failover Control Timer before main loop.	01
07040100	Unable to restart the Failover Control Timer.	01
07050100	Unable to allocate flush buffer.	01
07060100	Unable to allocate active receive failover control block (FCB).	01
07070100	The other controller killed this, but could not assert the kill line because nindy on or in debug. So it “killed” this now.	01
07080000	The other controller crashed, so this one must crash too.	00
07090100	A call to EXEC$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

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 28 of 43)

Last Failure Code	Description	Repair Action Code
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$TRANSACTION had a from field (ID) that was out of range for the NVFOC communication utility. Last Failure Parameter [0] contains the bad ID value.	01
08110101	NVFOC tried to defer more than one FOC send. Last Failure Parameter [0] contains the master ID of the connection that had the multiple delays.	01
08140100	Could not allocate memory to build a workblock to queue to the NVFOC thread.	01
08160100	A request to clear the remote configuration was received but the memory was not locked.	01
08170100	A request to read the next configuration was received but the memory was not locked.	01
08180100	Could not get enough memory for firmware licensing system (FLS) FCBs to receive information from the other controller.	01
08190100	An unlock command was received when the NV memory was not locked.	01
081A0100	Unable to allocate memory for remote work.	01
081B0101	Bad remote work received on remote work queue. Last Failure Parameter [0] contains the ID type value that was received on the NVFOC remote work queue.	01
081C0101	Bad member management work received. Last Failure Parameter [0] contains the bad member management value that was detected.	01
081D0000	In order to go into *mirrored* cache mode, the controllers must be restarted.	00
081E0000	Changes to *nonmirrored*.	
081F0000	An FLM$INSUFFICIENT_RESOURCES error was returned from a facility lock manager (FLM) lock or unlock call.	00

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 29 of 43)

Last Failure Code	Description	Repair Action Code
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 facility found.	01
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

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 30 of 43)

Last Failure Code	Description	Repair Action Code
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
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

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 31 of 43)

Last Failure Code	Description	Repair Action Code
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$LOG_ENTRY, page guard check failed. ■ Last Failure Parameter [0] contains the DWD address value. ■ Last Failure Parameter [1] contains the buffer address value.	01
0A330100	ILF_OUPUT_ERROR, MESSAGE_KEEPER_ARRAY full.	01
0A340101	ILF_OUTPUT_ERROR, no memory for message display. Last Failure Parameter [0] contains the message address value.	01
0A360100	Duplicate entry found in ILF_POPULATE_DWD_FROM_CACHE buffer stack.	01
0A370100	Duplicate entry found in ILF_REBIND_CACHE_BUFFS_TO_DWDS buffer stack.	01
0A380108	Next entry was partially loaded. ■ Last Failure Parameter [0] contains the next entry address. ■ Last Failure Parameter [1] contains the next entry record type. ■ Last Failure Parameter [2] contains the next entry time of day (TOD) flag. ■ Last Failure Parameter [3] contains the next entry interrupt (INT) flag. ■ Last Failure Parameter [4] contains the next entry byte count. ■ Last Failure Parameter [5] contains the next entry TOD ticks. ■ Last Failure Parameter [6] contains the next entry TOD days. ■ Last Failure Parameter [7] contains the next entry data start.	01
0B010010	Due to an operator request, the controller nonvolatile configuration information has been reset to its initial state.	00
0B020100	The controller has insufficient free memory to allocate a Configuration Manager work item needed to perform the requested configuration *reset*.	01
0B030100	Changes to *restore*.	
0B040100	The controller has insufficient free memory to allocate a Configuration Manager WWL work item needed to perform the requested World-Wide LUN ID change.	01
0B050100	More requests to WWL$NOTIFY have been made than can be supported.	01
0B060100	A call to WWL$UPDATE resulted in the need for another World-Wide LUN ID slot, and no free slots were available.	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 32 of 43)

Last Failure Code	Description	Repair Action Code
0B070100	The controller has insufficient free memory to allocate a Configuration Manager DNN work item needed to perform the requested Device Nickname change.	01
0B080100	More requests to DNN$NOTIFY have been made than can be supported.	01
0B090100	A call to DNN$UPDATE resulted in the need for another Device Nickname slot, and no free slots were available.	01
0B0A0100	Unable to find any unused partition group. With 127 available, we should be able to find at least one.	01
0B0B0100	Unable to find any unused partition group. With 128 available, we should be able to find at least one.	01
0B0C0100	Unable to allocate memory to use for communication with the DT manager.	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
0E000100	VA$ENABLE_NOTIFICATION failed with insufficient resources at controller initialization time.	01
0E010102	An invalid status was returned from CACHE$LOCK_READ during a remote copy. ■ Last Failure Parameter [0] contains the DD address. ■ Last Failure Parameter [1] contains the invalid status.	01
0E020100	Unable to allocate memory for the Fault Management Event Information Packet used in generating error logs to the host.	01
0E030100 0E040100 0E050100 0E060100	Unable to allocate memory for a Failover Control Block.	01
0E096980	This controller has detected a failed link during the heartbeat to a remote target. The other controller has a good link to the remote target. In order to resume operations to that remote target, this controller is restarted to fail over the initiator unit to the other controller.	69
0E0A6980	A remote copy write has failed all recovery attempts on this controller. As part of further error recovery, this controller is restarted, to force the initiator unit over to the other controller so the remote copy can be retried.	69
0E0B6980	This controller has detected a failed link upon dual controllers restarting. The other controller has a good link to the remote target. In order to resume operations to that remote target, this controller is restarted to fail over the initiator unit to the other controller.	69

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 33 of 43)

Last Failure Code	Description	Repair Action Code
0E0C0101	Unrecognized request to perform Write History Log (WHL) operation on other controller. Last Failure Parameter [0] contains operation request.	01
0E0D0101	Unrecognized WHL operation ID received from other controller. Last Failure Parameter [0] contains an operation ID.	01
0E0E0101	An illegal failover request was given to the WHL request handler. Last Failure Parameter [0] contains a failover request.	01
0E0F0101	An illegal failover response was given to the WHL response handler. Last Failure Parameter [0] contains a failover response.	01
0E100100	The Write History Log failover control had a bad send count.	01
0E110100	Unable to allocate memory for WHL DBs.	01
0E120100	Unable to allocate memory for WHL HTBs.	01
0E130100	Unable to allocate memory for WHL ESDs.	01
0E140100	Unable to allocate memory for WHL DDs.	01
0E150101	Unable to allocate memory for WHL metadata. Last Failure Parameter [0] contains response failure code.	01
0E160100	An illegal WHL lock state was detected.	01
0E170101	An invalid sense key was detected during WHL processing. Last Failure Parameter [0] contains unexpected sense key.	01
0E180100	Call to VA$ENABLE_NOTIFICATION( ) failed due to INSUFFICIENT_RESOURCES.	01
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 34 of 43)

Last Failure Code	Description	Repair Action Code
12020103	First value found *greater 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 *greater*.	
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
120C0101	Found invalid UPS Descriptor state. Last Failure Parameter[0] contains UPS Descriptor state.	01
120D0100	Initialization code was unable to allocate enough memory to set up the send data descriptors for local buffer transfers.	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 35 of 43)

Last Failure Code	Description	Repair Action Code
120E0310	An image upgrade that updated the cache metadata version failed, because the cache module hardware for non-volatile metadata contained therein was bad. Either this controller cache hardware failed (or for the case of mirrored cache, the other controller cache hardware), or the cache metadata was in an invalid state. Restart this controller using the pre-upgrade image, and use SHOW THIS_CONTROLLER to determine whether the hardware failed, or the metadata was in the INVALID CACHE state. Fix the condition and verify that it is fixed before restarting the upgrade procedure from the beginning.	03
120F0310	An image upgrade that updated the cache metadata version failed, because the cache module holds dirty data that needs to be flushed prior to image swap. Restart “this controller” using the pre-upgrade image, and restart the upgrade procedure from the beginning. This procedure causes dirty data to be flushed before the new image is installed.	03
12100310	An image upgrade that updated the cache metadata version failed, because the cache module held dirty data. This was likely caused by deviating from the required upgrade procedure (by not properly verifying the integrity of the system prior to the image swap, or by swapping hardware components as part of the procedure). The dirty data was permanently cleared from the cache. Restart this controller using the pre-upgrade image If either the SHOW THIS_CONTROLLER INVALID_CACHE or SHOW UNIT Lost Data conditions are found, they must be cleared.	03
12110310	An image upgrade that updated the cache metadata version failed, because the cache module held dirty data. This was likely caused by deviating from the required upgrade procedure (by not properly verifying the integrity of the system prior to the image swap, or by swapping hardware components as part of the procedure). The dirty data was permanently cleared from the cache. Restart this controller using the pre-upgrade image. If either the SHOW THIS_CONTROLLER INVALID_CACHE or SHOW UNIT Lost Data conditions are found, they must be cleared.	03
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
20030100	The type of work received on the CLI work queue was not of type CLI.	01
20060100	A work item of an unknown type was placed on the CLI SCSI Virtual Terminal thread work queue by the CLI.	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 36 of 43)

Last Failure Code	Description	Repair Action Code
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
201B0100	Insufficient resources to get memory to *lock* CLI.	01
201C0100	Changes to *unlock*.	

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 37 of 43)

Last Failure Code	Description	Repair Action Code
20200100	CLI$ALLOCATE_STRUCT( ) could not obtain memory for a new NVFOC_RW_REMOTE_NVMEM structure.	01
20220020	This controller requested this subsystem to power off.	00
20230000	A restart of both controllers is required when exiting multibus failover.	00
20260000	With “set failover copy=other”, the controller to which the configuration is copied will automatically be restarted by this bugcheck.	00
20640000	Nindy was turned *on*.	00
20650000	Changes to *off*.	
20692010	To enter dual-redundant mode, both controllers must be of the same type.	20
206A0000	Controller restart forced by DEBUG CRASH REBOOT command.	00
206B0010	Changes to DEBUG CRASH NOREBOOT.	
206C0020	Controller was forced to restart in order for new controller code image to take effect.	00
206D0000	Controller code load was not completed because the controller could not rundown all units.	00
206E0000	A restart of both controllers is required when entering multibus failover and the last failover mode of the source controller was transparent, or when entering transparent failover and the last failover mode of the source controller was multibus.	00
43000100	Encountered an unexpected structure type on hp_work_q.	01
43030100	Unable to allocate the necessary number of large Sense Data buckets in HPP_init( ).	01
43100100	Encountered a NULL completion routine pointer in a DD.	01
43130100	Could not allocate a large sense bucket.	01
43160100	A sense data bucket of unknown type (neither LARGE or SMALL) was passed to deallocate_SDB( ).	01
43170100	Call to VA$ENABLE_NOTIFICATION( ) failed due to INSUFFICIENT_RESOURCES.	01
43190100	Unable to allocate necessary memory in HPP_int( ).	01
431A0100	Unable to allocate necessary timer memory in HPP_int( ).	01
43210101	HPP detected unknown error indicated by HPT. Last Failure Parameter [0] contains the error value.	01
43220100	Unable to obtain Free CSR in HPP( ).	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 38 of 43)

Last Failure Code	Description	Repair Action Code
43230101	During processing to maintain consistency of the data for Persistent Reserve SCSI commands, an internal inconsistency was detected. Last Failure Parameter [0] contains a code defining the precise nature of the inconsistency.	01
44640100	Not enough abort requests in the system.	01
44650100	Exceeded the number of SEST abort retries.	01
44660100	Unable to allocate enough *abort requests* for Fibre Channel Host Port Transport software layer.	01
44670100	Changes to *command HTBs*.	
44680100	Changes to *FC HTBs*.	
44690100	Changes to *work requests*.	
446A0100	Changes to *HTBs*.	
446B0100	Changes to *TIS structures*.	
446C0100	Changes to *MFSs*.	
446D0100	Changes to *TACHYON headers*.	
446E0100	Changes to *EDB structures*.	
446F0100	Changes to *LSFS structures*.	
44700100	Unable to allocate enough TPS structures for Fibre Channel Host Port Transport software layer.	01
44720101	An illegal status was returned to the FLOGI command error handler. Last Failure Parameter [0] contains error value.	01
44730101	An illegal completion message was returned by the TACHYON to the i960 processor. Last Failure Parameter [0] contains the completion message type.	01
44740101	The Host Port Transport process handler received an illegal timer. Last Failure Parameter [0] contains the timer pointer type.	01
44750100	The Host Port Transport work handler received an illegal work request.	01
44760100	The Host Port Transport ran out of work requests.	01
44770102	An illegal script return value was received by the Host Port Transport init script handler. ■ Last Failure Parameter [0] contains the init function. ■ Last Failure Parameter [1] contains return value. The Host Port Transport ran out of work requests.	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 39 of 43)

Last Failure Code	Description	Repair Action Code
44780102	An illegal script return value was received by the Host Port Transport send script handler. ■ Last Failure Parameter [0] contains the send function. ■ Last Failure Parameter [1] contains return value. The Host Port Transport ran out of work requests.	01
44790102	An illegal script return value was received by the Host Port Transport response script handler. ■ Last Failure Parameter [0] contains the rsp function. ■ Last Failure Parameter [1] contains return value. The Host Port Transport ran out of work requests.	01
447A0102	An illegal script return value was received by the Host Port Transport error script handler. ■ Last Failure Parameter [0] contains the error function. ■ Last Failure Parameter [1] contains return value. The Host Port Transport ran out of work requests.	01
447B0100	The Host Port Transport response script handler received a response before a command was sent.	01
447C0101	Unhandled command HTB status. Last Failure Parameter [0] contains the status value. The Host Port Transport ran out of work requests.	01
447D0100	The Host Port Transport ran out of command HTBs.	01
44800101 44810101	An illegal status was returned to the *name service* command error handler. ■ Last Failure Parameter [0] contains error value. ■ Changes to *PLOGI*.	01
44820101	An illegal abort type was given to the Host Port Transport abort handler. Last Failure Parameter [0] contains abort type.	01
44830101	An illegal failover request was given to the Host Port Transport request handler. Last Failure Parameter [0] contains failover request.	01
44840101	An illegal failover response was given to the Host Port Transport failover response handler. Last Failure Parameter [0] contains failover response.	01
44850100	The Host Port Transport failover control had a bad send count.	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 40 of 43)

Last Failure Code	Description	Repair Action Code
44860100	Unable to allocate enough ESD structures for Fibre Channel Host Port Transport software layer.	01
44870101	An illegal abort type was given to the Host Port Transport abort handler. Last Failure Parameter [0] contains abort type.	01
44892091	Host Port Hardware diagnostic field at system initialization. Last Failure Parameter [0] contains failed port number.	20
448B0100	Host Port Transport software layer unable to allocate work item for updating NV memory during LOGI.	01
448C0100	Host Port Transport software layer unable to allocate work item for LOGI completion routine.	01
448E0100	Host Port Transport software layer unable to allocate memory for quick FC responses.	01
448F0100	Host Port Transport software layer unable to allocate memory for quick responses.	01
44900100	Host Port Transport software layer unable to allocate memory for HCBs.	01
44910100	Host Port Transport software layer unable to allocate memory for HTB TACHYON header.	01
44920101	An invalid work item was detected on abort pending work queue. Last Failure Parameter [0] contains invalid work type.	01
44930100	Unable to allocate enough Peer to Peer Remote Copy TACHYON headers for Fibre Channel Host Port Transport software layer.	01
44940100	Host Port Transport software layer detected an error during buffer-to-buffer credit check.	01
44950100	Host Port Transport software layer unable to acquire an FC quick response resource.	01
44960101	An invalid work item was detected on work pending queue. Last Failure Parameter [0] contains invalid work type.	01
44970100	Host Port Transport software layer unable to access TACHYON register.	01
449A0101	An invalid work item was detected on abort pending work queue. Last Failure Parameter [0] contains work type.	01
64000100	Insufficient buffer memory to allocate data structures needed to propagate SCSI Mode Select changes to other controller.	01
64010100	During an initialization of LUN specific mode pages, an unexpected device type was encountered.	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 41 of 43)

Last Failure Code	Description	Repair Action Code
64030104	A DD is already in use by an RCV DIAG command—cannot get two RCV_DIAGs without sending the data for the first. ■ Last Failure Parameter [0] contains DD_PTR. ■ Last Failure Parameter [1] contains blocking HTB_PTR. ■ Last Failure Parameter [2] contains HTB_PTR flags. ■ Last Failure Parameter [3] contains this HTB_PTR.	01
64040100	An attempt to allocate a free VAR failed.	01
80010100	An HTB was not available to issue an I/O when it should have been.	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$D_ABORT( ) but the HTBs have not been returned.	01
80090100	DILX received an end message which corresponds to an op code not supported by DILX.	01
800A0100	DILX was not able to restart HIS timer.	01
800B0100	DILX tried to issue an I/O for an opcode not supported.	01
800C0100	DILX tried to issue a oneshot I/O for an opcode not supported.	01
800D0100	A DILX device control block contains an unsupported UNIT_STATE.	01
800F0100	A DILX command completed with a sense key that DILX does not support.	01
80100100	DILX could not compare buffers because no memory was available from EXEC$ALLOCATE_MEM_ZEROED.	01
80110100	While DILX was deallocating its deferred error buffers, at least one could not be found.	01
80120100	DILX expected an EIP to be on the receive EIP queue but no EIPs were there.	01
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
83020100	An unsupported message type or terminal request was received by the CONFIG virtual terminal code from the CLI.	01

Table 6–3 Last Failure Codes and Repair Action Codes (Sheet 42 of 43)

Last Failure Code	Description	Repair Action Code
83030100	Not all ALTER_DEVICE requests from the CONFIG utility completed within the timeout interval.	01
83050100	An unsupported message type or terminal request was received by the CFMENU utility code from the CLI.	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 that 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 43 of 43)

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 HSG80 array controller troubleshooting resources guide. This glossary is not a comprehensive glossary of computer terms.

8B/10B

A type of byte encoding and decoding to reduce errors in data transmission patented by the IBM Corporation. This process of encoding and decoding data for transmission has been adopted by ANSI.

ACS

Array Controller Software. The software component of the HS-series array controller storage systems. ACS executes on the controller and processes input/output requests from the host, performing the device-level operations required to satisfy the requests.

adapter

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

AL_PA

Arbitrated loop physical address. A one-byte value used to identify a port in an Arbitrated Loop topology. The AL_PA value corresponds to bits 7:0 of the 24-bit Native Address Indentifier.

alias address

An AL_PA value recognized by an arbitrated loop port in addition to the assigned AL_PA.

ANSI

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

arbitrate

A process of selecting one L_Port from a collection of several ports that request use of the arbitrated loop concurrently.

arbitrated loop

A loop type of topology where two or more ports can be interconnected, but only two ports at a time can communicate.

arbitrated loop physical address

See AL_PA

array controller

See controller

array controller software

See ACS

association set

A group of remote copy sets that share selectable attributes for logging and failover. Members of an association set transition to the same state simultaneously. For example, if one association set member assumes the failsafe locked condition, then other members of the association set also assume the failsafe locked condition.

An association set can also be used to share a log between a group of remote copy set members that require efficient use of the log space.

See also remote copy set

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. Autospare aids the controller in automatically replacing failed disk drives. You can 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

battery hysteresis

The ability of the software to allow write-back caching during the time a battery is charging, but only when a previous down time has not drained more than 50 percent of rated battery capacity.

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

A number of consecutive bytes of data stored on a storage device. In most storage systems, a block is the same size as a physical disk sector. *Also called* 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. The objective of caching data in a system is to improve performance by placing the most frequently used data in the highest performance memory.

cache module

A fast storage buffer.

CCITT

Consultive Committee International Telephone and Telegraph. An international association that sets worldwide communication standards, 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 rack enclosures and fans.

channel

An interface that allows high speed transfer of large amounts of data. Another term for a SCSI bus. *See also* SCSI.

chunk

In any form of RAID that stripes data, data is stored in pieces called chunks. One chunk is stored on each member device in the unit. Taken together, the chunks make up a stripe. The chunk size can be used in some controllers to tune the stripeset for a specific application.

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

Computer Interconnect bus. A serial 70 MHz, dual path, party-line, bus. It is the host bus for the HSJ-series controller-based storage systems. The CI bus is used by OpenVMS hosts to connect the nodes in a clustered subsystem.

CLCP

Code-Load Code-Patch utility. This utility can be used to download patches to the ACS software.

CLI

Command Line Interpreter. A command line entry utility used to interface with the HS-series controllers. CLI enables the configuration and monitoring of a storage subsystem through textual commands.

coax or coaxial cable

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

command line interpreter

See CLI

computer interconnect bus

See CI bus

configuration file

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

container

(1) Any entity that is capable of storing data, whether it is a physical device or a group of physical devices. (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 that the controller uses to create units.

See also storage unit.

controller

A hardware device that, with proprietary software, facilitates communications between a host and one or more storage devices organized in a storage array. The HS-series of the StorageWorks family of controllers are all 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 (rack)

A generic reference to large subsystem racks, such as those in which StorageWorks products 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

In its physical form, a magnetic disk that can be attached to a SCSI bus. The term is also used to indicate a physical device that has been made part of a controller configuration; that is, a physical device that is known to the controller. Units (virtual disks) can be created from devices, once the devices have been made known to the controller.

The targets, initiators, hubs, converters, adapters, and similar items are interconnected to form a SCSI bus. Connectors, expanders, and hubs do not use a SCSI bus ID. *See also* 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 units 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.

DOC

DWZZA-on-a-chip. An SYM53C120 SCSI bus extender chip used to connect a SCSI bus in one enclosure to the corresponding SCSI bus in another enclosure.

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.

DWZZA

A StorageWorks SCSI bus signal converter used to connect 8-bit single-ended devices to hosts with 16-bit differential SCSI adapters. This converter extends the range of a single-ended SCSI cable to the limit of a differential SCSI cable.

See also DOC and SCSI bus signal converter.

DWZZB

A StorageWorks SCSI bus signal converter used to connect a variety of 16-bit single-ended devices to hosts with 16-bit differential SCSI adapters.

See also DOC and SCSI bus signal converter.

DWZZC

The 16-bit, SCSI table-top SCSI bus signal converter used to extend a differential SCSI bus, or connect a differential SCSI bus to a single-ended SCSI bus.

See also DOC and SCSI bus signal converter.

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 that 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 DOC chips, alarms, and fan speeds.

environmental monitoring unit

See EMU

ESD

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

extended subsystem

A subsystem in which one or two enclosures are connected to the primary enclosure.

external cache battery

See ECB

F_Port

A port in a fabric where an N_Port or NL_Port may attach.

fabric

A group of interconnections between ports that includes a fabric element.

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 disk drives that have been removed from RAIDsets due to a failure or a manual removal. Disk drives in the failedset should be considered defective and should be tested and repaired before being placed back into the spareset. *See also* spareset.

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. *See also* failback.

fault management utility

See FMU

FC–AL

The Fibre Channel Arbitrated Loop standard.

FC–ATM

ATM AAL5 over Fibre Channel.

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.

FC–FG

Fibre Channel Fabric Generic Requirements.

FC–FP

Fibre Channel Framing Protocol (HIPPI on FC).

FC–GS-1

Fibre Channel Generic Services-1.

FC–GS-2

Fibre Channel Generic Services-2.

FC–IG

Fibre Channel Implementation Guide.

FC–LE

Fibre Channel Link Encapsulation (ISO 8802.2).

FCP

The mapping of SCSI-3 operations to Fibre Channel.

FC–PH specification

Short for The Fibre Channel Physical and Signaling Interface Standard.

FC–SB

Fibre Channel Single Byte Command Code Set.

FC–SW

Fibre Channel Switched Topology and Switch Controls.

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.

FDDI

Fiber distributed data interface. An ANSI standard for 100 megabaud transmission over fiber optic cable.

fiber

A fiber or optical strand. Spelled fibre in Fibre Channel.

fiber optic cable

A transmission medium designed to transmit digital signals in the form of pulses of light. Fiber optic cables are noted for properties of electrical isolation and resistance to electrostatic contamination.

FL_Port

A port in a fabric where an N_Port or NL_Port may be connected.

flush

The act of writing dirty data from cache to a storage media. *See also* dirty data.

FMU

Fault Management Utility. A utility that is run to provide fault or error reporting information.

forced errors

A data bit indicating that a corresponding logical data block contains unrecoverable data.

frame

An invisible unit used to transfer information in Fibre Channel.

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.

GBIC

Gigabyte interface converter.

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 disk drive storage capacity, meaning a billion (10^9) bytes. The decimal value 1024 is usually used for one thousand.

GLM

Gigabit link module.

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.

hard address

The AL_PA that an NL_Port attempts to acquire during loop initialization.

HBVS

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

HIPPI–FC

Fibre Channel over HIPPI.

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.

host compatibility mode

A setting used by the controller to provide optimal controller performance with specific operating systems. This improves the controller performance and compatibility with the specified operating system.

hot disks

A disk containing multiple hot spots. Hot disks occur when the workload is poorly distributed across storage devices, preventing optimum subsystem performance. *See also* hot spots.

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-pluggable

A replacement method that allows normal I/O activity on a device bus to remain active during device removal and insertion. The device being removed or inserted is the only device that cannot perform operations during this process. *See also* pluggable.

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 SCSI bus, 16-bit single-ended SCSI bus, 16-bit differential SCSI bus, or Fibre Channel 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.

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 not configured into any other container type.

kernel

The most privileged processor access mode.

L_port

A node or fabric port capable of performing arbitrated loop functions and protocols. NL_Ports and FL_Ports are loop-capable ports.

LBN

Logical Block Number. A volume-relative address of a block on a mass storage device. The blocks that form the volume are labeled sequentially starting with LBN 0.

LED

Light-emitting diode.

link

A physical connection between two Fibre Channel ports.

local connection

A connection to the subsystem, by way of the controller serial maintenance port, to a maintenance terminal or the host terminal. A local connection enables you to connect to one subsystem controller to perform maintenance tasks. *See also* maintenance terminal and local terminal.

local terminal

A terminal plugged into the EIA-423 maintenance port located on the front bezel of the controller. *See also* maintenance terminal and local connection.

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 ID number. Logical units use their target's bus connection to communicate on the SCSI bus. *See also* unit.

logical unit number

See LUN

logon

Also called login. A procedure whereby a participant, either a person or network connection, is identified as being an authorized network participant.

loop

See arbitrated loop.

loop tenancy

The period of time between the following events: when a port wins loop arbitration and when the port returns to a monitoring state.

loop_ID

A seven-bit value numbered contiguously from zero to 126-decimal, representing the 127 legal AL_PA values on a loop. Not all of the 256 hex values are allowed as AL_PA values per FC-AL.

LRU

Least recently used. A cache term used to describe the block replacement policy for read cache.

LUN

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 a task's I/O operations. Each task in the system must establish its own correspondence between logical unit numbers and physical devices. *See also* logical unit.

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's status. The maintenance terminal is not required for normal operations. *See also* local terminal and local connection.

mass storage control protocol

See MSCP

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.

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.

MSCP

Mass storage control protocol. The protocol by which blocks of information are transferred between the host and the controller over the CI bus.

multibus failover

Allows the host to control the failover process by moving the unit(s) from one controller to another.

N_Port

A port attached to a node for use with point-to-point topology or fabric topology.

network

In data communication, a configuration in which two or more terminals or devices are connected to enable information transfer.

NL_Port

A port attached to a node for use in all three topologies.

node

In data communications, the point at which one or more functional units connect transmission lines. In Fibre Channel, a device that has at least one N_Port or NL_Port.

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.

Non-L_Port

A Node of Fabric port that is not capable of performing the Arbitrated Loop functions and protocols. N_Ports and F_Ports are loop-capable ports.

non-participating mode

A mode within an L_Port that inhibits the port from participating in loop activities. L_Ports in this mode continue to retransmit received transmission words but are not permitted to arbitrate or originate frames. An L_Port in non-participating mode may or may not have an AL_PA. *See also* participating mode.

nonredundant controller configuration

(1) A single controller configuration. (2) A controller configuration that does not include a second controller.

nonvolatile memory

See NVM

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

Nonvolatile memory. A type of memory where the contents survive power loss. *Also called* NVMEM. The NVMEM in the controller stores the configuration parameters for the storage subsystem.

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).

operator control panel

See OCP

"other controller"

The controller in a dual-redundant pair that is connected to the controller serving your current CLI session. *See also* "this controller."

outbound fiber

One fiber in a link that carries information away from a port.

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

participating mode

A mode within an L_Port that allows the port to participate in loop activities. A port must have a valid AL_PA to be in participating mode.

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

A replacement method that allows the complete system to remain online during device removal or insertion. The system bus must be halted, or quiesced, for a brief period of time during the replacement procedure. *See also* hot-pluggable.

point-to-point connection

A network configuration in which a connection is established between two, and only two, terminal installations. The connection may include switching facilities.

port

In general terms, the port is:

- A logical channel in a communications system.
- 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:

- 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.
- The hardware and software that connects a controller to a SCSI device.

port_name

A 64-bit unique identifier assigned to each Fibre Channel port. The Port_Name is communicated during the logon and port discovery process.

preferred address

The AL_PA that an NL_Port attempts to acquire first during initialization.

primary enclosure

The primary enclosure is the subsystem enclosure that contains the controllers, cache modules, external cache batteries, and the PVA module.

private NL_Port

An NL_Port that does not attempt login with the fabric and only communicates with NL_Ports on the same loop.

program card

The PCMCIA card containing the controller operating software. *See also* PCMCIA card.

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.

public NL_Port

An NL_Port that attempts login with the fabric and can observe the rules of either public or private loop behavior. A public NL_Port may communicate with both private and public NL_Ports.

PVA module

Power verification and addressing module.

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’s 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 specially developed RAID storageset that stripes data and parity across three or more members in a disk array. 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 3/5 storagesets are sometimes referred to as RAIDsets.

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 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.

read-ahead caching

A caching technique for improving performance of synchronous sequential reads by prefetching data from disk.

reconstruction

The process of regenerating the contents of a failed member's data. The reconstruct 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. (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.

remote copy

A feature intended for disaster tolerance and replication of data from one storage subsystem or physical site to another subsystem or site. Remote copy also provides methods of performing a backup at either the local or remote site. With remote copy, user applications continue to run while data movement goes on in the background. Data warehousing, continuous computing, and enterprise applications all require remote copy capabilities.

remote copy set

A bound set of two units, one located locally and one located remotely, for long distance mirroring. The units can be a single disk, or a storageset, mirrorset, or RAIDset. A unit on the local controller is designated as the "initiator" and a corresponding unit on the remote controller is designated as the "target." *See also* association set.

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 arrive at a servicing entity.

RFI

Radio frequency interference. The disturbance of a signal by an unwanted radio signal or frequency.

SCSI

Small Computer System Interface. (1) An American National Standards Institute (ANSI) interface standard defining the physical and electrical parameters of a parallel I/O bus used to connect initiators to devices. (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

(1) A device used to interface between the subsystem and a peripheral device unable to be mounted directly into the SBB shelf of the subsystem. (2) A device used to connect a differential SCSI bus to a single-ended SCSI bus. (3) A device used to extend the length of a differential or single-ended SCSI bus.

See also DOC, DWZZA, DWZZB, DWZZC, and I/O module. Also called adapter, *see* adapter.

SCSI device

(1) A host computer adapter, a peripheral controller, or an intelligent peripheral that can be attached to the SCSI bus. (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. (2) Hardware: The name of the logical socket at the back of the system unit to which a SCSI device is connected.

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.

Selective Storage Presentation

Selective Storage presentation is a feature of the HSG80 controller that enables the user to control the allocation of storage space and shared access to storage across multiple hosts. This is also known as "Restricting Host Access."

serial transmission

A method of transmission in which each bit of information is sent sequentially on a single channel rather than simultaneously as in parallel transmission.

service rate

The rate at which an entity is able to service requests. For example, the rate at which an Arbitrated Loop is able to service arbitrated requests.

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 set of connection panels, contained within a cabinet containing cable connections and transformers through which the nodes of a cluster connect to one another through the CI bus. *See also* nodes and 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 your subsystem and accessed by the host. A storage unit can be any entity that is capable of storing data, whether it is a physical device or a group of physical devices. *See also* container.

storageset

(1) A group of devices configured with RAID techniques to operate as a single container. (2) Any collection of containers, such as stripesets, mirrorsets, striped mirrorsets, and RAIDsets.

Storageset Expansion

The dynamic expansion of the storage capacity (size) of a unit. A storage container is created in the form of a concatenation set which is added to the existing storage set defined as a unit.

StorageWorks

A family of 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 devices and array controllers to form storage subsystems.

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. (2) Designates the target identification (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.

"this controller"

The controller that is serving your 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.

topology

An interconnection scheme that allows multiple Fibre Channel ports to communicate with each other. For example, point-to-point, Arbitrated Loop, and switched fabric are all Fibre Channel topologies.

transfer data rate

The speed at which data may be exchanged with the central processor, expressed in thousands of bytes per second.

transparent failover

Keeps the storage array available to the host(s) by allowing the surviving controller of a dual redundant pair to take over total control of the subsystem and is transparent (invisible) to the host(s).

ULP

Upper Layer Protocol.

ULP process

A function executing within a Fibre Channel node which conforms to the ULP requirements when interacting with other ULP processes.

Ultra SCSI bus

A wide, Fast-20 SCSI bus.

uninterruptible power supply

See UPS

unit

A container made accessible to a host. A unit may be created from a single disk 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 and target ID number.

unwritten cached data

Sometimes called unflushed data. *See also* 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 that is 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.

Worldwide name

A unique 64-bit number assigned to a subsystem by the Institute of Electrical and Electronics Engineers (IEEE) and set by manufacturing prior to shipping. *Also called* node ID within the CLI.

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

L

M

N

P

R

U

V

W