IBM TotalStorage FAStT

Hardware Maintenance Manual and Problem Determination Guide

Read Before Using

The IBM License Agreement for Machine Code is included in this book. Carefully read the agreement. By using this product you agree to abide by the terms of this agreement and applicable copyright laws.

GC26-7528-00

IBM TotalStorage FAStT

Hardware Maintenance Manual and Problem Determination Guide

GC26-7528-00

Note:

Before using this information and the product it supports, be sure to read the general information under “Notices” on page 457.

First Edition (March 2003)

Contents

Figures

Tables

Safety

Before installing this product, read the Safety information.

قبل تركيب هذا المنتج، يجب قراءة الملاحظات الآمنية

Antes de instalar este produto, leia as Informações de Segurança.

在安装本产品之前，请仔细阅读 Safety Information
（安全信息）。

安裝本產品之前，請先閱讀「安全資訊」。

Prije instalacije ovog produkta obavezno pročitajte Sigurnosne Upute.

Před instalací tohoto produktu si přečtěte příručku bezpečnostních instrukcí.

Læs sikkerhedsforskrifterne, før du installerer dette produkt.

Lees voordat u dit product installeert eerst de veiligheidsvoorschriften.

Ennen kuin asennat tämän tuotteen, lue turvaohjeet kohdasta Safety Information.

Avant d'installer ce produit, lisez les consignes de sécurité.

Vor der Installation dieses Produkts die Sicherheitshinweise lesen.

Πριν εγκαταστήσετε το προϊόν αυτό, διαβάστε τις πληροφορίες ασφάλειας
(safety information).

לפני שתתקינו מוצר זה, קראו את הוראות הבטיחות.

A termék telepítése előtt olvassa el a Biztonsági előírásokat!

Prima di installare questo prodotto, leggere le Informazioni sulla Sicurezza.

製品の設置の前に、安全情報をお読みください。

본 제품을 설치하기 전에 안전 정보를 읽으십시오.

Пред да се инсталира овој продукт, прочитајте информацијата за безбедност.

Les sikkerhetsinformasjonen (Safety Information) før du installerer dette produktet.

Przed zainstalowaniem tego produktu, należy zapoznać się
z książką "Informacje dotyczące bezpieczeństwa" (Safety Information).

Antes de instalar este produto, leia as Informações sobre Segurança.

Перед установкой продукта прочтите инструкции по
технике безопасности.

Pred inštaláciou tohto zariadenia si pečítaje Bezpečnostné predpisy.

Pred namestitvijo tega proizvoda preberite Varnostne informacije.

Antes de instalar este producto, lea la información de seguridad.

Läs säkerhetsinformationen innan du installerar den här produkten.

The following Danger notices and Caution notices are printed in English throughout this document. For translations of these notices, see *IBM Safety Information*.

Statement 1:

DANGER

Electrical current from power, telephone, and communication cables is hazardous.

To avoid a shock hazard:

- **Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.**
- **Connect all power cords to a properly wired and grounded electrical outlet.**
- **Connect to properly wired outlets any equipment that will be attached to this product.**
- **When possible, use one hand only to connect or disconnect signal cables.**
- **Never turn on any equipment when there is evidence of fire, water, or structural damage.**
- **Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless instructed otherwise in the installation and configuration procedures.**
- **Connect and disconnect cables as described in the following table when installing, moving, or opening covers on this product or attached devices.**

To Connect:	To Disconnect:
1. Turn everything OFF.	1. Turn everything OFF.
2. First, attach all cables to devices.	2. First, remove power cords from outlet.
3. Attach signal cables to connectors.	3. Remove signal cables from connectors.
4. Attach power cords to outlet.	4. Remove all cables from devices.
5. Turn device ON.	

Statement 2:

CAUTION:
When replacing the lithium battery, use only IBM Part Number 33F8354 or an equivalent type battery recommended by the manufacturer. If your system has a module containing a lithium battery, replace it only with the same module type made by the same manufacturer. The battery contains lithium and can explode if not properly used, handled, or disposed of.

Do not:

- **Throw or immerse into water**
- **Heat to more than 100°C (212°F)**
- **Repair or disassemble**

Dispose of the battery as required by local ordinances or regulations.

Statement 3:

CAUTION:
When laser products (such as CD-ROMs, DVD drives, fiber optic devices, or transmitters) are installed, note the following:

- **Do not remove the covers. Removing the covers of the laser product could result in exposure to hazardous laser radiation. There are no serviceable parts inside the device.**
- **Use of controls or adjustments or performance of procedures other than those specified herein might result in hazardous radiation exposure.**

DANGER

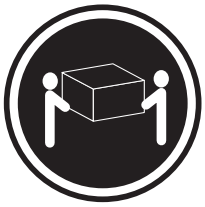
Some laser products contain an embedded Class 3A or Class 3B laser diode. Note the following.

Laser radiation when open. Do not stare into the beam, do not view directly with optical instruments, and avoid direct exposure to the beam.

Class 1 Laser statement

Class 1 Laser Product
Laser Klasse 1
Laser Klass 1
Luokan 1 Laserlaite
Appareil À Laser de Classe 1

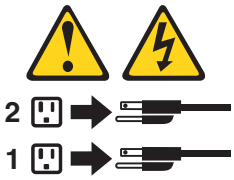
Statement 4:

		
≥ 18 kg (39.7 lb)	≥ 32 kg (70.5 lb)	≥ 55 kg (121.2 lb)

CAUTION:
Use safe practices when lifting.

Statement 5:

CAUTION:
The power control button on the device and the power switch on the power supply do not turn off the electrical current supplied to the device. The device also might have more than one power cord. To remove all electrical current from the device, ensure that all power cords are disconnected from the power source.



Statement 8:

CAUTION:
Never remove the cover on a power supply or any part that has the following label attached.

Hazardous voltage, current, and energy levels are present inside any component that has this label attached. There are no serviceable parts inside these components. If you suspect a problem with one of these parts, contact a service technician.

Safety information

Before you service an IBM computer, you must be familiar with the following safety information.

General safety

Follow these rules to ensure general safety:

- Observe good housekeeping in the area of the machines during and after maintenance.
- When lifting any heavy object:
  1. Ensure that you can stand safely without slipping.
  2. Distribute the weight of the object equally between your feet.
  3. Use a slow lifting force. Never move suddenly or twist when you attempt to lift.
  4. Lift by standing or by pushing up with your leg muscles; this action removes the strain from the muscles in your back. *Do not attempt to lift any objects that weigh more than 16 kg (35 lb) or objects that you think are too heavy for you.*
- Do not perform any action that causes hazards to the customer, or that makes the equipment unsafe.
- Before you start the machine, ensure that other service representatives and the customer's personnel are not in a hazardous position.
- Place removed covers and other parts in a safe place, away from all personnel, while you are servicing the machine.
- Keep your tool case away from walk areas so that other people will not trip over it.
- Do not wear loose clothing that can be trapped in the moving parts of a machine. Ensure that your sleeves are fastened or rolled up above your elbows. If your hair is long, fasten it.
- Insert the ends of your necktie or scarf inside clothing or fasten it with a nonconductive clip, approximately 8 centimeters (3 in.) from the end.
- Do not wear jewelry, chains, metal-frame eyeglasses, or metal fasteners for your clothing. **Remember:** Metal objects are good electrical conductors.
- Wear safety glasses when you are doing any of the following: hammering, drilling soldering, cutting wire, attaching springs, using solvents, or working in any other conditions that might be hazardous to your eyes.
- After service, reinstall all safety shields, guards, labels, and ground wires. Replace any safety device that is worn or defective.
- Reinstall all covers correctly before returning the machine to the customer.

Grounding requirements

Electrical grounding of the computer is required for operator safety and correct system function. Proper grounding of the electrical outlet can be verified by a certified electrician.

Electrical safety

Important
Use only approved tools and test equipment. Some hand tools have handles that are covered with a soft material that does not insulate you when working with live electrical currents. Many customers have, near their equipment, rubber floor mats that contain small conductive fibers to decrease electrostatic discharges. Do not use this type of mat to protect yourself from electrical shock.

Observe the following rules when working on electrical equipment.

- Find the room emergency power-off (EPO) switch, disconnecting switch, or electrical outlet. If an electrical accident occurs, you can then operate the switch or unplug the power cord quickly.
- Do not work alone under hazardous conditions or near equipment that has hazardous voltages.
- Disconnect all power before:
  - Performing a mechanical inspection
  - Working near power supplies
  - Removing or installing main units
- Before you start to work on the machine, unplug the power cord. If you cannot unplug it, ask the customer to power-off the wall box that supplies power to the machine and to lock the wall box in the off position.
- If you need to work on a machine that has *exposed* electrical circuits, observe the following precautions:
  - Ensure that another person, familiar with the power-off controls, is near you.

    Remember: Another person must be there to switch off the power, if necessary.
  - Use only one hand when working with powered-on electrical equipment; keep the other hand in your pocket or behind your back.

    Remember: There must be a complete circuit to cause electrical shock. By observing the previous rule, you might prevent a current from passing through your body.
  - When using testers, set the controls correctly and use the approved probe leads and accessories for that tester.
  - Stand on suitable rubber mats (obtained locally, if necessary) to insulate you from grounds such as metal floor strips and machine frames.

  Observe the special safety precautions when you work with very high voltages; these instructions are in the safety sections of maintenance information. Use extreme care when measuring high voltages.
- Regularly inspect and maintain your electrical hand tools for safe operational condition.
- Do not use worn or broken tools and testers.
- *Never assume* that power has been disconnected from a circuit. First, *check* that it has been powered-off.
- Always look carefully for possible hazards in your work area. Examples of these hazards are moist floors, nongrounded power extension cables, power surges, and missing safety grounds.

- Do not touch live electrical circuits with the reflective surface of a plastic dental mirror. The surface is conductive; such touching can cause personal injury and machine damage.
- Do not service the following parts (or similar units) *with the power on* when they are removed from their normal operating places in a machine. (This practice ensures correct grounding of the units.)
  - Power supply units
  - Pumps
  - Blowers and fans
  - Motor generators
- If an electrical accident occurs:
  - **Use caution; do not become a victim yourself.**
  - **Switch off power.**
  - **Send another person to get medical aid.**

Handling ESD-sensitive devices

Any computer part that contains transistors or integrated circuits (ICs) should be considered sensitive to electrostatic discharge (ESD). ESD damage can occur when there is a difference in charge between objects. Protect against ESD damage by equalizing the charge so that the machine, the part, the work mat, and the person that is handling the part are all at the same charge.

Notes:

1. Use product-specific ESD procedures when they exceed the requirements noted here.
2. Make sure that the ESD protective devices that you use have been certified (ISO 9000) as fully effective.

Use the following precautions when handling ESD-sensitive parts.

- Keep the parts in protective packages until they are inserted into the product.
- Avoid contact with other people.
- Wear a grounded wrist strap against your skin to eliminate static on your body.
- Prevent the part from touching your clothing. Most clothing is insulative and retains a charge even when you are wearing a wrist strap.
- Select a grounding system, such as those listed below, to provide protection that meets the specific service requirement.

  Note: The use of a grounding system is desirable but not required to protect against ESD damage.

  - Attach the ESD ground clip to any frame ground, ground braid, or green-wire ground.
  - Use an ESD common ground or reference point when working on a double-insulated or battery-operated system. You can use coax or connector-outside shells on these systems.
  - Use the round ground-prong of the ac plug on ac-operated computers.
- Use the black side of a grounded work mat to provide a static-free work surface. The mat is especially useful when handling ESD-sensitive devices.

Safety inspection procedure

Use this safety inspection procedure to identify potentially unsafe conditions on a product. Each machine, as it was designed and built, had required safety items installed to protect users and service personnel from injury. This procedure addresses only those items. However, good judgment should be used to identify any potential safety hazards due to attachment of non-IBM features or options not covered by this inspection procedure.

If any unsafe conditions are present, you must determine how serious the apparent hazard could be and whether you can continue without first correcting the problem.

Consider these conditions and the safety hazards they present:

- Electrical hazards, especially primary power (primary voltage on the frame can cause serious or fatal electrical shock).
- Explosive hazards, such as a damaged cathode ray tube (CRT) face or bulging capacitor
- Mechanical hazards, such as loose or missing hardware

Complete the following checks with the power off, and the power cord disconnected.

1. Check exterior covers for damage (loose, broken, or sharp edges).
2. Power-off the computer. Disconnect the power cord.
3. Check the power cord for the following:
   a. A third-wire ground connector in good condition. Use a meter to measure third-wire ground continuity for 0.1 ohm or less between the external ground pin and frame ground.
   b. The power cord should be the appropriate type as specified in the parts listings.
   c. Insulation must not be frayed or worn.
4. Remove the cover.
5. Check for any obvious non-IBM alterations. Use good judgment as to the safety of any non-IBM alterations.
6. Check the inside the unit for any obvious unsafe conditions, such as metal filings, contamination, water or other liquids, or signs of fire or smoke damage.
7. Check for worn, frayed, or pinched cables.
8. Check that the power-supply cover fasteners (screws or rivets) have not been removed or tampered with.

About this document

This document provides information about hardware maintenance and problem determination for the IBM TotalStorage™ FAStT product line. Use this document to:

- Diagnose and troubleshoot system faults
- Configure and service hardware
- Determine system specifications
- Interpret system data

Who should read this document

This document is intended for system operators and service technicians who have extensive knowledge of fibre channel and network technology.

FAStT installation process overview

The following flow chart gives an overview of the installation process for the FAStT hardware and the FAStT Storage Manager. The arrows in the flow chart indicate the current publications that cover, in detail, each step in the installation process.

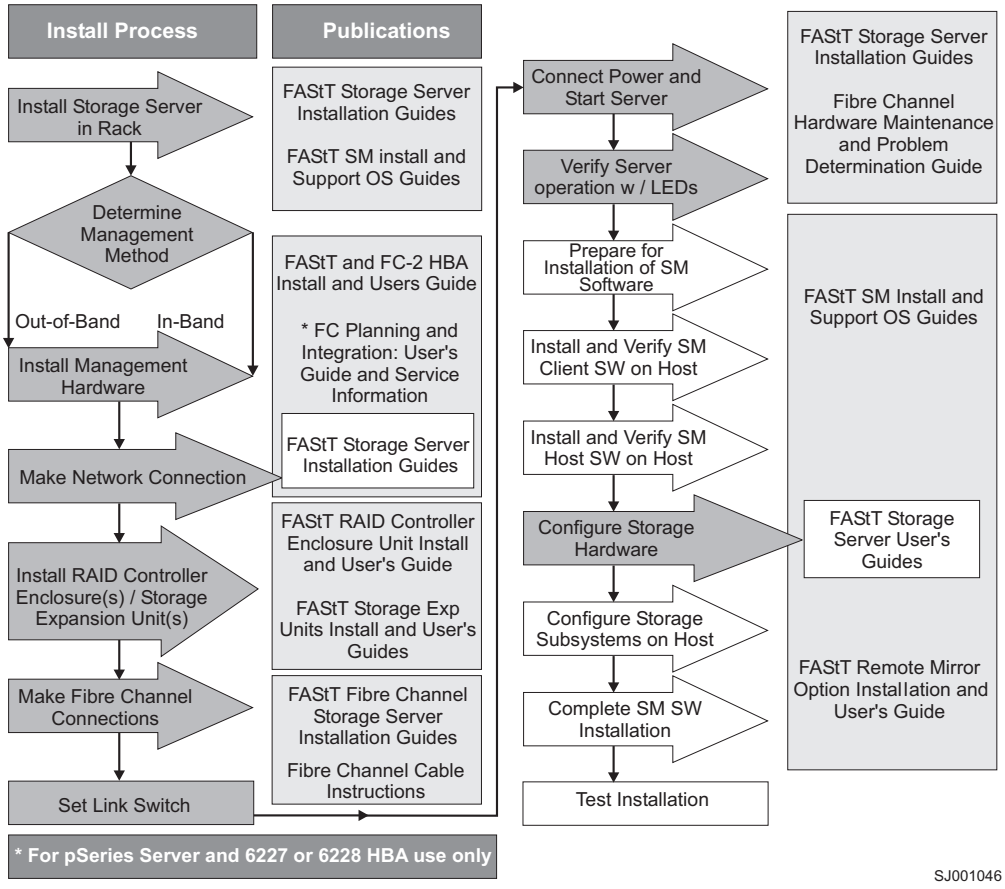


Figure 1. FAStT hardware and FAStT Storage Manager installation process overview by publication

FAStT documentation

The following three tables present an overview of the FAStT900 Fibre Channel Storage Server and FAStT Storage Manager document libraries, as well as related publications. Each table lists documents that are included in the libraries and where to locate information that you need to accomplish common tasks.

FAStT900 Fibre Channel Storage Server library

Table 1 associates each document in the FAStT900 Fibre Channel Storage Server library with its related common user tasks.

Table 1. TotalStorage FAStT900 Fibre Channel Storage Server document titles by user tasks

Title	User Tasks					
	Planning	**Hardware Installation**	**Software Installation**	**Configuration**	**Operation and Administration**	**Diagnosis and Maintenance**
FAStT900 Installation and Support Guide, GC26-7530	X	X		X		
FAStT900 Fibre Channel Cabling Instructions, 24P8135	X	X				
FAStT900 User's Guide, GC26-7534				X	X	X
FAStT Host Adapter Installation and User's Guide, 59P5712		X			X	
FAStT FC2-133 Dual Port Host Bus Adapter Installation and User's Guide, GC26-7532		X			X	
FAStT FC2-133 Host Bus Adapter Installation and User's Guide, 48P9823		X			X	
Fibre Channel Planning and Integration: User's Guide and Service Information, SC23-4329	X	X			X	X
FAStT Management Suite Java User's Guide, 32P0081					X	X

Table 1. TotalStorage FAStT900 Fibre Channel Storage Server document titles by user tasks (continued)

Fibre Channel Hardware Maintenance Manual and Problem Determination Guide, GC26-7528						X

FAStT Storage Manager Version 8.3 library

Table 2 associates each document in the FAStT Storage Manager library with its related common user tasks.

Table 2. TotalStorage FAStT Storage Manager Version 8.3 titles by user tasks

Title	User Tasks					
	Planning	**Hardware Installation**	**Software Installation**	**Configuration**	**Operation and Administration**	**Diagnosis and Maintenance**
Installation and Support Guide for Windows NT and Windows 2000, GC26-7522	X		X	X		
Installation and Support Guide for Linux, GC26-7519	X		X	X		
Installation and Support Guide for Novell NetWare, GC26-7520	X		X	X		
Installation and Support Guide for UNIX and AIX Environments, GC26-7521	X		X	X		
FAStT Remote Mirror Option Installation and User's Guide, 48P9821	X		X	X	X	
IBM FAStT Storage Manager Script Commands (see Product CD)				X		
IBM FAStT Storage Manager Version 7.10 Concepts Guide, 25P1661	X	X	X	X	X	X

FAStT Storage Manager related documents

Table 3 associates each of the following documents related to FAStT Storage Manager operations with its related common user tasks.

Table 3. TotalStorage FAStT Storage Manager related document titles by user tasks

Title	User Tasks					
	Planning	**Hardware Installation**	**Software Installation**	**Configuration**	**Operation and Administration**	**Diagnosis and Maintenance**
IBM FAStT500 RAID Controller Enclosure Unit Installation Guide, 59P6244		X			X	
IBM FAStT500 RAID Controller Enclosure Unit User's Reference, 48P9847		X			X	
IBM Netfinity Fibre Channel Cabling Instructions, 19K0906		X				
IBM FAStT200 and FAStT200 HA Storage Servers Installation and User's Guide, 59P6243		X			X	
IBM FAStT200 Fibre Channel Cabling Instructions, 21P9094		X				
IBM TotalStorage FAStT EXP700 Storage Expansion Unit Installation and User's Guide, 32P0178		X		X		
IBM FAStT EXP500 Installation and User's Guide, 59P5637		X		X		
IBM Fibre Channel SAN Configuration Setup Guide, 25P2509	X		X	X	X	

How this document is organized

The *IBM TotalStorage FAStT Hardware Maintenance Manual and Problem Determination Guide* is composed of two parts.

The Hardware Maintenance portion of this document contains basic information, such as specifications and symptom lists, about many of the components of a fibre channel configuration. This information will be useful in completing the tasks given in the problem determination procedures contained within the second portion of this document.

The Problem Determination portion of this document is useful when attempting to isolate and solve problems that might occur in your fibre channel configurations. It provides problem determination and resolution information for the issues most commonly encountered with IBM fibre channel devices and configurations.

Part 1, “Hardware Maintenance”, on page 1, as stated previously, contains specification and symptom listings for the various FAStT Hardware components.

Chapter 1, “IBM Fibre Channel”, on page 3 provides a brief overview on how to use the hardware maintenance, diagnostic, and test information provided in this document.

Chapter 2, “Type 3523 Fibre Channel Hub and GBIC”, on page 5 provides service and diagnostic information for the Type 3523 Fibre Channel Hub and GBIC.

Chapter 3, “Fibre Channel PCI Adapter (FRU 01K7354)”, on page 13 provides service and diagnostic information for the Fibre Channel Adapter (FRU01K7354).

Chapter 4, “IBM FAStT Host Adapter (FRU 09N7292)”, on page 15 provides service and diagnostic information for the FAStT Host Adapter (FRU09N7292).

Chapter 5, “IBM FAStT FC2-133 (FRU 24P0962) and IBM FAStT FC2-133 Dual Port (FRU 24P8053) Host Bus Adapters”, on page 19 provides service and diagnostic information for both the IBM FAStT FC2-133 (FRU 24P0962) and the IBM FAStT FC2-133 Dual Port (FRU 24P8053) Host Bus Adapters.

Chapter 6, “Type 3526 Fibre Channel RAID controller”, on page 23 provides service and diagnostic information for the Type 3526 Fibre Channel RAID Controller.

Chapter 7, “FAStT200, Type 3542 and FAStT200 HA, Type 3542”, on page 37 provides service and diagnostic information for the Type 3542 FAStT200 and Type 3542 FAStT200 HA.

Chapter 8, “Type 3552 FAStT500 RAID controller”, on page 49 provides service and diagnostic information for the Type 3552 FAStT500 RAID Controller.

Chapter 9, “Type 1742 FAStT700 Fibre Channel Storage Server”, on page 65 provides service and diagnostic information for the Type 1742 FAStT700 Fibre Channel Storage Server.

Chapter 10, “Type 1742 FAStT900 Fibre Channel Storage Server”, on page 77 provides service and diagnostic information for the Type 1742 FAStT900 Fibre Channel Storage Server.

Chapter 11, “IBM TotalStorage FAStT EXP15 and EXP200 Storage Expansion Units”, on page 89 provides service and diagnostic information for both the EXP15 and EXP200 Enclosures.

Chapter 12, “IBM TotalStorage FAStT EXP500 Storage Expansion Unit”, on page 95 provides service and diagnostic information for the EXP500 Enclosure.

Chapter 13, “IBM TotalStorage FAStT EXP 700 Storage Expansion Unit”, on page 103 provides service and diagnostic information for the EXP700 Storage Expansion Unit.

Chapter 14, “IBM Storage Area Network Data Gateway Router (2108-R03)”, on page 111 provides service and diagnostic information for the Storage Area Network Data Gateway Router.

Part 2, “Problem Determination”, on page 127 contains diagnostic and problem determination information for use with the various FAStT Hardware components.

Chapter 15, “Introduction to Fibre Channel problem determination”, on page 129 provides a starting point for the problem determination information found in this section.

Chapter 16, “Problem determination starting points”, on page 131 provides an introduction to problem determination tools and techniques contained in this section.

Chapter 17, “Problem determination maps”, on page 137 provides a series of flowcharts that assist you in isolating and resolving hardware issues.

Chapter 18, “Introduction to FAStT MSJ”, on page 173 introduces the IBM Fibre Array Storage Technology Management Suite Java (FAStT MSJ).

Chapter 19, “Introduction to SANavigator”, on page 217 provides an overview of the functions of SANavigator.

Chapter 20, “PD hints — Common path/single path configurations”, on page 249 provides problem determination hints for common path or single path configurations.

Chapter 21, “PD hints — RAID controller errors in the Windows NT event log”, on page 251 provides problem determination hints for event log errors stemming from the RAID controller.

Chapter 22, “PD hints — Configuration types”, on page 265 provides the various configuration types that can be encountered.

Chapter 23, “PD hints — Passive RAID controller”, on page 271 provides instructions on isolating problems occuring in a passive RAID controller.

Chapter 24, “PD hints — Performing sendEcho tests”, on page 275 contains information on performing loopback tests.

Chapter 25, “PD hints - Tool hints”, on page 279 contains information on generalized tool usage.

Chapter 26, “PD hints — Drive side hints and RLS Diagnostics”, on page 307 contains problem determination information for the drive or device side as well as read link status diagnostics.

Chapter 27, “PD hints — Hubs and switches”, on page 321 provides information on hub and switch problem determination.

Chapter 28, “PD hints — Wrap plug tests”, on page 327 provides information about tests that can be performed on wrap plugs.

Chapter 29, “Heterogeneous configurations”, on page 331 contains information on heterogeneous configurations.

Chapter 30, “Using IBM Fast!UTIL”, on page 335 provides detailed configuration information for advanced users who want to customize the configuration of the IBM Fibre Channel Adapter (FRU 01K7354), the IBM FAStT Host Adapter (FRU 09N7292), and the IBM FAStT FC2-133 Adapter (FRU 24P0962).

Chapter 31, “Storage Manager FAQs”, on page 343 contains frequently asked questions about storage manager.

Chapter 32, “PD hints — MEL data format”, on page 353 discusses MEL data format.

“Notices” on page 457 provides service information.

Notices used in this document

This document contains the following notices designed to highlight key information:

- **Note:** These notices provide important tips, guidance, or advice.
- **Important:** These notices provide information that might help you avoid inconvenient or problem situations.
- **Attention:** These notices indicate possible damage to programs, devices, or data. An attention notice is placed just before the instruction or situation in which damage could occur.
- **Caution:** These statements indicate situations that can be potentially hazardous to you. A caution statement is placed just before the description of a potentially hazardous procedure step or situation.
- **Danger:** These statements indicate situations that can be potentially lethal or extremely hazardous to you. A danger statement is placed just before the description of a potentially lethal or extremely hazardous procedure step or situation.

Getting information, help, and service

If you need help, service, or technical assistance or just want more information about IBM products, you will find a wide variety of sources available from IBM to assist you. This section contains information about where to go for additional information about IBM and IBM products, what to do if you experience a problem with your IBM @server xSeries™ or IntelliStation® system, and whom to call for service, if it is necessary.

Before you call

Before you call, make sure that you have taken these steps to try to solve the problem yourself:

- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the system is turned on.

- Use the troubleshooting information in your system documentation, and use the diagnostic tools that come with your system.
- Check for technical information, hints, tips, and new device drivers at the IBM Support Web site:
  www.ibm.com/pc/support
- Use an IBM discussion forum on the IBM Web site to ask questions.

You can solve many problems without outside assistance by following the troubleshooting procedures that IBM provides in the online help or in the documents that are provided with your system and software. The information that comes with your system also describes the diagnostic tests that you can perform. Most xSeries and IntelliStation systems, operating systems, and programs come with information that contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the information for the operating system or program.

Using the documentation

Information about your xSeries or IntelliStation system and preinstalled software, if any, is available in the documents that come with your system. This includes printed documents, online documents, readme files, and help files. See the troubleshooting information in your system documentation for instructions for using the diagnostic programs. The troubleshooting information or the diagnostic programs might tell you that you need additional or updated device drivers or other software.

Web sites

IBM maintains pages on the World Wide Web where you can get the latest technical information and download device drivers and updates.

- For FAStT information, go to the web site at:
  www.ibm.com/pc/support

  The support page has many sources of information and ways for you to solve problems, including:
  - Diagnosing problems, using the IBM Online Assistant
  - Downloading the latest device drivers and updates for your products
  - Viewing frequently asked questions (FAQ)
  - Viewing hints and tips to help you solve problems
  - Participating in IBM discussion forums
  - Setting up e-mail notification of technical updates about your products
- You can order publications through the IBM Publications Ordering System at:
  www.elink.ibmlink.ibm.com/public/applications/publications/cgibin/pbi.cgi
- For the latest information about IBM xSeries products, services, and support go to the Web site at:
  www.ibm.com/eserver/xseries
- For the latest information about the IBM IntelliStation information go to the Web site at:
  www.ibm.com/pc/intellistation

Software service and support

Through IBM Support Line, for a fee you can get telephone assistance with usage, configuration, and software problems with xSeries servers, IntelliStation

workstations, and appliances. For information about which products are supported by Support Line in your country or region, go to the following Web site: www.ibm.com/services/sl/products

For more information about the IBM Support Line and other IBM services, go to the following Web sites:

- www.ibm.com/services
- www.ibm.com/planetwide

Hardware service and support

You can receive hardware service through IBM Integrated Technology Services or through your IBM reseller, if your reseller is authorized by IBM to provide warranty service. Go to the following Web site for support telephone numbers: www.ibm.com/planetwide

In the U.S. and Canada, hardware service and support is available 24 hours a day, 7 days a week. In the U.K., these services are available Monday through Friday, from 9 a.m. to 6 p.m.

How to send your comments

Your feedback is important to help us provide the highest quality information. If you have any comments about this document, you can submit them in one of the following ways:

- E-mail

  Submit your comments electronically to:

  starpubs@us.ibm.com

  Be sure to include the name and order number of the document and, if applicable, the specific location of the text you are commenting on, such as a page number or table number.
- Mail or fax

  Fill out the Readers' Comments form (RCF) at the back of this document and return it by mail or fax (1-800-426-6209) or give it to an IBM representative. If the RCF has been removed, you can address your comments to:

  International Business Machines Corporation
  RCF Processing Department
  Dept. M86/Bldg. 050-3
  5600 Cottle Road
  San Jose, CA 95193-0001
  U.S.A

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Part 1. Hardware Maintenance

Chapter 1. IBM Fibre Channel

Note: If you are using a PDF version of this document, please be patient in allowing the software to take you from a link to its destination.

Fibre channel technology is outlined in the *Information Systems - Fibre Channel Protocol for SCSI (small computer system interface -FCP)* standard, revision 12, 30 May 1995. Fibre channel is a high-speed data transport technology used for mass storage and networking.

The IBM Host Bus Adapter connects:

- Mainframe computers
- Super computers
- Workstations
- Storage devices
- Servers

Using a Fibre Channel Arbitrated Loop (FC-AL), 126 devices can be supported, compared to 15 devices with Ultra SCSI.

Fibre channel supports data transfer rates of 100 MB per second. A multimode optical interface is used for distances up to 500 meters. With increased connectivity and performance, fibre channel is the technology preferred and used by system designers.

About hardware maintenance

The hardware maintenance portion of this manual contains basic information, such as specifications and symptom lists, about many of the components of a fibre channel configuration. This information will be useful in completing the tasks given in the problem determination procedures contained within the second portion of this guide.

Note: The component information provided in the maintenance portion of this manual has been extracted from the individual hardware maintenance manuals for each component. Therefore, you might find it helpful to refer to the individual hardware maintenance manuals for specific components.

Diagnostics and test information

Start with the ″General checkout″ sections in each chapter of this fibre channel hardware maintenance information to assist you in diagnosing the IBM fibre channel products described within this manual.

For Error Codes and Error Messages, refer to the ″Symptom-to-FRU index″ of the server that the Fibre Channel Hub, Adapter, or RAID Controller is connected to.

Note: For information about managed hubs and switches that can be in your installation, refer to the individual publications for those devices:

- *IBM 3534 SAN Fibre Channel Managed Hub Installation and Service Guide SY27-7616*
- *IBM SAN Fibre Channel Switch 2109 Model S8 Installation and Service Guide*

- *IBM SAN Fibre Channel Switch 2109 Model S16 Installation and Service Guide SG26-7352*

This installation and service information can be accessed on the World Wide Web:

http://www.storage.ibm.com/ibmsan/products.htm

Chapter 2. Type 3523 Fibre Channel Hub and GBIC

Note: The problem determination (PD) maps found in Chapter 17, “Problem determination maps”, on page 137 provide you with additional diagnostic aids.

The type 3523 Fibre Channel Hub and GBIC are compatible with the following IBM products:

- Fibre Channel Adapter (FRU 01K7354) (see Chapter 3 on page 13)
- IBM FAStT Host Adapter (FRU 09N7292) (see Chapter 4 on page 15)
- Type 3526 Fibre Channel RAID controller (see Chapter 6 on page 23)

The IBM Fibre Channel Hub is a 7-port central interconnection for Fibre Channel Arbitrated Loops that follow the ANSI FC-AL standard. Each Fibre Channel Hub port receives serial data from an attached node and retransmits the data out of the next hub port to the next node attached in the loop. Each reception includes data regeneration (both signal timing and amplitude) supporting full-distance optical links.

The Fibre Channel Hub detects any loop node that is missing or is inoperative and automatically routes the data to the next operational port and attached node in the loop. LED indicators provide status information to indicate whether the port is active or bypassed.

Each port requires a Gigabit Interface Converter (GBIC) to connect it to each attached node. The Fibre Channel Hub supports any combination of short-wave or long-wave optical GBICs. The GBICs are *hot-pluggable* into the Fibre Channel Hub, which means you can add host computers, servers, and storage modules to the arbitrated loop dynamically without powering off the Fibre Channel Hub or any connected devices. If you remove a GBIC from a Fibre Channel Hub port, that port is automatically bypassed. The remaining hub ports continue to operate normally with no degradation of system performance. Conversely, if you plug a GBIC into the Fibre Channel Hub, it is automatically inserted and becomes a node on the loop if valid fibre channel data is received from the device.

Data transfer within the Fibre Channel Hub is implemented in serial differential Positive Emitter Coupled Logic (PECL) AC coupled logic. Each Fibre Channel Hub port monitors the serial data input stream as well as the GBIC connected to it.

The following conditions cause the Fibre Channel Hub to bypass a port:

- TX_FAULT: Detects a GBIC transmitter fault.
- RX_LOS: Detects a loss of received signal amplitude from the device.
- MOD_DEF: Detects the absence of a GBIC.

The Fibre Channel Hub circuitry detects off-frequency data, excessive jitter, or inadequate edge transition density on a per-port basis. The Fibre Channel Hub uses the standardized AMP SCA2 20-pin connector to implement hot plugging. Surge currents, caused by hot plugging, are minimized by slow-start circuitry and a pin-sequencing procedure on the GBIC. Electrostatic discharge (ESD) transients are minimized by means of sequenced connector contacts.

The Fibre Channel Hub includes a universal power supply that can operate from 95 to 250 V ac and from 50 to 60 Hz.

General checkout

Installation and operational problems in an arbitrated loop environment are typically caused by one of the following:

- Faulty cabling or cable connector
- Incorrect cable plugging
- Faulty GBIC
- Faulty hubs
- Invalid fibre channel signaling from the host bus adapter (HBA) or disk array
- Device driver or microcode conflicts between the HBAs and other devices.

The following information will help you to isolate and correct the physical layer problems. For protocol-related problems, such as inoperability between devices, see the documentation that came with the individual devices.

Port Status LEDs

The hub provides two status LEDs for each port (see Table 4). Use these LEDs to help you quickly diagnose and recover from problems.

The upper, green LED is lit when an operational GBIC is installed. The lower, amber LED is lit when the port is in the bypass mode. In the bypass mode, a port is disabled, which prevents erratic signals or data from disrupting loop activity. The bypass mode could be triggered by the loss of valid signal or by a GBIC fault. The combination of green and amber LEDs indicates one of the four following states.

Table 4. Type 3523 Fibre Channel Hub port status LEDs

Green LED	Amber LED	Port State
Off	Off	No GBIC Installed
On	Off	Operational GBIC; Valid Signal
Off	On	Faulty GBIC; Port Bypassed
On	On	Operational GBIC; No Valid Signal; Port Bypassed

Verifying GBIC and cable signal presence

Note: Do *not* look directly into any fiber cable or GBIC optical output. Read "Safety" on page xi. To view an optical signal, use a mirror to view the reflected light.

Verifying signal presence

In addition to verifying port LED status, you can verify signal presence by using a mirror to look for a reflected light at the fiber-optic cable ends and the GBIC transmitter. To verify signal presence at the hub end of a link, insert a GBIC into the hub and place a mirror at the bottom of the SC connector. If a signal is present, you will see a low intensity red light in the mirror reflecting from the GBIC transmitter. See Figure 2 on page 7.

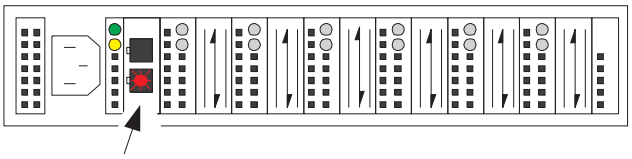


Figure 2. Verifying Signal Presence

Verifying node end

To verify the integrity of the fiber-optic cable at the node end of a link, make sure the cable is attached to the GBIC at the hub and the hub is turned on. Dual SC fiber-optic cable connectors are keyed and will insert into a GBIC in one direction only. Place a mirror at the node end of the link. A low intensity red light is visible in the mirror reflection of one of the SC leads, as shown in Figure 3.

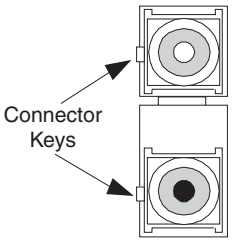


Figure 3. Verifying Node End

If a fiber-optic cable has good transmitter output but a broken or degraded receiver lead, the end node might sense a *loop down* state. Because the transmitter is good, the hub responds to the end node valid fibre channel signal and adds the device to the loop. But, because the end node is not receiving fibre channel signals, it will stream loop-down sequences onto the loop. This prevents all data communications among the devices on the loop and will continue to do so until the condition is corrected.

Verifying hub end

To verify the integrity of the fiber-optic cable at the hub end, make sure the fiber-optic cable is plugged into the host bus adapter at the host or into a disk-array controller and that the device is enabled on the loop. Using a mirror, examine the cable SC leads to verify that a low-intensity red light is visible on the receiver lead.

Note: Some fiber-optic cables are marked with an A on the receiver lead and a B on the transmitter lead and are keyed. Some multimode cables plugged into a GBIC, HBA, or disk array controller are key-oriented with the B lead inserted into the device transmitter. Place a mirror on the opposite end of the cable to see the low-intensity red light on the A receiver lead.

Additional service information

Applications and configurations

The Fibre Channel Hub modular interface provides flexibility and is upgradable to available short-wave and long-wave optical fibre channel product port interfaces. Fibre channel products that are commonly interconnected to the Fibre Channel Hub are fibre channel host bus adapters, FC-AL storage devices, and FC-AL storage

arrays. SCSI initiators (workstations and servers) set up and initiate the transfer of data to or from the storage devices. The storage devices that receive the requests made by the SCSI initiators are the SCSI targets. Initiators and targets represent individual nodes that are linked by the shared FC-AL. See Figure 4.

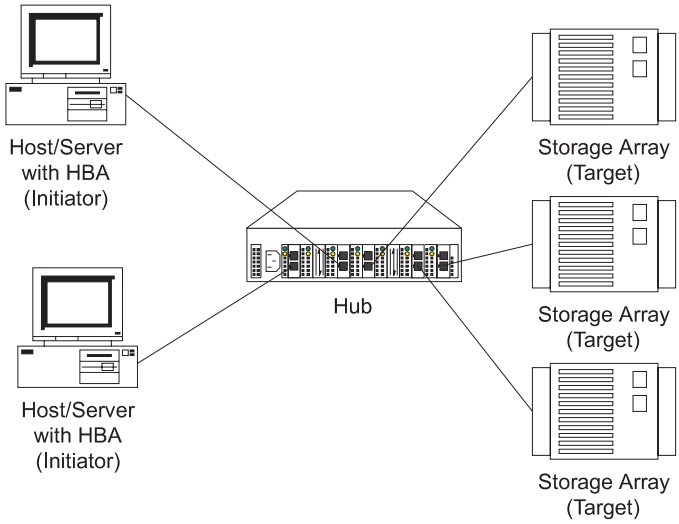


Figure 4. Fibre Channel Hub

Power on systems check — Fibre Channel Hub

Power on the storage modules first, then the controller and the Fibre Channel Hub, then everything else.

Note: Make sure the Fibre Channel Hub is powered on before the host adapter to insure proper loop initialization.

To insure proper operation:

1. Connect the power cord to the Fibre Channel Hub, then to the electrical outlet. See Figure 5.

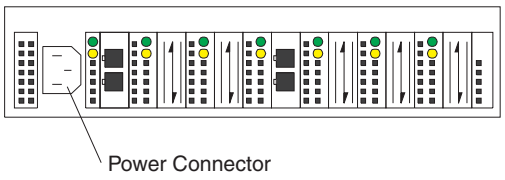


Figure 5. Power Connector

2. Power on the attached FC-AL compatible nodes.
3. Check the Device Active (green) LEDs on the Fibre Channel Hub ports. See Figure 6.

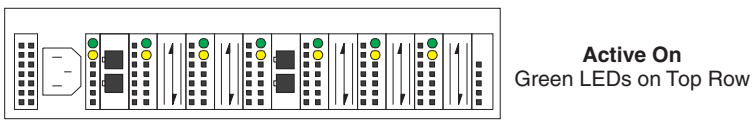


Figure 6. Active On

LED On

This indicates that a GBIC is present and functioning properly.

LED Off

This indicates a fault condition. Examples of a fault condition include: a GBIC transmitter fault, an improperly seated GBIC, an absent GBIC, or another failed device. The port will be in the bypass state, which precludes the port from participating in the FC-AL. This is the normal status of operation for Fibre Channel Hub ports in which GBICs are not installed.

Note: FC-AL compatible nodes must perform loop initialization procedures at power on to function properly on the loop. FC-AL nodes also perform loop initialization or reinitialization depending on their prior state of operation.

4. Check the Port Bypass (amber) LEDs. See Figure 7.

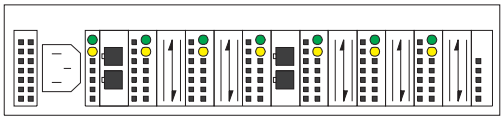


Figure 7. Port Bypass

LED On

If the Active (green) LED of the port is off, the port is nonoperational and the Bypass (amber) LED for the port is on. If a properly functioning port (the Active green LED is on) with a GBIC present also has the Bypass LED on, either the loss of signal or poor signal integrity has caused the port to go into the bypass state. When the port is in this state, it cannot participate in the FC-AL.

The bypass state is also the normal status condition when no GBIC is present in the port, a GBIC is present but not attached to a FC-AL node, or a GBIC is attached to a cable assembly with nothing attached at the opposite end. Replacing such a port (or removing and reinserting the GBIC into the same port twice) is considered to be a loop configuration change which invokes the Loop Initialization Procedure.

LED Off

This indicates that the Fibre Channel Hub port and device are fully operational and actively participating in the FC-AL.

5. The FC-AL should be fully operational. Check that proper loop discovery has taken place and all required devices are participating in the loop. Some host bus adapters might provide this level of functionality or it might be resident in the application software on the host operating system.

Symptom-to-FRU index

The Symptom-to-FRU index (see Table 5) lists symptoms, errors, and the possible causes. The most likely cause is listed first.

The PD maps found in Chapter 17, “Problem determination maps”, on page 137 provide you with additional diagnostic aids.

Note:

1. Always start with the “General checkout” on page 6. For IBM devices not supported by this index, refer to the manual for that device.
2. Do *not* look directly into any fiber cable or GBIC optical output. Read “Notices” on page 457. To view an optical signal, use a mirror to view the reflected light.

Table 5. Symptom-to-FRU index for Type 3523 Fibre Channel Hub and GBIC

Problem	FRU/Action
GBIC installed in one or more ports but no LED is lit.	1. **Power cord** 2. Power source
GBIC installed but only the amber LED is lit.	1. **Reseat GBIC** 2. GBIC
GBIC installed and both green and amber LEDs are lit.	**The hub is not receiving a valid fibre channel signal from the end node.** Do the following: 1. Unplug the fiber cable from the node and, using a mirror, verify that an optical signal is present on the cable. If no red light is visible, replace the cable. 2. Using a mirror, examine the SC connectors on the HBA or disk controller. If no red light is visible, check the HBA or disk controller. 3. If a light is present on both the cable lead and the end node, check the HBA or the disk controller.
GBIC is installed, only the green LED is lit, but no communication occurs between the devices.	**The hub is receiving a valid fibre channel signal from the end device, but no upper-level protocols are active.** 1. Verify that the proper HBA device drivers are loaded for the appropriate operating system and that the host has been configured to recognize the attached disk devices. 2. Unplug the fiber cable from the end node and verify that an optical signal is present on the cable lead. If no signal is present, the lead of the cable might be defective. Replace the cable.

Parts listing (Type 3523 Fibre Channel Hub & GBIC)

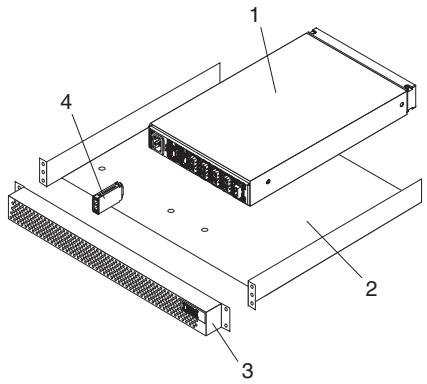


Figure 8. Fibre Channel Hub parts

Index	Fibre Channel Hub (Type 3523)	FRU
1	Port Fibre Hub Assembly	01K6738
2	Hub Tray Assembly	10L7042
3	Hub Tray Bezel	10L7041
4	Short-Wave GBIC	03K9206
	Long-Wave GBIC (option)	03K9208
	Misc. Hardware Kit	01K6739

Chapter 3. Fibre Channel PCI Adapter (FRU 01K7354)

Note: The problem determination (PD) maps found in Chapter 17, “Problem determination maps”, on page 137 provide you with additional diagnostic aids.

The Fibre Channel PCI Adapter (FRU 01K7354) is compatible with the following IBM products:

- Type 3523 Fibre Channel Hub and GBIC (see Chapter 2 on page 5)
- Type 3526 Fibre Channel RAID controller (see Chapter 6 on page 23)
- Type 2109 Fibre Channel Switch
- Type 3534 Managed Hub

Chapter 30, “Using IBM Fast!UTIL”, on page 335 provides detailed configuration information for advanced users who want to customize the configuration of the Fibre Channel PCI Adapter (FRU 01K7354).

General checkout

There are three basic types of problems that can cause the adapter to function incorrectly:

- Hardware problems
- System configuration problems
- Fibre Channel problems

Hardware problems

The following list will help you determine whether a problem was caused by the hardware:

- Verify that all of the adapters are installed securely.
- Verify that all of the cables are connected securely to the correct connectors. Be sure that the SC connectors that attach from the J1 connector on the adapter to the device are connected correctly.
- Verify that the adapter is installed correctly and seated firmly in the expansion slot.
- Verify that all peripheral devices are properly powered on. See “Scan fibre channel devices” on page 341 for information about displaying attached devices.

System configuration problems

To determine whether a problem was caused by the system configuration, check the system board to make sure it is configured properly (refer to the appropriate IBM TotalStorage FAStT Product Installation Guide).

Fibre channel problems

To determine whether a problem was caused by the fibre channel, verify that all of the FC devices were powered on before you powered on the server.

Additional service information

The following information supports the Fibre Channel PCI Adapter.

The IBM Fibre Channel PCI Adapter operating environment and specification information is detailed in Table 6 and Table 7.

Table 6. IBM Fibre Channel PCI Adapter operating environment

Environment	Minimum	Maximum
Operating temperature	0° C (32° F)	55° C (131° F)
Storage temperature	-20° C (-4° F)	70° C (158° F)
Relative humidity (noncondensing)	10%	90%
Storage humidity (noncondensing)	5%	95%

Table 7. IBM Fibre Channel PCI Adapter specifications

Type	Specification
Host bus	Conforms to PCI Local Bus Specification, revision 2.1
PCI signaling environment	3.3 V and 5.0 V buses supported
PCI transfer rate	264 MB per second maximum burst rate for 33 MHz operation (ISP2100 chip)
Fibre channel specifications	Bus type: fiber-optic media (QLA2100F) Bus transfer rate: 100 MB per second maximum
Central processing unit (CPU)	Single chip design that includes a RISC processor, fibre channel protocol manager, PCI DMA controller, and 1-gigabit transceivers
Host data transfer	64-bit, bus master DMA data transfers to 264 MB per second
RAM	128KB of SRAM
BIOS ROM	128KB of flash ROM in two 64KB, software selectable banks. The flash is field-programmable.
NVRAM	256 bytes, field-programmable
Onboard DMA	Three independent DMA channels: two data and one command. Integrated 4KB frame buffer FIFO for each data channel
Connectors (external)	SC-style connector that supports non-OFC, multimode fiber-optic cabling using 1x9 fiber-optic transceiver module. Total cable length cannot exceed 500 meters.
Form factor	17.78 cm x 10.67 cm (7.0 in. x 4.2 in.)
Operating power	Less than 15 watts

Chapter 4. IBM FAStT Host Adapter (FRU 09N7292)

Note: The problem determination (PD) maps found in Chapter 17, “Problem determination maps”, on page 137 provide you with additional diagnostic aids.

The IBM FAStT Host Adapter is a high-performance, direct memory access (DMA), bus-master host adapter designed for high-end systems. The function and performance are derived from the ISP2200A chip, making this FAStT Host Adapter a leading-edge host adapter.

The ISP2200A chip combines a powerful RISC processor, a fibre protocol module (FPM) with gigabit transceivers, and a 64-bit peripheral component interconnect (PCI) local bus interface in a single-chip solution. The FAStT Host Adapter supports all Fibre Channel (FC) peripheral devices that support private-loop direct attach (PLDA) and fabric-loop attach (FLA).

The IBM FAStT Host Adapter (FRU 09N7292) is compatible with the following IBM products:

- Type 3526 Fibre Channel RAID controller (see Chapter 6 on page 23)
- Type 3552 FAStT500 RAID controller (see Chapter 8 on page 49)
- FAStT200 type 3542 and FAStT200 HA type 3542 (see Chapter 7 on page 37)
- Type 2109 Fibre Channel Switch
- Type 3534 Managed Hub

Chapter 30, “Using IBM Fast!UTIL”, on page 335 provides detailed configuration information for advanced users who want to customize the configuration of the Fibre Channel Adapter (FRU 09N7292).

General checkout

There are two basic types of problems that can cause the adapter to malfunction:

- Hardware problems
- System configuration problems
- Fibre channel problems

Hardware problems

The following list will help you determine whether your installation problem is caused by the hardware:

- Verify that all adapters are installed securely.
- Verify that all cables are attached securely to the correct connectors. Be sure that the FC connectors that attach from the J1 connector on the adapter to the device are connected securely.
- Verify that the adapter is installed correctly and fully seated in the expansion slot. Check for interference due to nonstandard PCI connectors.
- Verify that all peripheral devices are turned on. See “Scan fibre channel devices” on page 341″ for information about displaying attached devices.

System configuration problems

To determine whether a problem was caused by the system configuration, check the system board to make sure that it was configured properly (refer to the appropriate IBM TotalStorage FAStT Product Installation Guide).

Fibre channel problems

To determine whether your installation problem is caused by the FC, verify that all of the FC devices were turned on before you turned on the server. Also, ensure that all cables are connected properly.

The problem determination (PD) maps found in Chapter 17, “Problem determination maps”, on page 137 provide you with additional diagnostic aids.

Additional service information

The following information supports the FAStT Host Adapter.

This section contains the FAStT Host Adapter operating environment and specification information.

Table 8. FAStT Host Adapter operating environment

Environment	Minimum	Maximum
Operating temperature	0° C (32° F)	55° C (131° F)
Storage temperature	-20° C (-4° F)	70° C (158° F)
Relative humidity (noncondensing)	10%	90%
Storage humidity (noncondensing)	5%	95%

Table 9. FAStT Host Adapter Specifications

Type	Specification
Host bus	Conforms to PCI Local Bus Specification, revision 2.2
PCI signaling environment	3.3 V and 5.0 V buses supported
PCI transfer rate	• 264 MB per second maximum burst rate for 33 MHz operation (ISP2200A chip) • Supports dual address bus cycles
Fibre channel specifications	• Bus type: fiber-optic media (shortwave 50 micron) • Bus transfer rate: 100 MB per second maximum (200 full-duplex) • Supports both FCP-SCSI and IP protocols • Supports point-to-point fabric connection: F-Port Fabric Login • Supports FC-AL public loop profile: FL-Port Login • Supports fibre channel services class 2 and 3 • FCP SCSI initiator and target operation • Full-duplex operation
Processor	Single chip design that includes a RISC processor, fibre channel protocol manager, PCI DMA controller, and 1-gigabit transceivers
Host data transfer	64-bit, bus master DMA data transfers to 528 MB per second
RAM	128 KB of SRAM
BIOS ROM	128 KB of flash ROM in two 64 KB, software selectable banks. The flash is field-programmable.
NVRAM	256 bytes, field-programmable
Onboard DMA	Three independent DMA channels: two data and one command. Integrated 4 KB frame buffer FIFO for each data channel
Connectors (external)	• SC-style connector that supports non-OFC, multimode fiber-optic cabling using 1x9 fiber-optic transceiver module • Total cable length cannot exceed 500 meters • Two three-position, point-to-point cable (internal)
Form factor	17.8 cm x 10.7 cm (7.0 in. x 4.2 in.)
Operating power	Less than 15 watts

Table 9. FAStT Host Adapter Specifications (continued)

Type	Specification
Other compliance	• PCI 98, including ACPI • Less than 28% processor utilization as measured in a TPCC benchmark • Operation system support for Micosoft Windows NT version 4, Windows 2000 version 1, NetWare version 4.x and 5.x, SCO UnixWare version 7.x • Worldwide agency compliance as defined for IBM products • 100% Plug and Play compatibility with our existing fibre channel RAID Controller

Chapter 5. IBM FAStT FC2-133 (FRU 24P0962) and IBM FAStT FC2-133 Dual Port (FRU 24P8053) Host Bus Adapters

Note: The problem determination (PD) maps found in Chapter 17, “Problem determination maps”, on page 137 provide you with additional diagnostic aids.

The IBM FAStT FC2-133 Host Bus Adapter is a 2 Gbps high-performance, direct memory access (DMA), bus master, fibre channel host adapter designed for high-end systems. The function and performance are derived from the ISP2310 chip, making this IBM FAStT FC2-133 Host Bus Adapter a leading-edge host adapter.

The ISP2310 chip combines a powerful, reduced instruction set computer (RISC) processor, a fibre channel protocol manager (FPM) with one 2 Gbps fibre channel transceiver, and a peripheral component interconnect (PCI) or peripheral component interconnect-extended (PCI-X) local bus interface in a single-chip solution. The IBM FAStT FC2-133 Host Bus Adapter supports all fibre channel (FC) peripheral devices that support private-loop direct attach (PLDA) and fabric-loop attach (FLA).

Chapter 30, “Using IBM Fast!UTIL”, on page 335 provides detailed configuration information for advanced users who want to customize the configuration of the FAStT FC2-133 Host Bus Adapter.

General checkout

There are three types of installation problems that might cause your FAStT FC2-133 Adapter to function incorrectly:

- Hardware problems
- System configuration problems
- Fibre channel problems

If you are having problems, use the following information to help you determine the cause of the problem and the action to take.

Hardware problems

Take the following actions to determine if your installation problem is caused by the hardware:

- Verify that all adapters are installed securely.
- Verify that all cables are attached securely to the correct connectors. Be sure that one end of the LC-LC fibre channel cable is attached to the optical interface connector (located at J1 on the adapter) and that the other end is connected to the fibre channel device.
- Verify that the FAStT FC2-133 Adapter is installed correctly and is fully seated in the expansion slot. Check for interference due to nonstandard PCI connectors.
- Verify that the Fast!UTIL data-rate setting is correct. See “Extended Firmware settings” on page 340. The Fast!UTIL data-rate setting must match the speed of the device to which you are connected.
- Verify that all peripheral devices are turned on. See “Scan fibre channel devices” on page 341 for information about displaying attached fibre channel devices.

System configuration problems

To verify that your installation problem is caused by the system configuration, check your server to ensure that it is configured properly (refer to the appropriate IBM TotalStorage FAStT Product Installation Guide).

Note: All PCI-compliant and PCI-X-compliant systems automatically detect 32-bit or 64-bit adapters and set the appropriate bus speed (for example, 66 MHz or 133 MHz).

Fibre channel problems

To determine if your installation problem is caused by an attached fibre channel device, do the following:

- Verify that all of the fibre channel devices were turned on before you turned on the server.
- Ensure that all cables are connected properly.
- Verify that you configured your RAID storage subsystems using the utilities provided by the manufacturer.
- If your fibre channel switch supports zoning, make sure that your peripheral device is configured to the same switch zone as the FAStT FC2-133 Adapter. For more information, refer to your fibre channel switch documentation.

Additional service information

The following information supports the FAStT FC2-133 Adapter.

Table 10 and Table 11 contain the FAStT FC2-133 Adapter operating environment and specification information.

Table 10. FAStT FC2-133 Adapter operating environment

Environment	Minimum	Maximum
Operating temperature	0°C (32°F)	55°C (131°F)
Storage temperature	-20°C (-4°F)	70°C (158°F)
Relative humidity (noncondensing)	10%	90%
Storage humidity (noncondensing)	5%	95%

Table 11. FAStT FC2-133 Adapter specifications

Type	Specification
Host bus	Conforms to Intel *PCI Local Bus Specification*, revision 2.2 and the *PCI-X Addendum*, revision 1.0.
PCI/PCI-X signaling environment	3.3 V and 5.0 V buses supported
PCI/PCI-X transfer rate	• Support for 32 bit and 64 bit PCI bus at 33 MHz and 64 MHz • Support for 64 bit PCI-X bus at 50 MHz, 100 MHz, and 133MHz • PCI transfer rate 264 MB per second maximum burst rate for 33 MHz operation (ISP2310 chip) • Support for dual address bus cycles

Table 11. FAStT FC2-133 Adapter specifications (continued)

Type	Specification
Fibre channel specifications	• Fiber-optic media (shortwave multimode 50 micron cable) • Bus transfer rate: 200 MB per second maximum at half-duplex and at 400 MB per second maximum full-duplex. • Interface chip: ISP2310 (PCI-X QLA23xx boards) • Support for both FCP-SCSI and IP protocols • Support for point-to-point fabric connection: F-Port Fabric Login • Support for FCAL public loop profile: FL-Port Login • Support for fibre channel services class 2 and 3 • Support for FCP SCSI initiator and target operation • Support for full-duplex operation
Processor	Single-chip design that includes a RISC processor, fibre channel protocol manager, PCI/PCI-X DMA controller, and integrated serializer/deserializer (SERDES) and electrical transceivers that can auto-negotiate a data rate of 2 Gb per second.
Host data transfer	64-bit, bus-master DMA data transfers to 528 MB per second
RAM	RAM 256 KB of SRAM supporting parity protection
BIOS ROM	BIOS ROM 128 KB of flash ROM in two 64 KB, software selectable banks. The flash is field programmable.
NVRAM	NVRAM 256 bytes, field-programmable
Onboard DMA	Five-channel DMA controller: two data, one command, one auto-DMA request, and one auto-DMA response.
Frame buffer FIFO	Integrated 4 KB transmit and 6 KB receive frame buffer FIFO for each data channel
Connectors (external)	• LC-style connector that supports non-OFC, multimode fiber-optic cabling using a small form factor (SFF) fiber-optic transceiver module. • Total cable length cannot exceed 500 meters.
Form factor	5.15 cm x 16.75 cm (2.5 in. x 6.7 in.)
Operating power	Less than 15 watts

Chapter 6. Type 3526 Fibre Channel RAID controller

Note: The problem determination (PD) maps found in Chapter 17, “Problem determination maps”, on page 137 provide you with additional diagnostic aids.

The Type 3526 Fibre Channel RAID controller is compatible with the following IBM products:

- Type 3523 Fibre Channel Hub and GBIC (see Chapter 2 on page 5)
- Fibre Channel Adapter (FRU 01K7354) (see Chapter 3 on page 13)
- IBM FAStT Host Adapter (FRU 09N7292) (see Chapter 4 on page 15)
- Type 2109 Fibre Channel Switch
- Type 3534 Managed Hub

General checkout

Use the status LEDs, the “Symptom-to-FRU index” on page 34, and the connected server HMM to diagnose problems.

Using the Status LEDs

The LEDs of the control unit indicate the hardware status:

- Green LED indicates normal operation
- Amber LED indicates a hardware problem

The LEDs on the controller unit indicate the status of the controller unit and its individual components. The green LEDs indicate a normal operating status; amber LEDs indicate a hardware fault. Check all of the LEDs on the front and back of the controller unit when it is powered on.

Note:

1. If power was just applied to the controller unit, the green and amber LEDs might turn on and off intermittently. Wait until the controller unit finishes powering up before you begin checking for faults.
2. To view the controller Customer Replaceable Unit (CRU) LEDs, the front cover must be removed from the controller unit.

Also use LEDs on the front cover, controller CRUs, and drive units (if applicable) to determine whether the controllers and drives are responding to I/O transmissions from the host.

The following list describes LED activities:

- If a Fast Write Cache operation to the controller unit (or attached drive units), or if other I/O activity is in progress, then you might see several green LEDs blinking, including: the Fast Write Cache LED (on the front cover), controller CRU status LEDs, or applicable drive activity LEDs.
- The green Heartbeat LEDs on the controller CRUs blink continuously. The number and pattern of green status LEDs lit on the controllers depend on how the system is configured. An active controller will not have the same status LEDs lit as a passive controller. Refer to the appropriate IBM TotalStorage FAStT Product Installation Guide.

Additional service information

Powering on the controller

Note: All drive modules must be powered on before you power on the controller.

The controller might take from three to 10 seconds to power on. During this time, the amber and green LEDs on the controller unit flash.

After power on, check all fault LEDs to make sure they are off. If a fault LED is on, see the “Symptom-to-FRU index” on page 34.

Recovering from a power supply shutdown

Both power supplies have a built-in temperature sensor designed to prevent the power supplies from overheating. If a temperature sensor detects an over-temperature condition (ambient air temperature of 70° C (158° F) or above), the ″overheated″ power supply automatically shuts down. The other power supply remains on as long as its temperature remains below 70° C (158° F). If not, the second power supply shuts down, which turns off all power to the controller unit.

After the air temperature cools to below 70° C (158° F), the power supplies automatically restart. An automatic restart resets the controllers, attempts to spin up the drives (which has no effect on the drives if they are already running), and returns the controller unit to a normal operating state. Typically, you will not need to perform recovery procedures after an automatic power supply shutdown and restart.

After a power supply shutdown, check all controller LEDs.

If the power supply power LED is off, or the amber power supply LED on the front cover is on, go to the “Symptom-to-FRU index” on page 34.

Connectors and Host IDs

The Host ID switches and connectors for interface cables are on the connector plate located on the back of the controller unit.

Host and drive ID numbers

Each controller must have a unique Fibre Host ID number (see Figure 9 on page 25). The Host ID numbers assigned to each controller are based on two elements:

- Host ID numbers set through hardware switches on the controller unit. There are five Host ID switches that allow you to set ID numbers 0 through 127 for each controller. The factory default settings are ID #5 for Controller A and ID #4 for controller B.
- Software algorithms that calculate the actual fibre channel address, based on the controller unit’s hardware settings and position on the loop or hub.

Note: The preferred ID is assigned on the fibre channel loop unless it is already being used. If the ID is already in use, a soft ID is assigned.

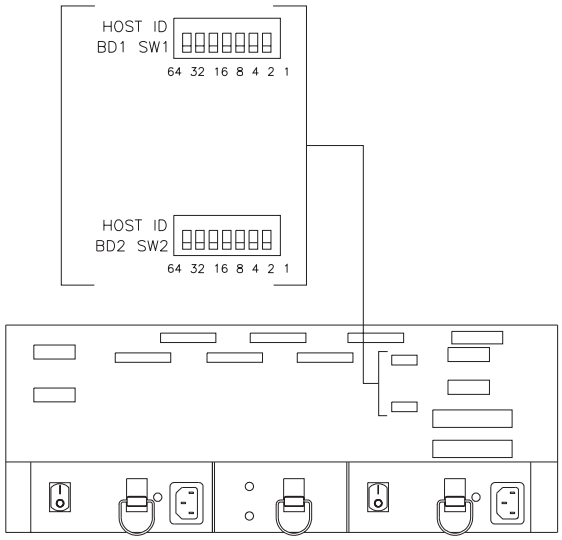


Figure 9. Fibre Host ID

Fibre channel host cable requirements

For the Type 3526 Fibre Channel RAID Controller, you must use multi-mode, 50-micrometer fiber-optic cable and a Media Interface Adapter (MIA), shown in Figure 10.

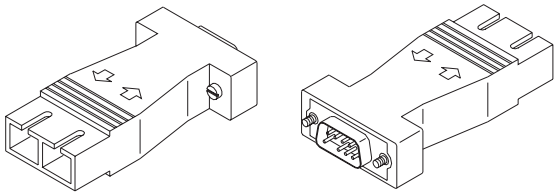


Figure 10. Media Interface Adapter

Table 12 provides specifications for the Media Interface Adapter (MIA).

Table 12. Media Interface Adapter (MIA) specifications

Cable	Media type	Data size	Transfer speed	Range
Fiber-optic (multi-mode, 50-micrometer)	Short-wave laser	100 MB/sec	1062.5 Mbaud	up to 500 m

LVD-SCSI drive cable requirements

To connect the controller unit to a drive module, you must use 68-pin, VHDCI (very high density cable interface) LVD, Ultra 2 SCSI cables. The controller unit has six drive connectors that support 16-bit interface protocols. Each connector represents a single drive channel that supports up to 10 drives per channel for a total of 60 drives.

Specifications

Size

- With front panel:
  - Depth: 610mm (24in.)
  - Height: 174mm (6.8in.)
  - Width: 482mm (19in.)

Weight

- Controller unit maximum weight: 34.5 kg (76 lb)
- Controller unit empty: 14.3 kg (31.6 lb)
- Battery: 9.7 kg (21.4 lb)

Electrical Input

- Sign-wave input (50 to 60 Hz)
  - Low range: Minimum: 90 V ac Maximum: 127 V ac
  - High range: Minimum: 198 V ac Maximum: 257 V ac
- Input Kilovolt-amperes (kVA) approximately:
  - Minimum configuration: 0.06 kVA
  - Maximum configuration: 0.39 kVA

Environment

- Air temperature:
  - hub on: 10° to 35° C (50° to 95° F) Altitude: 0 to 914 m (3000 ft.)
  - hub on: 10° to 32° C (50° to 90° F) Altitude: 914 m (3000 ft.) to 2133 m (7000 ft.)
- Humidity:
  - 8% to 80%

Heat Output

- Approximate heat output in British Thermal Units (BTU) per hour:
  - Maximum configuration: 731.8 BTU (214 watts)

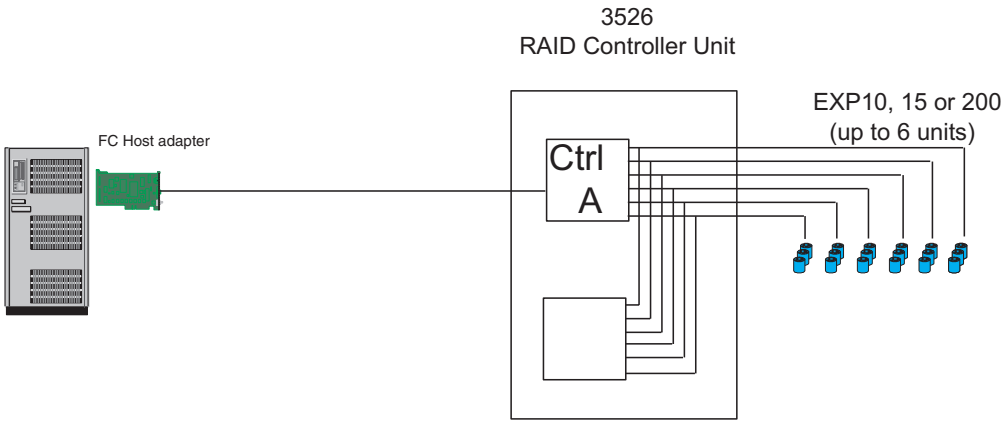
Acoustical Noise Emissions Values

- Sound Power (idling and operating):
  - 6.4 bels
- Sound Pressure (idling and operating):
  - 50 dBA

Tested configurations

The following configurations are for the Type 3526 Fibre Channel RAID Controller.

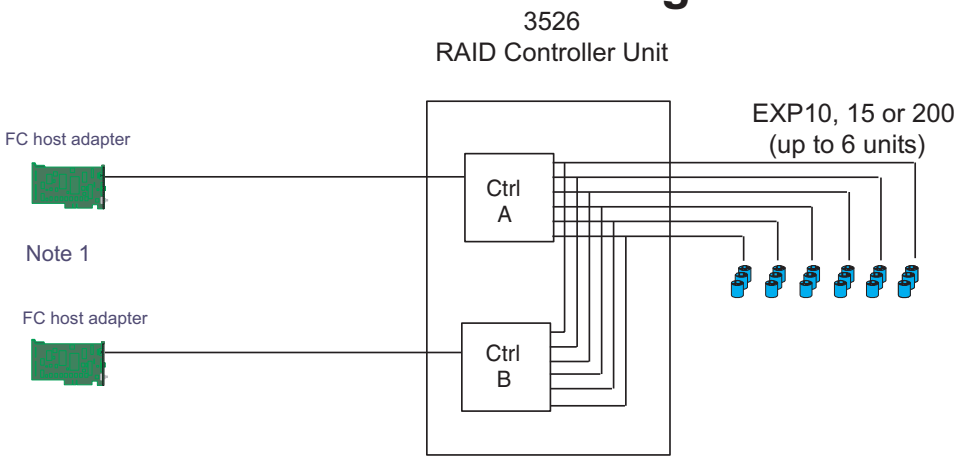
Basic Configuration



Note: Basic as shipped, single controller, no hubs or switches

Figure 11. Basic Configuration

Basic Dual Controller Configuration



Note 1: Adapters can be in the same or different systems; choice affects total redundancy
Note 2: No hubs or switches
Note 3: For max redundancy on the drive side use orthagonal striping (see orthagonal striping chart)
Note 4: This config does not provide for “NO single point of failure”

Figure 12. Basic Dual Controller Configuration

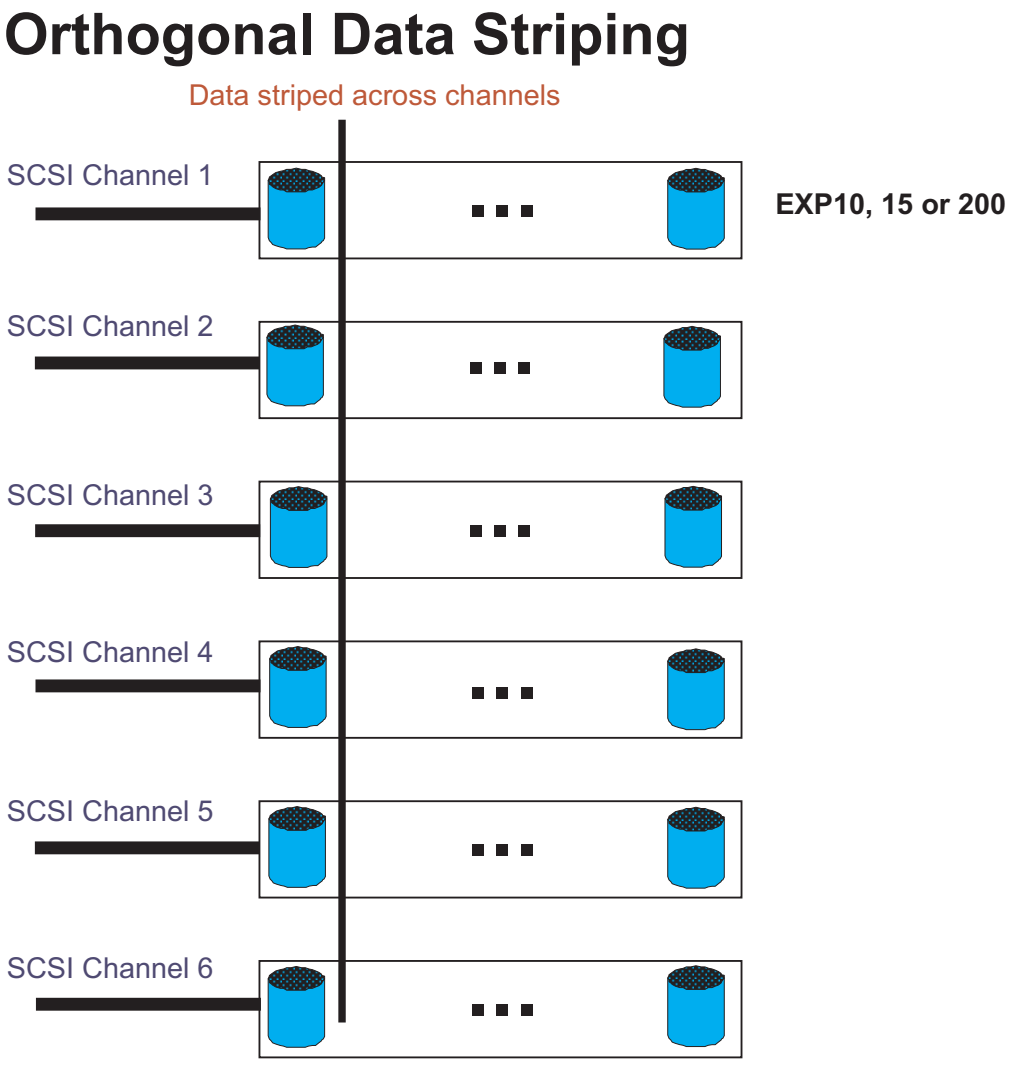
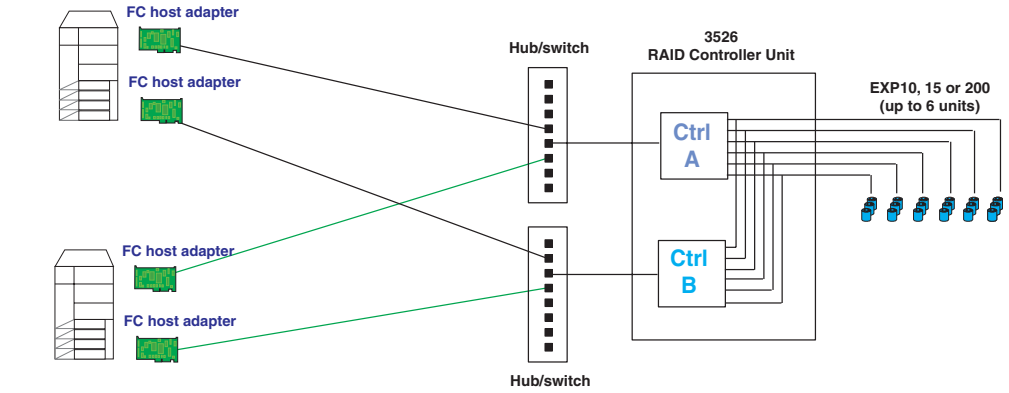


Figure 13. Orthogonal Data Striping

Simple Fully Redundant

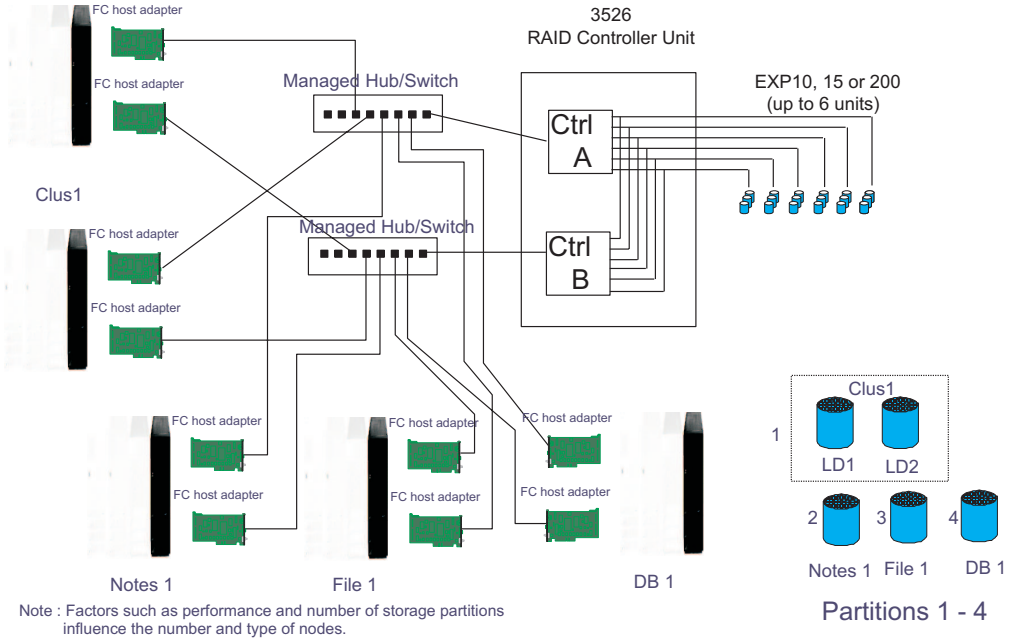


Redundant
Servers

Note 1: Since disks are seen from multiple places some form of protection such as MSCS, storage partitioning, Sanergy, Oracle etc must be used.
Note 2: For best performance and managibility, a managed hub switch is preferred.
Note 3: Always try to keep connections to hub on adjacent ports and unplug all unused GBICs

Figure 14. Simple Fully Redundant

Cluster/Non-Cluster Share



Note : Factors such as performance and number of storage partitions influence the number and type of nodes.

Figure 15. Cluster/Non-Cluster Share

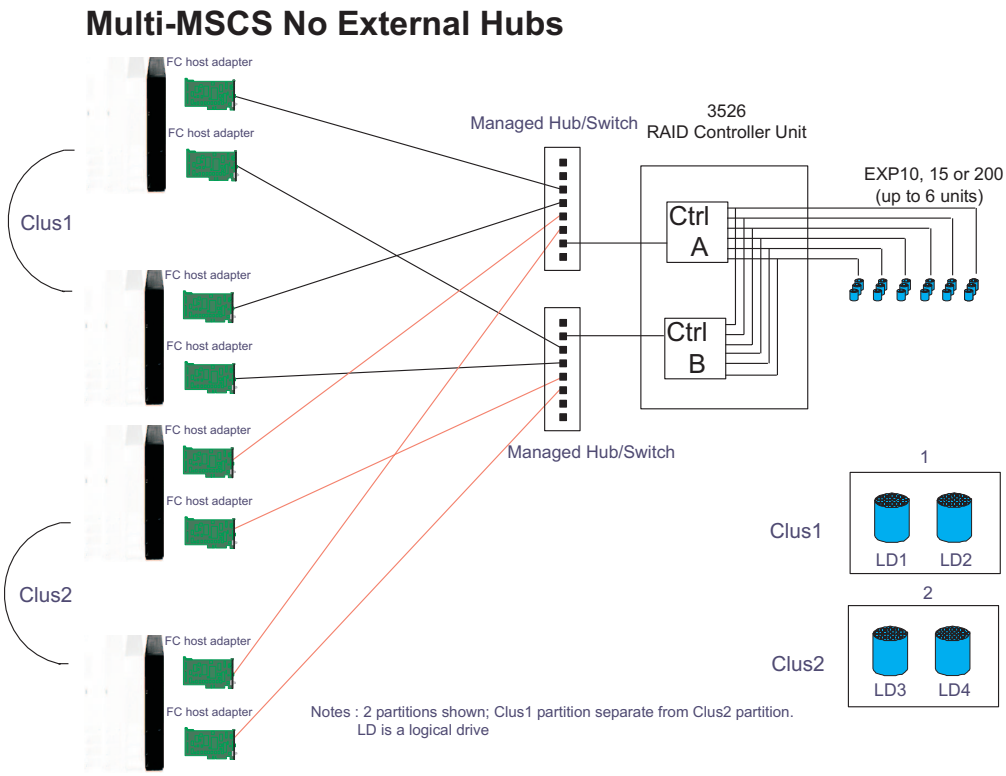


Figure 16. Multi-MSCS No External Hubs

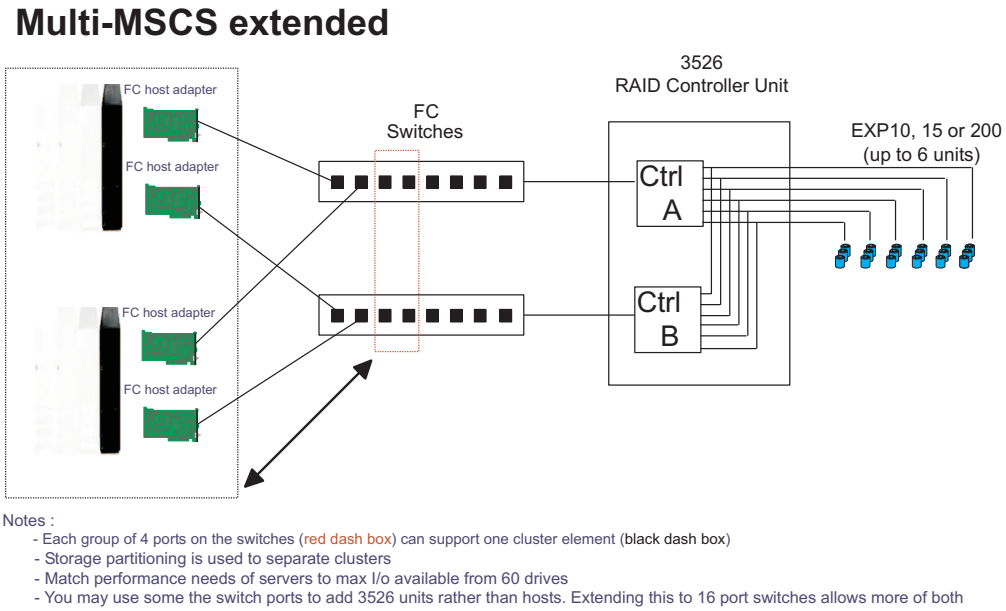


Figure 17. Multi-MSCS Extended

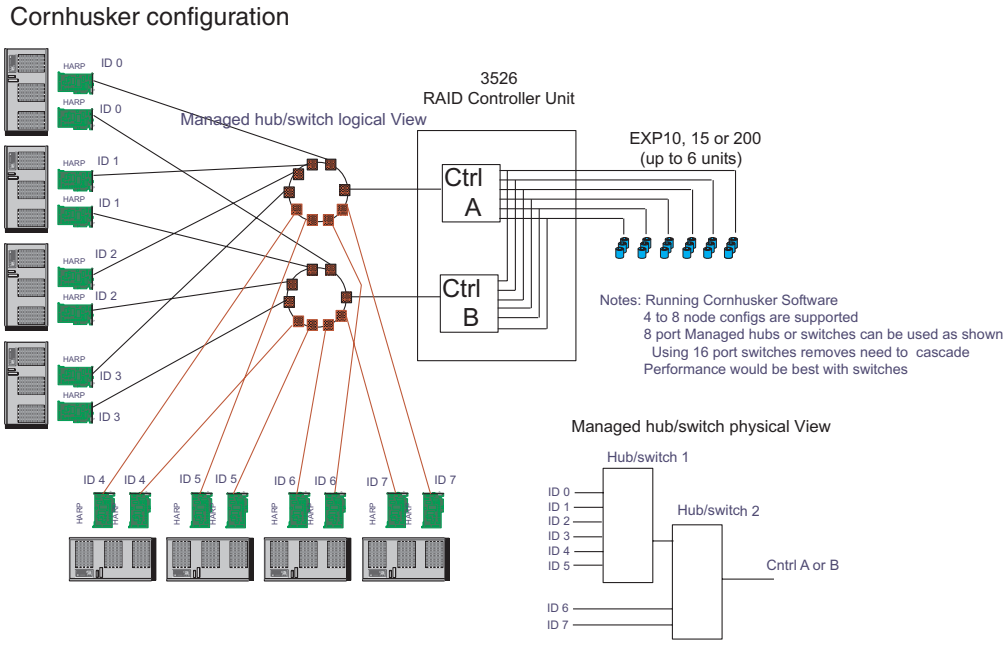


Figure 18. Cornhusker Configuration

Base Storage Partitions

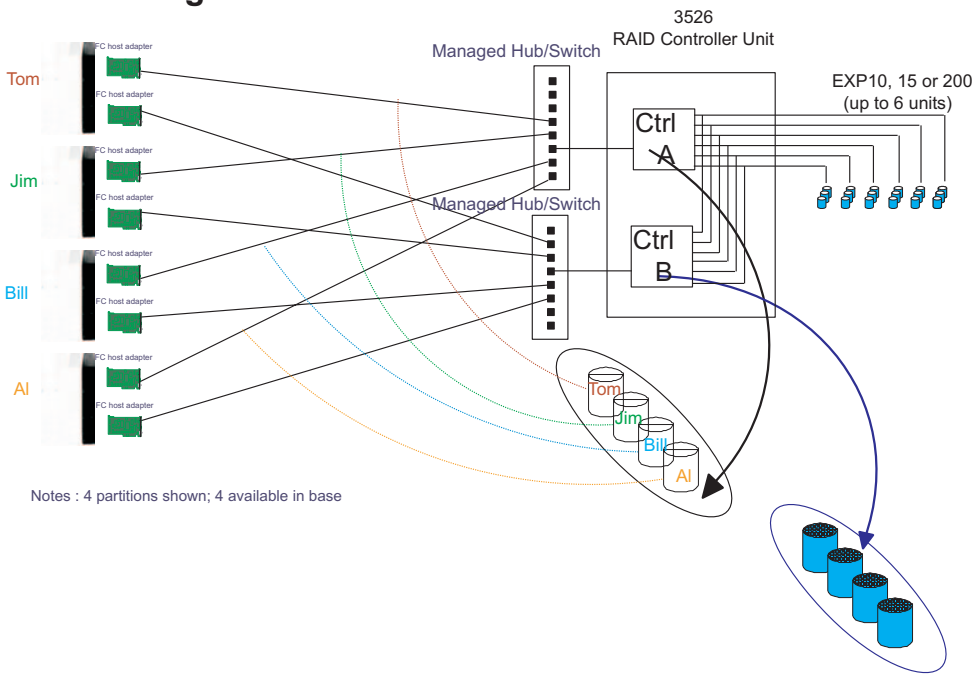


Figure 19. Basic Storage Partitions

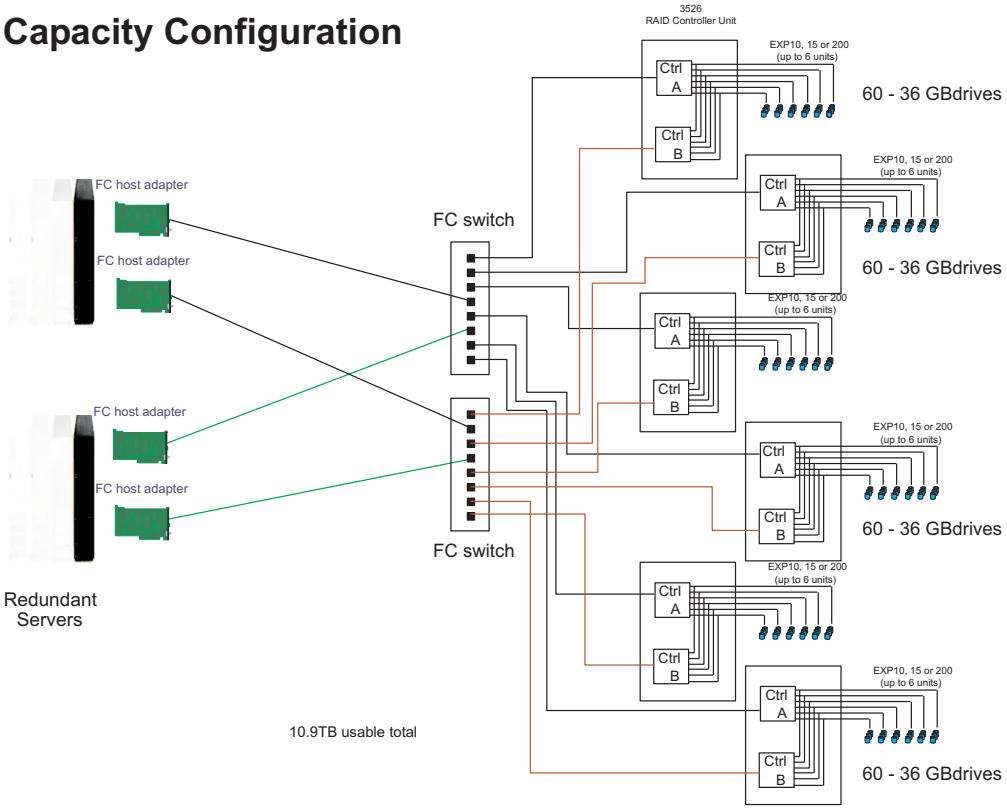


Figure 20. Capacity Configuration

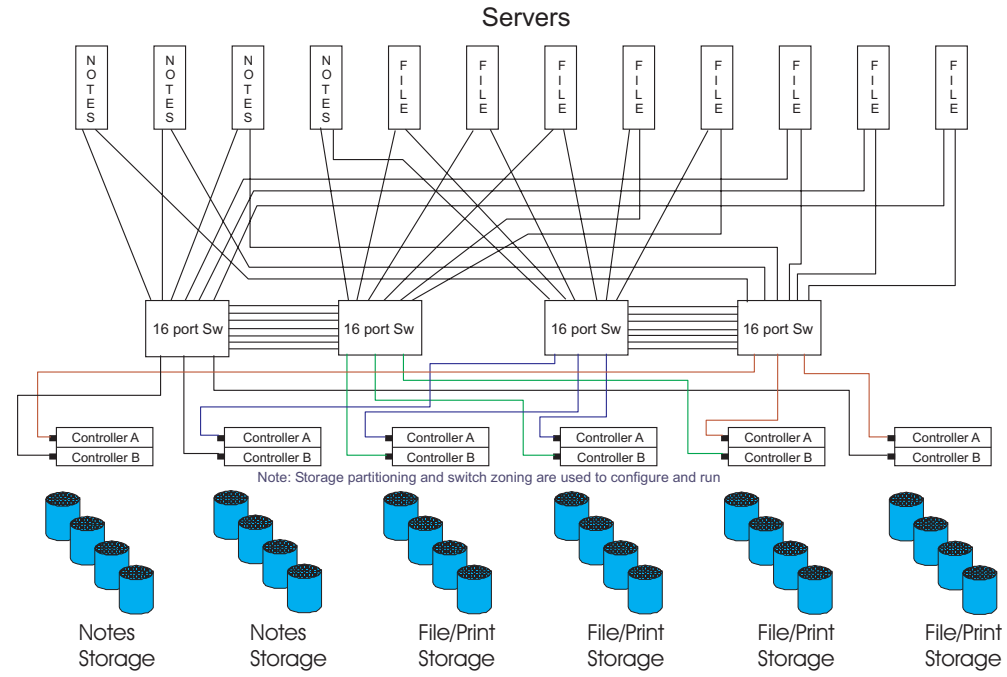


Figure 21. SAN - Using Partitions of Clusters

Legato HA/Replication for MSCS

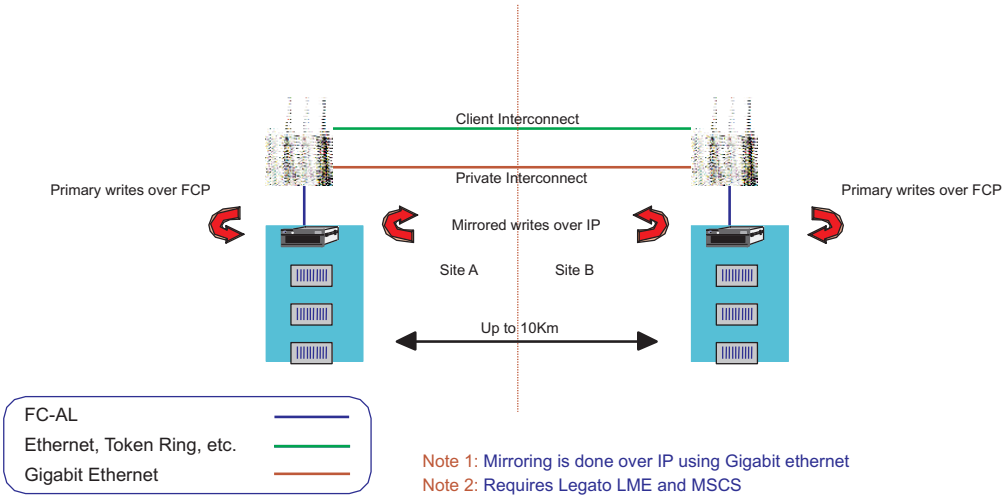


Figure 22. Legato HA/Replication for MSCS

Symptom-to-FRU index

The Symptom-to-FRU index (Table 13) lists symptoms and the possible causes. The most likely cause is listed first.

The PD maps found in Chapter 17, “Problem determination maps”, on page 137 also provide you with additional diagnostic aids.

Note:

1. Always start with the “General checkout” on page 23. For IBM devices not supported by this index, refer to the manual for that device.
2. Do *not* look directly into any fiber cable or GBIC optical output. Read “Notices” on page 457. To view an optical signal, use a mirror to view the reflected light.

Table 13. Symptom-to-FRU index for Type 3526 Fibre Channel RAID controller

Problem	FRU/Action
Controller LED (front cover) is on.	1. **Reseat Controller CRU** 2. Place Controller online using SM7 GUI 3. If in passive mode, check Fibre path/GBIC 4. Controller CRU
Software issued a controller error message.	1. **Check Controller Fan** 2. Controller CRU
Software errors occur when attempting to access controllers or drives.	1. **Check appropriate software and documentation to make sure the system is set up correctly and the proper command was executed**. 2. Power to the Controller 3. Interface cables 4. ID settings 5. Controller 6. Drive 7. Controller backpanel
Fan LED (front cover) is on.	1. **Power supply fan CRU** 2. Controller fan CRU
Controller and Fan fault LEDs (front cover) are on.	1. **Check both Fan and Controller CRUs for fault LED and replace faulty CRU.**
Fault-A or Fault-B LED (battery CRU) is on. **Note:** The Fault-A or Fault-B LED *will* be on during battery charging.	1. **Battery CRU**
Full Charge-A or Full Charge-B LED (battery CRU) is off.	1. **Power on Controller and allow batteries to charge for 24 hours until the Full Charge LEDs are on.** 2. Battery CRU 3. Both power supplies
No power to controller (all power LEDs off)	1. **Check power switches and power cords** 2. Power supplies

Table 13. Symptom-to-FRU index for Type 3526 Fibre Channel RAID controller (continued)

Problem	FRU/Action
Power Supply LED is off.	1. **Check and reseat power supply** 2. Check for overheating. Wait ten minutes for the power supply CRU to cool down. See “Recovering from a power supply shutdown” on page 24. 3. Power supply CRU
Power Supply CRU LEDs are on, but all other CRU LEDs are off.	1. **DC power harness**

Parts listing

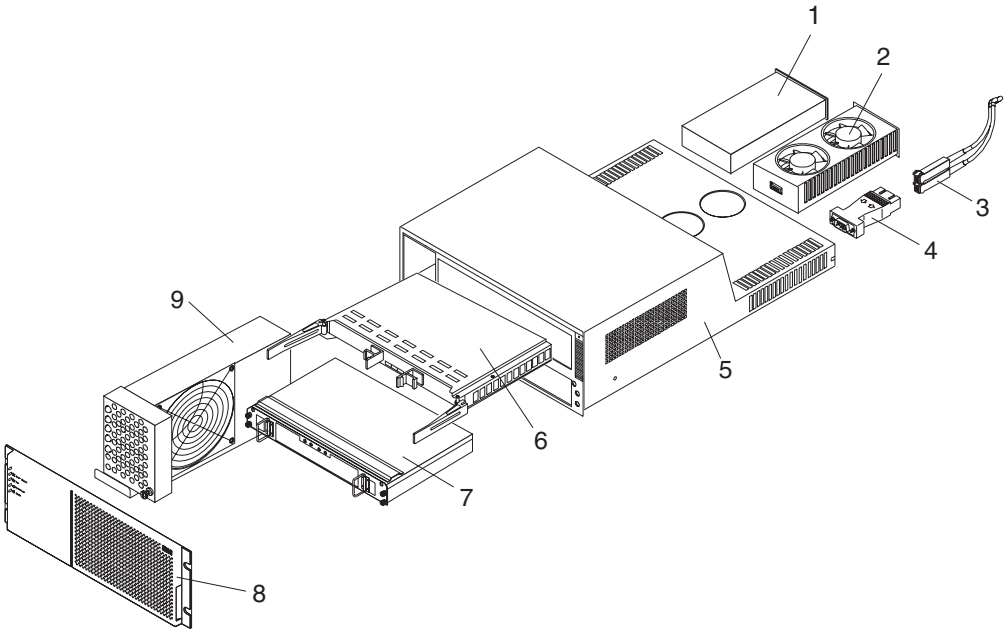


Figure 23. Type 3526 Fibre Channel RAID Controller parts list

Index	Fibre Channel RAID Controller (Type 3526)	FRU
1	350-Watt Power Supply	01K6743
2	Rear Fan Assembly (Power Supply Fan)	01K6741
3	Optical Cable - 5 Meters (option)	03K9202
3	Optical Cable - 25 Meters (option)	03K9204
4	Media Interface Adapter (MIA)	03K9280
5	Frame Assembly with Midplane	10L6981
6	Controller Assembly with 32 MB memory/128 MB cache	10L6993
7	Battery Backup Assembly	01K6742
8	Bezel Assembly	10L7043
9	Front Fan Assembly (Controller CRU Fan)	01K6740
	128 MB cache module	10L5862

Index	Fibre Channel RAID Controller (Type 3526)	FRU
	Battery Cable	03K9285
	Fan Cable	03K9281
	Power Cable	03K9284
	Miscellaneous Hardware Kit	01K6739
	Rail Kit	10L6982

Power cords

Table 14. Power cords (Type 3526 Fibre Channel RAID controller)

IBM power cord part number	Used in these countries and regions
13F9940	Argentina, Australia, China (PRC), New Zealand, Papua New Guinea, Paraguay, Uruguay, Western Samoa
13F9979	Afghanistan, Algeria, Andorra, Angola, Austria, Belgium, Benin, Bulgaria, Burkina Faso, Burundi, Cameroon, Central African Rep., Chad, Czech Republic, Egypt, Finland, France, French Guiana, Germany, Greece, Guinea, Hungary, Iceland, Indonesia, Iran, Ivory Coast, Jordan, Lebanon, Luxembourg, Macao S.A.R. of the PRC, Malagasy, Mali, Martinique, Mauritania, Mauritius, Monaco, Morocco, Mozambique, Netherlands, New Caledonia, Niger, Norway, Poland, Portugal, Romania, Senegal, Slovakia, Spain, Sudan, Sweden, Syria, Togo, Tunisia, Turkey, former USSR, Vietnam, former Yugoslavia, Zaire, Zimbabwe
13F9997	Denmark
14F0015	Bangladesh, Burma, Pakistan, South Africa, Sri Lanka
14F0033	Antigua, Bahrain, Brunei, Channel Islands, Cyprus, Dubai, Fiji, Ghana, Hong Kong S.A.R. of the PRC, India, Iraq, Ireland, Kenya, Kuwait, Malawi, Malaysia, Malta, Nepal, Nigeria, Polynesia, Qatar, Sierra Leone, Singapore, Tanzania, Uganda, United Kingdom, Yemen, Zambia
14F0051	Liechtenstein, Switzerland
14F0069	Chile, Ethiopia, Italy, Libya, Somalia
14F0087	Israel
1838574	Thailand
6952300	Bahamas, Barbados, Bermuda, Bolivia, Brazil, Canada, Cayman Islands, Colombia, Costa Rica, Dominican Republic, Ecuador, El Salvador, Guatemala, Guyana, Haiti, Honduras, Jamaica, Japan, Korea (South), Liberia, Mexico, Netherlands Antilles, Nicaragua, Panama, Peru, Philippines, Saudi Arabia, Suriname, Taiwan, Trinidad (West Indies), United States of America, Venezuela

Chapter 7. FAStT200, Type 3542 and FAStT200 HA, Type 3542

Note: The problem determination (PD) maps found in Chapter 17, “Problem determination maps”, on page 137 provide you with additional diagnostic aids.

The FAStT200 Type 3542 and FAStT200 HA Type 3542 are compatible with the following IBM products:

- IBM FAStT Host Adapter (FRU 09N7292) (see Chapter 4 on page 15)
- IBM FAStT EXP500 enclosure (see Chapter 12 on page 95)
- Type 3534 Managed Hub
- Type 2109 Fibre Channel Switch

General checkout

Use the status LEDs, Symptom-to-FRU list, and the storage management software to diagnose problems. See “Monitoring status through software” on page 42 and “Checking the LEDs” on page 42.

To diagnose a cluster system, use the cluster problem determination procedure. See “Cluster Resource PD map” on page 140.

Note: If power was just applied to the controller unit, the green and amber LEDs might turn on and off intermittently. Wait until the controller unit finishes powering up before you begin checking for faults.

General information

The Storage Server is available in two models. The (Model 3542-2RU) comes with two RAID controllers, two power supplies, and two cooling units and provides dual, redundant controllers, redundant cooling, redundant power, and battery backup of the RAID controller cache.

The (Model 3542-1RU) comes with one RAID controller, two power supplies, and two cooling units and provides battery backup of the RAID controller cache. A FAStT200 Redundant RAID Controller option is available for purchase. Contact your IBM reseller or IBM marketing representative.

The is designed to provide maximum host- and drive-side redundancy. Each RAID controller supports direct attachment of one host containing one or two host adapters. Using external managed hubs and switches in conjunction with the storage server, you can build even larger configurations. (Throughout this chapter, the use of hub or external hub refers to a managed hub.)

Note: Throughout this chapter, the term *storage server* refers to both the (Model 3542-1RU) and the (Model 3542-2RU). Model-specific information is noted where applicable.

Additional service information

Operating specifications

Table 15 on page 38 summarizes the operating specifications of the controller unit.

Table 15. Model 3542-2RU storage server operating specifications

Size (with front panel and without mounting rails) • Depth: 57.5 cm (22.6 in) • Height: 13.2 cm (5.2 in) • Width: 48 cm (18.9 in) **Weight** • Standard storage server as shipped: 25.74 kg (56.7 lb) • Typical storage server fully configured: 37.65 kg (83 lb) **Electrical input** • Sine-wave input (50 to 60 Hz) is required • Input voltage: – Low range: - Minimum: 90 V ac - Maximum: 136 V ac – High range: - Minimum: 198 V ac - Maximum: 264 V ac – Input kilovolt-amperes (kVA) approximately: - Minimum configuration: 0.06 kVA - Maximum configuration: 0.37 kVA	**Environment** • Air temperature: – Storage server on: 10° to 35° C (50° to 95° F) Altitude: 0 to 914 m (3000 ft) – Storage server on: 10° to 32° C (50° to 90° F) Altitude: 914 m (3000 ft) to 2133 m (7000 ft.) • Humidity: – 8% to 80%	**Acoustical noise emissions values:** For open bay (0 drives installed) and typical system configurations (8 hard disk drives installed). • Sound power (idling): – 6.3 bels (open bay) – 6.5 bels (typical) • Sound power (operating): – 6.3 bels (open bay) – 6.8 bels (typical) • Sound pressure (idling): – 47 dBA (open bay) – 65 dBA (typical) • Sound pressure (operating): – 47 dBA (open bay) – 68 dBA (typical) These levels are measured in controlled acoustical environments according ISO 7779 and are reported in accordance with ISO 9296. The declared sound power levels indicate an upper limit, below which a large portion of machines operate. Sound pressure levels in your location might exceed the average 1-meter values stated because of room reflections and other nearby noise.

Storage server components

The following sections show the components of the storage server.

The hot-swap features of the storage server enable you to remove and replace hard disk drives, power supplies, RAID controllers, and fans without turning off the storage server. Therefore, you can maintain the availability of your system while a hot-swap device is removed, installed, or replaced.

Front view

Figure 24 shows the components and controls on the front of the server.

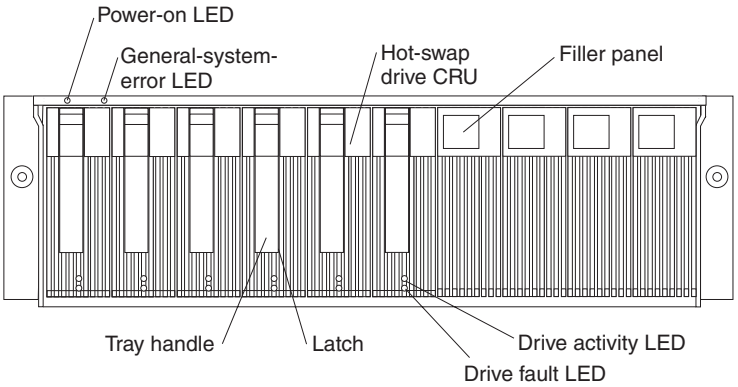


Figure 24. Server Front View

Power-on LED

When on, this green light indicates that the unit has adequate dc power.

General-system-error LED
When on, this amber LED indicates that the storage server has a fault, such as in a power supply, fan unit, or hard disk drive.

Note: If the General-system-error LED is on continuously (not flashing), there is a problem with the storage server. Use the storage-management software to diagnose and repair the problem. For more information, see “Checking the LEDs” on page 42.

Hot-swap drive CRU
You can install up to 10 hot-swap drive *customer replaceable units* (CRUs) in the storage server. Each drive CRU consists of a hard disk drive and tray.

Filler panel
The storage server comes without drives installed and contains filler panels in the unused drive bays. Before installing new drives, you must remove the filler panels and save them. Each of the 10 bays must always contain either a filler panel or a drive CRU. Each filler panel contains a filler piece for use with a slim drive.

Drive activity LED
Each drive CRU has a green Drive activity LED. When flashing, this green LED indicates drive activity. When on continuously, this green LED indicates that the drive is properly installed.

Drive fault LED
Each drive CRU has an amber Drive fault LED. When on, this amber LED indicates a drive failure. When flashing, this amber LED indicates that a drive identify or rebuild process is in progress.

Latch This multipurpose blue latch releases or locks the drive CRU in place.

Tray handle
You can use this multipurpose handle to insert and remove a drive CRU in the bay.

For information on installing and replacing drive CRUs, refer to the appropriate IBM TotalStorage FAStT Product Installation Guide. For more information about the LEDs, see “Checking the LEDs” on page 42.

Back view
Figure 25 on page 40 shows the components at the back of the storage server.

Note: If your storage server is a Model 1RU, there is only one RAID controller. There is a blank panel in the second RAID controller opening. The blank panel must remain in place to maintain proper cooling.

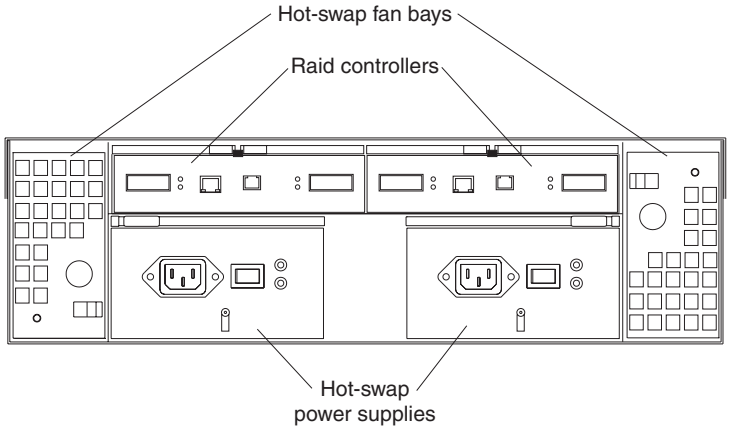


Figure 25. Storage Server Bays (back view)

RAID controller

The storage server comes with one or two hot-swap RAID controllers. Each RAID controller contains two ports for Gigabit Interface Converters (GBICs) which connect to the fibre channel cables. One GBIC connects to a host system. The other GBIC is used to connect additional expansion units to the storage server.

Each RAID controller also contains a battery to maintain cache data in the event of a power failure. For more information, refer to the appropriate IBM TotalStorage FAStT Product Installation Guide.

Hot-swap fans

The storage server has two interchangeable hot-swap and redundant fan CRUs. Each fan CRU contains two fans. If one fan CRU fails, the second fan CRU continues to operate. Both fan CRUs must be installed to maintain proper cooling within your storage server, even if one fan CRU is not operational.

Hot-swap power supplies

The storage server comes with two hot-swap power supplies. Both power supplies must be installed to maintain proper cooling.

Interface ports and switches

Figure 26 on page 41 shows the ports and switches on the back of the storage server.

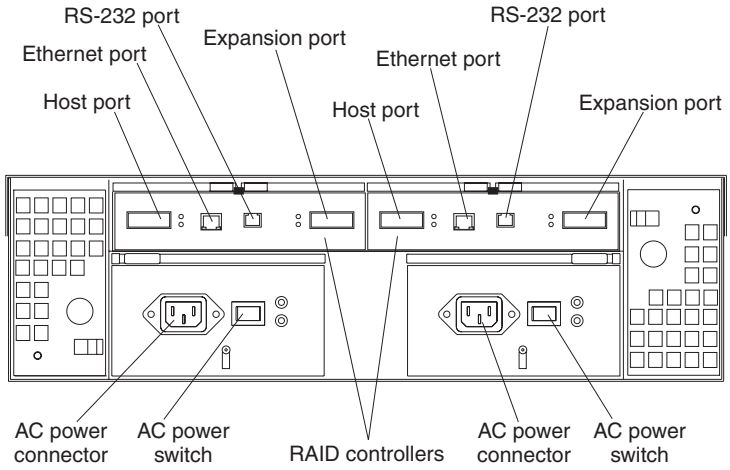


Figure 26. Interface Ports and Switches

RAID controller

Each RAID controller contains several connectors and LEDs. Each controller has one host port and one expansion port for connecting the storage server to hosts or expansion units. You first insert a GBIC into the port and then connect the fibre channel cables.

Host port

The host port is used to connect fibre channel cables from the host systems. You first insert a GBIC into the port and then connect the fibre channel cables.

Ethernet port

The Ethernet port is for an RJ-45 10 BASE-T or 100 BASE-T Ethernet connection. Use the Ethernet connection to directly manage storage subsystems.

Expansion port

The expansion port is used to connect additional expansion units to the RAID controllers. You can connect one expansion unit to each RAID controller.You first insert a GBIC into the port and then connect the fibre channel cables.

RS-232 port

The RS-232 port is a TJ-6 modular jack and is used for an RS-232 serial connection. The RS-232 port is used by service personnel to perform diagnostic operations on the RAID controllers. An RS-232 cable comes with the storage server.

Diagnostics

To diagnose fibre channel problems, use FAStT MSJ (see Chapter 18, “Introduction to FAStT MSJ”, on page 173).

To diagnose the Type 3542 storage system, use the following diagnostic tools:

- Storage-management software
- Checking LEDs

Monitoring status through software

Use the storage-management software to monitor the status of the storage server. Run the software constantly, and check it frequently.

The storage-management software provides the best way to diagnose and repair storage-server failures. The software can help you:

- Determine the nature of the failure
- Locate the failed component
- Determine the recovery procedures to repair the failure

Although the storage server has fault LEDs, these lights do not necessarily indicate which component has failed or needs to be replaced, or which type of recovery procedure that you must perform. In some cases (such as loss of redundancy in various components), the fault LED does not turn on. Only the storage-management software can detect the failure.

For example, the recovery procedure for a Predictive Failure Analysis® (PFA) flag (impending drive failure) on a drive varies depending on the drive status (hot spare, unassigned, RAID level, current logical drive status, and so on). Depending on the circumstances, a PFA flag on a drive can indicate a high risk of data loss (if the drive is in a RAID 0 volume) or a minimal risk (if the drive is unassigned). Only the storage-management software can identify the risk level and provide the necessary recovery procedures.

Note: For PFA flags, the General-system-error LED and Drive fault LEDs do not turn on, so checking the LEDs will not notify you of the failure, even if the risk of data loss is high.

Recovering from a storage-server failure might require you to perform procedures other than replacing the component (such as backing up the logical drive or failing a drive before removing it). The storage-management software gives these procedures.

Attention: Not following the software-recovery procedures can result in data loss.

Checking the LEDs

The LEDs display the status of the storage server and components. Green LEDs indicate a normal operating status; amber LEDs indicate a possible failure.

It is important to check all the LEDs on the front and back of the storage server when you turn on the power. In addition to checking for faults, you can use the LEDs on the front of the storage server to determine whether the drives are responding to I/O transmissions from the host.

Storage server LEDs (front)

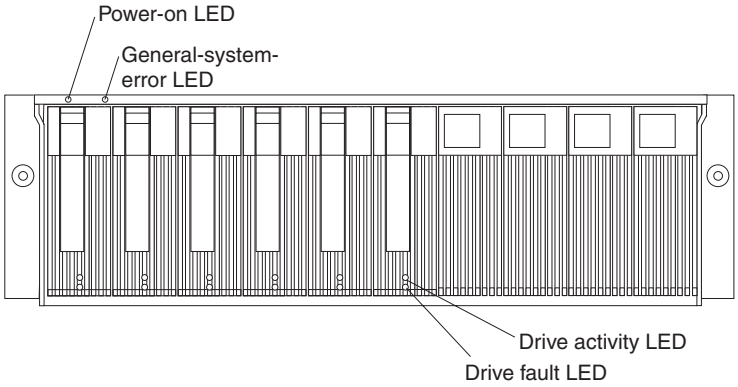


Figure 27. Storage server LEDs (front)

Table 16. Storage server LEDs (front)

LED	Color	Operating states[1]
Drive active	Green	• **On**- Normal operation. • **Flashing**- The drive is reading or writing data. • **Off** - One of the following situations has occurred: – The storage server has no power. – The storage subsystem has no power. – The drive is not properly seated in the storage server. – The drive has not spun up.
Drive fault	Amber	• **Off**- Normal operation. • **Flashing**- The storage-management software is locating a drive, logical drive, or storage subsystem. • **On** - The drive has failed, or a user failed the drive.
Power	Green	• **On**- Normal operation. • **Off** - One of the following situations has occurred: – The storage server has no power. – The storage subsystem has no power. – The power supply has failed. – There is an overtemperature condition.
General-system- error	Amber	• **Off**- Normal operation. • **On** - A storage server component has failed[2].
[1] Always use the storage-management software to identify the failure. [2] Not all component failures turn on this LED. For more information, see “Monitoring status through software” on page 42.		

Storage server LEDs (rear)

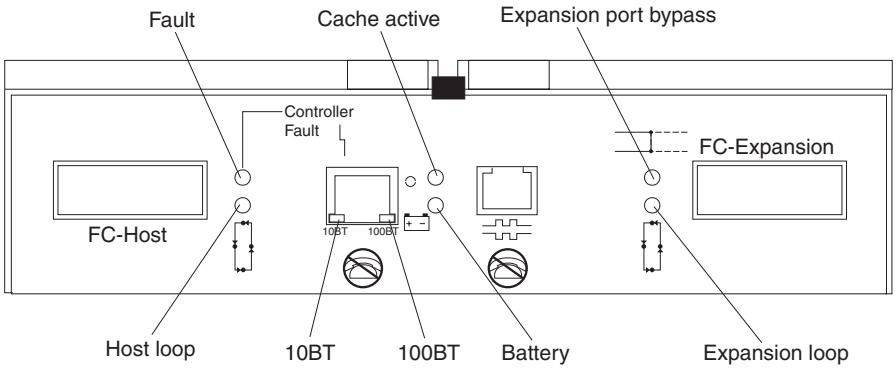


Figure 28. Storage Server LEDs (rear)

Table 17. RAID Controller LEDs

Icon	LED	Color	Operating states[1]
	Fault	Amber	• **Off**- Normal operation. • **On** - The RAID controller has failed.
	Host loop	Green	• **On**- Normal operation • **Off** - One of the following situations has occurred: – The host loop is down, not turned on, or not connected. – A GBIC has failed, or the host port is not occupied. – The RAID controller circuitry has failed, or the RAID controller has no power.
	Cache active	Green	• **On**- There is data in the RAID controller cache. • **Off** - One of the following situations has occurred: – There is no data in cache. – There are no cache options selected for this array. – The cache memory has failed, or the battery has failed.
	Battery	Green	• **On**- Normal operation. • **Flashing**- The battery is recharging or performing a self-test. • **Off** - The battery or battery charger has failed.
	Expansion port bypass	Amber	• **Off**- Normal operation. • **On** -One of the following situations has occurred: – The expansion port is not occupied. – The fibre channel cable is not attached to an expansion unit. – The attached expansion unit is not turned on. – A GBIC has failed, a fibre channel cable has failed, or a GBIC has failed on the attached expansion unit.
	Expansion loop	Green	• **On**- Normal operation. • **Off**- The RAID controller circuitry has failed, or the RAID controller has no power.

Table 17. RAID Controller LEDs (continued)

Icon	LED	Color	Operating states[1]
No icon	10BT	Green	• **If the Ethernet connection is 10BASE-T:** The 10BT LED is on, 100BT LED flashes faintly. • **If the Ethernet connection is 100BASE-T:** The 10BT LED is off, 100BT LED is on. • **If there is no Ethernet connection:** Both LEDs are off.
No icon	100BT		
[1] Always use the storage-management software to identify the failure.			

Fan and power supply LEDs

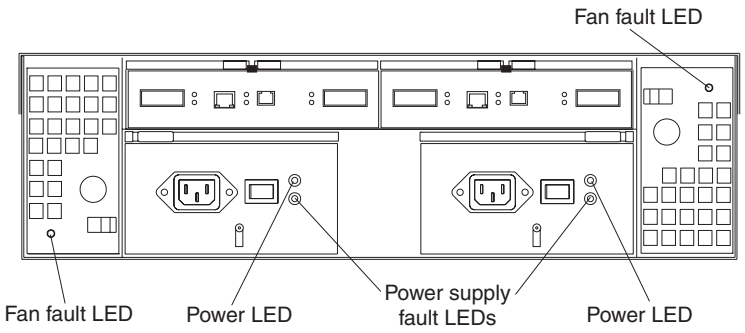


Figure 29. Fan and Power Supply LEDs

Table 18. Fan LEDs

LED	Color	Operating states[1]
Fault	Amber	• **Off**- Normal operation. • **On** - The fan CRU has failed.
[1] Always use the storage-management software to identify the failure.		

Table 19. Power supply LEDs

LED	Color	Operating states[1]
Fault	Amber	• **Off**- Normal operation. • **On** - One of the following situations has occurred: – The power supply has failed. – An overtemperature condition has occurred. – The power supply is turned off.
Power	Green	• **On**- Normal operation. • **Off** - One of the following situations has occurred: – The power supply is disconnected. – The power supply is seated incorrectly. – The storage server has no power.
[1] Always use the storage-management software to identify the failure.		

Symptom-to-FRU index

Use the storage-management software to diagnose and repair controller unit failures. Use Table 20 also to find solutions to problems that have definite symptoms.

Refer to the problem determination maps (PD maps) in Chapter 17, “Problem determination maps”, on page 137 for more detailed procedures for problem isolation.

Table 20. Symptom-to-FRU index for FAStT200, Type 3542 and FAStT200 HA, Type 3542 controller

Problem Indicator	Action/FRU
Amber LED on - Drive CRU	1. **Replace the drive that has failed**.
Amber LED on - Fan CRU	1. **Replace the fan that has failed.**
Amber LED on - RAID controller Fault LED	1. **If the RAID controller Fault LED is lit, replace the RAID controller.**
Amber LED on - Expansion port Bypass LED	1. **No corrective action needed if system is properly configured and no attached expansion units.** 2. Reattach the GBICs and fibre channel cables. Replace input and output GBICs or cables as necessary. 3. Expansion unit
Amber LED on - Front panel	1. **Indicates that a Fault LED somewhere on the storage server has turned on. (Check for amber LEDs on CRUs).**
Amber LED on and green LED off - Power supply CRU	1. **Turn on all power supply power switches** 2. Check ac power
Amber and green LEDs on - Power-supply CRU	1. **Replace the failed power-supply CRU**
All green LEDs off - All CRUs	1. **Check that all storage-server power cords are plugged in and the power switches are on** 2. Check that the main circuit breakers for the rack are turned on. 3. Power supply 4. Midplane
Amber LED flashing - Drive CRUs	1. **No corrective action is needed. (Drive rebuild or identity is in process)**
One or more green LEDs off - Power supply CRUs	1. **Make sure that the power cord is plugged in and the power-supply switches are turned on.**
One or more green LEDs off - All drive CRUs	1. **Midplane**
One or more green LEDs off - Front panel	1. **Make sure that the cords are plugged in and power supplies are turned on** 2. Midplane
One or more green LEDs off - Battery	1. **Battery**
One or more green LEDs off - Cache active	1. **Use the storage-management software to enable the cache.** 2. RAID controller 3. Battery
One or more green LEDs off - Host Loop	1. **Check if host managed hub or switch is on. Replace attached devices that have failed.** 2. Fibre channel cables 3. GBIC 4. RAID controller

Table 20. Symptom-to-FRU index for FAStT200, Type 3542 and FAStT200 HA, Type 3542 controller (continued)

One or more green LEDs off - Expansion Loop	1. **Ensure drives are properly seated** 2. RAID controller 3. Drive 4. GBIC or fibre channel cable
Intermittent or sporadic power loss to the storage server - Some or all CRUs	1. **Check the ac power source** 2. Reseat all installed power cables and power supplies 3. Replace defective power cords 4. Check for a Fault LED on the power supply, and replace the failed CRU 5. Midplane
Unable to access drives on Drives and fibre channel loop	1. **Ensure that the fibre channel cables are undamaged and properly connected.** 2. RAID controller
Random errors on Subsystem	1. **Midplane**

Note: If you cannot find the problem in Table 20 on page 46, test the entire system.

Parts listing

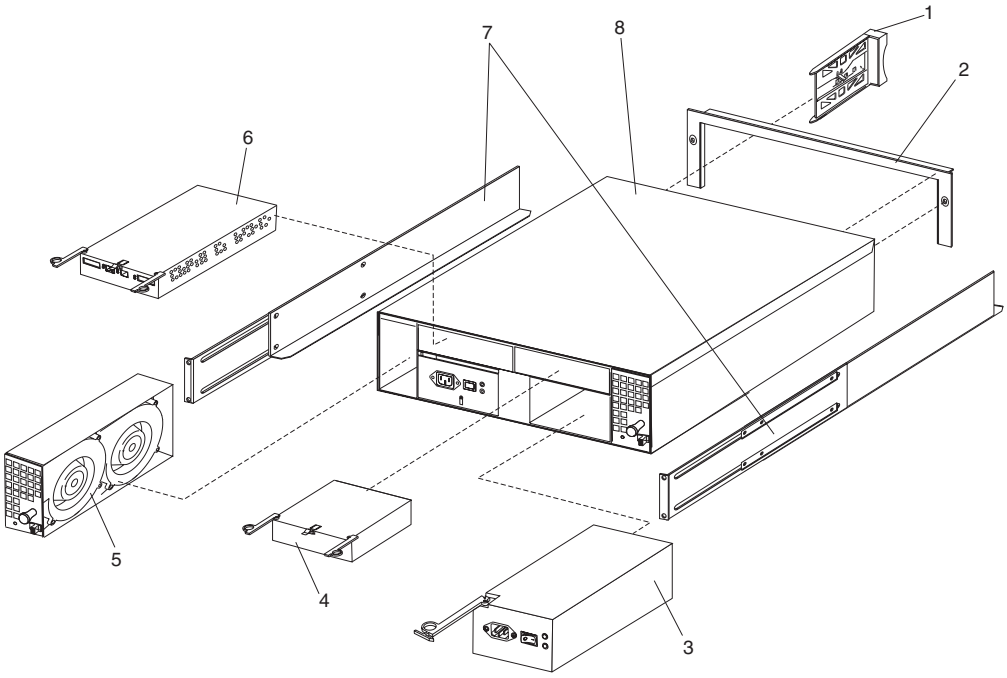


Figure 30. Parts list (FAStT200, Type 3542 and FAStT200 HA, Type 3542 controller)

This parts listing supports the following models: 1RU, 1RX, 2RU, and 2RX.

Index	Type 3542- IBM FAStT200, FAStT200 HA Storage Server	FRU No.
1	DASD Bezel Filler Asm (all models)	37L0198
2	Decorative Bezel (all models)	09N7307
3	Power Supply Asm (350 W) (all models)	19K1164

Index	Type 3542- IBM FAStT200, FAStT200 HA Storage Server	FRU No.
4	Blank, controller (model 1RU, 1RX)	19K1229
5	Blower Asm (all models)	09N7285
6	FC Controller, (all models)	19K1115
7	Rail Kit Left/Right (all models)	37L0067
8	Midplane/Frame (all models)	19K1220
	Misc. Hardware Kit (all models)	09N7288
	Short Wave GBIC (all models)	03K9206
	Long Wave GBIC (all models)	03K9208
	FAStT Storage Manager Software CD (all models)	19K1230
	Cable, 5M Optical (all models)	03K9202
	Cable, 25M Optical (all models)	03K9204
	Cable, Serial (all models)	19K1179
	Cable, 1M Optical (all models)	37L0083
	9' Line Cord (all models)	6952300
	Battery, Cache (all models)	19K1219
	Line Cord Jumper, High Voltage (model 1RX, 2RX)	36L8886

Power cords

Table 21. Power cords (FAStT200, Type 3542 and FAStT200 HA, Type 3542 controller)

IBM power cord part number	Used in these countries and regions
13F9940	Argentina, Australia, China (PRC), New Zealand, Papua New Guinea, Paraguay, Uruguay, Western Samoa
13F9979	Afghanistan, Algeria, Andorra, Angola, Austria, Belgium, Benin, Bulgaria, Burkina Faso, Burundi, Cameroon, Central African Rep., Chad, Czech Republic, Egypt, Finland, France, French Guiana, Germany, Greece, Guinea, Hungary, Iceland, Indonesia, Iran, Ivory Coast, Jordan, Lebanon, Luxembourg, Macao S.A.R. of the PRC, Malagasy, Mali, Martinique, Mauritania, Mauritius, Monaco, Morocco, Mozambique, Netherlands, New Caledonia, Niger, Norway, Poland, Portugal, Romania, Senegal, Slovakia, Spain, Sudan, Sweden, Syria, Togo, Tunisia, Turkey, former USSR, Vietnam, former Yugoslavia, Zaire, Zimbabwe
13F9997	Denmark
14F0015	Bangladesh, Burma, Pakistan, South Africa, Sri Lanka
14F0033	Antigua, Bahrain, Brunei, Channel Islands, Cyprus, Dubai, Fiji, Ghana, Hong Kong S.A.R. of the PRC, India, Iraq, Ireland, Kenya, Kuwait, Malawi, Malaysia, Malta, Nepal, Nigeria, Polynesia, Qatar, Sierra Leone, Singapore, Tanzania, Uganda, United Kingdom, Yemen, Zambia
14F0051	Liechtenstein, Switzerland
14F0069	Chile, Ethiopia, Italy, Libya, Somalia
14F0087	Israel
1838574	Thailand
6952300	Bahamas, Barbados, Bermuda, Bolivia, Brazil, Canada, Cayman Islands, Colombia, Costa Rica, Dominican Republic, Ecuador, El Salvador, Guatemala, Guyana, Haiti, Honduras, Jamaica, Japan, Korea (South), Liberia, Mexico, Netherlands Antilles, Nicaragua, Panama, Peru, Philippines, Saudi Arabia, Suriname, Taiwan, Trinidad (West Indies), United States of America, Venezuela

Chapter 8. Type 3552 FAStT500 RAID controller

Note: The problem determination (PD) maps found in Chapter 17, “Problem determination maps”, on page 137 provide you with additional diagnostic aids.

The IBM FAStT500 RAID controller is compatible with the following IBM products:

- IBM FAStT Host Adapter (FRU 09N7292) (see Chapter 4 on page 15)
- IBM FAStT EXP500 enclosure (see Chapter 12 on page 95)
- Type 2109 Fibre Channel Switch
- Type 3534 Managed Hub

General checkout

Use the indicator lights, the “Symptom-to-FRU index” on page 60, and the connected server HMM to diagnose problems.

The problem determination (PD) maps found in Chapter 17, “Problem determination maps”, on page 137 provide you with additional diagnostic aids.

Checking the indicator lights

The controller unit indicator lights (see Figure 31 on page 50) display the status of the controller unit and its components. Green indicator lights mean normal operating status; amber indicator lights mean a possible failure.

It is important that you check all the indicator lights on the front and back of the controller unit when you turn on the power. After you turn on the power, the indicator lights might blink intermittently. Wait until the controller unit completes its power up before checking for faults. It can take up to 15 minutes for the battery to complete its self-test and up to 24 hours to fully charge, particularly after an unexpected power loss of more than a few minutes.

Use the following procedure to check the controller unit indicator lights and operating status.

1. To view the indicator lights, remove the controller unit bezel.
2. Check the indicator lights on the front of the controller unit.
3. Check the indicator lights on the back of the controller unit.
4. Check the indicator lights on the mini hubs.
5. If all indicator lights show a normal status, replace the bezel; otherwise, run the storage-management software to diagnose and repair the problem.

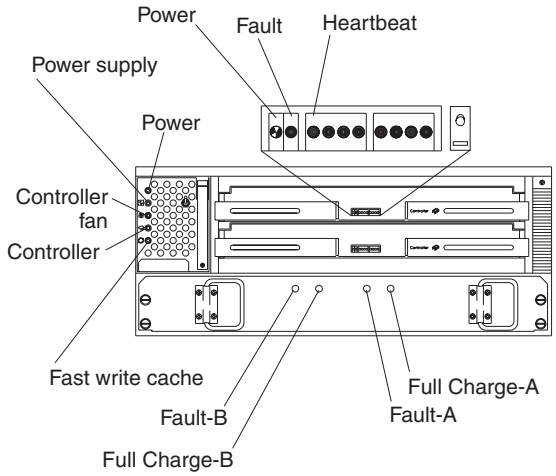


Figure 31. Type 3552 FAStT500 RAID controller indicator lights (front panel)

Table 22. Type 3552 FAStT500 RAID controller indicator lights (front panel)

Indicator light	Color	Normal Operation	Problem Indicator	Possible Conditions indicated by the problem indicator (1)
Component: controller CRU				
Power	Green	On	Off	• No power to controller unit • No power to storage subsystem • Cables are loose or the switches are off • Power supply has failed, is missing, or is not fully seated • Overtemperature condition
Fault	Amber	Off	On	Controller failure; controller fault condition
Heartbeat	Green	Blinking (2)	Not blinking (2)	No controller activity
Status (eight lights including Heartbeat)	Green	Various patterns depending on the condition	Various patterns depending on the condition	If the second, third, sixth, and seventh lights are on or if all eight lights are on, there is a memory fault indicating that the controller CRU has failed.
Component: controller fan				
Power	Green	On	Off	• No power to controller unit • No power to storage subsystem • Cables are loose or the switches are off • Power supply has failed, is missing, or is not fully seated in controller unit • Overtemperature condition
Power supply fault	Amber	Off	On	• Power supply has failed • Overtemperature • Power supply is turned off, disconnected, or not fully seated in controller unit • No power to controller unit or storage subsystem (all indicator lights are off)

Table 22. Type 3552 FAStT500 RAID controller indicator lights (front panel) (continued)

Indicator light	Color	Normal Operation	Problem Indicator	Possible Conditions indicated by the problem indicator (1)
Controller fan fault	Amber	Off	On	• Controller fan has failed • Fan and communications module is missing, unplugged, or has failed • Circuitry failure • Overtemperature condition
Controller fault	Amber	Off	On	Controller has failed; one or more memory modules failed (SIMMs or DIMMs)
Fast write cache	Green	Steady or blinking (3)	Software dependent (3)	Normal operation is off if: • Cache is not enabled • Battery is not ready
Component: battery				
Fault-A or Fault-B	Amber	Off	On	• Left or right battery bank has failed • Battery is either discharged or defective
Full Charge-A or Full Charge-B	Green	On (4)	Off	• Left or right battery bank is not fully charged • Power has been off for an extended period and has drained battery power • Batteries are weak

1. Always use the storage-management software to identify the failure.
2. There are eight status lights (the Heartbeat and seven others) that glow in various patterns, depending on the controller status.
3. The fast write cache indicator light is on when there is data in cache and blinks during a fast write operation.
4. If either Full Charge-A or Full Charge-B indicator light blink, the battery is in the process of charging.

More indicator lights are located on the back of the controller unit, as shown in Figure 32.

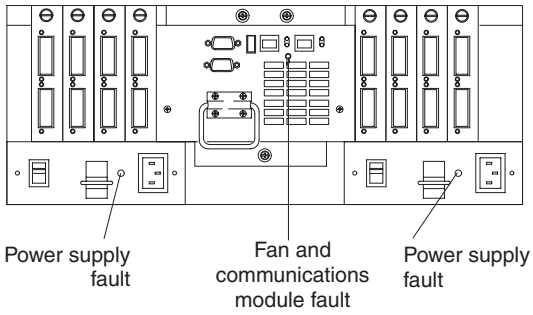


Figure 32. Type 3552 FAStT500 RAID controller indicator lights (back panel)

Table 23 on page 52 describes the back panel Type 3552 FAStT500 RAID controller indicator lights.

Table 23. Type 3552 FAStT500 RAID controller indicator lights (back panel)

Indicator light	Color	Normal Operation	Problem Indicator	Possible Conditions indicated by the problem indicator (1)
Fan and communications module				
Fan and communication fault	Amber	Off	On	• Fan and communications module has failed or is installed incorrectly • Overtemperature condition
Power supply				
Power supply	Green	On	Off	• No power to controller unit • No power to storage subsystem • Power supply has failed • Overtemperature condition
1. Always use the storage-management software to identify the failure.				

The mini hub indicator lights on the back of the controller unit are shown in Figure 33.

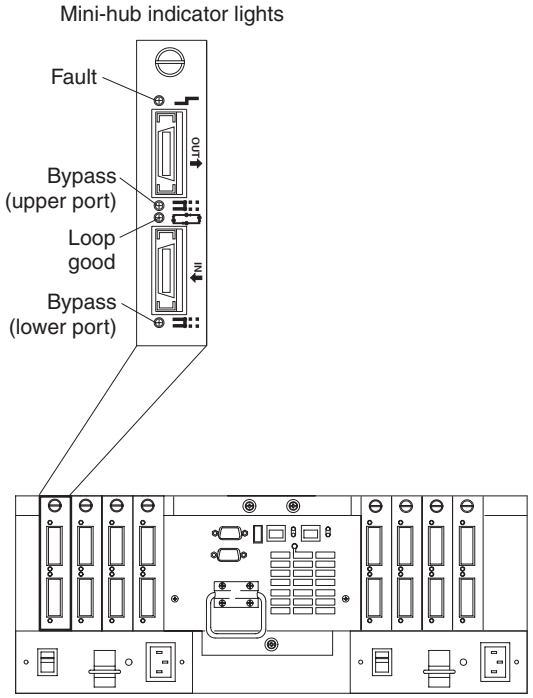


Figure 33. Type 3552 FAStT500 RAID controller mini-hub indicator lights

Table 24 on page 53 describes the mini hub indicator lights.

Table 24. Type 3552 FAStT500 RAID controller mini hub indicator lights

Icon	Indicator light	Color	Normal Operation	Problem Indicator	Possible condition indicated by the problem indicator
Component: mini hub (host-side)					
	Fault	Amber	Off	On	Mini hub or GBIC has failed **Note:** If a host-side mini- hub is not connected to a controller, this fault light is always on.
	Bypass (upper port)	Amber	Off	On	• Upper mini hub port is bypassed • Mini hub or GBIC has failed, is loose, or is missing • Fiber-optic cables are damaged **Note:** If the port is unoccupied, the light is on.
	Loop good	Green	On	Off	• The loop is not operational • Mini hub has failed or a faulty device might be connected to the mini hub • Controller has failed **Note:** If a host-side mini hub is not connected to a controller, the green light is always off and the fault light is always on.
	Bypass (lower port)	Amber	Off	On	• Lower mini hub port is bypassed • Mini hub or GBIC has failed, is loose, or is missing • Fiber-optic cables are damaged **Note:** If the port is unoccupied, the light is on.
Component: mini hub (drive-side)					
	Fault	Amber	Off	On	Mini hub or GBIC has failed **Note:** If a drive-side mini hub is not connected to a controller, this fault light is always on.

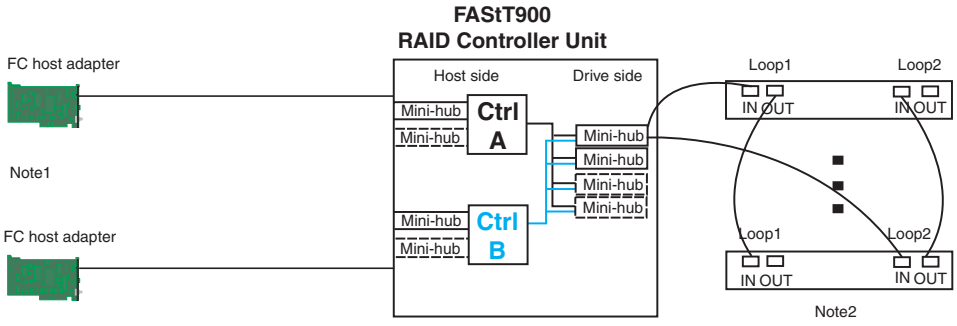
Table 24. Type 3552 FAStT500 RAID controller mini hub indicator lights (continued)

Icon	Indicator light	Color	Normal Operation	Problem Indicator	Possible condition indicated by the problem indicator
	Bypass (upper port)	Amber	Off	On	• Upper mini hub port is bypassed • Mini hub or GBIC has failed, is loose, or is missing • Fiber-optic cables are damaged **Note:** If the port is unoccupied, the light is on.
	Loop good	Green	On	Off	• The loop is not operational • Mini hub has failed or a faulty device might be connected to the mini hub • Drive has failed **Note:** If a drive-side mini hub is not connected to a controller, the green light is always off and the fault light is always on.
	Bypass (lower port)	Amber	Off	On	• Lower mini hub port is bypassed • Mini hub or GBIC has failed, is loose, or is missing • Fiber-optic cables are damaged **Note:** If the port is unoccupied, the light is on.

Tested configurations

The following configurations are for the Type 3552 IBM FAStT500 RAID Controller.

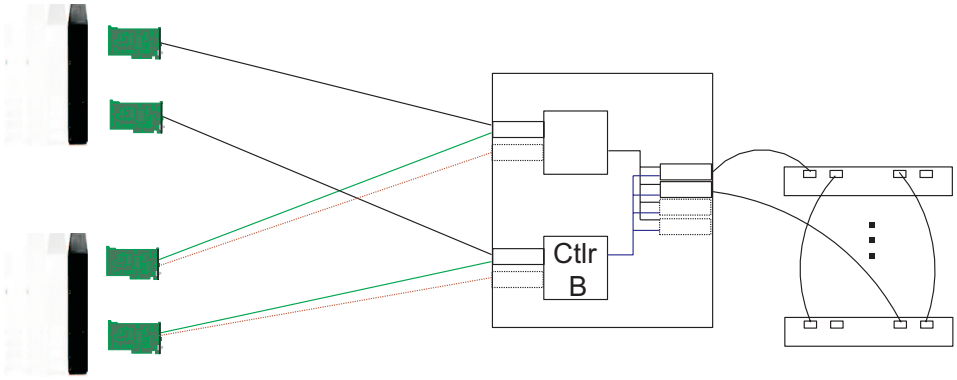
Basic Configuration



Note1: Adapters can be in the same or different systems
Note 2: Redundant drive loops are shown and required
Note 3: Mini-hubs in dashes are options
Note 4: For dual redundant loops connect to the optional set of mini-hubs shown as dashed on the drive side

Figure 34. Type 3552 IBM FAStT500 RAID Controller Basic Configuration

Simple Fully Redundant



must .

.

Figure 35. Type 3552 IBM FAStT500 RAID Controller Simple Fully Redundant

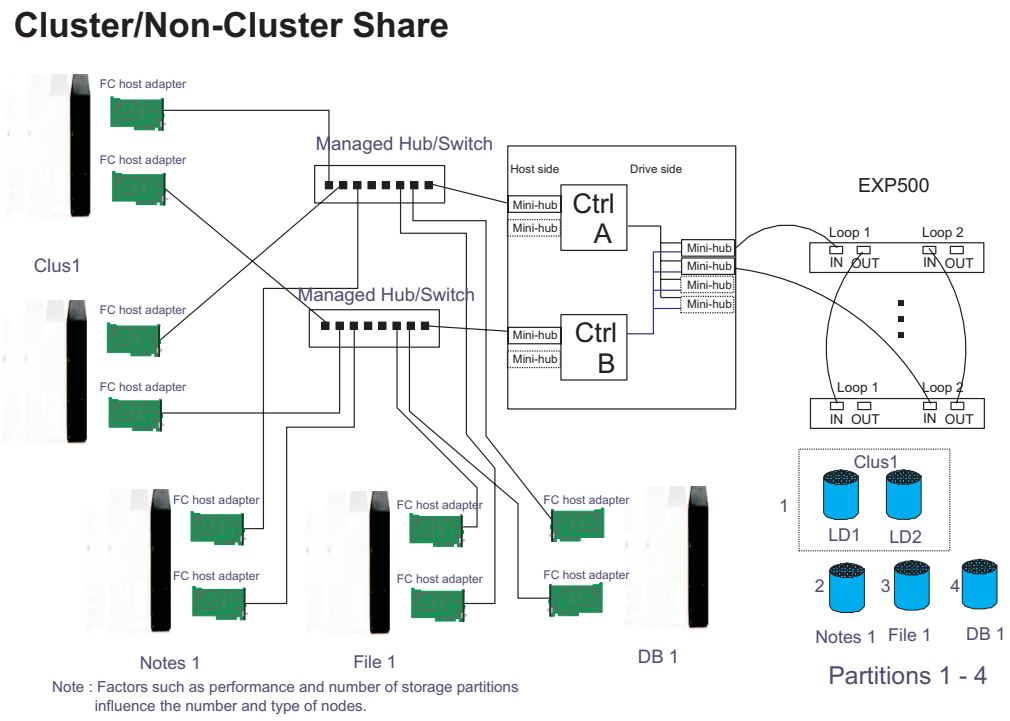


Figure 36. Type 3552 IBM FAStT500 RAID Controller Cluster/Non-cluster Share

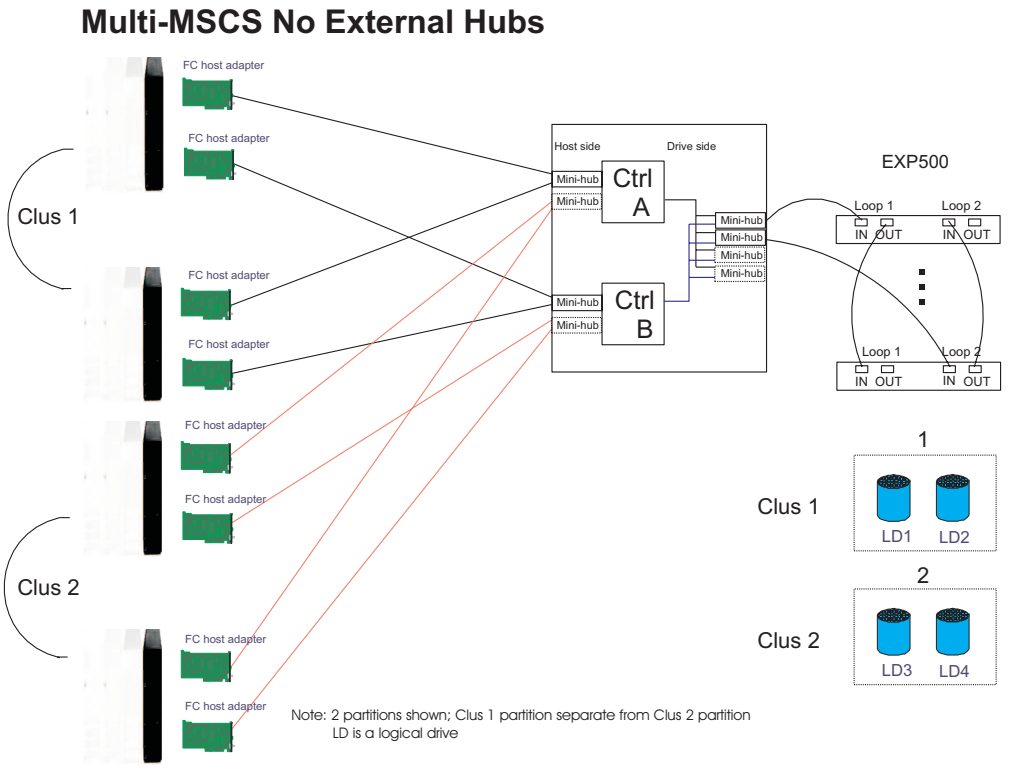
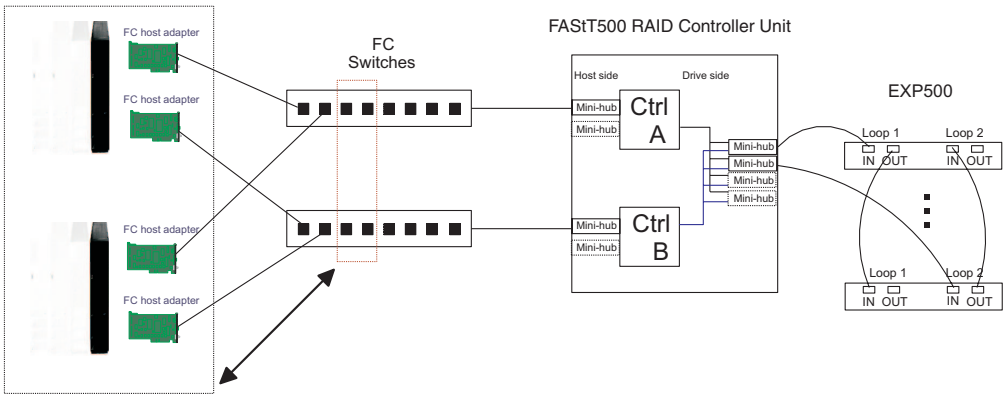


Figure 37. Type 3552 IBM FAStT500 RAID Controller Multi-MSCS No External Hubs

Multi-MSCS extended



Notes:
- Each group of 4 ports on the switches (red dash box) can support one cluster element (black dash box)
- Storage partitioning is used to separate clusters
- 16 port switches allow more clusters but this has to be within performance needs and available partitions

Figure 38. Type 3552 IBM FAStT500 RAID Controller Multi-MSCS Extended

Cornhusker configuration

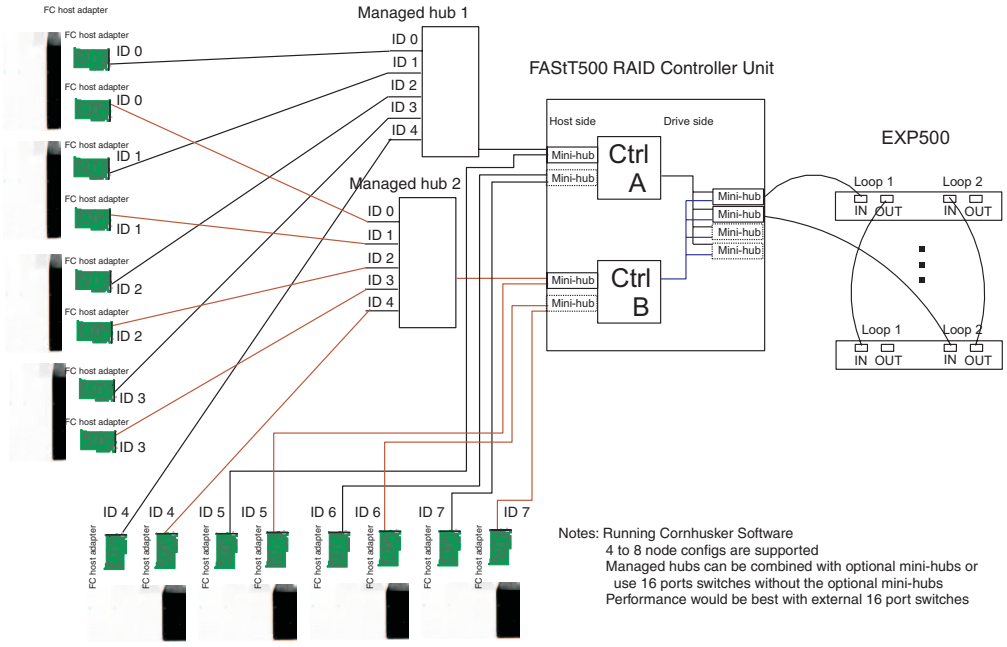


Figure 39. Type 3552 IBM FAStT500 RAID Controller Conhusker Configuration

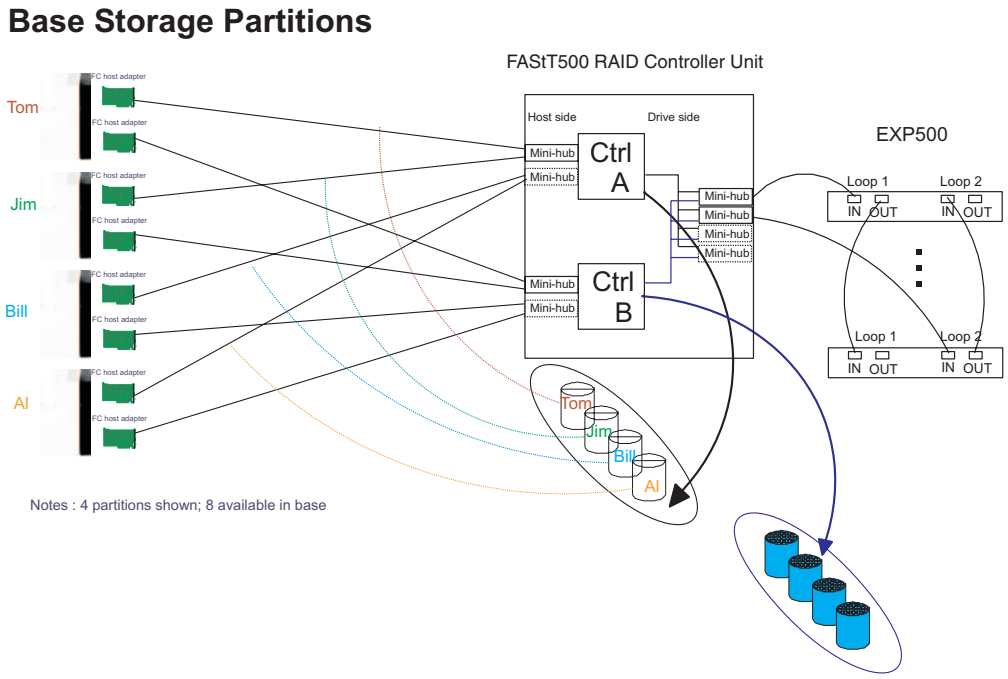


Figure 40. Type 3552 IBM FAStT500 RAID Controller Basic Storage Partitions

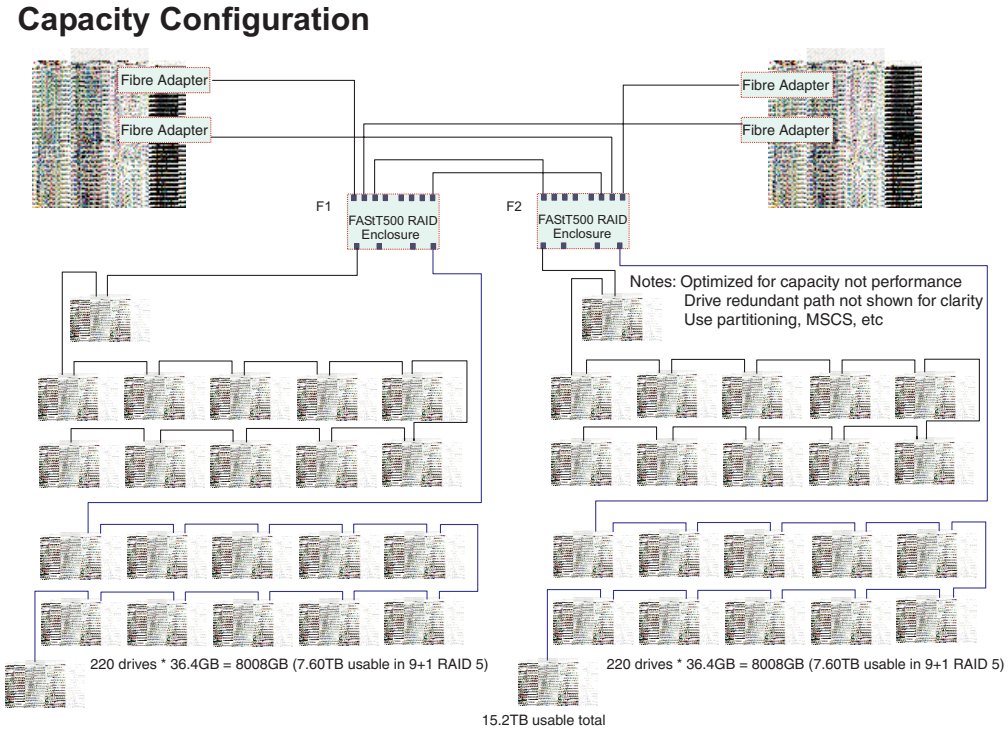


Figure 41. Type 3552 IBM FAStT500 RAID Controller Capacity Configuration

Capacity Configuration - host detail

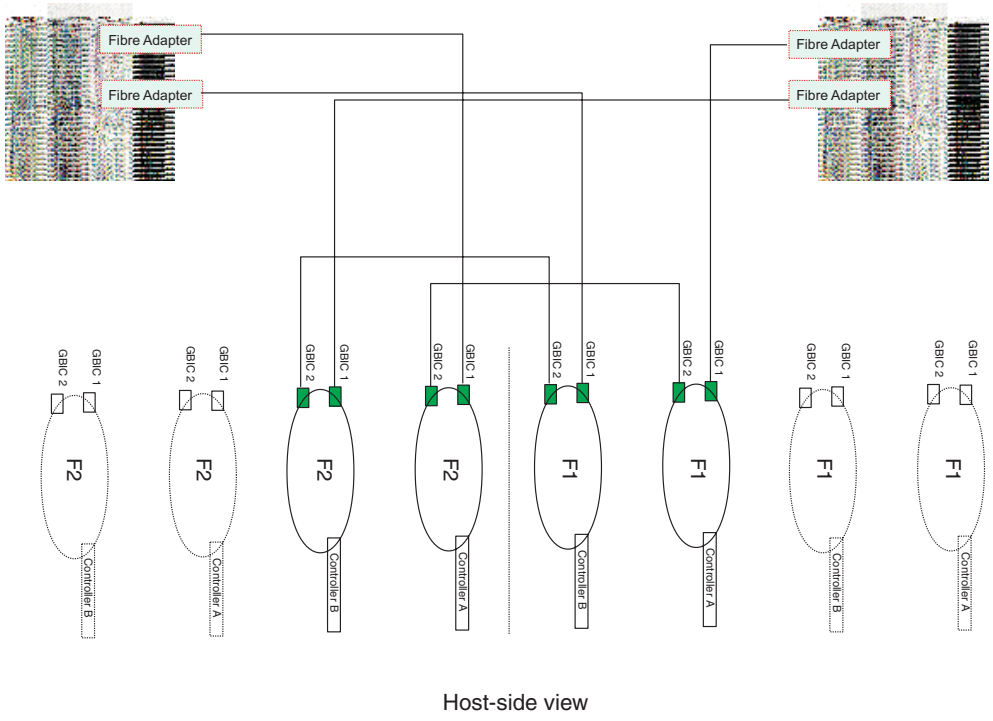


Figure 42. Type 3552 IBM FAStT500 RAID Controller Capacity Configuration Host Detail

SAN - Using Partitions of Clusters

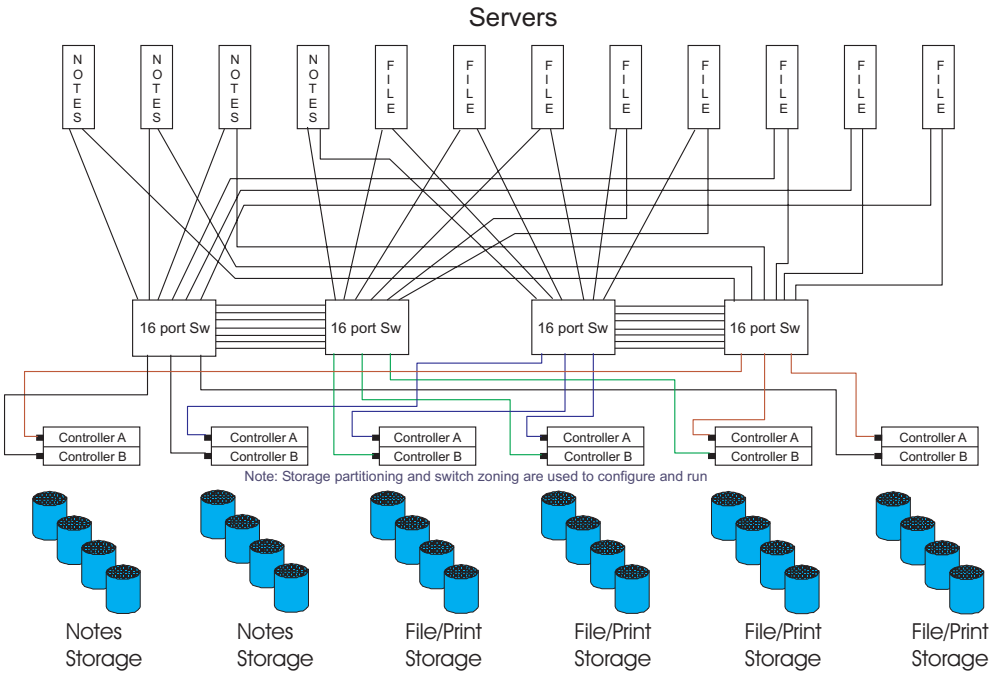


Figure 43. Type 3552 IBM FAStT500 RAID Controller SAN Using Partitions of Clusters

Legato HA/Replication for MSCS

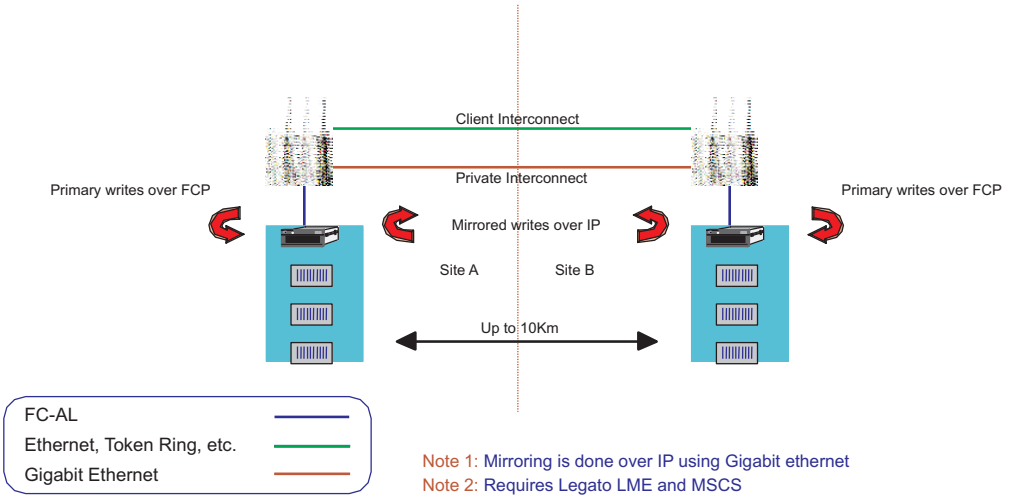


Figure 44. Type 3552 IBM FAStT500 RAID Controller Legato HA/Replication for MS

Symptom-to-FRU index

The Symptom-to-FRU index (Table 25) lists symptoms and the possible causes. The most likely cause is listed first.

The PD maps found in Chapter 17, “Problem determination maps”, on page 137 also provide you with additional diagnostic aids.

Note: Always start with the “General checkout” on page 49. For IBM devices not supported by this index, refer to the manual for that device.

Note: Do *not* look directly into any fiber cable or GBIC optical output. Read “Safety” on page xi. To view an optical signal, use a mirror to view the reflected light.

Table 25. Symptom-to-FRU index for Type 3552 FAStT500 RAID controller

Problem	FRU/Action
Controller LED (front cover) is on.	1. **Reseat Controller CRU.** 2. Place Controller online using SM7 GUI. 3. If in passive mode, check Fibre path/GBIC. 4. Controller CRU
Software issued a controller error message.	1. **Check Controller Fan** 2. Controller CRU

Table 25. Symptom-to-FRU index for Type 3552 FAStT500 RAID controller (continued)

Problem	FRU/Action
Software errors occur when attempting to access controllers or drives.	1. **Check appropriate software and documentation to make sure the system is set up correctly and the proper command was executed.** 2. Power to the Controller 3. Interface cables 4. ID settings 5. Controller 6. Drive 7. Controller backpanel
Fan LED (front cover) is on.	1. **Power supply fan CRU** 2. Controller fan CRU
Controller and Fan fault LEDs (front cover) are on.	1. **Check both Fan and Controller CRUs for fault LED and replace faulty CRU.**
Fault-A or Fault-B LED (battery CRU) is on.	1. **Battery CRU**
Full Charge-A or Full Charge-B LED (battery CRU) is off.	1. **Power-on Controller and allow batteries to charge for 24 hours until the Full Charge LEDs are on.** 2. Battery CRU 3. Both power supplies
No power to controller (all power LEDs off).	1. **Check power switches and power cords.** 2. Power supplies
Power Supply LED is off.	1. **Check and reseat power supply.** 2. Check for overheating. Wait ten minutes for the power supply CRU to cool down. 3. Power supply CRU
Power Supply CRUs LED are on, but all other CRU LEDs are off.	1. **DC power harness**

Parts listing

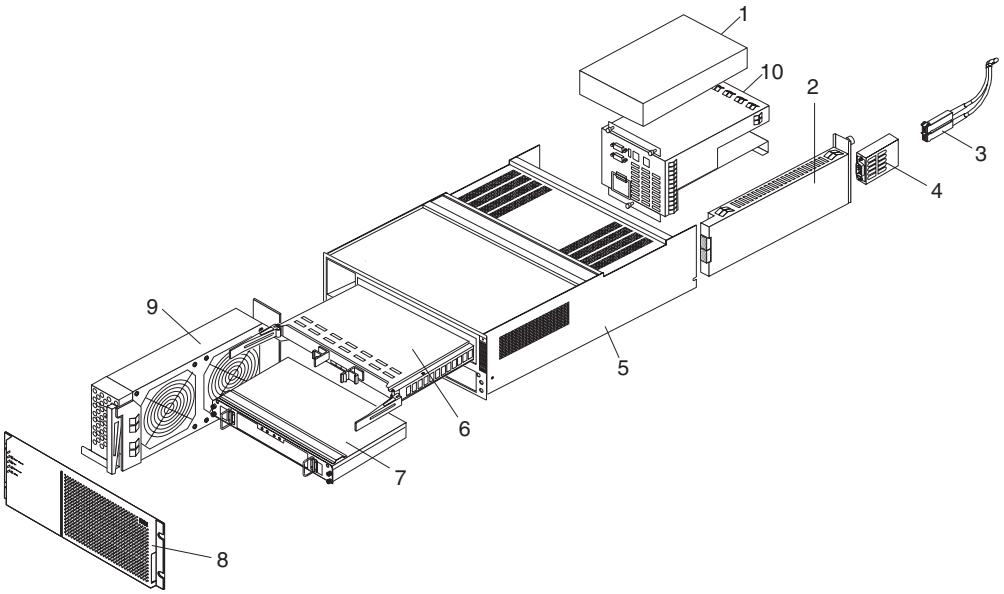


Figure 45. Type 3552 FAStT500 RAID controller parts listing

Index	Fibre Channel RAID Controller (Type 3552)	FRU
1	175W-Watt Power Supply	01K6743
2	GBIC Card Assembly	37L0096
3	Optical Cable - 1 Meter	37L0083
3	Optical Cable - 5 Meters	03K9202
3	Optical Cable - 25 Meters	03K9204
4	Short Wave GBIC	03K9206
4	Long Wave GBIC	03K9208
5	Frame Assembly with Midplane	37L0093
6	RAID Controller	37L0098
7	Battery Backup Assembly	37L0099
8	Bezel Assembly	10L7043
9	Front Fan Assembly (Controller CRU Fan)	37L0094
10	Rear Fan Assembly	37L0102
	IBM FAStT FC Host Adapter	00N6881
	Fibre Channel Host Adapter	09N7292
	256 MB DIMM	37L0095
	Battery Cable	03K9285
	Blank Cannister	37L0098
	Line Cord Jumper, High Voltage	36L8886
	Power Cable	37L0101
	Miscellaneous Hardware Kit	37L0092
	Rail Kit	37L0085
	Fibre Channel Host Adapter (optional)	19K1273

Power cords

Table 26. Type 3552 FAStT500 RAID controller power cords

IBM power cord part number	Used in these countries and regions
13F9940	Argentina, Australia, China (PRC), New Zealand, Papua New Guinea, Paraguay, Uruguay, Western Samoa
13F9979	Afghanistan, Algeria, Andorra, Angola, Austria, Belgium, Benin, Bulgaria, Burkina Faso, Burundi, Cameroon, Central African Rep., Chad, Czech Republic, Egypt, Finland, France, French Guiana, Germany, Greece, Guinea, Hungary, Iceland, Indonesia, Iran, Ivory Coast, Jordan, Lebanon, Luxembourg, Macao S.A.R. of the PRC, Malagasy, Mali, Martinique, Mauritania, Mauritius, Monaco, Morocco, Mozambique, Netherlands, New Caledonia, Niger, Norway, Poland, Portugal, Romania, Senegal, Slovakia, Spain, Sudan, Sweden, Syria, Togo, Tunisia, Turkey, former USSR, Vietnam, former Yugoslavia, Zaire, Zimbabwe
13F9997	Denmark
14F0015	Bangladesh, Burma, Pakistan, South Africa, Sri Lanka
14F0033	Antigua, Bahrain, Brunei, Channel Islands, Cyprus, Dubai, Fiji, Ghana, Hong Kong S.A.R. of the PRC, India, Iraq, Ireland, Kenya, Kuwait, Malawi, Malaysia, Malta, Nepal, Nigeria, Polynesia, Qatar, Sierra Leone, Singapore, Tanzania, Uganda, United Kingdom, Yemen, Zambia
14F0051	Liechtenstein, Switzerland
14F0069	Chile, Ethiopia, Italy, Libya, Somalia
14F0087	Israel
1838574	Thailand
6952300	Bahamas, Barbados, Bermuda, Bolivia, Brazil, Canada, Cayman Islands, Colombia, Costa Rica, Dominican Republic, Ecuador, El Salvador, Guatemala, Guyana, Haiti, Honduras, Jamaica, Japan, Korea (South), Liberia, Mexico, Netherlands Antilles, Nicaragua, Panama, Peru, Philippines, Saudi Arabia, Suriname, Taiwan, Trinidad (West Indies), United States of America, Venezuela

Chapter 9. Type 1742 FAStT700 Fibre Channel Storage Server

Note: The problem determination (PD) maps found in Chapter 17, “Problem determination maps”, on page 137 provide you with additional diagnostic aids.

The IBM FAStT700 Fibre Channel Storage Server provides dual, redundant controllers with fibre channel interfaces to both the host and drive loops. The FAStT700 Storage Server has redundant cooling, redundant power, and battery backup of the controller cache.

Designed to provide maximum host and drive-side redundancy, the FAStT700 Storage Server supports direct attachment of up to four hosts containing two host adapters each. Using external fibre channel managed hubs and switches in conjunction with the FAStT700 Storage Server, you can attach up to 64 hosts with two adapters each to a FAStT700 storage server.

General checkout

Use the indicator lights, the Symptom-to-FRU index, and the connected server HMM to diagnose problems.

The problem determination (PD) maps found in Chapter 17, “Problem determination maps”, on page 137 provide you with additional diagnostic aids.

Checking the indicator lights

The FAStT700 Storage Server indicator lights display the status of the FAStT700 Storage Server and its components. Green indicator lights mean normal operating status; amber indicator lights mean a possible failure.

It is important that you check all the indicator lights on the front and back of the controller unit after you turn on the power. After you turn on the power, the indicator lights might blink intermittently. Wait until the FAStT700 Storage Server completes its power up before checking for faults. It can take up to 15 minutes for the battery to complete its self-test and up to 24 hours to fully charge, particularly after an unexpected power loss of more than a few minutes.

The indicator lights for the components of the FAStT700 Storage Server are described in the following sections.

Storage server indicator lights

The storage server has five indicator lights, as shown in Figure 46 on page 66. To view the storage server indicator lights, you do not have to remove the FAStT700 Storage Server bezel.

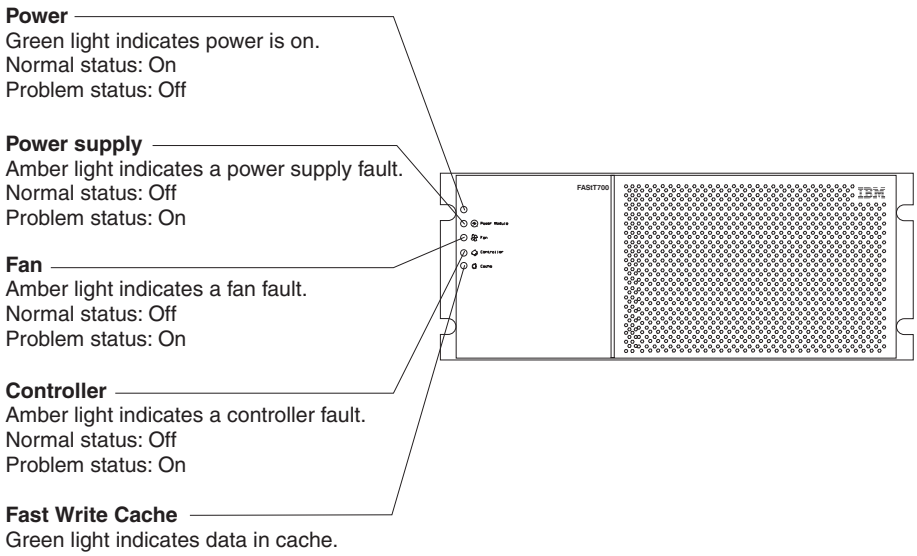


Figure 46. Type 1742 FAStT700 Storage Server Indicator Lights

Table 27 describes the storage server indicator lights.

Table 27. Type 1742 FAStT700 storage server indicator lights

Indicator light	Color	Normal operation	Problem indicator	Possible conditions indicated by the problem indicator[1]
Power	Green	On	Off	• No power to FAStT700 Storage Server • No power to storage subsystem • Cables are loose or the switches are off • Power supply has failed, is missing, or is not fully seated in FAStT700 Storage Server • Overtemperature condition
Power supply fault	Amber	Off	On	• Power supply has failed or if the Power supply is turned off, disconnected, or not fully seated in FAStT700 Storage Server • Overtemperature • No power to FAStT700 Storage Server or storage subsystem (all indicator lights are off)
Storage server fan fault	Amber	Off	On	• Storage server fan has failed • Fan and communications module is missing, unplugged, or has failed • Circuitry failure • Overtemperature condition
Controller fault	Amber	Off	On	Controller has failed; one or more memory modules failed (SIMMs or DIMMs)
Fast write cache	Green	Steady or blinking[2]	Software dependent[1]	Normal operation is off if: • Cache is not enabled • Battery is not ready

[1] Always use the storage-management software to identify the failure.
[2] The fast write cache indicator light is on when there is data in cache and blinks during a fast write operation.

RAID controller indicator lights

Each RAID controller has ten indicator lights: one power, one fault, and eight status lights, as shown in Figure 47.

Note: To view the RAID controller indicator lights, remove the FAStT700 Storage Server bezel.

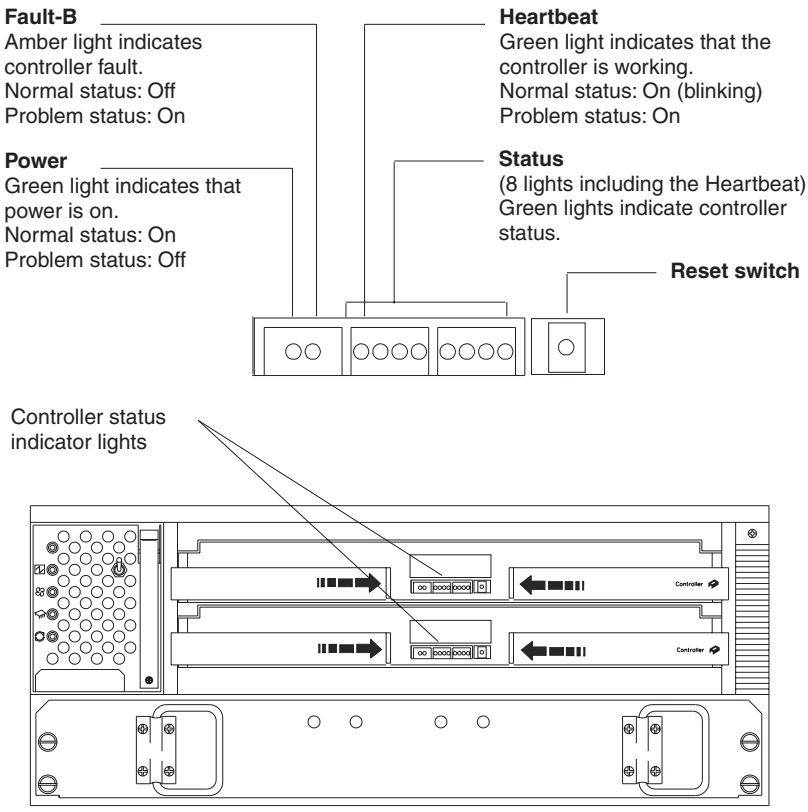


Figure 47. RAID Controller Indicator Lights

Table 28 describes the RAID controller indicator lights.

Table 28. RAID controller indicator lights

Indicator light	Color	Normal operation	Problem indicator	Possible conditions indicated by the problem indicator[1]
Power	Green	On	Off	• No power to storage subsystem • Cables are loose or the switches are off • Power supply has failed, is missing, or is not fully seated • Overtemperature condition
Fault3	Amber	Off	On	Controller failure; controller fault condition
Heartbeat	Green	Blinking	Not blinking	No controller activity
Status3 (seven lights, not including Heartbeat)	Green	Various patterns depending on the condition[2]	Various patterns depending on the condition[2]	If any status indicator lights are lit and the controller is not off line, there is a memory fault indicating that the controller CRU has failed.

Table 28. RAID controller indicator lights (continued)

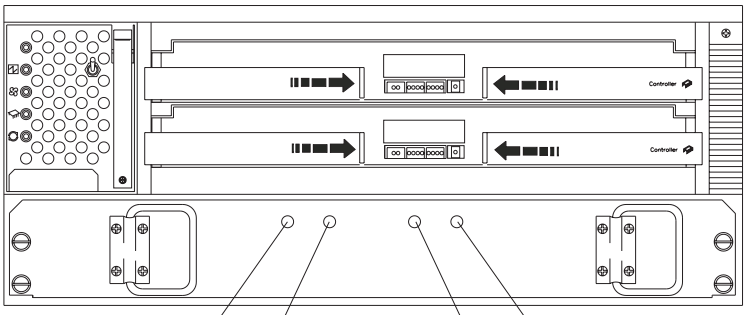
Indicator light	Color	Normal operation	Problem indicator	Possible conditions indicated by the problem indicator[1]

[1] Always use the storage-management software to identify the failure.
[2] There are eight status lights (the Heartbeat and seven others) that glow in various patterns, depending on the controller status.
[3]If the controller is off line, all of the indicator lights will be lit. This does not indicate failure.

Battery indicator lights

The battery has four indicator lights as shown in Figure 48.

Note: To view the battery indicator lights, remove the FAStT700 Storage Server bezel.



Fault-B
Amber light indicates a fault in the left battery bank.
Normal status: Off
Problem status: On

Full Charge-A
Green light indicates the right battery bank is fully charged.
Normal status: On
Problem status: Off
Changing status: Blinking

Full Charge-B
Green light indicates the left battery bank is fully charged.
Normal status: On
Problem status: Off
Changing status: Blinking

Fault-A
Amber light indicates a fault in the left battery bank.
Normal status: Off
Problem status: On

Figure 48. Battery Indicator Lights

Table 29 describes the battery indicator lights.

Table 29. Battery indicator lights

Indicator light	Color	Normal operation	Problem indicator	Possible conditions indicated by the problem indicator[1]
Fault-A or Fault-B	Amber	Off	On	• Left or right battery bank has failed • Battery is either discharged or defective
Full Charge-A or Full Charge-B	Green	On[2]	Off	• Left or right battery bank is not fully charged • Power has been off for an extended period and has drained battery power • Batteries are weak

[1] Always use the storage-management software to identify the failure.
[2] If either Full Charge-A or Full Charge-B indicator light is blinking, the battery is in the process of charging.

Fan and communications module indicator light

The fan and communications module has one indicator light as shown in Figure 49.

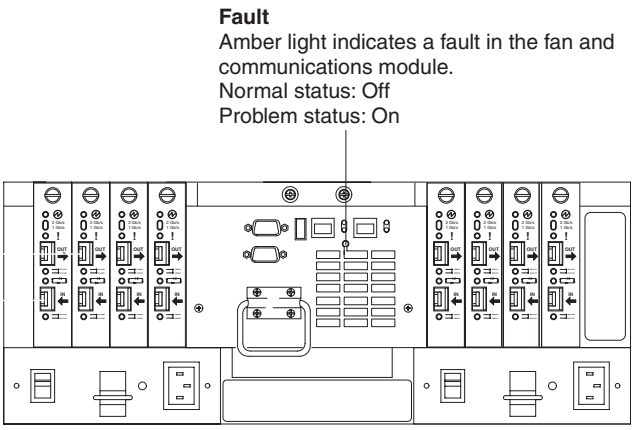


Figure 49. Fan and Communciations Module Indicator Light

Table 30 describes the fan and communications module indicator light.

Table 30. Fan and communications module indicator light

Indicator light	Color	Normal operation	Problem indicator	Possible conditions indicated by the problem indicator[1]
Fan and communication fault	Amber	Off	On	• Fan and communications module has failed or is installed incorrectly • Overtemperature condition

[1] Always use the storage-management software to identify the failure.

Power supply indicator light

The power supply has one indicator light, as shown in Figure 50.

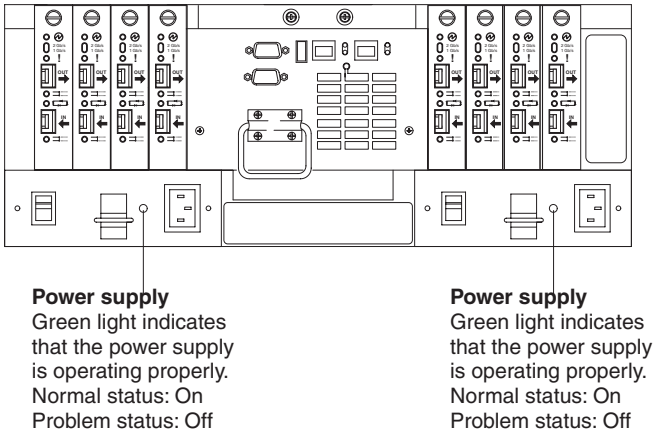


Figure 50. Power Supply Indicator Light

Table 31 on page 70 describes the power supply indicator light.

Table 31. Power supply indicator light

Indicator light	Color	Normal operation	Problem indicator	Possible conditions indicated by the problem indicator[1]
Power supply	Green	On	Off	• No power to FAStT700 Storage Server • No power to storage subsystem • Power supply has failed or is turned off • Overtemperature condition

[1] Always use the storage-management software to identify the failure.

Mini hub indicator lights

There are five host-side mini hub indicator lights and five drive-side mini hub indicator lights. Figure 51 shows the host-side indicator lights. The drive side indicator lights are the same; however, the possible conditions indicated by the problem indicators (described in Table 32) might be different.

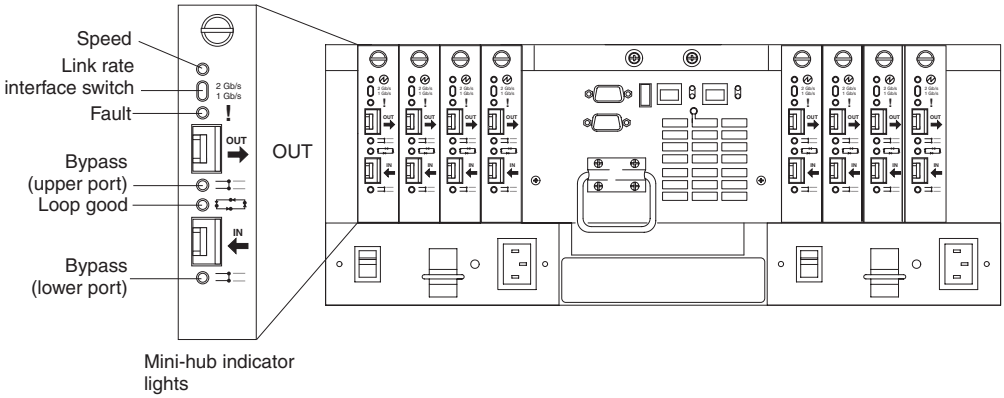


Figure 51. Mini-hub Indicator Lights

Table 32 describes describes the indicator light status when there are fibre channel connections between host-side and drive-side mini hubs.

Table 32. Host-side and drive-side mini hub indicator lights

Icon	Indicator light	Color	Normal operation	Problem indicator	Possible condition indicated by the problem indicator
	Speed	Green	On for 2 Gb Off for 1 Gb		Light on indicates data transfer rate of 2 Gb per second. Light off indicates data transfer rate of 1 Gb per second.
!	Fault	Amber	Off	On	Mini hub or SFP module has failed **Note:** If a host-side mini hub is not connected to a controller, this fault light is always lit.

Table 32. Host-side and drive-side mini hub indicator lights (continued)

Icon	Indicator light	Color	Normal operation	Problem indicator	Possible condition indicated by the problem indicator
	Bypass (upper port)	Amber	Off	On	• Upper mini hub port is bypassed • Mini hub or SFP module has failed, is loose, or is missing • Fiber-optic cables are damaged **Note:** When there are two functioning SFP modules installed into the mini hub ports and there are no fibre channel cables connected to them, the bypass indicator is lit. If there is only one functioning SFP module installed in a host-side mini hub port and there are no fibre channel cables connected to it, the indicator light will not be lit. However, the drive-side mini hub bypass indicator light will be lit when there is one SFP module installed in the mini hub and the mini hub has no fibre channel connection.
	Loop good	Green	On	Off	• The loop is not operational, no devices are connected • Mini hub has failed or a faulty device is connected to the mini hub • If there is no SFP module installed, the indicator will be lit • If one functioning SFP module is installed in the host-side mini hub port and there is no fibre channel cable connected to it, the loop good indicator light will not be lit. If one functioning SFP module is installed in the drive-side mini hub port and there is no fibre channel cable connected to it, the loop good indicator light will be lit. • Drive enclosure has failed (drive-side mini hub only)

Table 32. Host-side and drive-side mini hub indicator lights (continued)

Icon	Indicator light	Color	Normal operation	Problem indicator	Possible condition indicated by the problem indicator
	Bypass (lower port)	Amber	Off	On	• Lower mini hub port is bypassed; there are no devices connected • Mini hub or SFP module has failed or is loose • Fiber-optic cables are damaged **Note:** When there are two functioning SFP modules installed into the mini hub port and there are no fibre channel cables connected to them, the bypass indicator light is lit. If there is only one functioning SFP module installed in a host-side mini hub and there are no fibre channel cables connected to it, the indicator light is not lit. However, the drive-side mini hub bypass indicator light will be lit when there is one functioning SFP module installed in the mini hub port and the mini hub has no fibre channel cables connected to it.

Using the diagnostic hardware

The FAStT700 Fibre Channel Storage Server comes with a wrap-plug adapter and LC coupler. The wrap-plug adapter and LC coupler are used to identify Fibre path problems. The loopback test is described in Chapter 18, “Introduction to FAStT MSJ”, on page 173. For information on the sendEcho test, see Chapter 24, “PD hints — Performing sendEcho tests”, on page 275.

Symptom-to-FRU index

The Symptom-to-FRU index (Table 33) lists symptoms and the possible causes. The most likely cause is listed first.

The problem determination (PD) maps found in Chapter 17, “Problem determination maps”, on page 137 provide you with additional diagnostic aids.

Table 33. Symptom-to-FRU index for FAStT700 RAID controller

Problem	FRU/Action
Controller LED (front cover) is on.	1. **Reseat Controller CRU.** 2. Place Controller online using SM7 GUI. 3. If in passive mode, check Fibre path/GBIC. 4. Controller CRU

Table 33. Symptom-to-FRU index for FAStT700 RAID controller (continued)

Problem	FRU/Action
Software issued a controller error message.	1. **Check Controller Fan** 2. Controller CRU
Software errors occur when attempting to access controllers or drives.	1. **Check appropriate software and documentation to make sure the system is set up correctly and the proper command was executed.** 2. Power to the Controller 3. Interface cables 4. ID settings 5. Controller 6. Drive 7. Controller backpanel
Fan LED (front cover) is on.	1. **Power supply fan CRU** 2. Controller fan CRU
Controller and Fan fault LEDs (front cover) are on.	1. **Check both Fan and Controller CRUs for fault LED and replace faulty CRU.**
Fault-A or Fault-B LED (battery CRU) is on.	1. **Battery CRU**
Full Charge-A or Full Charge-B LED (battery CRU) is off.	1. **Power-on Controller and allow batteries to charge for 24 hours until the Full Charge LEDs are on.** 2. Battery CRU 3. Both power supplies
No power to controller (all power LEDs off).	1. **Check power switches and power cords.** 2. Power supplies
Power Supply LED is off.	1. **Check and reseat power supply.** 2. Check for overheating. Wait ten minutes for the power supply CRU to cool down. 3. Power supply CRU
Power Supply CRUs LED are on, but all other CRU LEDs are off.	1. **DC power harness**

Parts listing

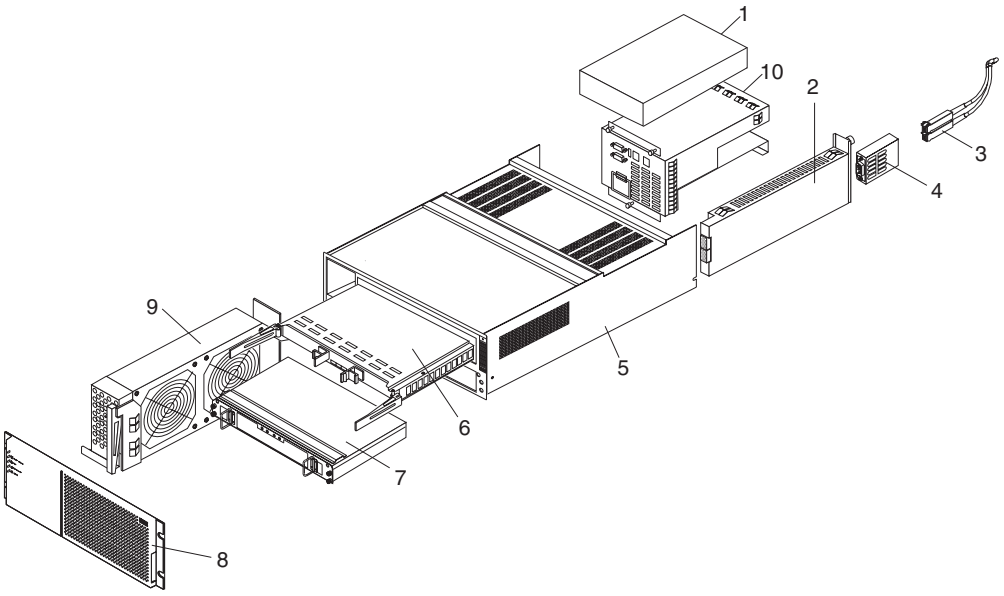


Figure 52. FAStT700 Parts Listing

Index	Fibre Channel RAID Controller (Type 3552)	FRU
1	175W-Watt Power Supply	01K6743
2	Mini hub Card Assembly	19K1270
3	Optical Cable - 1 Meter	19K1265
3	Optical Cable - 5 Meters	19K1266
3	Optical Cable - 25 Meters	19K1267
	LC-SC Adapter	19K1250
4	Short Wave GBIC	19K1280
4	Long Wave GBIC	19K1281
5	Frame Assembly with Midplane	19K1277
6	RAID Card	19K1284
7	Battery Backup Assembly	37L0099
8	Bezel Assembly	19K1279
9	Front Fan Assembly (Controller CRU Fan)	37L0094
10	Rear Fan Assembly	37L0102
	512 MB 100 Mhz DIMM	19K1283
	Battery Cable	03K9285
	Blank Cannister	37L0100
	Line Cord Jumper, High Voltage	36L8886
	Power Cable	37L0101
	Miscellaneous Hardware Kit	37L0092
	Rail Kit	37L0085
	Fibre Channel Host Adapter (optional)	19K1273

Power cords

Table 34. Power cords (Type 1742 FAStT700 Storage Server)

IBM power cord part number	Used in these countries and regions
13F9940	Argentina, Australia, China (PRC), New Zealand, Papua New Guinea, Paraguay, Uruguay, Western Samoa
13F9979	Afghanistan, Algeria, Andorra, Angola, Austria, Belgium, Benin, Bulgaria, Burkina Faso, Burundi, Cameroon, Central African Rep., Chad, Czech Republic, Egypt, Finland, France, French Guiana, Germany, Greece, Guinea, Hungary, Iceland, Indonesia, Iran, Ivory Coast, Jordan, Lebanon, Luxembourg, Macao S.A.R. of the PRC, Malagasy, Mali, Martinique, Mauritania, Mauritius, Monaco, Morocco, Mozambique, Netherlands, New Caledonia, Niger, Norway, Poland, Portugal, Romania, Senegal, Slovakia, Spain, Sudan, Sweden, Syria, Togo, Tunisia, Turkey, former USSR, Vietnam, former Yugoslavia, Zaire, Zimbabwe
13F9997	Denmark
14F0015	Bangladesh, Burma, Pakistan, South Africa, Sri Lanka
14F0033	Antigua, Bahrain, Brunei, Channel Islands, Cyprus, Dubai, Fiji, Ghana, Hong Kong S.A.R. of the PRC, India, Iraq, Ireland, Kenya, Kuwait, Malawi, Malaysia, Malta, Nepal, Nigeria, Polynesia, Qatar, Sierra Leone, Singapore, Tanzania, Uganda, United Kingdom, Yemen, Zambia
14F0051	Liechtenstein, Switzerland
14F0069	Chile, Ethiopia, Italy, Libya, Somalia
14F0087	Israel
1838574	Thailand
6952300	Bahamas, Barbados, Bermuda, Bolivia, Brazil, Canada, Cayman Islands, Colombia, Costa Rica, Dominican Republic, Ecuador, El Salvador, Guatemala, Guyana, Haiti, Honduras, Jamaica, Japan, Korea (South), Liberia, Mexico, Netherlands Antilles, Nicaragua, Panama, Peru, Philippines, Saudi Arabia, Suriname, Taiwan, Trinidad (West Indies), United States of America, Venezuela

Chapter 10. Type 1742 FAStT900 Fibre Channel Storage Server

Note: The problem determination (PD) maps found in Chapter 17, “Problem determination maps”, on page 137 provide you with additional diagnostic aids.

The IBM FAStT900 Fibre Channel Storage Server provides dual, redundant controllers with fibre channel interfaces to both the host and drive loops. The FAStT900 Storage Server has redundant cooling, redundant power, and battery backup of the controller cache.

Designed to provide maximum host and drive-side redundancy, the FAStT900 Storage Server supports direct attachment of up to four hosts containing two host adapters each. Using external fibre channel managed hubs and switches in conjunction with the FAStT900 Storage Server, you can attach up to 64 hosts with two adapters each to a FAStT900 storage server.

General checkout

Use the indicator lights, the Symptom-to-FRU index, and the connected server HMM to diagnose problems.

The problem determination (PD) maps found in Chapter 17, “Problem determination maps”, on page 137 provide you with additional diagnostic aids.

Checking the indicator lights

The FAStT900 Storage Server indicator lights display the status of the FAStT900 Storage Server and its components. Green indicator lights mean normal operating status; amber indicator lights mean a possible failure.

It is important that you check all the indicator lights on the front and back of the controller unit after you turn on the power. After you turn on the power, the indicator lights might blink intermittently. Wait until the FAStT900 Storage Server completes its power up before checking for faults. It can take up to 15 minutes for the battery to complete its self-test and up to 24 hours to fully charge, particularly after an unexpected power loss of more than a few minutes.

The indicator lights for the components of the FAStT900 Storage Server are described in the following sections.

Storage server indicator lights

The storage server has five indicator lights, as shown in Figure 53 on page 78. To view the storage server indicator lights, you do not have to remove the FAStT900 Storage Server bezel.

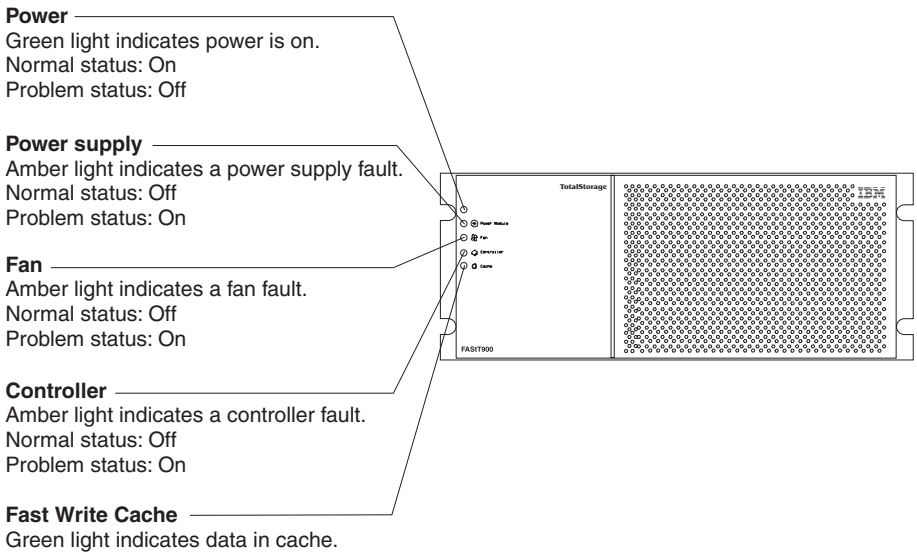


Figure 53. Type 1742 FAStT900 Storage Server Indicator Lights

Table 27 on page 66 describes the storage server indicator lights.

Table 35. Type 1742 FAStT900 storage server indicator lights

Indicator light	Color	Normal operation	Problem indicator	Possible conditions indicated by the problem indicator[1]
Power	Green	On	Off	• No power to FAStT900 Storage Server • No power to storage subsystem • Cables are loose or the switches are off • Power supply has failed, is missing, or is not fully seated in FAStT900 Storage Server • Overtemperature condition
Power supply fault	Amber	Off	On	• Power supply has failed or if the Power supply is turned off, disconnected, or not fully seated in FAStT900 Storage Server • Overtemperature • No power to FAStT900 Storage Server or storage subsystem (all indicator lights are off)
Storage server fan fault	Amber	Off	On	• Storage server fan has failed • Fan and communications module is missing, unplugged, or has failed • Circuitry failure • Overtemperature condition
Controller fault	Amber	Off	On	Controller has failed; one or more memory modules failed (SIMMs or DIMMs)
Fast write cache	Green	Steady or blinking[2]	Software dependent[1]	Normal operation is off if: • Cache is not enabled • Battery is not ready

[1] Always use the storage-management software to identify the failure.
[2] The fast write cache indicator light is on when there is data in cache and blinks during a fast write operation.

RAID controller indicator lights

Each RAID controller has ten indicator lights: one power, one fault, and eight status lights, as shown in Figure 54.

Note: To view the RAID controller indicator lights, remove the FAStT900 Storage Server bezel.

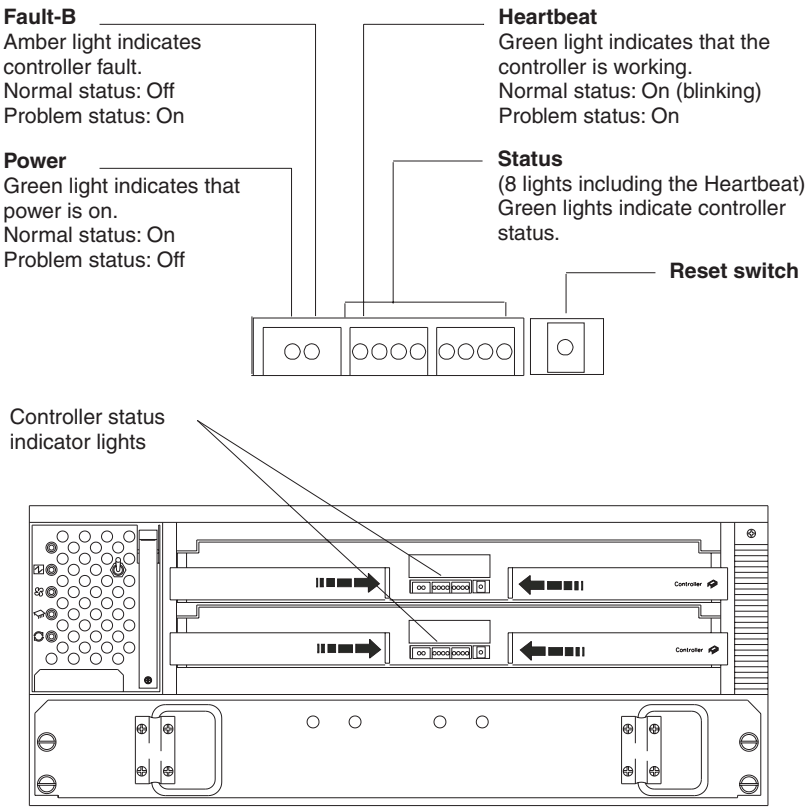


Figure 54. RAID Controller Indicator Lights

Table 28 on page 67 describes the RAID controller indicator lights.

Table 36. RAID controller indicator lights

Indicator light	Color	Normal operation	Problem indicator	Possible conditions indicated by the problem indicator[1]
Power	Green	On	Off	• No power to storage subsystem • Cables are loose or the switches are off • Power supply has failed, is missing, or is not fully seated • Overtemperature condition
Fault3	Amber	Off	On	Controller failure; controller fault condition
Heartbeat	Green	Blinking	Not blinking	No controller activity
Status3 (seven lights, not including Heartbeat)	Green	Various patterns depending on the condition[2]	Various patterns depending on the condition[2]	If any status indicator lights are lit and the controller is not off line, there is a memory fault indicating that the controller CRU has failed.

Table 36. RAID controller indicator lights (continued)

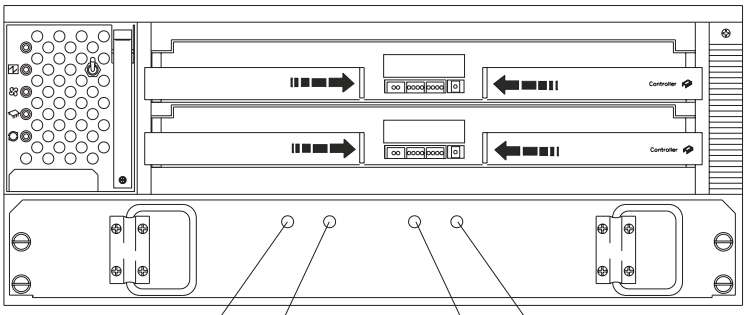
Indicator light	Color	Normal operation	Problem indicator	Possible conditions indicated by the problem indicator[1]

[1] Always use the storage-management software to identify the failure.
[2] There are eight status lights (the Heartbeat and seven others) that glow in various patterns, depending on the controller status.
[3]If the controller is off line, all of the indicator lights will be lit. This does not indicate failure.

Battery indicator lights

The battery has four indicator lights as shown in Figure 56 on page 81.

Note: To view the battery indicator lights, remove the FAStT900 Storage Server bezel.



Fault-B
Amber light indicates a fault in the left battery bank.
Normal status: Off
Problem status: On

Full Charge-A
Green light indicates the right battery bank is fully charged.
Normal status: On
Problem status: Off
Changing status: Blinking

Full Charge-B
Green light indicates the left battery bank is fully charged.
Normal status: On
Problem status: Off
Changing status: Blinking

Fault-A
Amber light indicates a fault in the left battery bank.
Normal status: Off
Problem status: On

Figure 55. Battery Indicator Lights

Table 29 on page 68 describes the battery indicator lights.

Table 37. Battery indicator lights

Indicator light	Color	Normal operation	Problem indicator	Possible conditions indicated by the problem indicator[1]
Fault-A or Fault-B	Amber	Off	On	• Left or right battery bank has failed • Battery is either discharged or defective
Full Charge-A or Full Charge-B	Green	On[2]	Off	• Left or right battery bank is not fully charged • Power has been off for an extended period and has drained battery power • Batteries are weak

[1] Always use the storage-management software to identify the failure.
[2] If either Full Charge-A or Full Charge-B indicator light is blinking, the battery is in the process of charging.

Fan and communications module indicator light

The fan and communications module has one indicator light as shown in Figure 56.

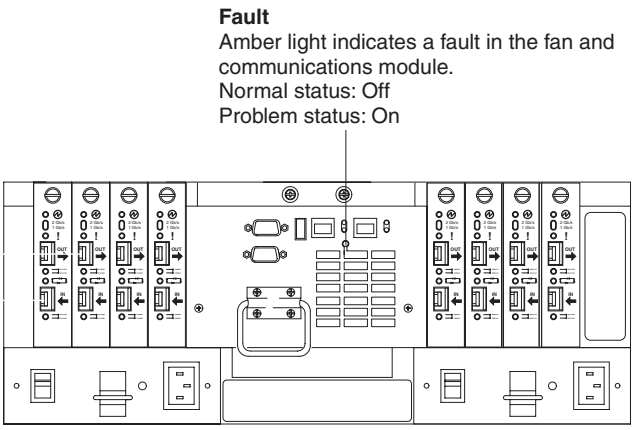


Figure 56. Fan and Communciations Module Indicator Light

Table 30 on page 69 describes the fan and communications module indicator light.

Table 38. Fan and communications module indicator light

Indicator light	Color	Normal operation	Problem indicator	Possible conditions indicated by the problem indicator[1]
Fan and communication fault	Amber	Off	On	• Fan and communications module has failed or is installed incorrectly • Overtemperature condition

[1] Always use the storage-management software to identify the failure.

Power supply indicator light

The power supply has one indicator light, as shown in Figure 57.

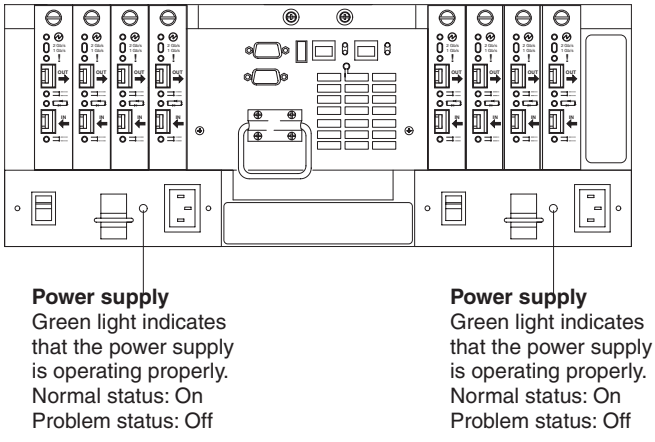


Figure 57. Power Supply Indicator Light

Table 31 on page 70 describes the power supply indicator light.

Table 39. Power supply indicator light

Indicator light	Color	Normal operation	Problem indicator	Possible conditions indicated by the problem indicator[1]
Power supply	Green	On	Off	• No power to FAStT900 Storage Server • No power to storage subsystem • Power supply has failed or is turned off • Overtemperature condition

[1] Always use the storage-management software to identify the failure.

Mini hub indicator lights

There are five host-side mini hub indicator lights and five drive-side mini hub indicator lights. Figure 58 shows the host-side indicator lights. The drive side indicator lights are the same; however, the possible conditions indicated by the problem indicators (described in Table 32 on page 70) might be different.

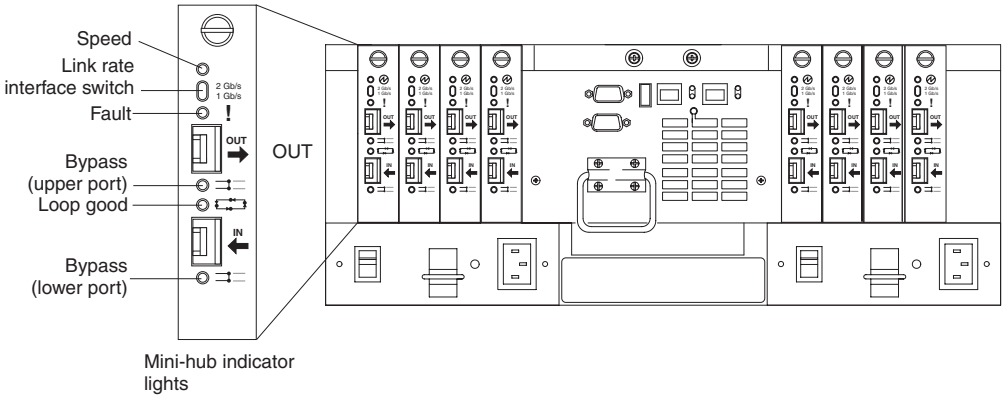


Figure 58. Mini-hub Indicator Lights

Table 32 on page 70 describes describes the indicator light status when there are fibre channel connections between host-side and drive-side mini hubs.

Table 40. Host-side and drive-side mini hub indicator lights

Icon	Indicator light	Color	Normal operation	Problem indicator	Possible condition indicated by the problem indicator
	Speed	Green	On for 2 Gb Off for 1 Gb		Light on indicates data transfer rate of 2 Gb per second. Light off indicates data transfer rate of 1 Gb per second.
!	Fault	Amber	Off	On	Mini hub or SFP module has failed **Note:** If a host-side mini hub is not connected to a controller, this fault light is always lit.

Table 40. Host-side and drive-side mini hub indicator lights (continued)

Icon	Indicator light	Color	Normal operation	Problem indicator	Possible condition indicated by the problem indicator
	Bypass (upper port)	Amber	Off	On	• Upper mini hub port is bypassed • Mini hub or SFP module has failed, is loose, or is missing • Fiber-optic cables are damaged **Note:** When there are two functioning SFP modules installed into the mini hub ports and there are no fibre channel cables connected to them, the bypass indicator is lit. If there is only one functioning SFP module installed in a host-side mini hub port and there are no fibre channel cables connected to it, the indicator light will not be lit. However, the drive-side mini hub bypass indicator light will be lit when there is one SFP module installed in the mini hub and the mini hub has no fibre channel connection.
	Loop good	Green	On	Off	• The loop is not operational, no devices are connected • Mini hub has failed or a faulty device is connected to the mini hub • If there is no SFP module installed, the indicator will be lit • If one functioning SFP module is installed in the host-side mini hub port and there is no fibre channel cable connected to it, the loop good indicator light will not be lit. If one functioning SFP module is installed in the drive-side mini hub port and there is no fibre channel cable connected to it, the loop good indicator light will be lit. • Drive enclosure has failed (drive-side mini hub only)

Table 40. Host-side and drive-side mini hub indicator lights (continued)

Icon	Indicator light	Color	Normal operation	Problem indicator	Possible condition indicated by the problem indicator
	Bypass (lower port)	Amber	Off	On	• Lower mini hub port is bypassed; there are no devices connected • Mini hub or SFP module has failed or is loose • Fiber-optic cables are damaged **Note:** When there are two functioning SFP modules installed into the mini hub port and there are no fibre channel cables connected to them, the bypass indicator light is lit. If there is only one functioning SFP module installed in a host-side mini hub and there are no fibre channel cables connected to it, the indicator light is not lit. However, the drive-side mini hub bypass indicator light will be lit when there is one functioning SFP module installed in the mini hub port and the mini hub has no fibre channel cables connected to it.

Using the diagnostic hardware

The FAStT900 Fibre Channel Storage Server comes with a wrap-plug adapter and LC coupler. The wrap-plug adapter and LC coupler are used to identify Fibre path problems. The loopback test is described in Chapter 18, “Introduction to FAStT MSJ”, on page 173. For information on the sendEcho test, see Chapter 24, “PD hints — Performing sendEcho tests”, on page 275.

Symptom-to-FRU index

The Symptom-to-FRU index (Table 41) lists symptoms and the possible causes. The most likely cause is listed first.

The problem determination (PD) maps found in Chapter 17, “Problem determination maps”, on page 137 provide you with additional diagnostic aids.

Table 41. Symptom-to-FRU index for FAStT900 RAID controller

Problem	FRU/Action
Controller LED (front cover) is on.	1. **Reseat Controller CRU.** 2. Place Controller online using SM7 GUI. 3. If in passive mode, check Fibre path/GBIC. 4. Controller CRU

Table 41. Symptom-to-FRU index for FAStT900 RAID controller (continued)

Problem	FRU/Action
Software issued a controller error message.	1. **Check Controller Fan** 2. Controller CRU
Software errors occur when attempting to access controllers or drives.	1. **Check appropriate software and documentation to make sure the system is set up correctly and the proper command was executed.** 2. Power to the Controller 3. Interface cables 4. ID settings 5. Controller 6. Drive 7. Controller backpanel
Fan LED (front cover) is on.	1. **Power supply fan CRU** 2. Controller fan CRU
Controller and Fan fault LEDs (front cover) are on.	1. **Check both Fan and Controller CRUs for fault LED and replace faulty CRU.**
Fault-A or Fault-B LED (battery CRU) is on.	1. **Battery CRU**
Full Charge-A or Full Charge-B LED (battery CRU) is off.	1. **Power-on Controller and allow batteries to charge for 24 hours until the Full Charge LEDs are on.** 2. Battery CRU 3. Both power supplies
No power to controller (all power LEDs off).	1. **Check power switches and power cords.** 2. Power supplies
Power Supply LED is off.	1. **Check and reseat power supply.** 2. Check for overheating. Wait ten minutes for the power supply CRU to cool down. 3. Power supply CRU
Power Supply CRUs LED are on, but all other CRU LEDs are off.	1. **DC power harness**

Parts listing

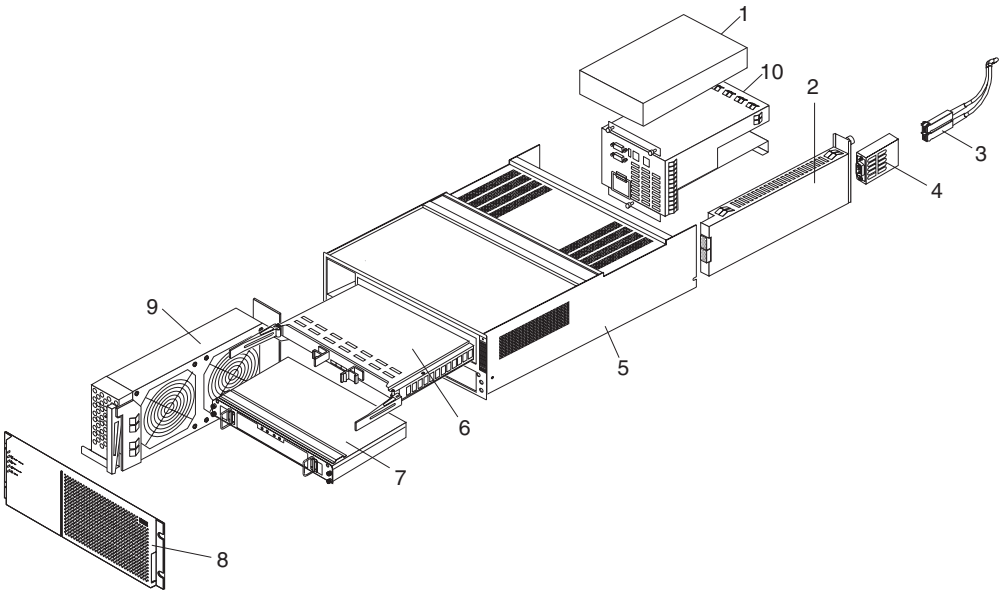


Figure 59. FAStT900 Parts Listing

Index	Fibre Channel RAID Controller (Type 1442)	FRU
1	175W-Watt Power Supply	01K6743
2	Mini hub Card Assembly	19K1270
3	Optical Cable - 1 Meter	19K1265
3	Optical Cable - 5 Meters	19K1266
3	Optical Cable - 25 Meters	19K1267
	LC-SC Adapter	19K1250
4	Short Wave SFP Module	19K1280
4	Long Wave SFP Module	19K1281
5	Frame Assembly with Midplane	71P8142
6	RAID Card	71P8144
7	Battery Backup Assembly	24P0953
8	Bezel Assembly	71P8141
9	Front Fan Assembly (Controller CRU Fan)	37L0094
10	Rear Fan Assembly	37L0102
	512 MB 100 Mhz DIMM	19K1283
	Battery Cable	03K9285
	Blank Cannister	37L0100
	Line Cord Jumper, High Voltage	36L8886
	Power Cable	37L0101
	Miscellaneous Hardware Kit	24P0954
	Rail Kit	37L0085
	Fibre Channel Host Adapter (optional)	19K1273

Index	Fibre Channel RAID Controller (Type 1442)	FRU
	Fibre Channel Host Adapter (Dual Port) (optional)	24P8053

Power cords

Table 42. Power cords (Type 1742 FAStT900 Storage Server)

IBM power cord part number	Used in these countries and regions
36L8880	Argentina, Australia, China (PRC), New Zealand, Papua New Guinea, Paraguay, Uruguay, Western Samoa
13F9940	Afghanistan, Algeria, Andorra, Angola, Austria, Belgium, Benin, Bulgaria, Burkina Faso, Burundi, Cameroon, Central African Rep., Chad, Czech Republic, Egypt, Finland, France, French Guiana, Germany, Greece, Guinea, Hungary, Iceland, Indonesia, Iran, Ivory Coast, Jordan, Lebanon, Luxembourg, Macao S.A.R. of the PRC, Malagasy, Mali, Martinique, Mauritania, Mauritius, Monaco, Morocco, Mozambique, Netherlands, New Caledonia, Niger, Norway, Poland, Portugal, Romania, Senegal, Slovakia, Spain, Sudan, Sweden, Syria, Togo, Tunisia, Turkey, former USSR, Vietnam, former Yugoslavia, Zaire, Zimbabwe
13F9997	Denmark
14F0015	Bangladesh, Burma, Pakistan, South Africa, Sri Lanka
14F0033	Antigua, Bahrain, Brunei, Channel Islands, Cyprus, Dubai, Fiji, Ghana, Hong Kong S.A.R. of the PRC, India, Iraq, Ireland, Kenya, Kuwait, Malawi, Malaysia, Malta, Nepal, Nigeria, Polynesia, Qatar, Sierra Leone, Singapore, Tanzania, Uganda, United Kingdom, Yemen, Zambia
14F0051	Liechtenstein, Switzerland
14F0069	Chile, Ethiopia, Italy, Libya, Somalia
14F0087	Israel
1838574	Thailand
6952300	Bahamas, Barbados, Bermuda, Bolivia, Brazil, Canada, Cayman Islands, Colombia, Costa Rica, Dominican Republic, Ecuador, El Salvador, Guatemala, Guyana, Haiti, Honduras, Jamaica, Japan, Korea (South), Liberia, Mexico, Netherlands Antilles, Nicaragua, Panama, Peru, Philippines, Saudi Arabia, Suriname, Taiwan, Trinidad (West Indies), United States of America, Venezuela

Chapter 11. IBM TotalStorage FAStT EXP15 and EXP200 Storage Expansion Units

Note: The problem determination (PD) maps found in Chapter 17, “Problem determination maps”, on page 137 provide you with additional diagnostic aids.

The IBM TotalStorage EXP15 and EXP200 enclosures are compatible with:

- Type 3526 Fibre Channel RAID controller (see Chapter 6 on page 23)

This chapter contains the information for the EXP15 and EXP200 enclosures. Information that is common to both enclosures is given first. Information that is specific to each enclosure is given second.

Diagnostics and test information

Important

The service procedures are designed to help you isolate problems. They are written with the assumption that you have model-specific training on all computers, or that you are familiar with the computers, functions, terminology, and service-related information provided in this manual and the appropriate IBM PC/Netfinity Server Hardware Maintenance Manual.

The following is a list of problems and references for diagnosing the IBM EXP15 Storage Expansion Unit - Type 3520 and IBM EXP200 Storage Expansion Unit - Type 3530.

Problem	Reference
Hard Disk Drive Numbering	Refer to the IBM TotalStorage FAStT Product Installation Guide.
Error Codes/Error Messages	Refer to the Symptom-to-FRU Index for the server that the Storage Expansion Unit you are servicing is connected to.
Expansion Unit Options Switches	Refer to the IBM TotalStorage FAStT Product Installation Guide.
Fan Controls and Indications	Refer to the IBM TotalStorage FAStT Product Installation Guide.
Performing a Shutdown	See “Performing a shutdown” on page 90.
Power Supply Controls and Indicators	Refer to the IBM TotalStorage FAStT Product Installation Guide.
Rear Controls and Indications	Refer to the IBM TotalStorage FAStT Product Installation Guide.
Turning the Power On	See “Turning the power on” on page 90.

Additional service information

This section provides service information that is common to both the EXP15 and EXP200 enclosures.

- “Performing a shutdown” on page 90
- “Turning the power on” on page 90
- “Specifications” on page 90

Performing a shutdown

Note: If the Expansion Unit loses power unexpectedly, it might be due to a hardware failure in the power system or midplane (see “Symptom-to-FRU index” on page 92).

To perform a shutdown:

1. Make sure that all I/O activity has stopped. If applicable, logically disconnect from the host controller.
2. Make sure that all amber Fault LEDs are off. If any Fault LEDs are lit (drives, power supplies, or fans), correct the problem before you turn off the power.
3. Turn off *both* power supply switches on the back of the expansion unit.

Turning the power on

Use this procedure to power-on the EXP15 and EXP200 Storage Expansion unit.

- **Initial start-up:**
  1. Verify that all communication and power cables are plugged into the back of the expansion unit.
     a. All hard disk drives are locked securely in place.
     b. **For EXP15:** The option ID switch on the expansion unit is set correctly.
        For EXP200: Option switches 1 through 5 and the tray number switch on the expansion unit are set correctly.
     c. The host controller and other SCSI bus devices are ready for the initial power-up.
     d. Power-on the expansion unit before powering on the server.
  2. Turn on the power to each device, based on this power-up sequence.
  3. Turn on *both* power supply switches on the back of the expansion unit.
  4. Only the green LEDs on the front and back should be on. If one or more of the amber Fault LEDs are on, see “Symptom-to-FRU index” on page 92.
- **Re-starting:**

  If you are re-starting after a normal shutdown, wait at least ten seconds before you attempt to turn on *either* power supply switch.

Specifications

Table 43. Specifications for EXP15 type 3520 and EXP200 type 3530

Specification	EXP15 type 3520	EXP200 type 3530
Size (with front panel)	Depth: 57.9 cm (22.8 in.)	Depth: 56.3 cm (22.2 in.)
	Height: 13.2 cm (5.2 in.)	Height: 12.8 cm (5 in.)
	Width: 48.2 mm (18.97 in.)	Width: 44.7 mm (17.6 in.)
Weight	Typical expansion unit as shipped: 39 kg (86 lb)	Typical expansion unit as shipped: 22.5 kg (49.5 lb)
Electrical Input:	Sign-wave input (50 to 60 Hz) • Low range: Minimum: 90 V ac / Maximum: 127 V ac • High range: Minimum: 198 V ac / Maximum: 257 V ac	
	Input Kilovolt-amperes (kVA) approximately • Minimum configuration: 0.06 kVA • Maximum configuration: 0.39 kVA	

Table 43. Specifications for EXP15 type 3520 and EXP200 type 3530 (continued)

Specification	EXP15 type 3520	EXP200 type 3530
Environment	**Air Flow:** Air flow is from front to back	
	Air temperature: • Expansion unit on: 10° to 35° C (50° to 95° F) Altitude: 0 to 914 m (3000 ft.) • Expansion unit on: 10° to 32° C (50° to 90° F) Altitude: 914 m (3000 ft.) to 2133 m (7000 ft.)	
	Humidity: 10% to 80%	
Heat Output	Approximate heat output in British Thermal Units (BTU) per hour: • Minimum configuration: 205.2 BTU (60 watts) • Maximum configuration: 1333.8 BTU (390 watts)	
Acoustical Noise Emissions Values	For open bay (0 hard disk drives installed) and typical system configurations (8 hard disk drives installed).	
	• Sound Power (idling): – 6.2 bels (open bay) – 6.4 bels (typical) • Sound Power (operating): – 6.2 bels (open bay) – 6.5 bels (typical) • Sound Pressure (idling): – 47 dBA (open bay) – 49 dBA (typical) • Sound Pressure (operating): – 47 dBA (open bay) – 50 dBA (typical)	• Sound Power (idling): – 6.3 bels (open bay) – 6.5 bels (typical) • Sound Power (operating): – 6.3 bels (open bay) – 6.6 bels (typical) • Sound Pressure (idling): – 47 dBA (open bay) – 49 dBA (typical) • Sound Pressure (operating): – 47 dBA (open bay) – 50 dBA (typical)
	These levels are measured in controlled acoustical environments according to ISO 7779 and are reported in accordance with ISO 9296. The declared sound power levels indicate an upper limit, below which a large portion of machines operate. Sound pressure levels in your location might exceed the average 1-meter values stated because of room reflections and other nearby noise.	

Symptom-to-FRU index

Note: The PD maps found in Chapter 17, “Problem determination maps”, on page 137 provide you with additional diagnostic aids.

Use Table 44 to find solutions to problems that have definite symptoms.

Table 44. Symptom-to-FRU index for EXP15 and EXP200 Storage Expansion units

Problem Indicator	FRU/Action
EXP200 only: Amber LED On (Front Panel)	1. **General Machine Fault** Check for amber LED on expansion unit
EXP15 only: Amber and Green LEDs flashing (Drive)	1. **Host issued a drive rebuild command**
EXP15 only: Amber and Green LEDs Off (Power supply)	1. **Reseat hard disk drive** 2. Hard disk drive
Amber LED On (Drive)	1. **Hard Disk Drive**
Amber LED On (Fan)	1. **Fan**
Amber LED On (ESM board)	1. **ESM board** 2. Check for fan fault LED 3. Unit is overheating. Check temperature.
Amber LED On, Green LED Off (Power supply)	1. **Turn Power Switch On** 2. Power cord 3. Reseat Power Supply 4. Power Supply
Amber and Green LEDs On (Power supply)	1. **Power Supply**
All Green LEDs Off (Power supply)	1. **Check AC voltage cabinet AC voltage line inputs** 2. Power Supplies 3. Midplane board
Intermittent power loss to expansion unit	1. **Check AC voltage line inputs and cabinet power components** 2. Power Supplies 3. Midplane board
One or more Green LEDs Off (All)	1. **Turn Power Switch On** 2. Power cord 3. Reseat Power Supply 4. Power Supply
One or more Green LEDs Off (Drive)	1. **No activity to the drive** 2. This can be normal activity
One or more Green LEDs Off (All Hard Disk Drives or those on one Bus)	1. **Use SCSI RAID Manager to check drive status** 2. SCSI Cables 3. ESM Board 4. Midplane board

Table 44. Symptom-to-FRU index for EXP15 and EXP200 Storage Expansion units (continued)

Problem Indicator	FRU/Action
EXP15 type 3520: Unable to access drives on one or both SCSI buses	1. **Check SCSI cables and connections** 2. Option switch 2 must be set to off 3. ESM board
EXP200 type 3530: Unable to access drives on one or both SCSI buses	1. **Check SCSI cables and connections** 2. Check the drive SCSI ID setting 3. ESM board 4. Ensure that option switches 1 and 5 are set to the appropriate position (change the switch position only when the expansion unit is powered off).
Intermittent Power Loss	1. **AC power or plug** 2. Power supply 3. Midplane
Random errors	1. **Midplane board** 2. **(For EXP15 only)** Make sure option switches 1 and 2 are set to Off

Note: If you cannot find the problem using this Symptom-to-FRU Index, test the entire system.

Chapter 12. IBM TotalStorage FAStT EXP500 Storage Expansion Unit

Note: The problem determination (PD) maps found in Chapter 17, “Problem determination maps”, on page 137 provide you with additional diagnostic aids.

The IBM TotalStorage FAStT EXP500 enclosure is compatible with the following IBM products:

- Type 3552 FAStT500 RAID controller (see Chapter 8 on page 49)
- Type 1742 FAStT700 Fibre Channel Storage Server (see Chapter 10 on page 77)
- FAStT200 type 3542 and FAStT200 HA type 3542 (see Chapter 7 on page 37)

Diagnostics and test information

Important

The service procedures are designed to help you isolate problems. They are written with the assumption that you have model-specific training on all computers, or that you are familiar with the computers, functions, terminology, and service-related information provided in this manual and the appropriate IBM PC/Netfinity Server Hardware Maintenance Manual.

The following is a list of problems and references for diagnosing the IBM FAStT EXP500 type 3530.

Problem	Reference
Hard Disk Drive Numbering	Refer to the IBM TotalStorage FAStT Product Installation Guide.
Error Codes/Error Messages	Refer to the Symptom-to-FRU Index for the server that the Storage Expansion Unit you are servicing is connected to.
Expansion Unit Options Switches	Refer to the IBM TotalStorage FAStT Product Installation Guide.
Front Controls and Indications	Refer to the IBM TotalStorage FAStT Product Installation Guide.
Rear Controls and Indications	Refer to the IBM TotalStorage FAStT Product Installation Guide.

Additional service information

Turning the expansion unit on and off

This section contains instructions for turning the expansion unit on and off under normal and emergency circumstances.

If you are turning on the expansion unit after an emergency shutdown or power outage, see “Restoring power after an emergency” on page 97.

Turning on the expansion unit

Use this procedure to turn on the power for the initial startup of the expansion unit.

1. Verify that:
   a. All communication and power cables are plugged into the back of the expansion unit and an ac power outlet.
   b. All hard disk drives are locked securely in place.
   c. The tray number switches on the expansion unit are set correctly. (refer to the IBM TotalStorage FAStT Product Installation Guide for more information.)
2. Check the system documentation for all the hardware devices you intend to turn on and determine the proper startup sequence.

   Note: Be sure to turn on the IBM EXP500 before the server.
3. Turn on the power to each device, based on the startup sequence.

   Attention: If you are restarting the system after a normal shutdown, wait at least 10 seconds before you turn on the power supply switches.
4. Turn on both power supply switches on the back of the unit.

   The expansion unit might take a few seconds to power up. During this time, you might see the amber and green LEDs on the expansion unit turn on and off intermittently. When the startup sequence is complete, only the green LEDs on the front and back and the amber Bypass LEDs for unconnected GBIC ports should remain on. If other amber LEDs remain lit, see “Symptom-to-FRU index” on page 99.

Turning off the expansion unit

Attention: Except in an emergency, never turn off the power if any Fault LEDs are lit on the expansion unit. Correct the fault before you turn off the power, using the proper troubleshooting or servicing procedure. This will ensure that the expansion unit will power up correctly later. For guidance, see “Symptom-to-FRU index” on page 99.

The expansion unit is designed to run continuously, 24 hours a day. After you turn on the expansion unit, do not turn it off. Turn off the power only when:

- Instructions in a hardware or software procedure require you to turn off the power.
- A service technician tells you to turn off the power.
- A power outage or emergency situation occurs (see “Performing an emergency shutdown” on page 97).

CAUTION:
The power control button on the device and the power switch on the power supply do not turn off the electrical current supplied to the device. The device also might have more than one power cord. To remove all electrical current from the device, ensure that all power cords are disconnected from the power source.

Use this procedure to turn off the power.

1. Check the system documentation for all hardware devices you intend to turn off and determine the proper power-down sequence.
2. Make sure that all I/O activity has stopped.
3. Make sure that all amber Fault LEDs are off. If any Fault LEDs are lit (drives, power supplies, or fans), correct the problem before you turn off the power. For guidance, see “Symptom-to-FRU index” on page 99.

4. Turn off both power supply switches on the back on the expansion unit.

Performing an emergency shutdown

Attention: Emergency situations might include fire, flood, extreme weather conditions, or other hazardous circumstances. If a power outage or emergency situation occurs, always turn off all power switches on all computing equipment. This will help safeguard your equipment from potential damage due to electrical surges when power is restored. If the expansion unit loses power unexpectedly, it might be due to a hardware failure in the power system or midplane (see "Symptom-to-FRU index" on page 99).

Use this procedure to shut down during an emergency.

1. If you have time, stop all activity and check the LEDs (front and back). Make note of any Fault LEDs that are lit so you can correct the problem when you turn on the power again.
2. Turn off all power supply switches; then, unplug the power cords from the expansion unit.

Restoring power after an emergency

Use this procedure to restart the expansion unit if you turned off the power supply switches during an emergency shut down, or if a power failure or a power outage occurred.

1. After the emergency situation is over or power is restored, check the expansion unit for damage. If there is no visible damage, continue with step 2; otherwise, have your system serviced.
2. After you have checked for damage, ensure that the power switches are in the off position; then, plug in the expansion unit power cords.
3. Check the system documentation for the hardware devices you intend to power up and determine the proper startup sequence.

   Note: Be sure to turn on the IBM EXP500 before the server.
4. Turn on the power to each device, based on the startup sequence.
5. Turn on both power supply switches on the back of the IBM EXP500.
6. Only the green LEDs on the front and back and the amber Bypass LEDs for unconnected GBIC ports should remain on. If other amber Fault LEDs are on, see "Symptom-to-FRU index" on page 99 for instructions.
7. Use your installed software application as appropriate to check the status of the expansion unit.

Clustering support

Clustering is a means of sharing array groups among controllers to provide redundancy of controllers and servers. This redundancy is important if a hardware component fails. If a hardware component failure occurs after clustering has been set up, another server takes ownership of the array group.

Clustering requires additional hardware and specialized software. For more information about clustering, visit the following IBM Web site:

http://www.ibm.com/pc/us/netfinity/clustering

Getting help on the World Wide Web

You can obtain up-to-date information about your IBM EXP500, a complete listing of the options that are supported on your model, and information about other IBM server products by accessing the IBM Web page at the following address:

http://www.ibm.com/pc/us/netfinity

Specifications

The following summarizes the operating specifications of the EXP500.

Size (with front panel and without mounting rails)

- Depth: 56.3 cm (22.2 in)
- Height: 12.8 cm (5 in)
- Width: 44.7 cm (17.6 in)

Weight

- Standard expansion unit as shipped: 25 kg (54.5 lbs)
- Typical expansion unit fully loaded: 35.5 kg (78 lbs)

Electrical input

- Sine-wave input (50 to 60 Hz) is required
- Input Voltage:
  - Low range:
    - Minimum: 90 V ac
    - Maximum: 127 V ac
  - High range:
    - Minimum: 198 V ac
    - Maximum: 257 V ac
  - Input kilovolt-amperes (kVA) approximately:
    - Minimum configuration: 0.06 kVA
    - Maximum configuration: 0.36 kVA

Environment

- Air temperature:
  - Expansion unit on:
    10° to 35° C
    (50° to 95° F)
    Altitude: 0 to 914 m (3000 ft.)
  - Expansion unit on:
    10° to 32° C
    (50° to 90° F)
    Altitude: 914 m (3000 ft.) to 2133 m (7000 ft.)
- Humidity:
  - 8% to 80%

Acoustical noise emissions values

For open bay (0 drives installed) and typical system configurations (8 hard drives installed).

– Sound Power (idling):
  - 6.3 bels (open bay)
  - 6.5 bels (typical)
– Sound Power (operating):
  - 6.3 bels (open bay)
  - 6.6 bels (typical)
– Sound Pressure (idling):
  - 47 dBA (open bay)
  - 49 dBA (typical)
– Sound Pressure (operating):
  - 47 dBA (open bay)
  - 50 dBA (typical)

These levels are measured in controlled acoustical environments according ISO 7779 and are reported in accordance with ISO 9296. The declared sound power levels indicate an upper limit, below which a large portion of machines operate. Sound pressure levels in your location might exceed the average 1-meter values stated because of room reflections and other nearby noise.

Symptom-to-FRU index

Note: The PD maps found in Chapter 17, “Problem determination maps”, on page 137 provide you with additional diagnostic aids.

Use Table 45 to find solutions to problems that have definite symptoms.

Table 45. Symptom-to-FRU index for FAStT EXP500 Storage Expansion unit

Problem Indicator	FRU/Action
Amber LED On (Front Panel)	1. **General Machine Fault** Check for amber LED on expansion unit. Use the RAID manager software to check the status.
Amber LED On (Hard Disk Drive)	1. **Hard Disk Drive**
Amber LED On (Fan)	1. **Fan**
Amber LED On	1. **ESM board**
Amber LED On, Green LED Off (Power Supply)	1. **Turn Power Switch On** 2. Power cord 3. Reseat Power Supply 4. Power Supply
Amber and Green LEDs On (Power Supply)	1. **Power Supply**
All Green LEDs Off	1. **Check AC voltage cabinet AC voltage line inputs** 2. Power Supplies 3. Midplane board
Intermittent power loss to expansion unit	1. **Check AC voltage line inputs, and cabinet power components** 2. Power Supplies 3. Midplane board

Table 45. Symptom-to-FRU index for FAStT EXP500 Storage Expansion unit (continued)

Problem Indicator	FRU/Action
One or more Green LEDs Off (Power Supply)	1. **Turn Power Switch On** 2. Power cord 3. Reseat Power Supply 4. Power Supply
One or more Green LEDs On (Drives)	1. **No activity to the drive** 2. This can be normal activity
Intermittent Power Loss	1. **AC power or plug** 2. Power supply 3. Midplane
Random errors	1. **Midplane board**
One or more Green LEDs blinking slowly. (All hard disk drives.)	1. **Check cabling scheme** 2. FC Cable 3. GBIC
Hard disk drive not visible in RAID management software.	1. **Hard Disk Drive** 2. Midplane Board
Amber temperature LED enabled in RAID management software. (ESM Board)	1. **Check for fan fault LED** 2. Unit is overheating; check temperature. 3. ESM Board
Amber conflict LED on. (ESM Board)	1. **Tray numbers of ESM boards within a single FAStT EXP500 do not match**
GBIC bypass LED. **Note:** It is normal for the LED to be on when no GBIC or cable is installed.	1. **Check ESM fault LED** 2. GBIC does not detect an incoming signal a. FC Cable b. GBIC or other end on the FC cable c. GBIC adjacent to amber LEDC cable

Note: If you cannot find the problem using this Symptom-to-FRU Index, test the entire system. See the server documentation for more detailed information on testing and diagnostic tools.

Parts listing

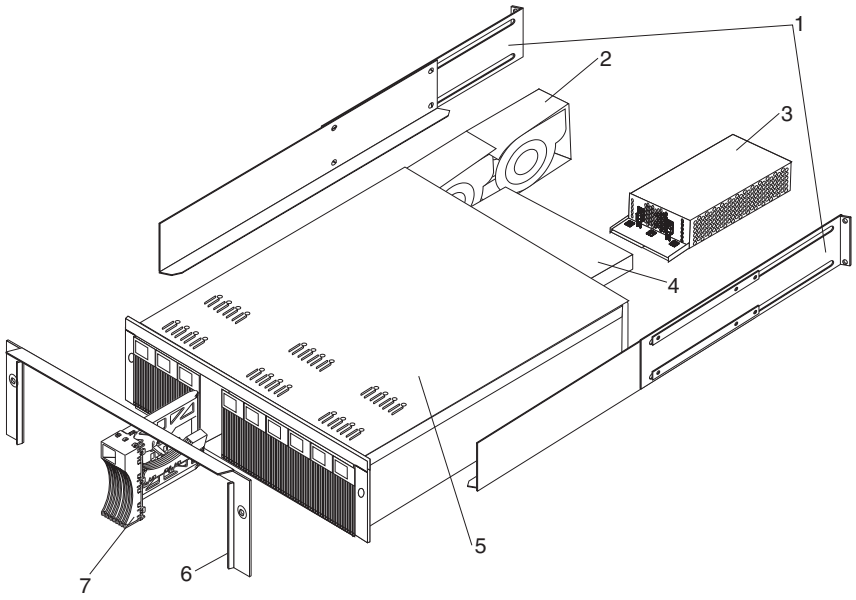


Figure 60. FAStT EXP500 Parts List

Index	System (IBM FAStT EXP500 - Type 3560, Model 1RU)	FRU No.
1	Rail Kit Left/Right (Model 1RU)	37L0067
2	Blower Assembly (Model 1RU)	09N7285
3	350W Power Supply Assembly (Model 1RU)	37L0059
4	Electronic Module (ESM, LVD/LVD) (Model 1RU)	37L0103
5	Midplane/Frame (Model 1RU) **Note:** The midplane board and frame are replaced as a unit. If either part is needed, order the above FRU.	37L0104
6	Decorative Bezel (Model 1RU)	37L0074
7	Blank Tray Assembly (Model 1RU)	37L6708
	Miscellaneous Hardware Kit (Model 1RU)	09N7288
	Line Cord, 9 Foot (Model 1RU)	6952300
	Line Cord Jumper, High Voltage (Model 1RU)	36L8886

Table 46. Power cords (FAStT EXP500 Storage Expansion Unit)

Power Cords	FRU No.
Arabic	14F0033
Argentina	13F9940
Australia	13F9940
Belgium	13F9979
Bulgaria	13F9979
Canada	6952300
Czech Republic	13F9979
Denmark	13F9997

Table 46. Power cords (FAStT EXP500 Storage Expansion Unit) (continued)

Power Cords	**FRU No.**
Finland	13F9979
France	13F9979
Germany	13F9979
Hungary	13F9979
Israel	14F0087
Italy	14F0069
Latvia	13F9979
Netherlands	13F9979
Norway	13F9979
Poland	13F9979
Portugal	13F9979
Serbia	13F9979
Slovakia	13F9979
South Africa	14F0015
Spain	13F9979
Switzerland	13F9979
Switzerland (French/German)	14F0051
Thailand	1838574
U.S. English	6952300
U.K./Ireland	14F0033
Yugoslavia	13F9979

Chapter 13. IBM TotalStorage FAStT EXP 700 Storage Expansion Unit

Note: The problem determination (PD) maps found in Chapter 17, “Problem determination maps”, on page 137 provide you with additional diagnostic aids.

This chapter describes the IBM TotalStorage FAStT EXP 700 Storage Expansion Unit.

General Checkout

Use the indicator lights, the Symptom-to-FRU index, and the connected server HMM to diagnose problems.

The problem determination (PD) maps found in Chapter 17, “Problem determination maps”, on page 137 provide you with additional diagnostic aids.

Operating specifications

Table 47 provides general information about the FAStT EXP700. All components plug directly into the backplane.

Table 47. IBM TotalStorage FAStT EXP700 Storage Expansion Unit specifications

Size

- **Width**: 44.5 cm (17.52 in.)
- **Height**: 12.8 cm (5.03 in.)
- **Depth**: 56.3 cm (22.17 in.)

Weight: 30.12 kg (66.4 lb)

Electrical input

- Sine-wave input (50 to 60 Hz) is required
- Input voltage low range:
  - Minimum: 90 V ac
  - Maximum: 127 V ac
- Input voltage high range:
  - Minimum: 198 V ac
  - Maximum: 257 V ac
- Input kilovolt-amperes (kVA), approximately:
  - Minimum configuration: 0.06 kVA
  - Maximum configuration: 0.39 kVA

Environment

- Air temperature
  - Expansion unit on:
    - 10° to 35°C (50° to 95°F)
    - Altitude: 0 to 914 m (3000 ft)
  - Expansion unit off:
    - 10° to 32°C (50° to 90°F)
    - Altitude: 914 m (3000 ft) to 2133 m (7000 ft)
- Humidity
  - 8% to 80%

Heat dissipation

- Fully configured expansion unit (14 FAStT 2 GB hard disk drives)
  - 1,221 BTU per hour

Acoustical noise emission values

For open-bay (0 drives installed) and typical system configurations (Eight hard disk drives installed):

- Sound power (idling):
  - 5.9 bel (open bay)
  - 6.1 bel (typical)
- Sound power (operating):
  - 5.9 bel (open bay)
  - 6.2 bel (typical)
- Sound pressure (idling):
  - 44 dBA (open bay)
  - 46 dBA (typical)
- Sound pressure (operating):
  - 44 dBA (open bay)
  - 47 dBA (typical)

These levels are measured in controlled acoustical environments according to ISO 7779 and are reported in accordance with ISO 9296. The declared sound power levels indicate an upper limit, below which a large portion of machines operate. Sound pressure levels in your location might exceed the average 1-meter values stated because of room reflections and other nearby noise.

Diagnostics and test information

Table 48 contains information to help you solve some of the problems you might have with the expansion unit. It contains the problem symptoms and error messages along with suggested actions to take to resolve problems.

Table 48. Diagnostic information

Problem indicator	Component	Possible cause	Possible solutions
Amber LED is lit	Drive CRU	Drive failure	Replace failed drive.
	Fan CRU	Fan failure	Replace failed fan.
	ESM over-temperature LED	Subsystem is overheated	Check fans for faults. Replace failed fan if necessary.
		Environment is too hot	Check the ambient temperature around the expansion unit. Cool as necessary.
		Defective LED or hardware failure	If you cannot detect a fan failure or overheating problem, replace the ESM.
	ESM Fault LED	ESM failure	Replace the ESM. See your controller documentation for more information.
	ESM Bypass LED	No incoming signal detected	Reconnect the SFP modules and fibre channel (fibre channel) cables. Replace input and output SFP modules or cables as necessary.
		ESM failure	If the ESM Fault LED is lit, replace the ESM.
	Front panel	General machine fault	A Fault LED is lit somewhere on the expansion unit (check for Amber LEDs on CRUs).
		SFP transmit fault	Check that the CRUs are properly installed. If none of the amber LEDs are lit on any of the CRUs, this indicates an SFP module transmission fault in the expansion unit. Replace the failed SFP module. See your storage-manager software documentation for more information.
Amber LED is lit and green LED is off	Power-supply CRU	The power switch is turned off or there is an ac power failure	Turn on all power-supply switches.
Amber and green LEDs are lit	Power-supply CRU	Power-supply failure	Replace the failed power-supply CRU.

Table 48. Diagnostic information (continued)

Problem indicator	Component	Possible cause	Possible solutions
All green LEDs are off	All CRUs	Subsystem power is off	Check that all expansion-unit power cables are plugged in and the power switches are on. If applicable, check that the main circuit breakers for the rack are powered on.
		AC power failure	Check the main circuit breaker and ac outlet.
		Power-supply failure	Replace the power supply.
		Midplane failure	See “Symptom-to-FRU index” on page 99.
Amber LED is flashing	Drive CRUs	Drive rebuild or identity is in process	No corrective action needed.
One or more green LEDs are off	Power supply CRUs	Power cable is unplugged or switches are turned off	Make sure the power cable is plugged in and the switches are turned on.
	All drive CRUs	Midplane failure	Replace the midplane.
	Several CRUs	Hardware failure	Replace the affected CRUs. If this does not correct the problem, have the ESMs replaced, followed by the midplane.
	Front panel	Power-supply problem	Make sure that the power cables are plugged in and that the power supplies are turned on.
		Hardware failure	If any other LEDs are lit, replace the midplane.
Intermittent or sporadic power loss to the expansion unit	Some or all CRUs	Defective ac power source or improperly connected power cable	Check the ac power source. Reseat all installed power cables and power supplies. If applicable, check the power components (power units or UPS). Replace defective power cables.
		Power-supply failure	Check the power supply Fault LED on the power supply. If the LED is lit, replace the failed CRU.
		Midplane failure	Replace the midplane.
Unable to access drives	Drives and fibre channel loop	Incorrect expansion unit ID settings	Ensure that the fibre channel optical cables are undamaged and properly connected. Check the expansion unit ID settings. **Note:** Change switch position only when your expansion unit is powered off.
		ESM failure	Replace one or both ESMs.
Random errors	Subsystem	Midplane feature	Replace the midplane.

Symptom-to-FRU index

Note: The PD maps found in Chapter 17, “Problem determination maps”, on page 137 provide you with additional diagnostic aids.

Use Table 49 to find solutions to problems that have definite symptoms.

Table 49. Symptom-to-FRU index for FAStT EXP700 Storage Expansion unit

Problem Indicator	FRU/Action
Amber LED On (Front Panel)	1. **General Machine Fault** Check for amber LED on expansion unit. Use the RAID manager software to check the status.
Amber LED On (Hard Disk Drive)	1. **Hard Disk Drive**
Amber LED On (Fan)	1. **Fan**
Amber LED On	1. **ESM board**
Amber LED On, Green LED Off (Power Supply)	1. **Turn Power Switch On** 2. Power cord 3. Reseat Power Supply 4. Power Supply
Amber and Green LEDs On (Power Supply)	1. **Power Supply**
All Green LEDs Off	1. **Check AC voltage cabinet AC voltage line inputs** 2. Power Supplies 3. Midplane board
Intermittent power loss to expansion unit	1. **Check AC voltage line inputs, and cabinet power components** 2. Power Supplies 3. Midplane board
One or more Green LEDs Off (Power Supply)	1. **Turn Power Switch On** 2. Power cord 3. Reseat Power Supply 4. Power Supply
One or more Green LEDs On (Drives)	1. **No activity to the drive** 2. This can be normal activity
Intermittent Power Loss	1. **AC power or plug** 2. Power supply 3. Midplane
Random errors	1. **SFP** 2. Optical board 3. Midplane board 4. switch harness
One or more Green LEDs blinking slowly. (All hard disk drives.)	1. **Change GBIC to SFP**

Table 49. Symptom-to-FRU index for FAStT EXP700 Storage Expansion unit (continued)

Problem Indicator	FRU/Action
Hard disk drive not visible in RAID management software.	1. **Hard Disk Drive** 2. FC cable 3. SFP 4. ESM 5. Midplane board
Amber temperature LED enabled in RAID management software. (ESM Board)	1. **Check for fan fault LED** 2. Unit is overheating; check temperature. 3. ESM Board
Amber conflict LED on. (ESM Board)	1. **Tray numbers of switch plate are set to identical values on two or more EXP700s on the same FC loop**
SFP bypass LED. **Note:** It is normal for the LED to be on when no SFP or cable is installed.	1. **Change GBIC to SFP in all locations**

Note: If you cannot find the problem using this Symptom-to-FRU Index, test the entire system. See the server documentation for more detailed information on testing and diagnostic tools.

Parts listing

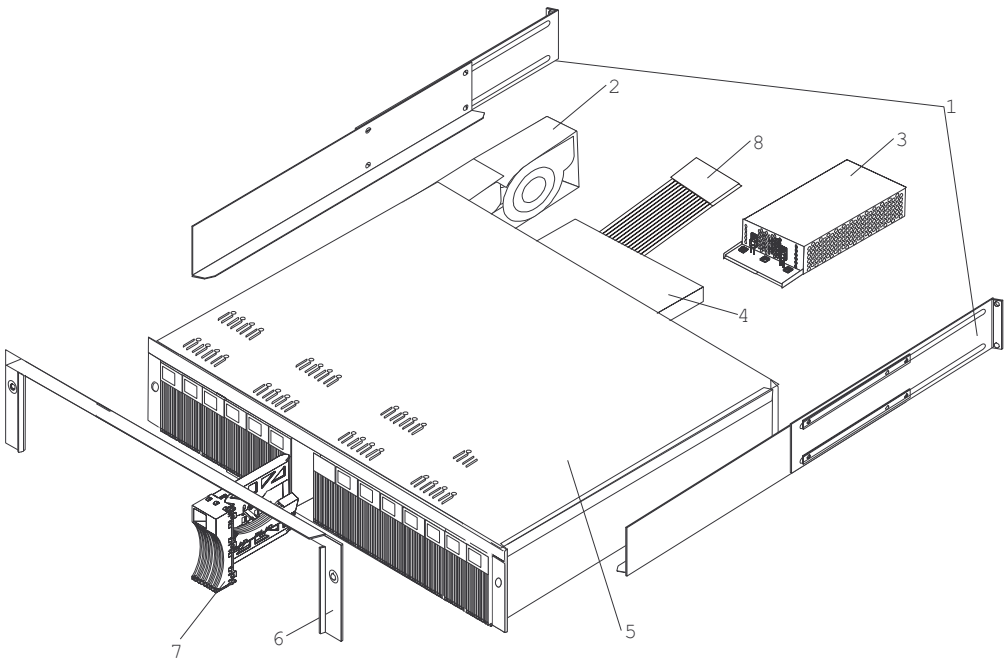


Figure 61. FAStT EXP700 Parts List

Table 50. Parts listing (FAStT EXP700 Storage Expansion Unit)

Index	FAStT- EXP 700 Storage Expansion Unit (1740-1RU&1RX)	FRU P/N
1	rail kit	37L0067
2	blower ASM CRU	19K1293
3	power supply CRU, 400W	19K1289
4	CDPOP, FC ESM 2GB	19K1287
5	Frame, Midplane	19K1288
6	bezel ASM CRU	19K1285
7	tray, blank	19K1291
8	switch, harness	19K1297
	Miscellaneous hardware	09N7288
	cable, CRU-1M	19K1265
	cable, CRU-5M	19K1266
	cable, CRU-25M	19K1267
	cable, CRU Adapter	19K1268
	CRU, SFP LC (shortwave)	19K1280
	CRU, SFP LC (longwave)	19K1281
	power cord, 2.8M	36L8886
	power cord	6952300

Power cords

For your safety, IBM® provides a power cord with a grounded attachment plug to use with this IBM product. To avoid electrical shock, always use the power cord and plug with a properly grounded outlet.

IBM power cords used in the United States and Canada are listed by Underwriter's Laboratories (UL) and certified by the Canadian Standards Association (CSA).

For units intended to be operated at 115 volts: Use a UL-listed and CSA-certified cord set consisting of a minimum 18 AWG, Type SVT or SJT, three-conductor cord, a maximum of 15 feet in length and a parallel blade, grounding-type attachment plug rated 15 amperes, 125 volts.

For units intended to be operated at 230 volts (U.S. use): Use a UL-listed and CSA-certified cord set consisting of a minimum 18 AWG, Type SVT or SJT, three-conductor cord, a maximum of 15 feet in length and a tandem blade, grounding-type attachment plug rated 15 amperes, 250 volts.

For units intended to be operated at 230 volts (outside the U.S.): Use a cord set with a grounding-type attachment plug. The cord set should have the appropriate safety approvals for the country in which the equipment will be installed.

IBM power cords for a specific country or region are usually available only in that country or region.

IBM power cord part number	Used in these countries and regions
13F9940	Argentina, Australia, China (PRC), New Zealand, Papua New Guinea, Paraguay, Uruguay, Western Samoa
13F9979	Afghanistan, Algeria, Andorra, Angola, Austria, Belgium, Benin, Bulgaria, Burkina Faso, Burundi, Cameroon, Central African Rep., Chad, Czech Republic, Egypt, Finland, France, French Guiana, Germany, Greece, Guinea, Hungary, Iceland, Indonesia, Iran, Ivory Coast, Jordan, Lebanon, Luxembourg, Macao S.A.R. of the PRC, Malagasy, Mali, Martinique, Mauritania, Mauritius, Monaco, Morocco, Mozambique, Netherlands, New Caledonia, Niger, Norway, Poland, Portugal, Romania, Senegal, Slovakia, Spain, Sudan, Sweden, Syria, Togo, Tunisia, Turkey, former USSR, Vietnam, former Yugoslavia, Zaire, Zimbabwe
13F9997	Denmark
14F0015	Bangladesh, Burma, Pakistan, South Africa, Sri Lanka
14F0033	Antigua, Bahrain, Brunei, Channel Islands, Cyprus, Dubai, Fiji, Ghana, Hong Kong S.A.R. of the PRC, India, Iraq, Ireland, Kenya, Kuwait, Malawi, Malaysia, Malta, Nepal, Nigeria, Polynesia, Qatar, Sierra Leone, Singapore, Tanzania, Uganda, United Kingdom, Yemen, Zambia
14F0051	Liechtenstein, Switzerland
14F0069	Chile, Ethiopia, Italy, Libya, Somalia
14F0087	Israel
1838574	Thailand
6952301	Bahamas, Barbados, Bermuda, Bolivia, Brazil, Canada, Cayman Islands, Colombia, Costa Rica, Dominican Republic, Ecuador, El Salvador, Guatemala, Guyana, Haiti, Honduras, Jamaica, Japan, Korea (South), Liberia, Mexico, Netherlands Antilles, Nicaragua, Panama, Peru, Philippines, Saudi Arabia, Suriname, Taiwan, Trinidad (West Indies), United States of America, Venezuela

Chapter 14. IBM Storage Area Network Data Gateway Router (2108-R03)

Note: The problem determination (PD) maps found in Chapter 17, “Problem determination maps”, on page 137 provide you with additional diagnostic aids.

Service Aids

The SDG Router service capabilities include the following:

- LED indicators
- Power-on–self-test (POST)
- Health Check
- Event Log
- Service Port commands
- Diagnostics

LED indicators

Shown in Figure 62, the LEDs on the front panel provides a visual indication of the status and activity of the SDG and its interfaces. The LEDs are refreshed automatically about 5 times per second.

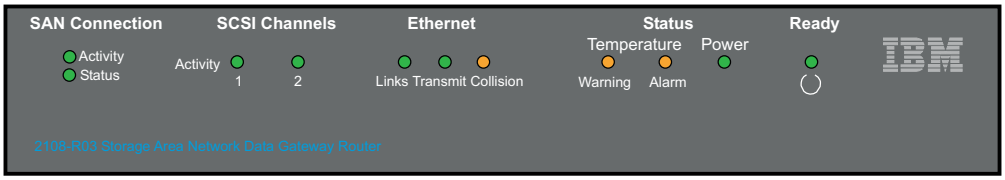


Figure 62. Front Panel LEDs

Table 51. LED Indicators

LED’s (G=Green) (A=Amber)	Function	On	Off	Flash
SAN Connection				
Activity (G)	Link traffic			SAN interface activity
Status (G)	Link status	Link Active	No transmission (Link down)	
SCSI (G)				
Activity (1 and 2)	SCSI Activity	SCSI traffic	No SCSI traffic	SCSI Interface activity
ETHERNET				
Link (G)	Status	Link active	Link down	
Transmit (G)	Status	Transmission in progress		

Table 51. LED Indicators (continued)

LED's (G=Green) (A=Amber)	Function	On	Off	Flash
Collision (A)	Status	Collision occurred		
TEMPERATURE				
WARNING (A)	Preventive failure indicator	Temperature Warning	No temperature problem	N/A
Alarm (A)	Information	Temperature exceeded	No temperature problem	N/A
Power Main (G)	Information	Power applied	No power	N/A
Ready (G)	Information	SDG Failure if on for more than 2 sec.	SDG Failure	Flashes during Startup cycle and once every second thereafter (normal)

Power-on-self-test (POST)

POST is divided into two functionally distinct parts: the initial-POST (IPOST) and the secondary-POST (SPOST)

IPOST is the first stage of POST and it thoroughly tests the on-board, dynamic random-access memory (DRAM) arrays. IPOST runs from the on-board flash memory. Upon successful completion, IPOST locates SPOST, copies it to DRAM, and then transfers program control to SPOST.

SPOST is the second stage of post. SPOST configures the SDG Router's PCI bus. SPOST then locates, loads, and runs the licensed internal code (LIC).

Health Check

The health check program queries all subsystems for their operational status. The health check has four levels. A level 1 health check is the most basic, and health check level 4 is the most complete check.

Event Log

The SDG Router maintains an event log within its on-board flash file system. You can query these logs from the SDG Router service port. Event codes and messages that are generated by the SDG Router subsystems are recorded in this log file.

Service Port Commands

An extensive command set is available to manage the SDG Router, obtain Status, and run Diagnostics. The commands described in Table 52 on page 113 have been extracted from the *SDG Service Guide*. They have been selected to provide you with some basic tools to determine the functional status of the SDG Router. Refer to Appendixes A and B of the *SDG Service Guide* for a description of all the commands.

Table 52. Service Port Commands

Group	Description	Page
diagBoot	Used to transition the SDG Router from normal operation to Diagnostic mode (see normalBoot below)	113
diagHelp	Displays a list of diagnostic commands	114
fcShow	Displays the status of the fibre channel interface	114
fcShowDevs	Displays information about the devices that are accessible from the fibre channel interface	115
fcShowNames	Displays the node and port names (addresses) of the fibre channel	116
hardwareConfig	**Diagnostic mode only**. Stores FRU VPD information in the SDG non-volatile memory (see sysVpdShow below)	116
help	Displays a list of the commands	116
hlthChkHelp	Displays the list of health check commands	117
hlthChkNow	Initiates the health check for the SDG. Results are displayed.	117
loggerDump	Dumps records from the system event log to the terminal console	118
loggerDumpCurrent	Dumps only the records that were logged since the system was last started are dumped.	118
macShow	Displays the Media Access Control address for the Ethernet interface	118
mapShowDatabase	Device database listing the connected devices	119
mapShowDevs	Displays the cross-reference map of device addresses.	119
normalBoot	Restores the SDG to normal operating conditions. Used only to transition from diagnostic mode to normal mode.	120
reboot	Preferred method for restarting the SDG Router	120
scsiRescan	Performs a rescan of the SCSI channel(s) to look for new devices	120
scsiShow	Lists all SCSI channels and the attached devices for each channel	121
showBox	Displays a picture of the SDG showing the components present	122
sysConfigShow	Displays current parameter settings.	122
sysVpdShow	Displays Vital Product Data (VPD) information	122
targets	Lists and describes each device currently attached	124
version	Lists the firmware version level	124

The following descriptions are from *Storage Area Network Data Gateway Router Installation and User's Guide* pages 73-97; they also are listed in the *Storage Area Network Data Gateway Router Service Guide* as Appendixes A and B.

diagBoot

Use the **diagBoot** command only to transition the SDG Router from normal operation to the special diagnostic mode. The command first ensures that the ffs0:mt directory exists, then it verifies that the files diagnstk.o and diagnstk.rc are in the flash file system. If they are in the root directory, it moves them to the ffs0:mt directory.

The **diagBoot** command copies the existing boot parameters to a file in the ffs0:mt directory on the SDG Router. It then installs the new boot parameters that direct the SDG Router to start using the special diagnostic startup script, ffs0:mt/diagnstk.rc. It renames the persistent map file config/device.map as config/device.bak. Finally, **diagBoot** issues a reboot command to put the changes into effect.

Note: Power cycling the SDG Router does not re-instate it to normal mode if previously set to diagnostic mode. Use **normalBoot** command (page 120) to re-initialize the router to normal mode

diagHelp

The **diagHelp** command displays a list of the diagnostic commands.

```
Router > diagHelp
```

The following commands are available in diagnostic mode only:

```
ddfTest: Test DDF Memory
elTest: Test Ethernet port w/loop-back cable
fcSlotTest <portnum> : Test specified fibre channel port w/loop-back cable
hardwareConfig: Re-inventory FRUs and update Vital Product Data
normalBoot: Shutdown and restart in normal mode
scsiChannelTest <x,y>: Test specified SCSI Channels w/loop-back cable
```

fcShow

The **fcShow** command displays the channel status for the fibre channel interface.

The following example is for a SDG Router single-port fibre channel PMC card (ISP2200 controller). The firmware state for interfaces that have a live connection to a fibre channel device are shown as Ready. An interface that has no live connection is shown as "Sync Lost".

```
Router > fcShow
-------------------------------------------------------------
Fibre Channel Controllers
-------------------------------------------------------------------------
Ctlr : PCI Addr : ISP : Firmware : FW : Ctrl : Nvram : Loop
Id : Bs Dv Fn : Type : State : Version : Addr : Addr : ID}
-------------------------------------------------------------------------
1 : 00 06 00 : 2200 : Ready : 2.01.2 : c0d98700 : 90001100 : 2 1
-------------------------------------------------------------------------
value = 80 = 0x50 = ©P©
Router >
```

The following describes the example fields:

Ctlr ID The channel number for this interface

PCI Addr The PCI address of the interface, showing bus, device ID, and function number

ISPType The type of fibre channel controller, ISP2100 or ISP2200

Firmware State The current state of the interface as reported by the Fibre Channel PMC adapter firmware. The firmware states are:

- **Configuration Wait**: Firmware is not initialized.
- **Waiting for AL_PA** : Firmware is performing or waiting to perform loop initialization.
- **Waiting for login**: Firmware is attempting port and process logins with all loop ports.
- **Ready**: Indicates that the interface is connected, operational and ready to process SCSI commands. Any other value indicates intermediate states or interface failure.

- **Sync Lost**: The firmware has detected a loss-of-sync condition and is resynchronizing the serial link receiver. This is the state reported when the fibre channel link does not detect a connection to a fibre channel device.
- **Error**: The firmware has detected an unrecoverable error condition.
- **Nonparticipating**: The firmware is not participating on the loop because it did not acquire an arbitrated loop physical address (AL_PA) during initialization.
- **Failed**: The firmware is not responding to commands.

FW Version The version of firmware on the Fibre Channel PMC adapter

Ctrl Addr A pointer to an internal data structure that is used for some diagnostic operations

Nvram Addr The memory address of the parameter RAM for this interface

Loop ID The fibre channel loop ID for this interface

fcShowDevs

The **fcShowDevs** command displays information about the devices that are accessible from each fibre channel interface. The display shows the LUN that the SDG Router has assigned to each device, the SCSI Channel that the device is attached to, the actual SCSI ID and LUN of the device, the vendor, product, revision and serial number of the device.

```
Router > fcShowDevs
FC 1:
LUN Chan Id Lun Vendor Product Rev SN
-------------------------------------------------------------------
0 0 0 0PATHLIGHT SAN Router Local 0252 00000060450d00c0
2 3 4 0IBM 03570c11 5324 000000000260
3 3 4 1IBM 03570c11 5324 000000000260
value = 3 = 0x3
Router > Router > fcShowDevs
FC 1:
LUN Chan Id Lun Vendor Product Rev SN
 ---------------------------------------------------
0 0 0 0PATHLGHT SAN Router 0339 00000060451600db
1 1 0 0 ATL L500 6320000 001E JF91101163
2 1 1 0QUANTUM DLT7000 2150 CX921S1423
4 1 2 0QUANTUM DLT7000 2150 CX905S4607
6 2 0 0QUANTUM Powerstor L200 001E JW81477118
8 2 1 0QUANTUM DLT7000 2150 CX919S5223
LUN Chan Id Lun Vendor Product Rev SN
FC 4:
0 0 0 0PATHLGHT SAN Router 0339 00000060451600db
-----------------------------------------------------
1 1 0 0 ATL L500 6320000 001E JF91101163
2 1 1 0QUANTUM DLT7000 2150 CX921S1423
4 1 2 0QUANTUM DLT7000 2150 CX905S4607
6 2 0 0QUANTUM Powerstor L200 001E JW81477118
8 2 1 0QUANTUM DLT7000 2150 CX919S5223
value =6 =0x6
Router >
```

fcShowNames

The **fcShowNames** command displays the node and port names (addresses) of the fibre channels.

```
Router > fcShowNames
-----------------------------------------------------------------
Ctlr : PCI Addr : ISP : Node : Port
Id : Bs Dv Fn : Type : Name : Name
-----------------------------------------------------------------
1 : 00 06 00 : 2200 : 10000060.451603bb :   20010060.451603bb
4 : 00 07 00 : 2200 : 10000060.451603bb :   20020060.451603bb
-----------------------------------------------------------------
value = 64 = 0x40 = ©@©
Router >
```

The following describes the example fields:

Ctlr id The channel number for the interface

PCI Addr The PCI address of the interface, showing bus, device ID, and function number

ISPType The type of fibre channel controller, ISP2100 or ISP2200

Node Name The fibre channel node name for the SDG Router

Port Name The fibre channel port name for the interface

hardwareConfig

In order to use this command, the SDG Router must be in diagnostic mode. The **hardwareConfig** command records the configurations of installed FRUs by copying them to the nonvolatile vital product data (VPD) stored on the SDG Router base.

The fields that are updated are the SCSI channel types and PMC type. The service representative enters the **hardwareConfig** command after replacing any FRUs. This causes the SDG Router to update the VPD.

```
Router> hardwareConfig
==== Recording Hardware Configuration ====
Scanning PMC option slots...
Scanning SCSI IO Modules...
Checking memory sizes...
MemSize PCI-0 is 64 Mbytes ...Done
value = 0 = 0x0
Router >
```

help

The **help** command displays a list of the shell commands.

```
Router > help
help Print this list
cleHelp Print Command Log Entry info
diagHelp Print Diagnostic Help info
hlthChkHelp Print Health Check Help info
mapHelp Print Device Map Help info
netHelp Print Network Help info
```

```
snmpHelp Print SNMP Help info
userHelp Print User account info
cd "path" Set current working path
copy ["in"][,"out"] Copy in file to out file (0 = std in/out)
h [n] Print (or set) shell history
ls ["path"[,long]] List contents of directory
ll ["path"] List contents of directory - long format
pwd Print working path
rename "old","new" Change name of file
rm ["name"] Remove (delete) a file
shellLock Lock or unlock shell command interface
version Print Version info
whoami Print user name
clearReservation [devId] Clear reservation on a target (may reset target)
diagBoot Shutdown and restart in diagnostic mode
initializeBox Delete all device maps, restore factory defaults, reboot
ridTag ["value"] Display and set serial number of replaced base unit
disableCC [option] Disable Command and Control Interface
option 1 - Report as Invalid (AIX mode)
option 2 - Fully disabled
enableCC Enable Command and Control Interface
scsiRescan [chan] Rescan SCSI Channel (all if chan not specified)
scsiShow Display info for SCSI Channels
fcShow Display info for fibre channels
fcShowDevs Display devices available on each fibre channel
fcShowNames Display Node and Port names for fibre channels
hostTypeShow Display Default Host Type settings
loggerDump [count] Display Logger Dump Records
loggerDumpCurrent [level] Display Logger Dump Records for current boot
reboot Shut down and restart
reset Restart without shut down
setFcScsiChanMask [chan],[scsi],[allow] Set Channel Access Control
setFcFrameSize [chan],[size] Set FC Frame Size
setFcHardId [chan],[id] Set FC Loop ID
setHost [chan],["OS"] Set default host type for FC Channel
OS may be "aix", "nt", "solaris", "hpux"
setSnaCCLun Set LUN for Controller Device (typically zero)
showBox Display graphic of current hardware configuration
sysConfigShow Display System Config Parameters
sysVpdShow Display Vital Product Data
sysVpdShowAll Display Vital Product Data for all subsystems
targets List all known target devices
uptime Display time since last boot
```

hlthChkHelp

The **hlthChkHelp** command displays a list of the health check commands.

```
Router > hlthChkHelp
hlthChkIntervalGet - Show Check Interval
hlthChkIntervalSet <interval> - Set Check Interval
hlthChkLevelGet - Show Check Level
hlthChkLevelSet <level> - Set Check Level
hlthChkNow - Run Health Check Now
```

hlthChkNow

The command causes the SDG Router to execute an immediate, level 4 health check. Results are displayed that will indicate which devices or subsystems failed the check.

```
Router> hlthChkNow
```

loggerDump [number]

The **loggerDump** command dumps records from the system event log to the console. A numeric parameter can be used to indicate the number of events to display. With no parameter specified, all events in the log file are displayed starting with the most recent events.

```
Router > loggerDump 4
*** Dumping 4 (1018 through 1021) of 1021 records ***
000008 1018 0d:00h:00m:07s:22t -- SCSI 2: Bus RESET
000009 1019 0d:00h:00m:07s:22t -- Target device added: index 0, handle 0xc0ec2600
000010 1020 0d:00h:00m:08s:18t -- Target device added: index 10, handle 0xc0ad2590
000011 1021 0d:00h:00m:08s:28t -- SCSI 2: New Device at Id 6, Lun 0
Router >
```

loggerDumpCurrent [level]

The **loggerDumpCurrent** command dumps records from the system event log to the console. Only the records that were logged since the system was last started are dumped. Level specifies the event log level for the events as shown in Table 53.

Table 53. Event Log Levels

Level	Name	Explanation
0	Private	Events that are never shown by the remote event viewer but are recorded in the SDG Router event log
1	Notice	Conditions that should always be reported, such as temperature alarms and device removals
2	Warning	Events that might result in a later problem
3	Information	Events that are not errors or warnings

The following is an example dump after a typical start sequence with four target devices added (one additional device is shown, which is the command and control LUN of the SDG Router itself).

```
Router > loggerDumpCurrent 1
*** Dumping 9 (1010 through 1018) current records with level >= 0 ***
000001 0d:00h:00m:05s:56t -- NOTICE: CS and LOGGING STARTED
000002 0d:00h:00m:07s:19t -- FCAL 1: LIP occurred
000003 0d:00h:00m:07s:19t -- FCAL 1: Loop up
000004 0d:00h:00m:07s:22t -- SCSI 1: Bus RESET
000005 0d:00h:00m:07s:22t -- SCSI 2: Bus RESET
000006 0d:00h:00m:07s:22t -- Target device added:index 0, handle 0xc0ec2600
000007 0d:00h:00m:08s:18t -- Target device added: index 9, handle 0xc1f9e090
000008 0d:00h:00m:08s:18t -- Target device added: index 10, handle 0xc0ad2590
000009 0d:00h:00m:08s:28t -- SCSI 2: New Device at Id 6, Lun 0
value = 0 = 0x0
Router >
```

macShow

The **macShow** command displays the media access control (MAC) address for the Ethernet interface.

```
Router > macShow
Enet MAC Address: 0.60.45.d.0.80
value = 33 = 0x21 = ©!©
Router >
```

mapShowDatabase

The SDG Router maintains a database of attached devices to ensure that each time a host attaches to the SDG Router, the target devices are seen at a consistent address. The database lists not only the devices presently connected, but also devices that have previously been connected. If a previously attached device is later reattached, it is assigned its previous address. Use the **mapShowDatabase** command to display the persistent device map table.

```
Router > mapShowDatabase
devId Type Chan tId tLun UID
-------------------------------------------
000 SNA 127 127 127 00000060:450d00c0
001 SCSI 001 003 000 00000060:450d00c0
002 SCSI 001 002 000 00000060:450d00c0
003 SCSI 001 001 000 00000060:450d00c0
004 SCSI 002 002 000 00000060:450d00c0
005 SCSI 002 000 000 00000060:450d00c0
006 SCSI 002 006 000 00000060:450d00c0
007 SCSI 002 009 000 00000060:450d00c0
008 SCSI 002 002 001 00000060:450d00c0
009 SCSI 002 005 000 00000060:450d00c0
010 SCSI 002 005 001 00000060:450d00c0
011 SCSI 001 000 000 00000060:450d00c0
012 SCSI 001 006 000 00000060:450d00c0
value = 0 = 0x0
Router >
```

The following describes the example fields:

devId The index of the device in the database.

Type The type of interface where the device is connected. SNA indicates an internal device. SCSI or fibre channel indicate I/O interfaces.

Chan The channel number of the interface where the device is attached.

TId Target ID mapping for SCSI initiators.

TLun Target LUN mapping for SCSI initiators.

UID For a fibre channel interface, the unique ID of the device. For SCSI interface, the unique ID of the SDG Router.

mapShowDevs

The SDG Router maintains a cross-reference map of device addresses. Information about the presently attached and available devices in the map can be displayed using the **mapShowDevs** command.

```
Router > mapShowDevs
devId Type Chan iId iLun UID tId tLun Handle Itl
-----------------------------------------------------------------
000 SNA 127 127 127 00000060.450d00c0 001 000 c0ec2600h 00000000h
009 SCSI 002 005 000 09000060.450d00c0 255 255 c1f9e090h 00000000h
010 SCSI 002 005 001 0a000060.450d00c0 255 255 c0ad2590h 00000000h
012 SCSI 001 006 000 0c000060.450d00c0 255 255 c1ffdf10h c1ffdc80h
value = 0 = 0x0
Router >
```

The following describes the example fields:

devId The index of the device in the database.

Type The type of interface where the device is attached to the SDG Router.

Chan The channel number of the interface

iId For a SCSI interface only, device ID of the device

tLun For a SCSI interface only, the logical unit number of the device.

UID For a fibre channel interface, unique ID of the device. For SCSI interface, a constructed unique ID based on the unique ID of SDG Router.

tId Target ID mapping for SCSI initiators

tLun Target LUN mapping for SCSI initiators

Handle An internal pointer used for some diagnostic operations

Itl An internal pointer used for some diagnostic operations

normalBoot

Certain commands and tests are only available in diagnostic mode. Switching to diagnostic mode saves all configuration parameters so that they are restored before returning to normal operation. Use the **normalBoot** command to restore the SDG Router to normal operating conditions.

This command is used only to transition a SDG Router from the special diagnostic mode to normal operations. It restores the boot parameters that was copied by **diagBoot**. The new persistent device map is erased, and the original map file is renamed config/device.map restoring it for use when the SDG Router restarts. The **normalBoot** command then restarts the SDG Router.

reboot

The **reboot** command requests that the SDG Router shut down existing operations and then restart. This is the preferred method of restarting the SDG Router. There are processes running within the SDG Router that might have writes pending to files within the SDG Router's flash file system. Following a **reboot** command, these processes flush their data to the flash file system, and the flash file system writes all pending data out to the flash memory. The SDG Router starts a reset cycle only after all pending data has been successfully written to the flash file system.

```
Router > reboot
```

scsiRescan [channel]

The **scsiRescan** command requests a SCSIrescan to look for new devices. If channel is specified (1 or 2), then only that channel is scanned. If channel is not specified or if channel is 0, then all channels are scanned.

Notes:

1. Rescanning a SCSI bus can delay I/O commands pending on that bus for several seconds. Do not rescan SCSI buses when this delay cannot be tolerated. If possible, scan only the bus where a new device has been added.
2. If a channel is specified, that channel is scanned and the prompt is returned on completion. If no channel is specified (or 0 is specified), SCSI channels 1 and 2 are scanned in sequence and the prompt is returned on completion.
3. When a device is discovered, there can be further device specific initialization that continues after the scan has completed. In this case, the device might not show up immediately when you issue the **fcShowDevs** command. (Tape and changer devices that indicate a ready status are available after the scan is completed.)
4. If a SCSI target device requires replacement, remove the old device. Set the new device to the same SCSI bus ID as the old device and attach it to the same channel. Rescan the channel to update the configuration data. The new device should be available to host systems with the same LUN as the old device.

scsiShow

The **scsiShow** command lists all SCSI channels and the attached devices for each channel.

```
Router > scsiShow
SCSI Initiator Channel 1: 0xc195e670
ID LUN Vendor Product Rev | Sync/Off Width
--------------------------|------------
0 0 IBMAS400 DFHSS4W 4545 | 12/15 16 S W Q
SCSI Initiator Channel 2: 0xc0ed3900
ID LUN Vendor Product Rev | Sync/Off Width
--------------------------|------------
  4 0 IBM 0357011 5324 | 25/15 16 S W
4 1 IBM 0357011 5324 |
value = 0 = 0x0
 Router >
```

The following describes the example fields:

ID The SCSI ID of the target device

LUN The SCSI LUN of the target device

Vendor The content of the Vendor ID field from the SCSI inquiry data

Product The content of the Product ID field from the SCSI inquiry data

Rev The content of the Revision ID field from the SCSI inquiry data

Sync/Off The negotiated synchronous transfer period and offset. The period is the negotiated transfer period. Multiply the period times 4 ns. to determine the actual period. However, if the period is negotiated to 12, then 50 ns. is used. The offset indicates the request/acknowledge (REQ/ACK) offset that was negotiated. A zero in these fields indicates that asynchronous transferis in use.

Width The negotiated transfer width in bits, either 8 or 16

showBox

The **showBox** command displays the components currently in the SDG Router using characters to form a picture of the unit, as viewed from the rear. The following figure demonstrates how the **showBox** command displays a SDG Router that has a single-port fibre channel PMC installed.

Note: For SAN connection port-number assignments, see *Storage Area Network Data Gateway Router Service Guide*.

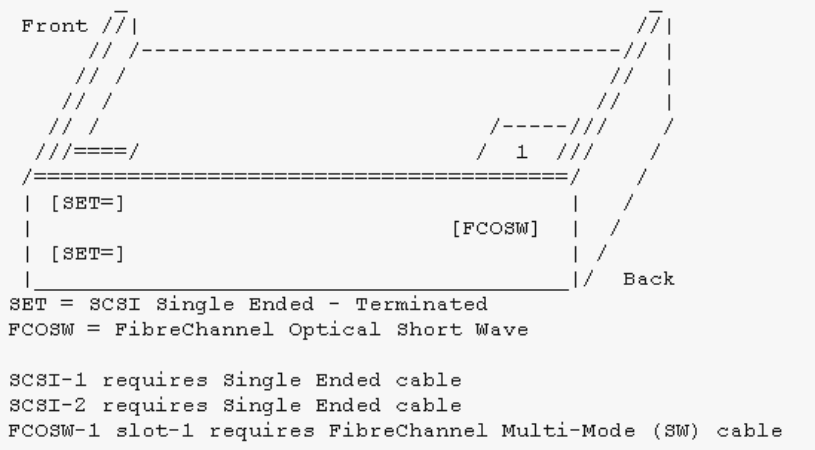


Figure 63. showBox Command Output

sysConfigShow

The **sysConfigShow** command displays the current system parameter settings.

The display shows whether the SDG Router command and control interface is enabled or disabled. It also shows the LUN that is assigned to it, whether enhanced tape performance features are enabled, the MAC address of the Ethernet port, and the SDG Router fibre channel node address.

```
Router > sysConfigShow
Current System Parameter Settings:
Command and Control Device (CC) : 0 Enabled
 LUN : 0
Allow Early Write Status for Tape : 1 Enabled
Allow R/W Acceleration for Tape : 1 Enabled
Enet MAC Address: 0.60.45.16.1.4
FC Node WWN: 10000060.45160104
value =0 =0x0 Router >
```

sysVpdShow or sysVpdShowAll

The **sysVpdShow** command displays vital product data (VPD) information. The VPD for the SDG Router includes such items as serial numbers and installed memory sizes.

```
Router > sysVpdShow
====== VPD ======
name SAN Router
uid 00:60:45:16:01:04
```

```
s/n 100111
mfg Pathlight Tech
board OntarioII 1.1
" s/n 08357659
flash 2Mbyte
dram 32Mbyte
slot1 10772100 FCOSW
scsi 1: DET 2: DET
EC OTA08000H
RID Tag
value =0 =0x0
Router >
```

The following describes the example fields:

name Product name: up to 16 characters

uid Unique Ethernet MAC address of the product: 32 characters displayed as hexadecimal bytes separated by colons

s/n Product serial number: up to 16 characters

mfg Product manufacturer: up to 16 characters

board Name of the system board contained in the base unit: up to 16 characters

″ **s/n** System board serial number: up to 16 characters

flash Size of the flash memory on the system board

dram Size of the DRAM on the system board

slot1 Card type installed in SAN connection slot one

scsi 1 SCSI type for each of the two channels, DET for ″differential, terminated″ and SET for ″single-ended, terminated″

EC Engineering change (EC) level for the system board: up to 16 characters

RID RID tag identifier: up to 16 characters

The **sysVpdShowAll** command shows more information and includes product data for the fibre channel PMC card.

```
Router > sysVpdShowAll
 ===[ Vital Product Data ]===
 -=[ Base Assembly ]-------
Name SAN Data Gateway Router
Mfg Pathlight Tech
UID 00:60:45:16:01:04
S/N 100111Assy HCO OTA08000H
Assy HCO OTA08000H
Board OntarioII 1.1
" S/N 08357659
```

```
Flash 2 Mbyte
Dram 32 Mbyte
RID Tag 100111
-=[ Slot 1 ]=-------------
 Type 10772100 FCOSW
S/N 123456
UID 0060.45160065
HCO SC004120H
value =0 =0x0
Router >
```

targets

The SDG Router maintains a list of target devices that are attached to the I/O channels. The **targets** command lists each device that is currently attached and provides a description of each device.

```
Router > targets
Idx Tdev Vendor Product Rev | Type Specific
----------------------------|---------------------------------
0 0xc194a400 PATHLGHT SAN Router Local 0252 | Cmd/Cntrl Status 0h
2 0xc1ffc390 IBM 03570C11 5324 | Tape: Blk Size  32768 , flags 7h
3 0xc1ffc290 IBM 03570C11 5324 | Changer: flags 7h
 value =4 =0x4
Router >
```

Idx Device Index in the target list

Tdev An internal pointer, used for some diagnostic operations

Vendor Content of the Vendor ID field from the SCSI Inquiry Data

Product Content of the Product ID field from the SCSI Inquiry Data

Rev Content of the Revision ID field from the SCSI Inquiry Data

Type Specific For each device type, information pertinent to the device

version

The SDG Router has software that controls all functions. The **version** command displays the revision of that operating software. The first line displayed is the SDG Router firmware version. The lines that follow pertain to the operating system software version.

```
Router > version
SAN Data Gateway Router Version 0339.11 Built Dec 13 1999, 15:14:14
VxWorks (for Pathlight (i960RD)) version 5.3.1.
Kernel: WIND version 2.5.
value = 26 = 0x1a
Router >
```

Diagnostics

The diagnostic suite is a subset of the manufacturing test program. When enabled, the diagnostic suite is capable of performing external loopback testing of all major hardware interfaces (SCSI, fibre channel, and Ethernet).

Toolkit P/N 34L2606 (supplied with the Router) contains the necessary loopback plugs to run the Diagnostics. It includes the following:

- Service port cable: One RS-232 null-modem cable with 9-pin connectors
- SCSI loopback cable: One short wide-Ultra cable with 68-pin connectors
- Fibre channel: One fibre channel short-wavelength or long-wavelenh
  fiber-optic loopback plug
- Ethernet: One 10Base-T Ethernet loopback cable
- Fuses: Two 250 V, 4 A time-lag fuses (type F4AL)

Diagnostic tests

To verify proper operation of the SDG or whenever a FRU has been replaced, a complete diagnostic check of the router can be performed. It is recommended that you perform these tests prior to returning the SDG Router to the customer.

Diagnostic test preparation

1. Attach the service terminal to the SDG Router.
2. Turn on the SDG Router and wait until it has finished the startup cycle.
3. From the service terminal, type **diagBoot**
4. Wait until the SDG Router has finished the startup cycle. The Shell prompt should be **diagmode>**
5. From the service terminal, type **showBox**.
6. Verify that the SDG Router is configured according to the customer's requirements.
   a. If all installed FRUs are shown, go to ″fibre channel tests″
   b. If all installed FRUs are not shown, go to Chapter 3 of the *2108 Model R03 Service Guide (MAP)*.

Fibre channel tests

1. Attach the fibre channel loopback plug to the card in PMC slot 1. (You can also use the plug from FAStT MSJ).

   Note: This test works only if the card is an ISP2200. If the card is an ISP 2100, the following error is displayed: ″Card in slot 0 is not fibre channel.″ You can also run FAStT MSJ to verify if the SDG Router is being detected. However, you cannot run the diagnostics (Loopback and Read/Write Buffer test) on the SDG Router.
2. From the service terminal, type **fcSlotTest 1**
   a. If the **fcSlotTest** test completes successfully, remove the loopback plug and go to ″SCSI test″.
   b. If not, go to Chapter 3 of the *2108 Model R03 Service Guide (MAP)*.

SCSI test

1. If there is only one SCSI interface installed, proceed to ″Ethernet Test″.
2. Attach the SCSI loopback cable to SCSI channels 1 and 2.
3. From the service terminal, type **scsiChannelTest 1, 2**.
   a. If the test completes successfully, go to step 4.
   b. If not, go to Chapter 3 of the *2108 Model R03 Service Guide (MAP)*.
4. Remove the SCSI loopback cable.
5. Proceed to ″Ethernet Test″.

Ethernet test

1. Obtain the SDG Router Ethernet network parameters from the customer. Configure the Ethernet port host name, address, routes, and enable the Ethernet. Refer to the IBM TotalStorage FAStT Product Installation Guide.
2. Attach the Ethernet loopback plug to the Ethernet port.
3. From the service terminal, type **elTest**
4. If the test completes successfully, go to step 5. If not, go to Chapter 3 of the *2108 Model R03 Service Guide (MAP)*.
5. Remove the Ethernet loopback plug.

Verifying SDG Router operation

1. From the service terminal, type **normalBoot**
2. Wait until the SDG Router has finished the startup cycle. The Ready light should be blinking once every second indicating the SDG Router POST was successful. If the light remains on or is off, go to Chapter 3 of the *2108 Model R03 Service Guide (MAP)*.

Part 2. Problem Determination

Chapter 15. Introduction to Fibre Channel problem determination

Fibre channel technology, outlined in the *Information Systems - Fibre Channel Protocol for SCSI (small computer system interface -FCP)* standard, revision 12, 30 May 1995, is a high-speed data transport technology used for mass storage and networking. This technology enables a network host bus adapter to connect the following components:

- Mainframe computers
- Super computers
- Workstations
- Storage devices
- Servers

Using a Fibre Channel Arbitrated Loop (FC-AL), a network can support 126 devices, compared to 15 devices with Ultra SCSI.

Fibre channel technology supports data transfer rates of 100 MB per second. A multimode optical interface is used for distances up to 500 meters. With increased connectivity and performance, fibre channel is the technology preference of system designers.

About problem determination

The problem determination portion of this manual provides problem determination and resolution information for the issues most commonly encountered with IBM® fibre channel devices and configurations. The problem determination portion of this manual contains useful component information, such as specifications, replacement and installation procedures, and basic symptom lists.

To use the problem determination portion of this guide correctly, begin by identifying a particular problem area from the lists provided in “Starting points for problem determination” on page 133. The starting points direct you to the related problem determination maps, which provide graphical directions for identifying and resolving problems. The problem determination maps in Chapter 16 might also refer you to other PD maps or to other chapters or appendices in this document. When completing tasks required by the PD maps, it might be helpful to refer to the component information provided in the hardware maintenance portion of this guide.

The procedures in the problem determination portion of this guide are designed to help you isolate problems. They are written with the assumption that you have model-specific training on all computers, or that you are familiar with the computers, functions, terminology, and service-related information provided in this manual and the appropriate IBM server hardware maintenance manual.

Installation and service information

For information about managed hubs and switches that might be in your network, refer to the individual publications for those devices:

- *IBM 3534 SAN Fibre Channel Managed Hub Installation and Service Guide SY27-7616*

- *IBM SAN Fibre Channel Switch 2109 Model S8 Installation and Service Guide SC26-7350*
- *IBM SAN Fibre Channel Switch 2109 Model S16 Installation and Service Guide SG26-7352*

This installation and service information can also be accessed on the World Wide Web:

http://www.ibm.com/storage/ibmsan/products.htm

Chapter 16. Problem determination starting points

This chapter contains information to help you perform the tasks required when following problem determination (PD) procedures. Review this information before attempting to isolate and resolve Fibre Channel problems. This chapter also provides summaries of the tools that might be useful in following the problem determination procedures provided in Chapter 17, “Problem determination maps”, on page 137.

Note: The PD maps in this document are not to be used in order of appearance. *Always begin working with the PD maps from the starting points provided in this chapter* (see “Starting points for problem determination” on page 133). Do not use a PD map unless you are directed there from a particular symptom or problem area in one of the lists of starting points, or from another PD map.

Problem determination tools

The problem determination maps in Chapter 17, “Problem determination maps”, on page 137 rely on numerous tools and diagnostic programs to isolate and fix the problems. You will use the following tools when performing the tasks directed by the PD maps:

Loopback Data Test

Host bus adapters type 2200 and above support loopback testing, which has now been integrated in the Fast!UTIL utility that can be invoked during system POST. Depending on the BIOS level or the type of adapter, the Alt+Q or Ctrl+Q key sequence starts the Fast!UTIL utility. (For more information on Fast!UTIL, see Chapter 30, “Using IBM Fast!UTIL”, on page 335.) The Loopback Data Test is a menu item in the utility. The Loopback test can also be run from the FAStT MSJ Diagnostics. (For more information on FAStT MSJ, see Chapter 18, “Introduction to FAStT MSJ”, on page 173.)

Wrap plugs

Wrap plugs are required to run the Loopback test at the host bus adapter or at the end of cables. There are two types of wrap plugs: SC and LC. SC wrap plugs are used for the larger connector cables. LC wrap plugs are smaller than SC wrap plugs and are used for the IBM FAStT700 Storage Server and the IBM FAStT FC-2 HBA. A coupler is provided for each respective form-factor to connect the wrap plugs to cables. The part numbers for the wrap plugs are:

- SC: 75G2725 (wrap/coupler kit)
- LC
  - 24P0950 (wrap connector/coupler kit)
  - 11P3847 (wrap connector packaged with FAStT700 Storage Server)
  - 05N6766 (coupler packaged with FAStT700 Storage Server)

Note: Many illustrations in this document depict the SC wrap plug. Substitute the LC wrap plug for the FAStT700 Storage Server (1742) and the IBM FAStT FC-2 HBA (2300).

SANavigator

SANavigator is a SAN discovery tool that displays link, device, and interconnecting problems. It monitors the health of the SAN and identifies problem areas. It provides a topological view of the SAN, displaying the devices, the interconnection, and the switch and controller port assignments. The SAN discovery is accomplished out-of-band through the network and (optionally) in-band through the Fibre medium. The HBA API library (supplied) is required for in-band management.

Install SANavigator to help you monitor your SAN and diagnose problems. See Chapter 19, “Introduction to SANavigator”, on page 217 for further details.

FAStT Management Suite Java® (FAStT MSJ)

FAStT MSJ is a network-capable application that can connect to and configure remote systems. With FAStT MSJ, you can perform loopback and read/write buffer tests to help you isolate problems.

See Chapter 18, “Introduction to FAStT MSJ”, on page 173 for further details on FAStT MSJ.

IBM FAStT Storage Manager 7.2 and 8.xx

The newest versions of FAStT Storage Manager (versions 7.2 and 8.xx) enable you to monitor events and manage storage in a heterogeneous environment. These new diagnostic and storage management capabilities fulfill the requirements of a true SAN, but also increase complexity and the potential for problems. Chapter 29, “Heterogeneous configurations”, on page 331 shows examples of heterogeneous configurations and the associated profiles from the FAStT Storage Manager. These examples can help you identify improperly configured storage by comparing the customer’s profile with those supplied (assuming similar configurations).

Event Monitoring has also been implemented in these versions of Storage Manager. The Event Monitor handles notification functions (e-mail and SNMP traps) and monitors storage subsystems whenever the Enterprise Management window is not open. Previous versions of the IBM FAStT storage-manager software did not have the Event Monitor and required that the Enterprise Management window be open in order to monitor the storage subsystems and receive alerts. The Event Monitor is a separate program bundled with the Storage Manager client software; it is a background task that runs independently of the Enterprise Management window.

In addition to these enhancements, controller run-time diagnostics have been implemented for Storage Controllers types 3526, 3542, 3552, and 1742. The FAStT Storage Manager version 8.xx also implements Read Link Status (RLS), which enables diagnostics to aid in troubleshooting drive-side problems. Storage Manager establishes a time stamped ″baseline″ value for drive error counts and keeps track of drive error events. The end user receives deltas over time as well as trends.

Considerations before starting PD maps

Because a wide variety of hardware and software combinations are possible, use the following information to assist you in problem determination. Before you use the PD maps, do the following:

- Verify any recent hardware changes.
- Verify any recent software changes.

- Verify that the BIOS is at the latest level. See “File updates” and specific server hardware maintenance manuals for details about this procedure.
- Verify that device drivers are at the latest levels. Refer to the device driver installation information in the installation guide for your device.
- Verify that the configuration matches the hardware.
- Verify that FAStT MSJ is at the latest level. For more information, see Chapter 18, “Introduction to FAStT MSJ”, on page 173.
- If SANavigator is not installed, install it to assist you in isolating problems. For more information, see Chapter 19, “Introduction to SANavigator”, on page 217. After SANavigator is installed, export the SAN to capture its current state. This will be useful in later diagnoses.

As you go through the problem determination procedures, consider the following questions:

- Do diagnostics fail?
- Is the failure repeatable?
- Has this configuration ever worked?
- If this configuration has been working, what changes were made prior to it failing?
- Is this the original reported failure? If not, try to isolate failures using the lists of indications (see “General symptoms” on page 134, “Specific problem areas” on page 134, and “PD maps and diagrams” on page 134).

Important

To eliminate confusion, systems are considered identical only if the following are *exactly* identical for *each* system:

- Machine type and model
- BIOS level
- Adapters and attachments (in same locations)
- Address jumpers, terminators, and cabling
- Software versions and levels

Comparing the configuration and software setup between working and non-working systems will often resolve problems.

File updates

Use the IBM support area on the World Wide Web (WWW) to download diagnostic, BIOS flash, and device driver files:

http://www.ibm.com/pc/support

SANavigator automatically links to the xSeries® Fibre Channel Solutions Web site. Right-click the desired device (a host bus adapter or a controller) and select IBM Solutions Support.

Starting points for problem determination

The lists of indications contained in this section provide you with entry points to the problem determination maps found in this chapter. (Links to useful appendix materials are also provided.) Use the following lists of problem areas as a guide for determining which PD maps will be most helpful.

General symptoms

- **RAID Controller passive**

  If you determine that a RAID Controller is passive, go to “RAID Controller Passive PD map” on page 139.
- **Failed or moved cluster resource**

  If you determine that a cluster resource has failed or has been moved, go to “Cluster Resource PD map” on page 140.
- **Startup long delay**

  If at startup you experience a long delay (more than 10 minutes), go to “Boot-up Delay PD map” on page 141.
- **Systems Management or Storage Manager performance problems**

  If you discover a problem through the Systems Management or Storage Management tools, go to “Systems Management PD map” on page 142.

Specific problem areas

- **Storage Manager**

  “Systems Management PD map” on page 142

  See also Chapter 31, “Storage Manager FAQs”, on page 343.
- **Port configuration (Linux)**

  “Linux Port Configuration PD map 1” on page 169
- **Windows NT Event Log**

  Chapter 21, “PD hints — RAID controller errors in the Windows NT event log”, on page 251
- **Indicator lights on devices**

  “Indicator lights and problem indications” on page 313
- **Major Event Log (MEL)**

  Chapter 32, “PD hints — MEL data format”, on page 353
- **Control panel or SCSI adapters**

  Refer to the driver installation information in the appropriate hardware chapter of the installation guide for your device.
- **Managed hub or switch logs**

  Chapter 27, “PD hints — Hubs and switches”, on page 321
- **Cluster Administrator**

PD maps and diagrams

- **Configuration Type Determination**

  To determine whether your configuration is type 1 or type 2, go to “Configuration Type PD map” on page 138.

  In order to break larger configurations into manageable units for debugging, see Chapter 22, “PD hints — Configuration types”, on page 265.
- **Hub or Switch PD**

  If you determine that a problem exists within a hub or switch, go to “Hub/Switch PD map 2” on page 145.
- **Fibre Path PD**

  If you determine that a problem exists within the Fibre Path, go to “Fibre Path PD map 1” on page 148.
- **Device PD**

If you determine that a problem exists within a device, go to “Device PD map 1” on page 154.

- **SANavigator PD**

  If SANavigator is installed (as is strongly suggested), go to “Diagnosing with SANavigator PD map 1” on page 156.

Chapter 17. Problem determination maps

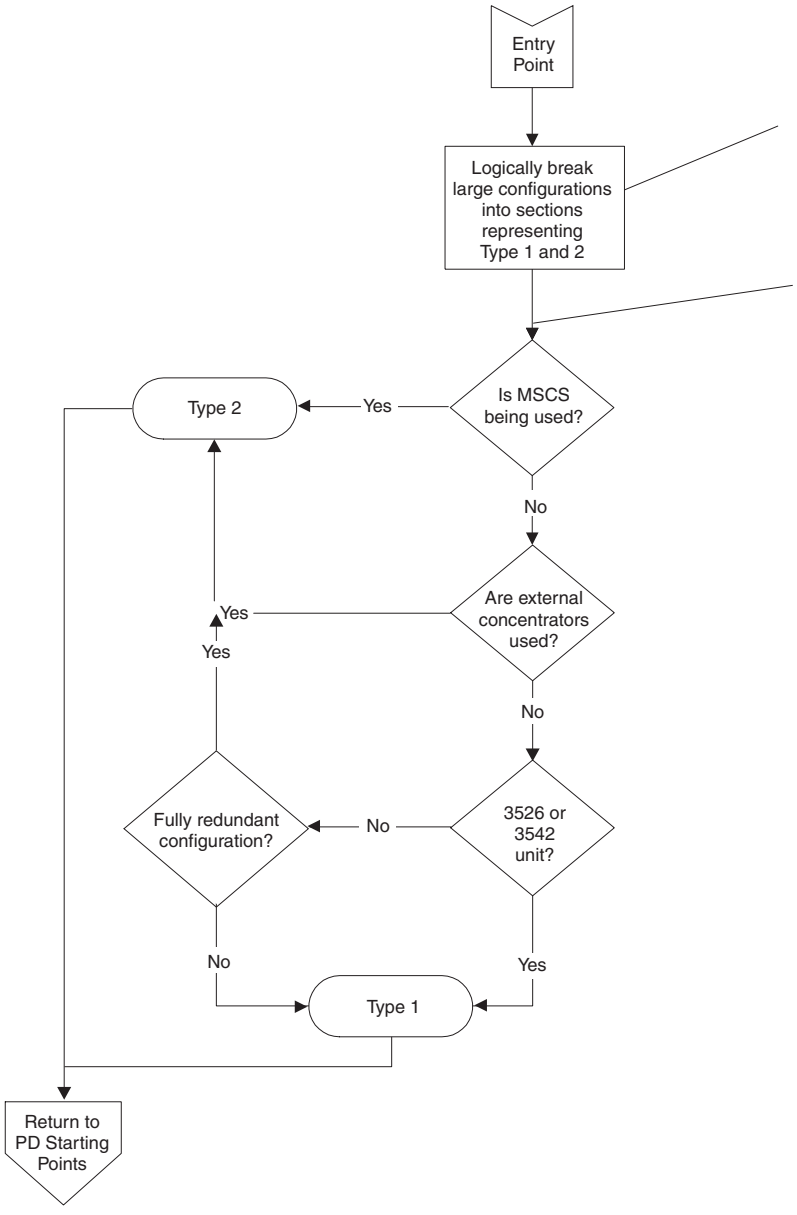
This chapter contains a series of problem determination maps which guide you through problem isolation and resolution. Before you use any of the following PD maps, you should have reviewed the information in Chapter 16, “Problem determination starting points”, on page 131.

The PD maps in this chapter are not to be used in order of appearance. *Always begin working with the PD maps from the starting points provided in the previous chapter* (see “Starting points for problem determination” on page 133). Do not use a PD map unless you are directed there from a particular symptom or problem area in one of the lists of starting points, or from another PD map.

Configuration Type PD map

To perform certain problem determination procedures, you need to determine whether your fibre configuration is Type 1 or Type 2. Use this map to make that determination. You will need this information for later PD procedures.

Configuration Type PD map



Additional information: See Chapter 22, “PD hints — Configuration types”, on page 265.

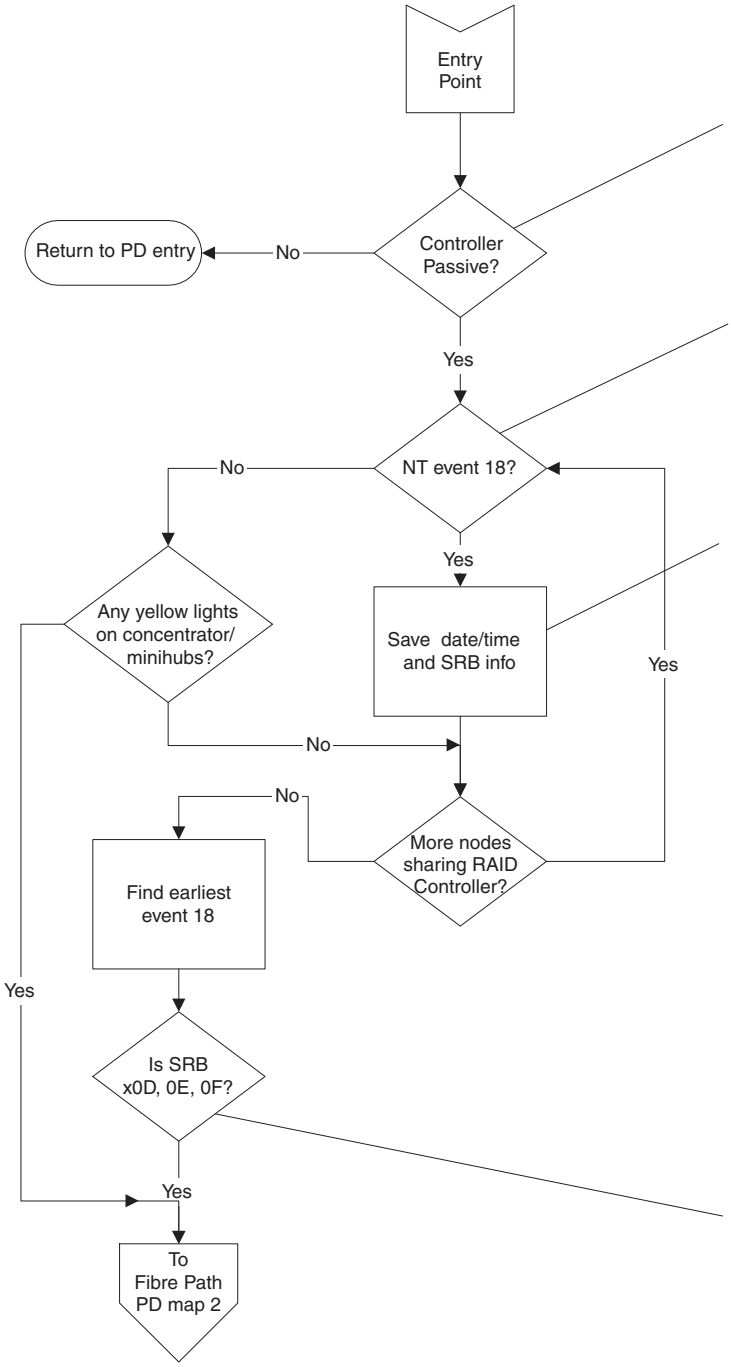
Note: Repeat this process for each section.

To return to the PD starting points, go to page 131.

RAID Controller Passive PD map

From: “General symptoms” on page 134; “Cluster Resource PD map” on page 140.

Controller Passive PD map



Additional information: See Chapter 23, “PD hints — Passive RAID controller”, on page 271.

Additional information: Use MEL information to find the approximate fail time in the Windows NT Event Log. See Chapter 32, “PD hints — MEL data format”, on page 353.

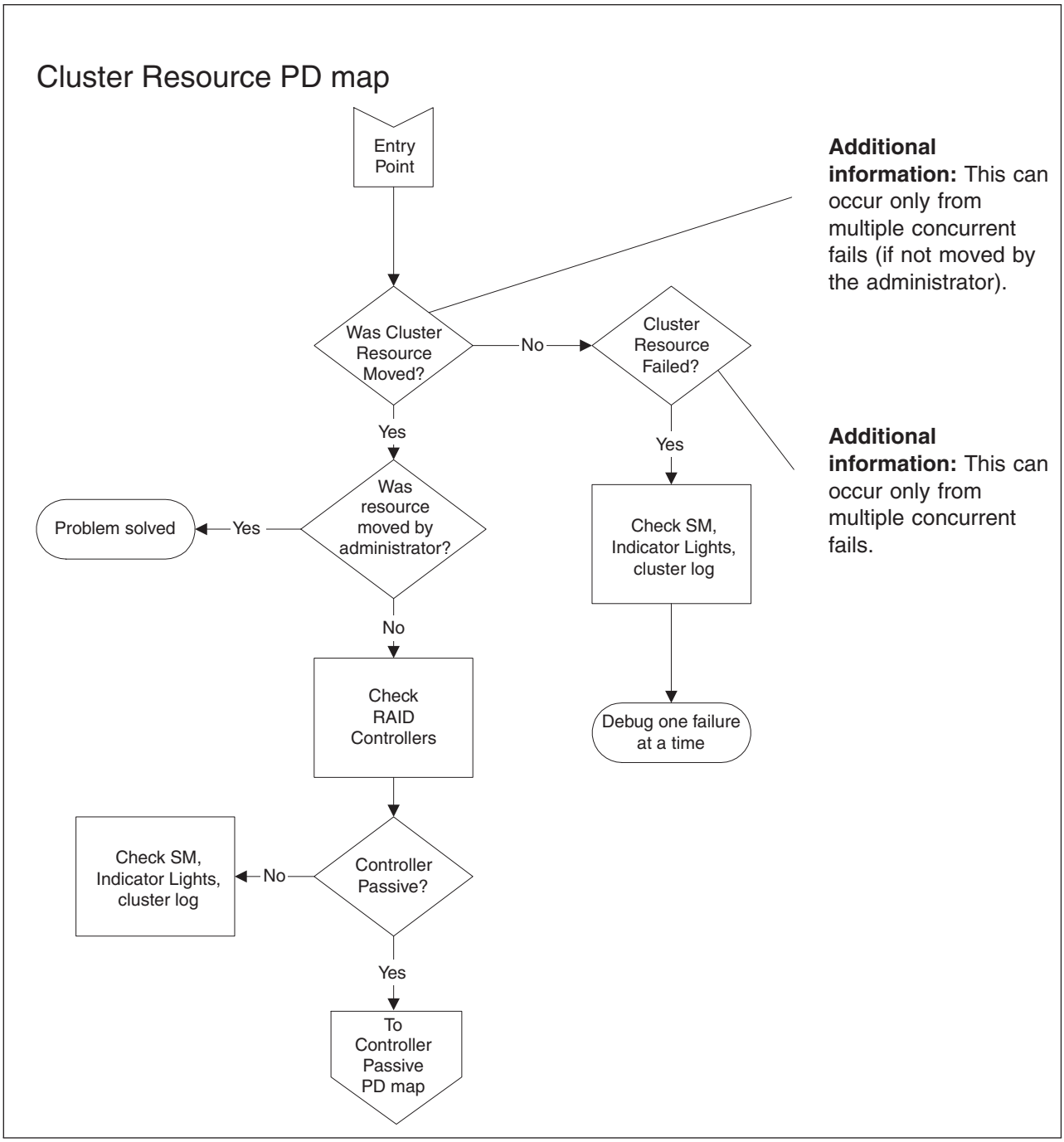
Additional information: See Chapter 21, “PD hints — RAID controller errors in the Windows NT event log”, on page 251.

Additional information: See Chapter 21, “PD hints — RAID controller errors in the Windows NT event log”, on page 251.

To see Fibre Path PD map 2, go to “Fibre Path PD map 2” on page 149.

Cluster Resource PD map

From: “General symptoms” on page 134.

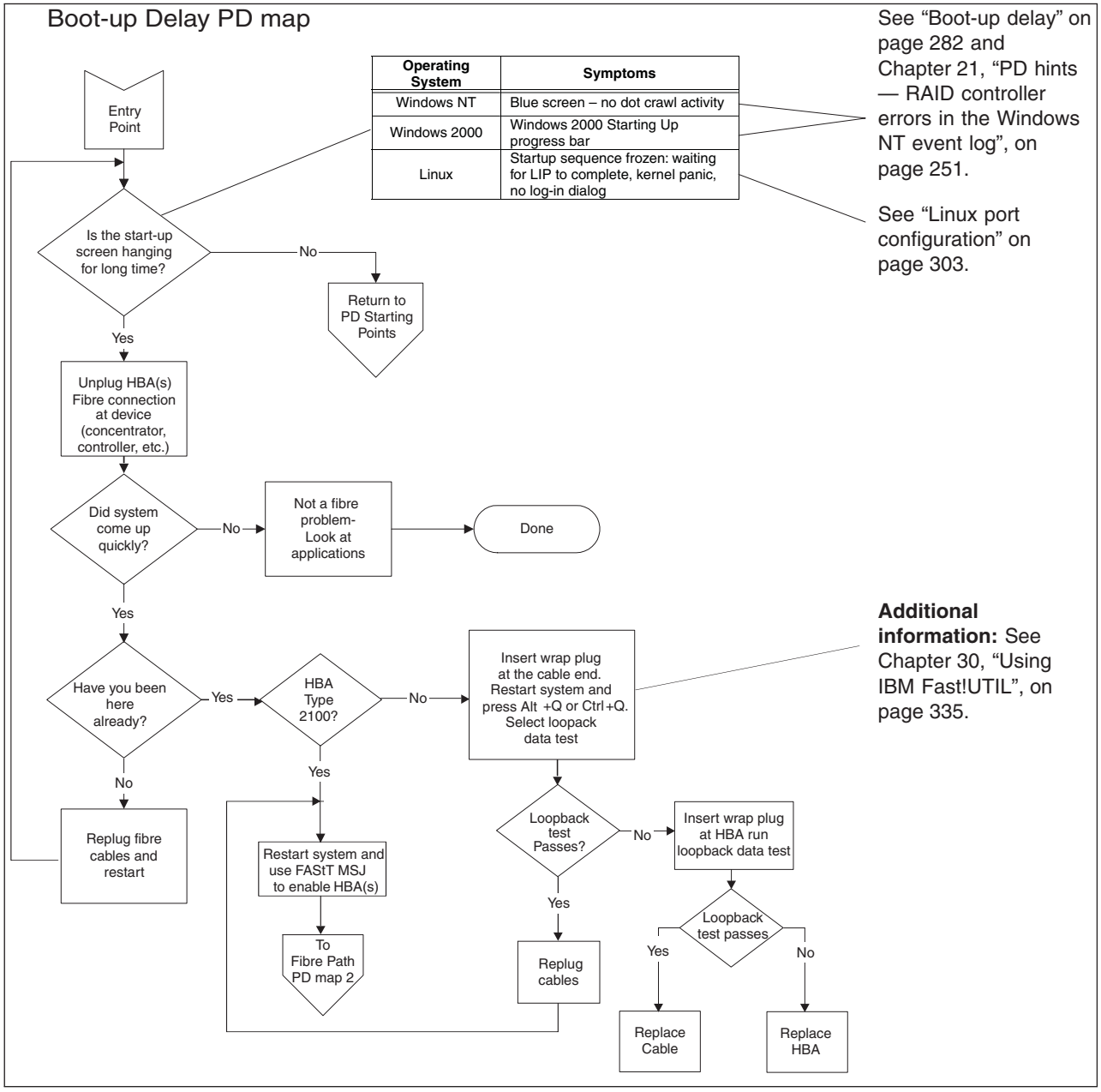


To see the Controller Passive PD map, go to “RAID Controller Passive PD map” on page 139.

Boot-up Delay PD map

From: “General symptoms” on page 134.

To see the screens necessary to perform this check, see “Boot-up delay” on page 282.



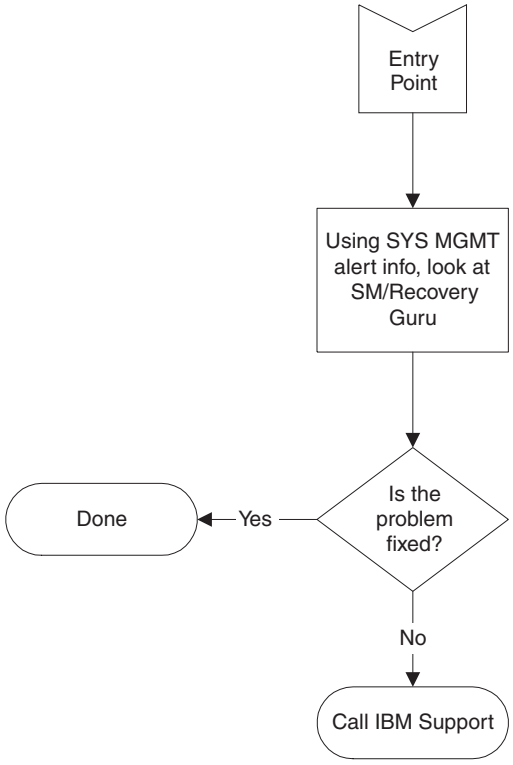
To return to the options for PD entry, go to page 131.

To see Fibre Path PD map 2, go to “Fibre Path PD map 2” on page 149.

Systems Management PD map

From: “General symptoms” on page 134.

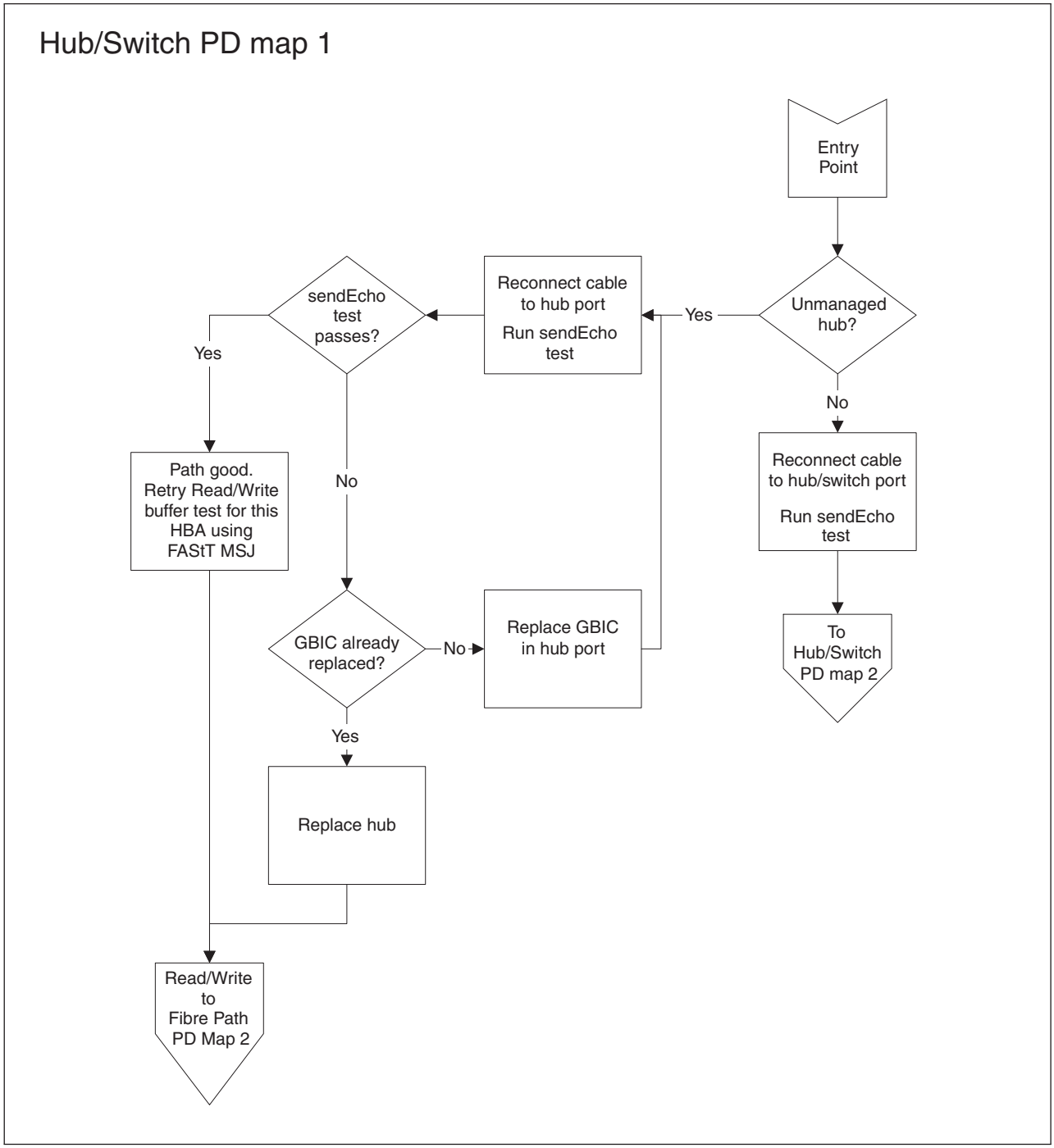
Systems Management



Additional information:
See Chapter 31, “Storage Manager FAQs”, on page 343

Hub/Switch PD map 1

From: “PD maps and diagrams” on page 134; “Single Path Fail PD map 2” on page 151.



For information about sendEcho tests, see Chapter 24, “PD hints — Performing sendEcho tests”, on page 275.

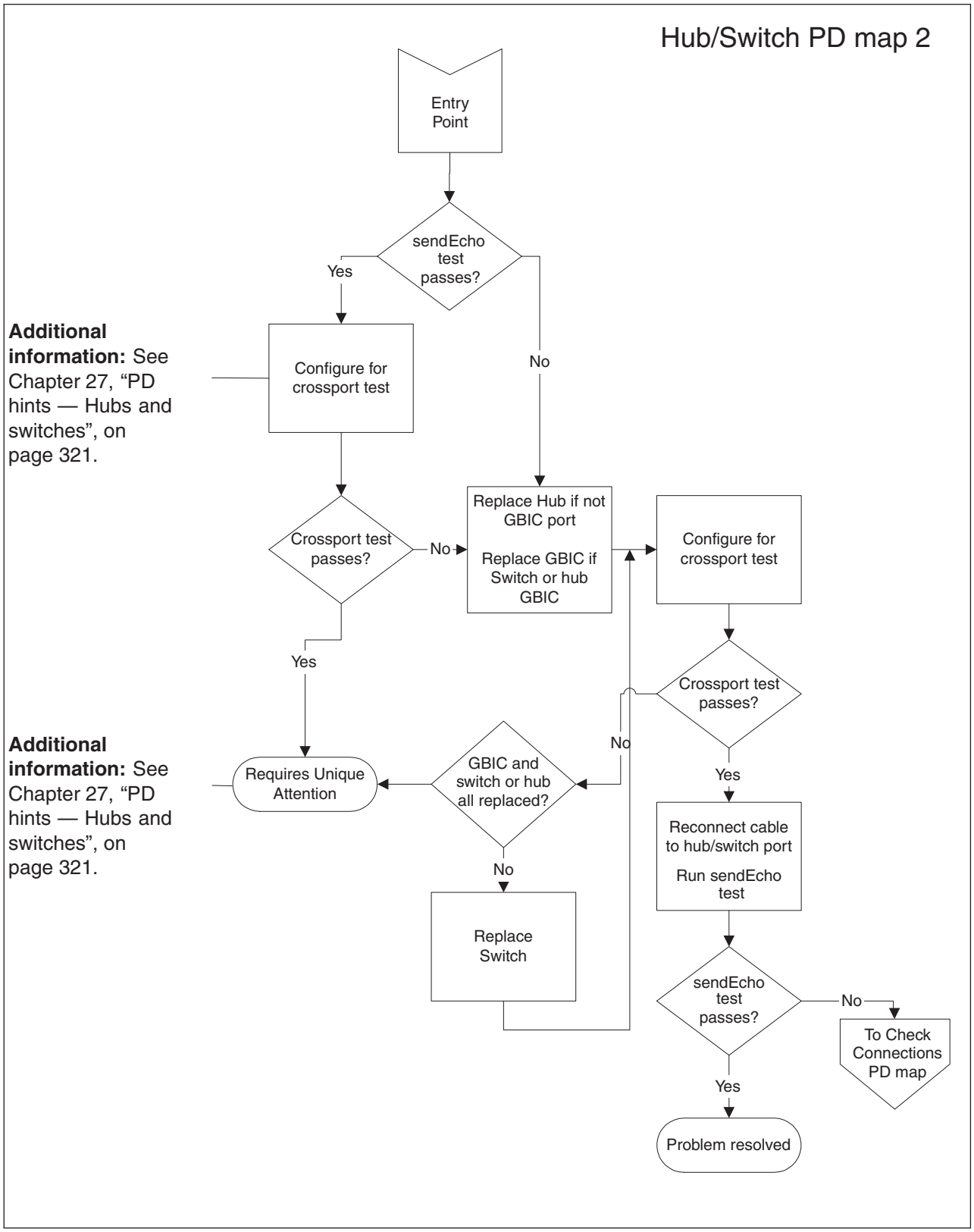
For information about Read/Write Buffer tests, see Chapter 18, “Introduction to FAStT MSJ”, on page 173.

To see Hub/Switch PD map 2, go to “Hub/Switch PD map 2” on page 145.

To see Fibre Path PD map 2, go to “Fibre Path PD map 2” on page 149.

Hub/Switch PD map 2

From: “Hub/Switch PD map 1” on page 143.



Additional information: See Chapter 27, “PD hints — Hubs and switches”, on page 321.

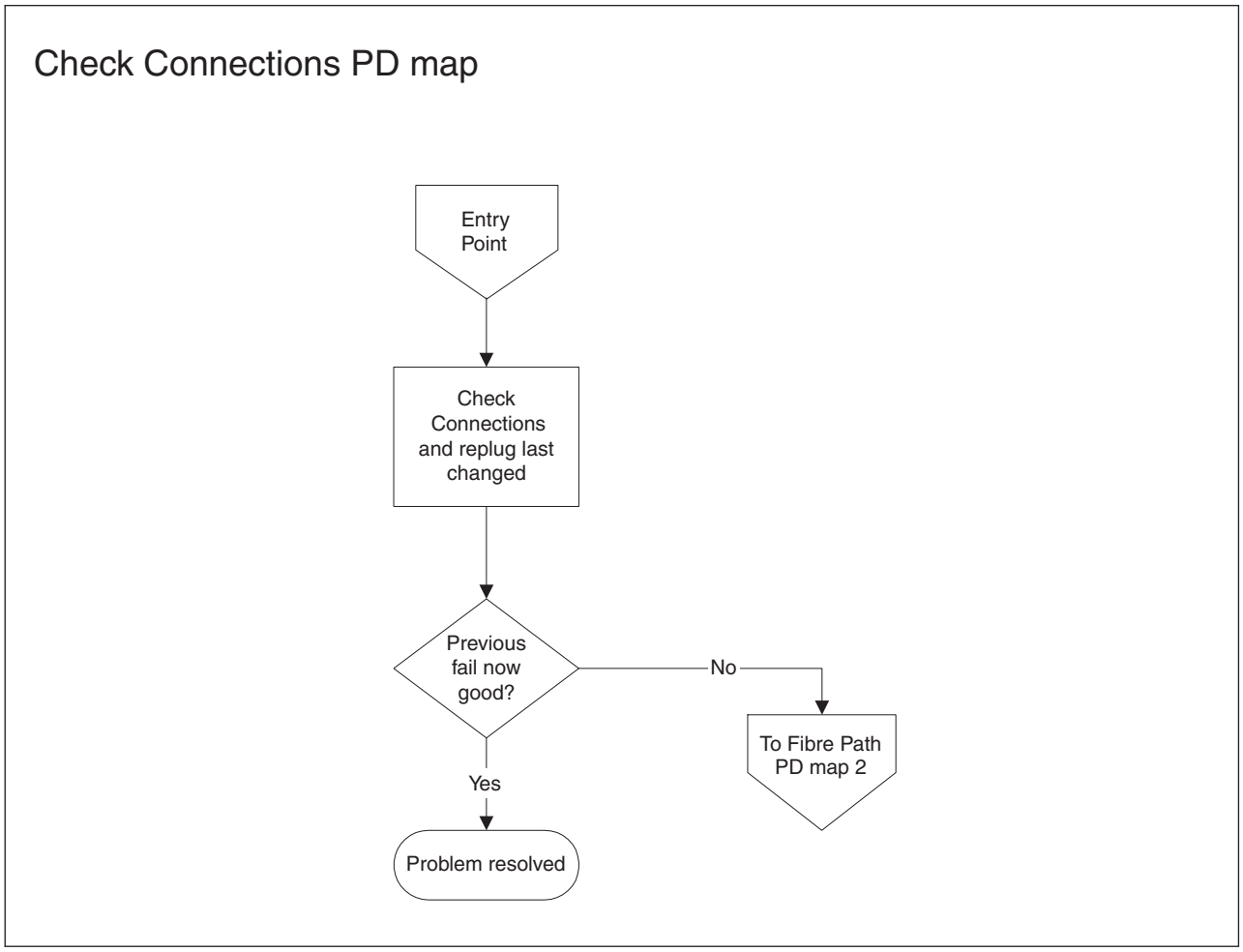
Additional information: See Chapter 27, “PD hints — Hubs and switches”, on page 321.

For information about sendEcho tests, see Chapter 24, “PD hints — Performing sendEcho tests”, on page 275.

To see the Check Connections PD map, see “Check Connections PD map” on page 147.

Check Connections PD map

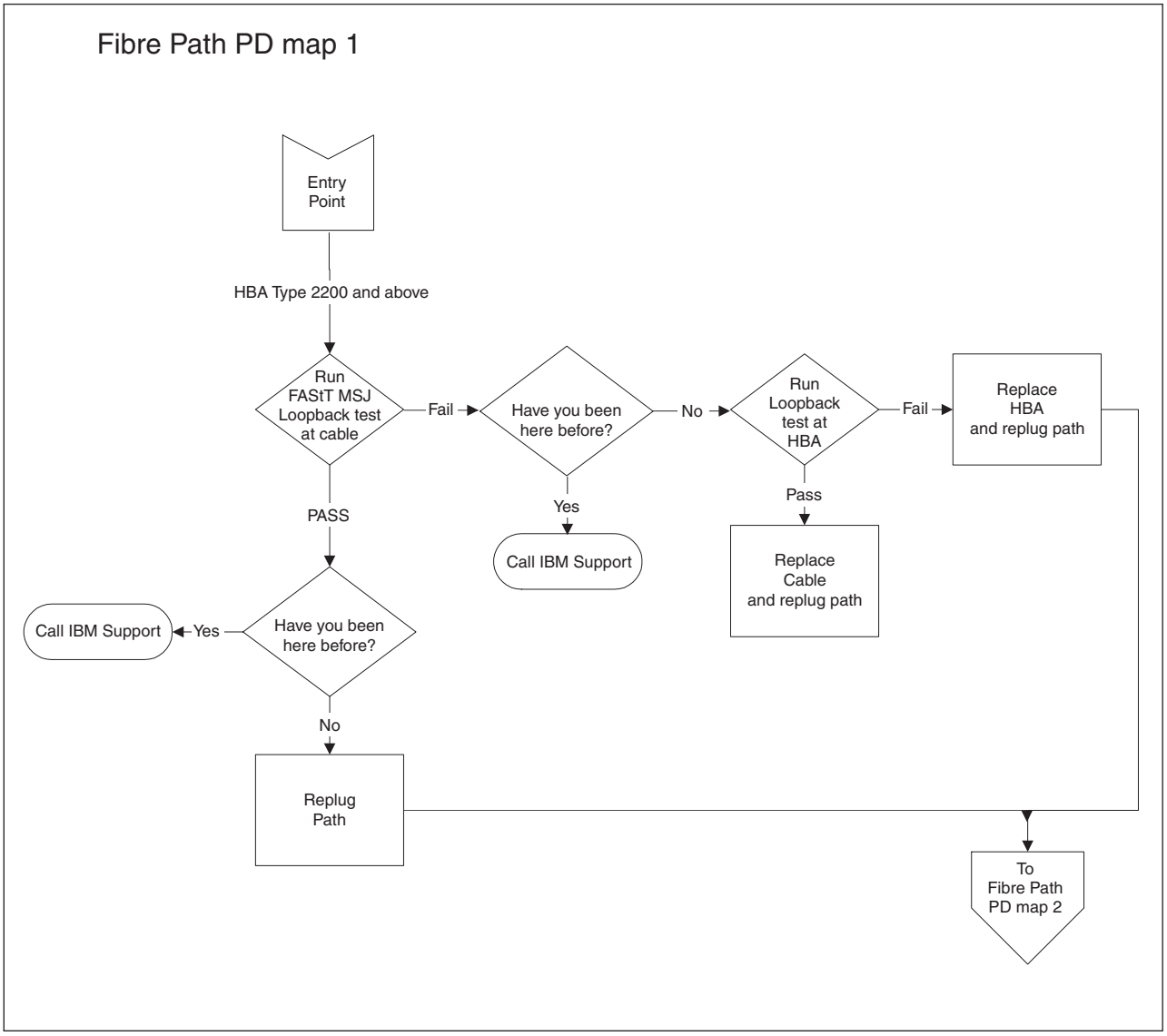
From: “Hub/Switch PD map 2” on page 145.



To see Fibre Path PD map 2, go to “Fibre Path PD map 2” on page 149.

Fibre Path PD map 1

From: “Common Path PD map 2” on page 153; “Diagnosing with SANavigator PD map 2” on page 159.

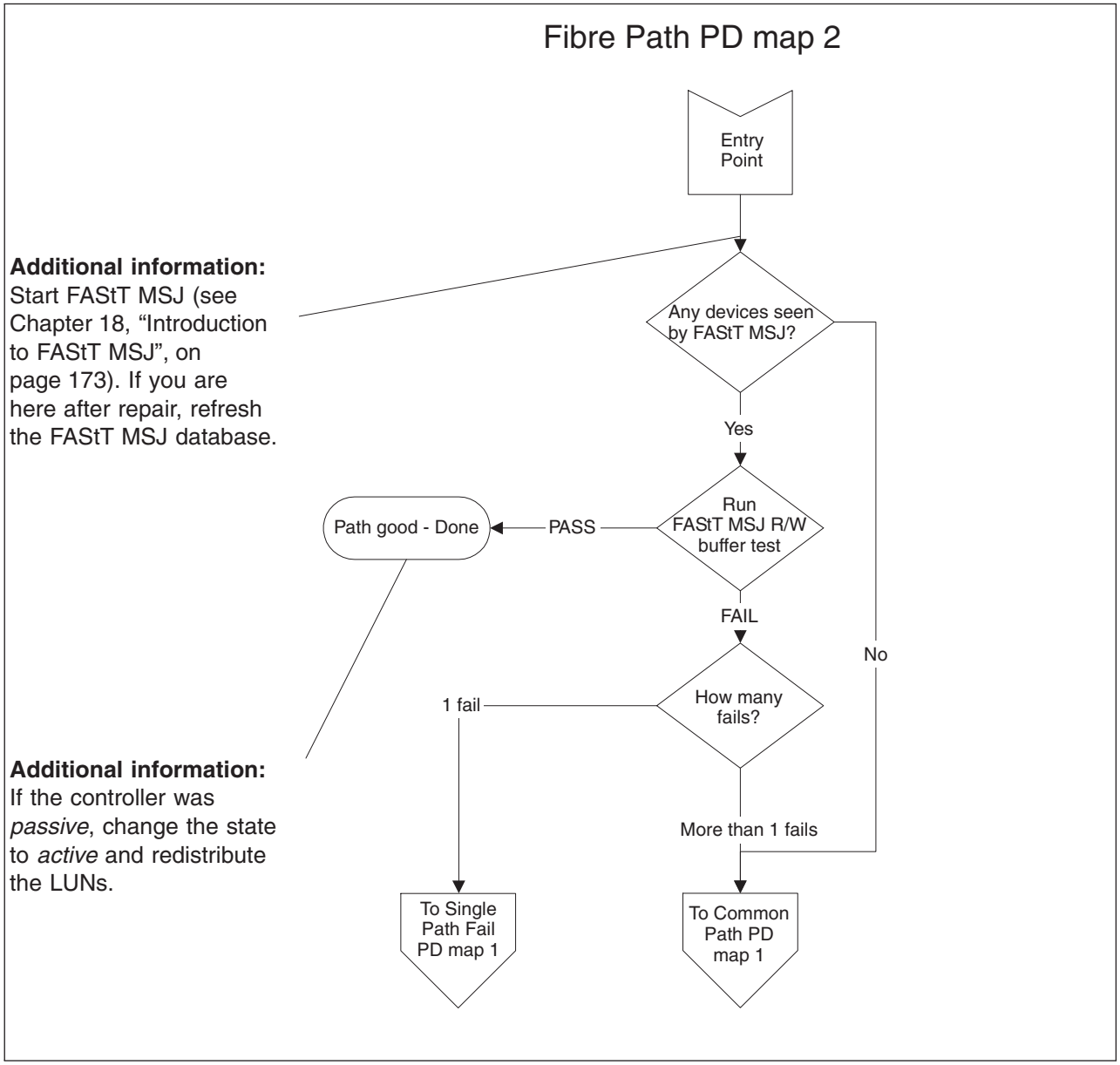


For information about running loopback tests, see Chapter 18, “Introduction to FAStT MSJ”, on page 173.

To see Fibre Path PD map 2, go to “Fibre Path PD map 2” on page 149.

Fibre Path PD map 2

From: “Fibre Path PD map 1” on page 148; “Check Connections PD map” on page 147; “RAID Controller Passive PD map” on page 139; “Boot-up Delay PD map” on page 141; “Hub/Switch PD map 1” on page 143; “Diagnosing with SANavigator PD map 2” on page 159.

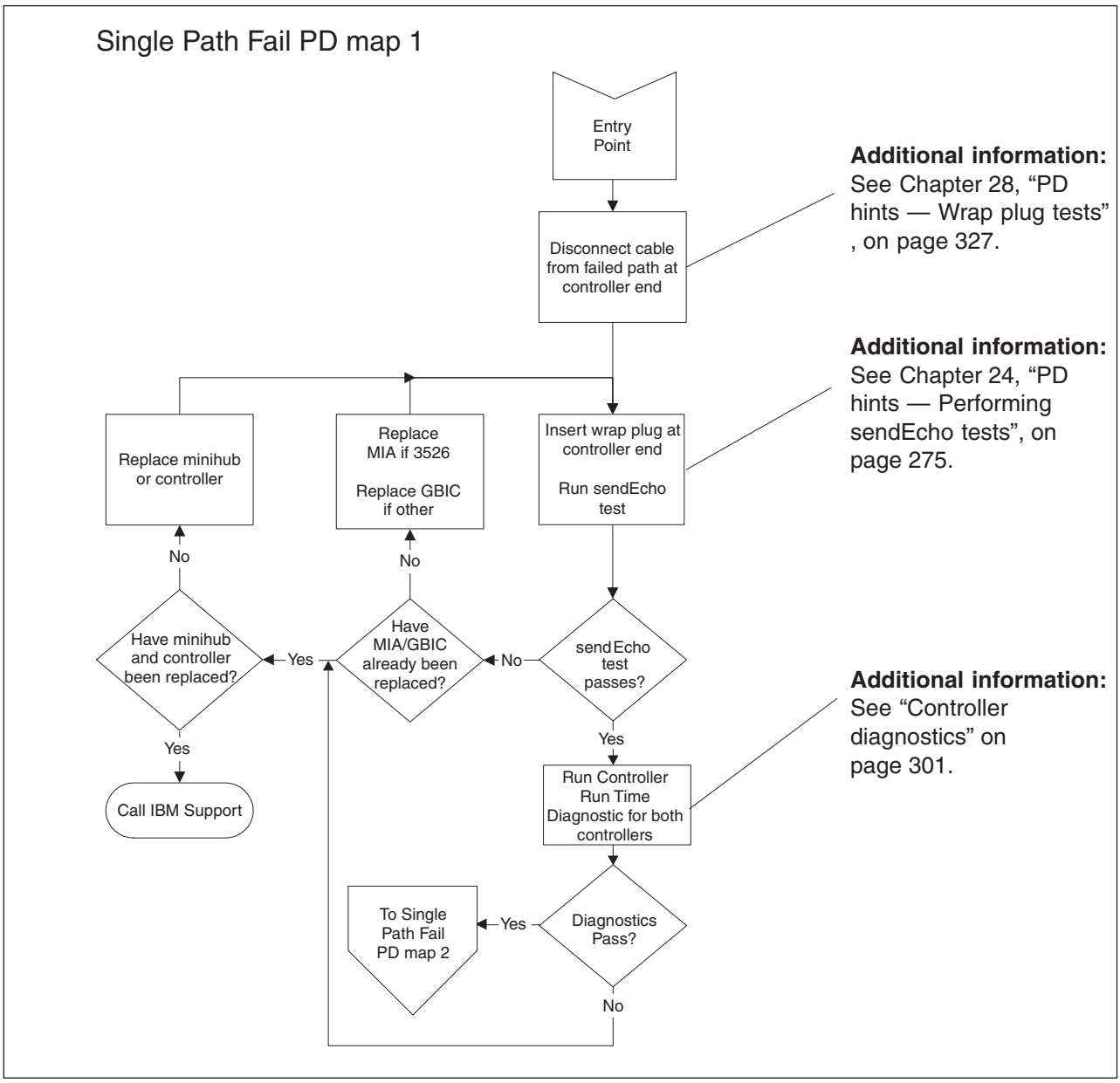


To see Single Path Fail PD map 1, go to “Single Path Fail PD map 1” on page 150.

To see Common Path PD map 1, go to “Common Path PD map 1” on page 152.

Single Path Fail PD map 1

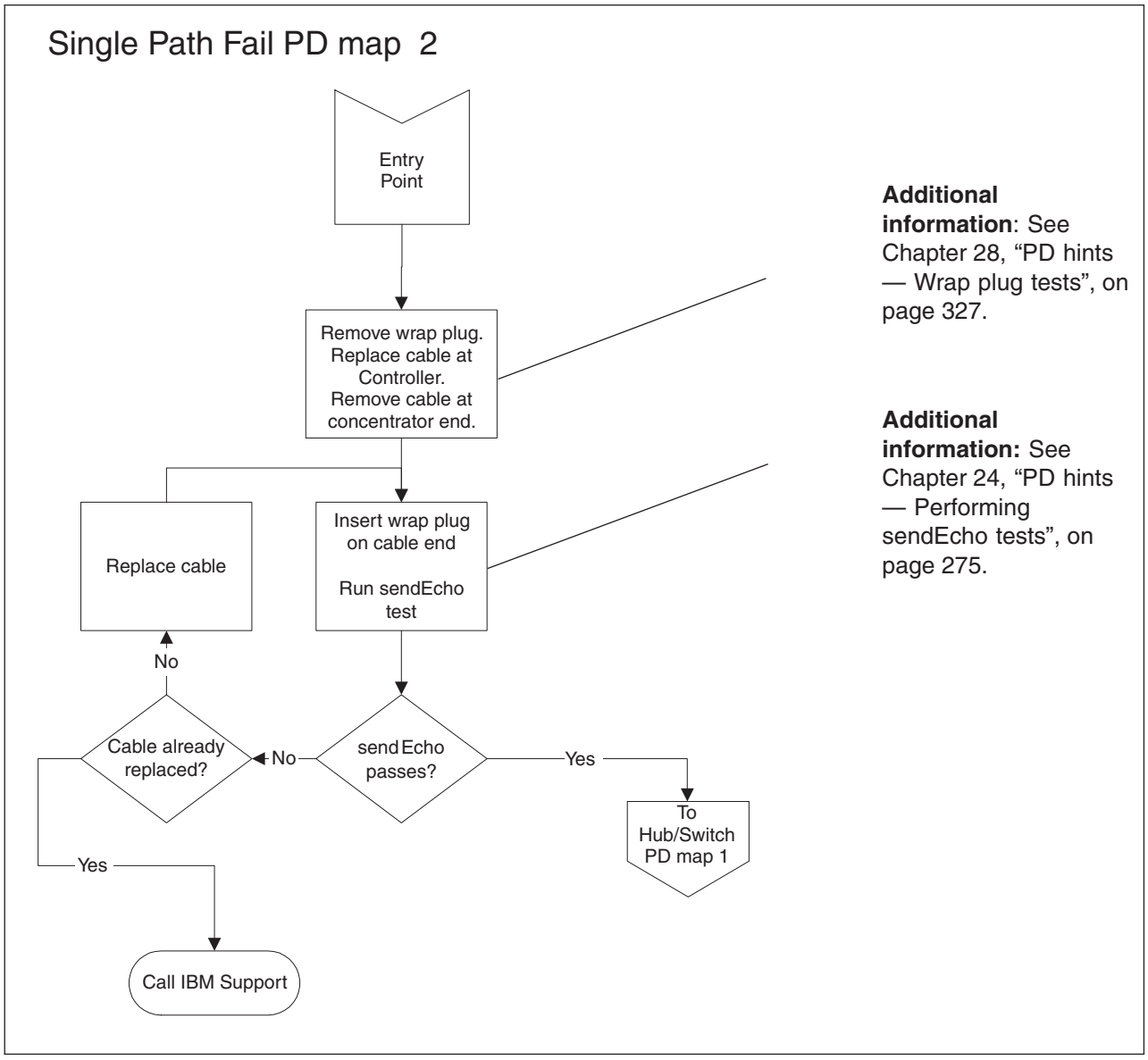
From: “Fibre Path PD map 2” on page 149; “Diagnosing with SANavigator PD map 1” on page 156; “Diagnosing with SANavigator PD map 3” on page 161.



To see Single Path Fail PD map 2, go to “Single Path Fail PD map 2” on page 151.

Single Path Fail PD map 2

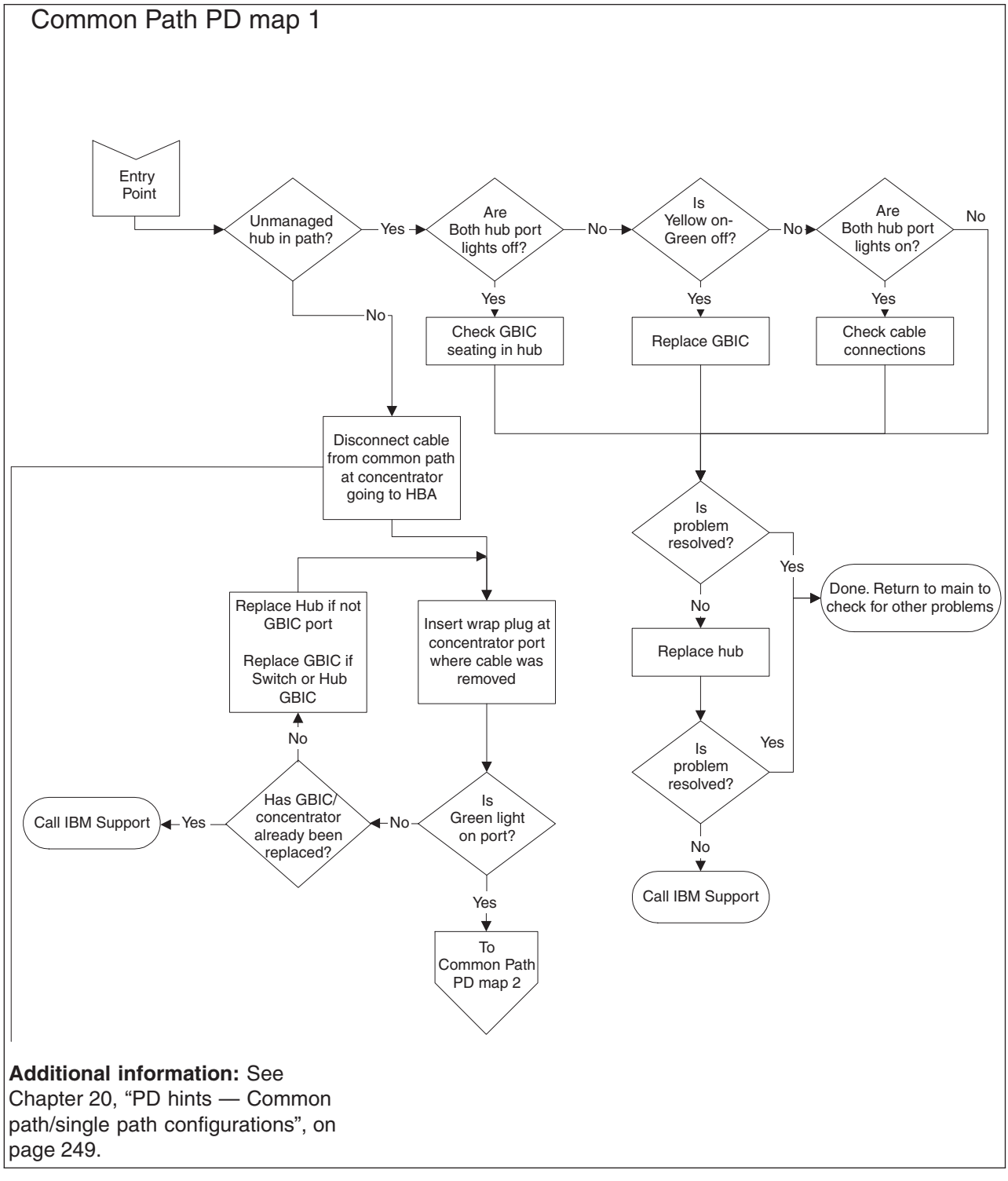
From: “Single Path Fail PD map 1” on page 150.



To see Hub/Switch PD map 1, go to “Hub/Switch PD map 1” on page 143.

Common Path PD map 1

From: “Fibre Path PD map 2” on page 149.

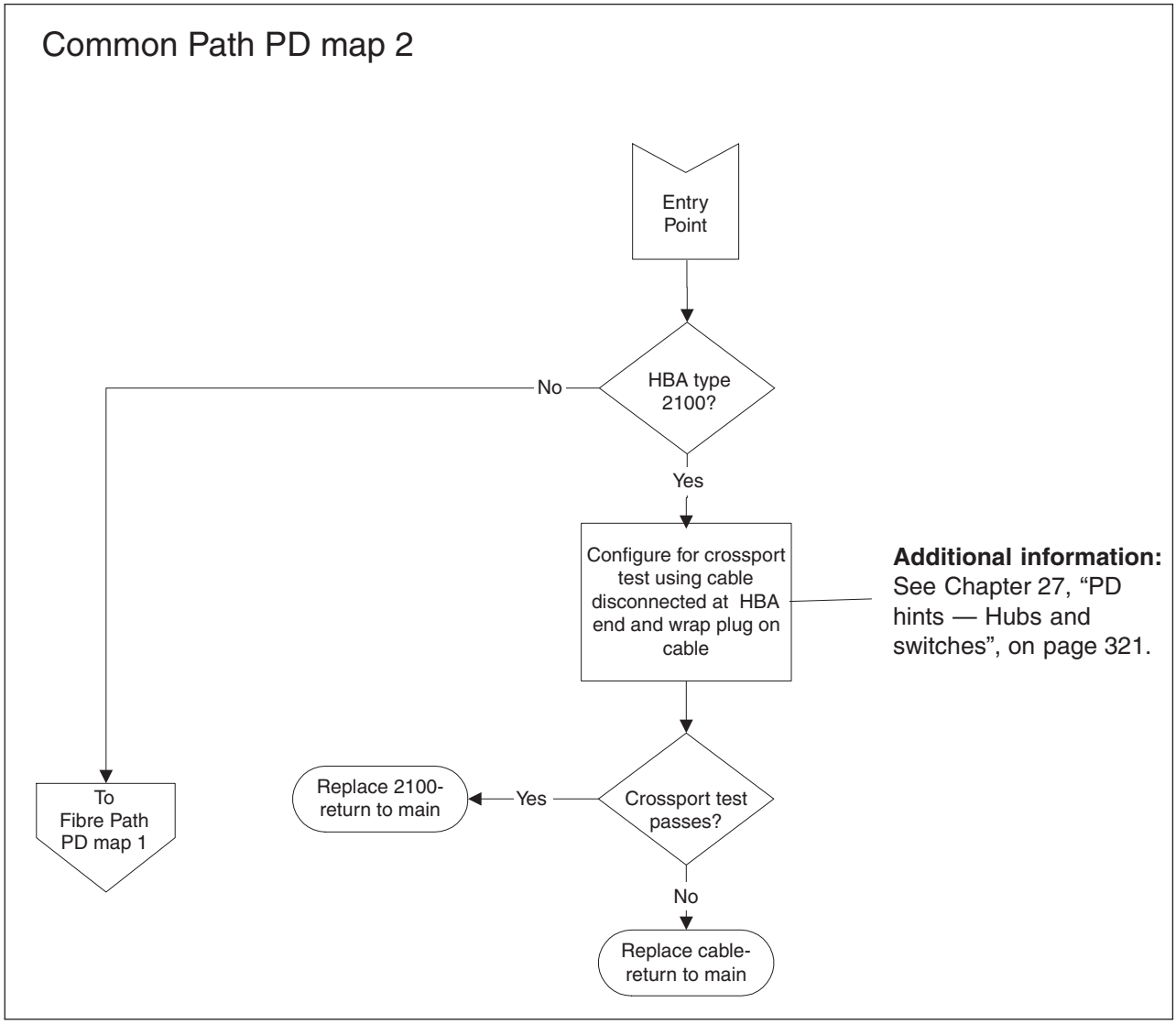


Additional information: See Chapter 20, “PD hints — Common path/single path configurations”, on page 249.

To see Common Path PD map 2, go to “Common Path PD map 2” on page 153.

Common Path PD map 2

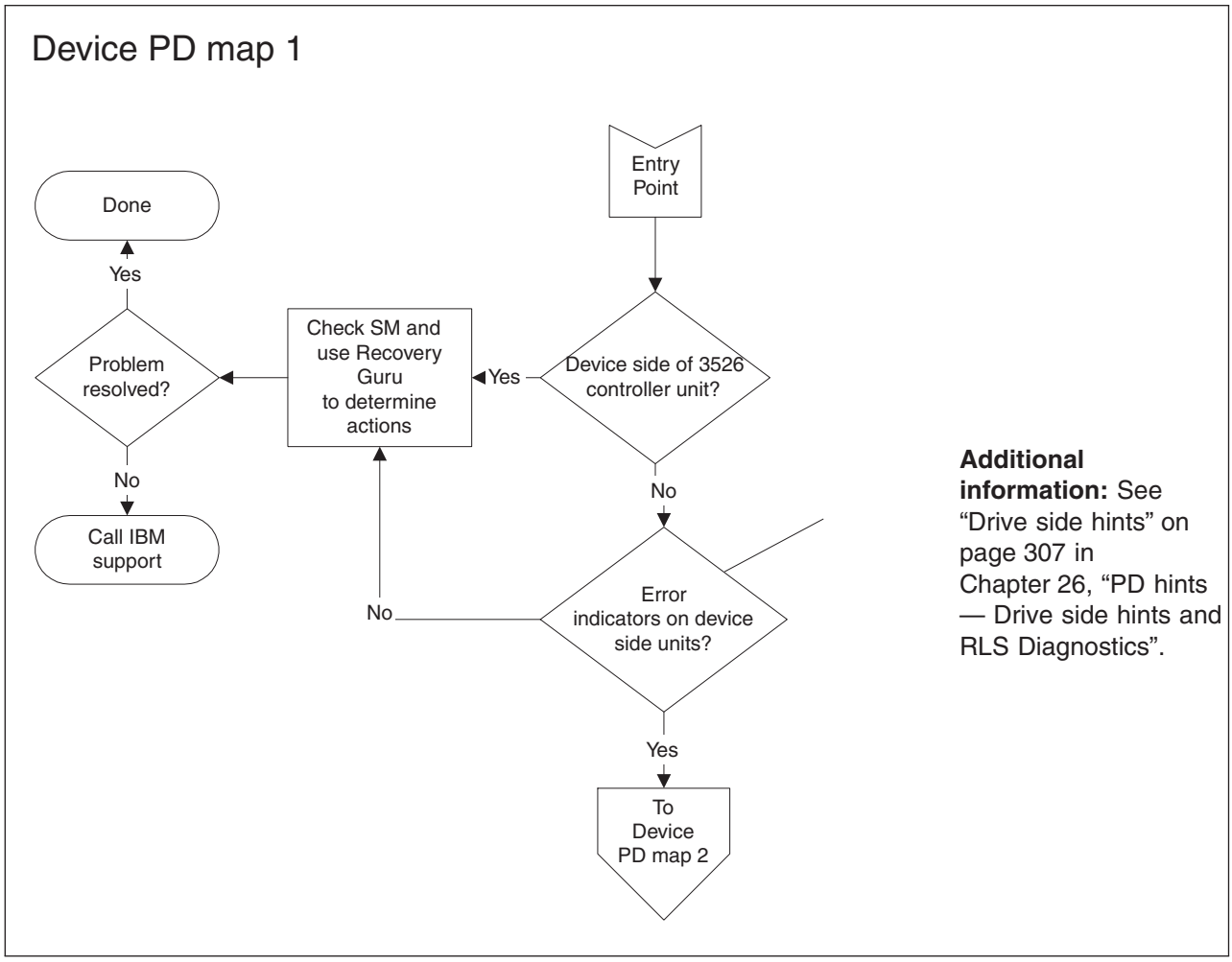
From: “Common Path PD map 1” on page 152; “Diagnosing with SANavigator PD map 1” on page 156.



To see Fibre Path PD map 1, go to “Fibre Path PD map 1” on page 148.

Device PD map 1

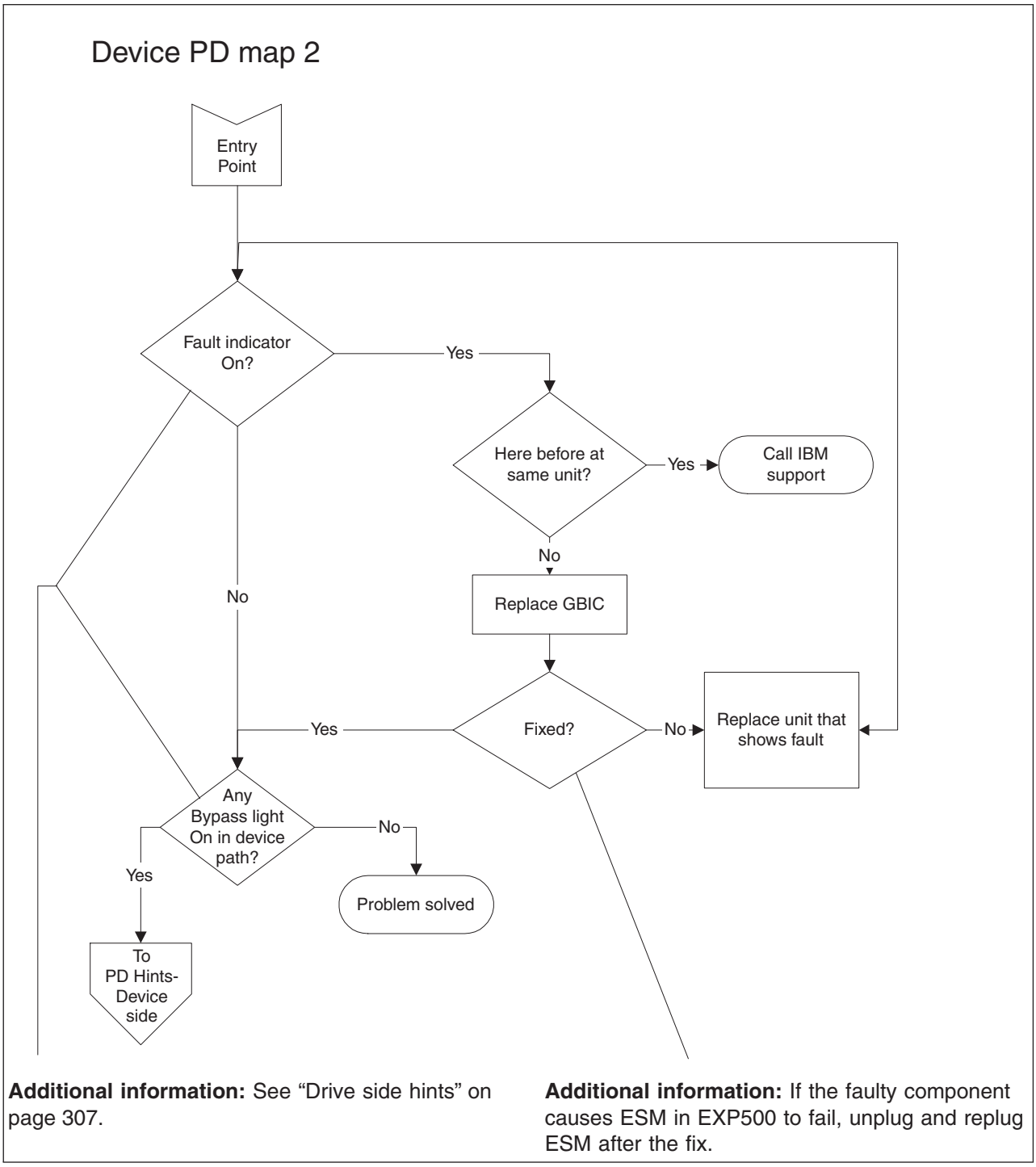
From: “PD maps and diagrams” on page 134.



To see Device PD map 2, go to “Device PD map 2” on page 155.

Device PD map 2

From: “Device PD map 1” on page 154.



Additional information: See “Drive side hints” on page 307.

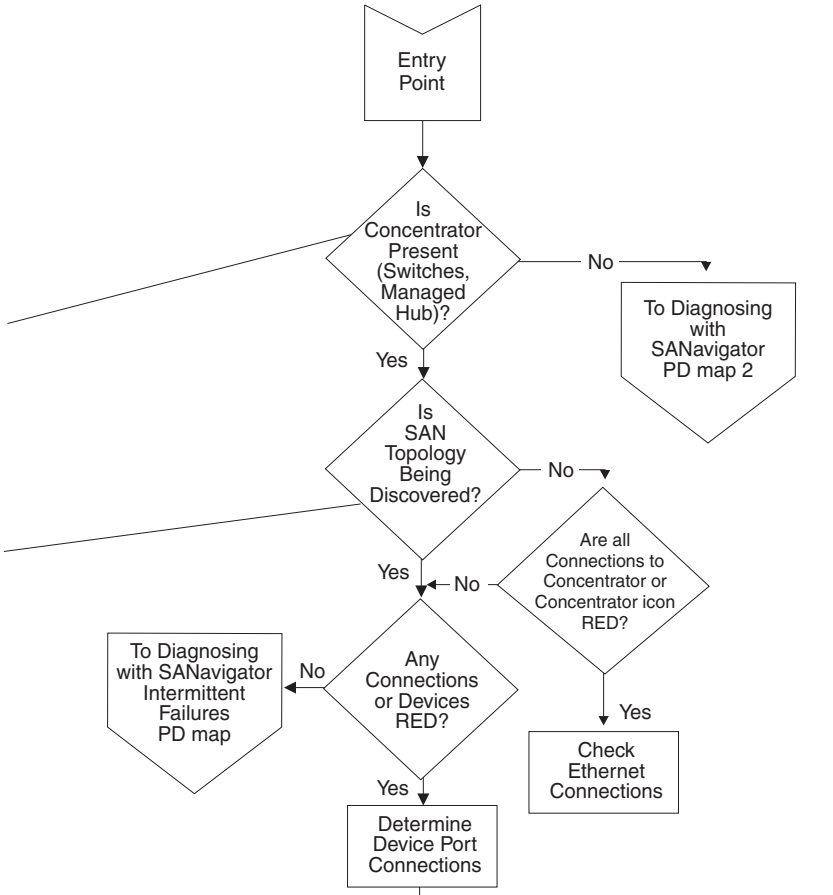
Additional information: If the faulty component causes ESM in EXP500 to fail, unplug and replug ESM after the fix.

To see PD hints about troubleshooting the device (drive) side, go to “Drive side hints” on page 307 in Chapter 26, “PD hints — Drive side hints and RLS Diagnostics”.

Diagnosing with SANavigator PD map 1

From: “PD maps and diagrams” on page 134.

Diagnosing with SANavigator PD map 1



If unsure, see "Configuration Type PD map" on page 138.

Additional information: See Chapter 19, "Introduction to SANavigator", on page 217. Verify that both In-band and Out-of-band are enabled.

Go to Table 65 on page 297.

HBA Inner Diamond	HBA Outer Diamond	All Storage Devices Inner Diamond on same Concentrator	All Storage Devices Outer Diamond on same Concentrator	Action
R	G	R	G	Suspect HBA. To Common Path PD Map 2
G	R	R	G	Suspect cable from HBA, GBIC\Port at concentrator. To Common Path PD Map 2
R	R	R	G	Suspect HBA. To Common Path PD Map 2
C	R	C	G	To Common Path PD Map 2

R-Red
G=Green
C=Clear (In-band disabled)

Storage Server Icon	Storage Server Inner Diamond	Storage Server Outer Diamond	Controller Connection to Concentrator	HBA on same Concentrator Inner Diamond	HBA on same Concentrator Outer Diamond	Action
R	R or C	R	--	G or C	G	Check all cables between Concentrator and Storage Server. Suspect concentrator or Storage Server.
G	R	G	--	R	G	Make sure in-band is enabled. If enabled, suspect HBA. Go to Common Path PD Map 2.
G	R or C	G	R	G or C	G	Go to Single Path Fail PD Map 1

R-Red
G=Green
C=Clear (In-band disabled)
--=Don't care

To see Diagnosing with SANavigator PD map 2, see “Diagnosing with SANavigator PD map 2” on page 159.

To see Common Path PD map 2, see “Common Path PD map 2” on page 153.

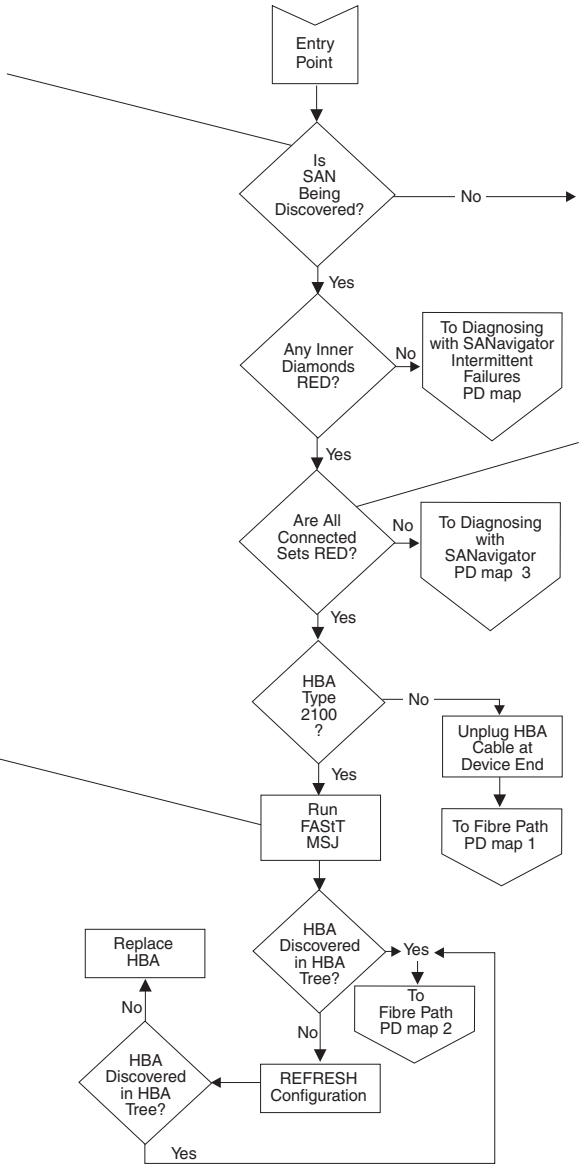
To see the Intermittent Failures PD map, see “Diagnosing with SANavigator - Intermittent Failures PD map” on page 162.

To see Single Path Fail PD map 1, see “Single Path Fail PD map 1” on page 150.

Diagnosing with SANavigator PD map 2

From: “Diagnosing with SANavigator PD map 1” on page 156. This PD map is applicable only to Direct Connect Configurations (either to Controllers or un-managed hubs). It assumes that In-Band discovery is enabled.

Diagnosing with SANavigator PD map 2



Hint: Verify that in-band discovery is enabled.

SANavigator Set-up problem: See Chapter 19, “Introduction to SANavigator”, on page 217.

Hint: No device is being detected by HBA and HBA inner diamond is RED.

Additional Information: see Chapter 18, “Introduction to FAStT MSJ”, on page 173

To see Fibre Path PD map 1, see “Fibre Path PD map 1” on page 148.

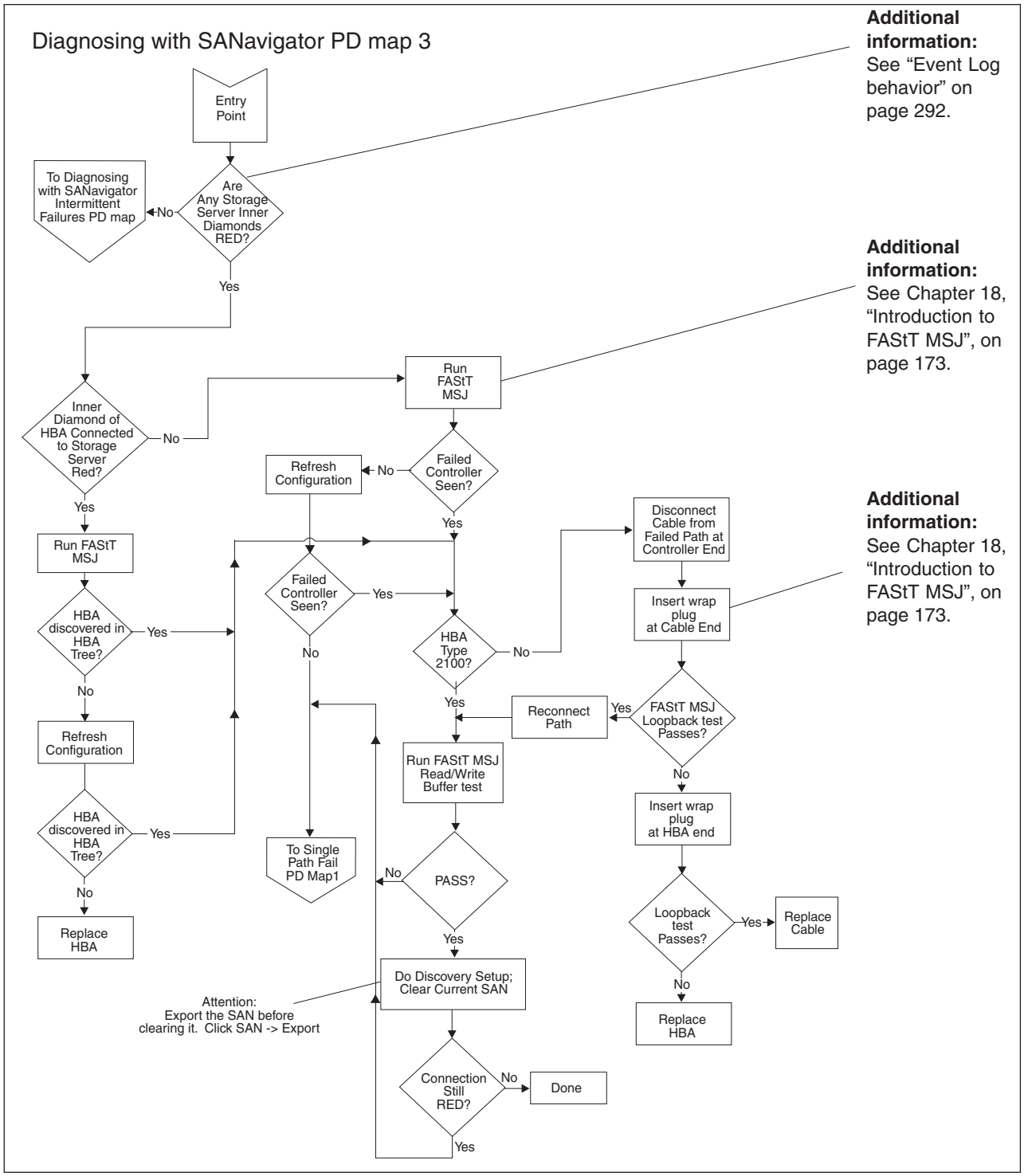
To see Fibre Path PD map 2, see “Fibre Path PD map 2” on page 149.

To see the Intermittent Failures PD map, see “Diagnosing with SANavigator - Intermittent Failures PD map” on page 162.

To see Diagnosing with SANavigator PD map 3, see “Diagnosing with SANavigator PD map 3” on page 161.

Diagnosing with SANavigator PD map 3

From: “Diagnosing with SANavigator PD map 2” on page 159.



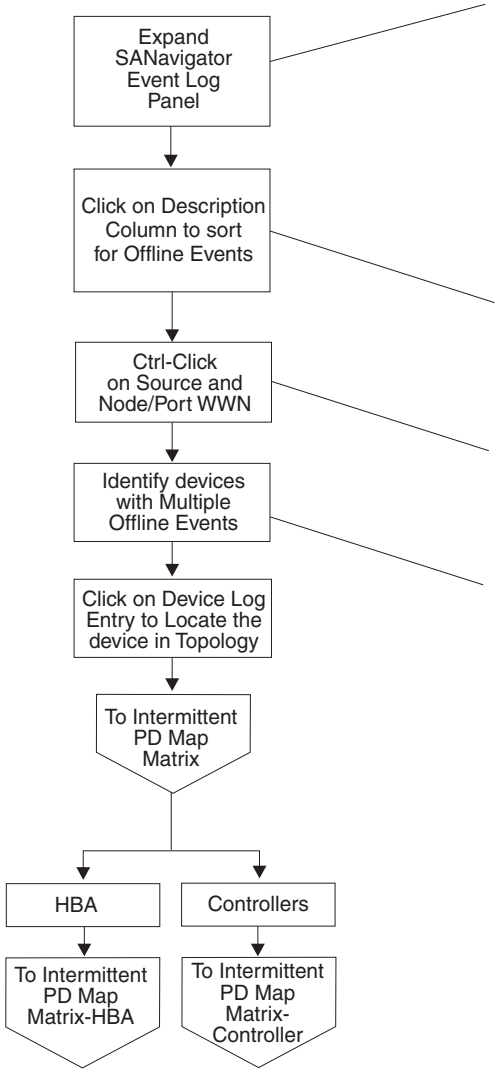
To see the Intermittent Failures PD map, see “Diagnosing with SANavigator - Intermittent Failures PD map” on page 162.

To see Single Path Fail PD map 1, see “Single Path Fail PD map 1” on page 150.

Diagnosing with SANavigator - Intermittent Failures PD map

From: “Diagnosing with SANavigator PD map 1” on page 156; “Diagnosing with SANavigator PD map 2” on page 159; “Diagnosing with SANavigator PD map 3” on page 161.

Diagnosing with SANavigator - Intermittent Failures PD map



Additional information: See Chapter 19, “Introduction to SANavigator”, on page 217.

Hint: Filter the Event Log to display fatal errors only.

Hint: You can move the columns in the Event Log to any desired location by clicking on and then dragging the title bar.

Additional information: See “Event Log behavior” on page 292.

(**Hint:** Connection Offline events for devices are also preceded or followed by Concentrator Connection Offline events. When looking for multiple offline events to isolate the intermittent device, focus on the device events rather than the concentrator events.)

To see the Intermittent Failures PD table for a host bus adapter, go to “Intermittent PD table - Host bus adapter” on page 163.

To see the Intermittent Failures PD table for a controller, go to “Intermittent PD table - Controller” on page 163.

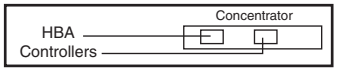
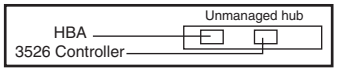
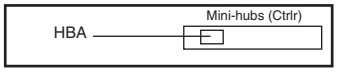
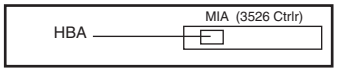
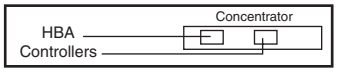
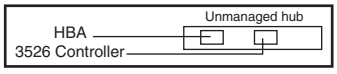
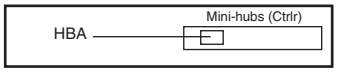
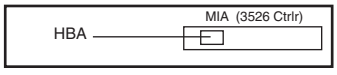
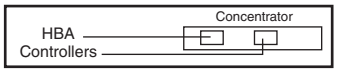
Intermittent Failures PD tables

Use the following tables to help you isolate intermittent failures. Use the SANavigator Event Log to determine which device has a history of intermittent failures. See “Event Log behavior” on page 292 to aid your understanding of event logging.

You can also check the operating status change of your SAN to determine the online/offline status of devices. To generate the report, select Monitor **->** Reports and check ″operating status change″ box. See “Generating, viewing, and printing reports” on page 243.

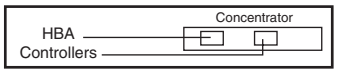
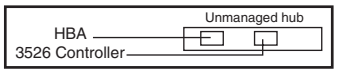
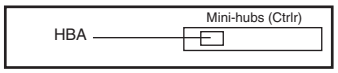
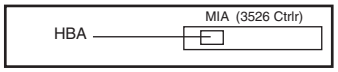
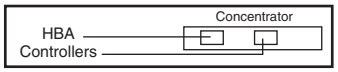
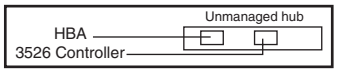
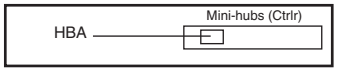
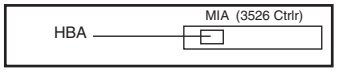
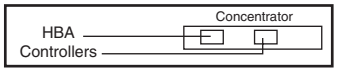
Intermittent PD table - Controller

From: “Diagnosing with SANavigator - Intermittent Failures PD map” on page 162.

ID	Connection type/device	Offline events (Out-of-band discovery)	Offline events (In-band discovery)	Action*
1		**X**		Go to “Controller Fatal Event Logged PD map 1” on page 165.
2		**N/A**		Not applicable (Out-of-band discovery requires switch or managed hubs.)
3		**N/A**		Not applicable (Out-of-band discovery requires switch or managed hubs.)
4		**N/A**		Not applicable (Out-of-band discovery requires switch or managed hubs.)
5			**N/A**	Not applicable out-of-band discovery is required.
6			**X**	Go to “Controller Fatal Event Logged PD map 1” on page 165.
7			**X**	Go to “Controller Fatal Event Logged PD map 1” on page 165.
8			**X**	Go to “Controller Fatal Event Logged PD map 1” on page 165.
9		**X**	**X**	Go to “Controller Fatal Event Logged PD map 3” on page 167.
* When inspecting the event log, look for devices that consistently go offline and come back online before suspecting the component.				
Note: In these diagrams, the term *concentrator* refers to either a switch or a managed hub.				

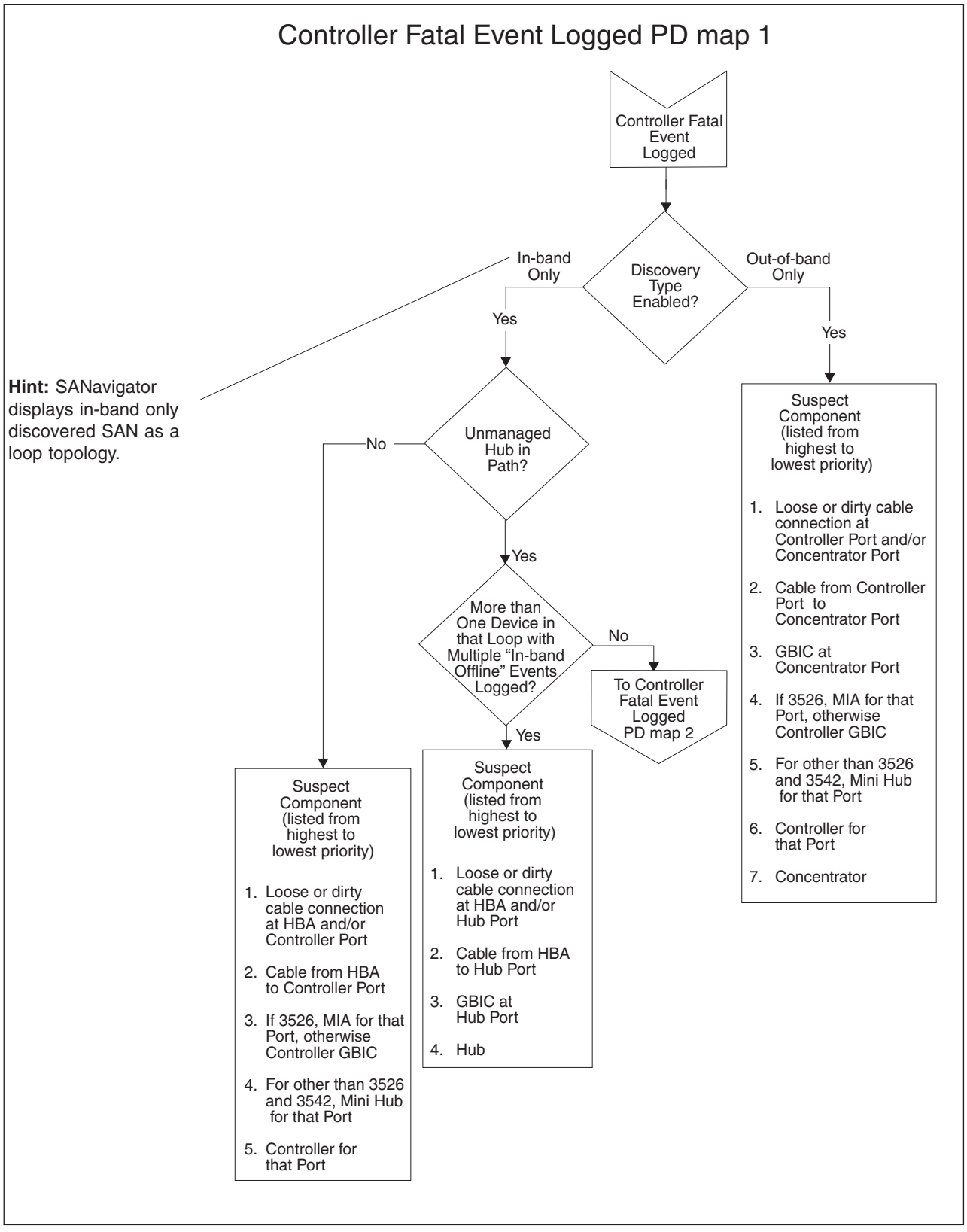
Intermittent PD table - Host bus adapter

From: “Diagnosing with SANavigator - Intermittent Failures PD map” on page 162.

ID	Connection type/device	Offline events (Out-of-band discovery)	Offline events (In-band discovery)	Action*
1		**X**		Go to “HBA Fatal Event Logged PD map” on page 168.
2		**N/A**		Not applicable (Out-of-band discovery requires switch or managed hubs.)
3		**N/A**		Not applicable (Out-of-band discovery requires switch or managed hubs.)
4		**N/A**		Not applicable (Out-of-band discovery requires switch or managed hubs.)
5			**N/A**	Not applicable out-of-band discovery is required.
6			**X**	Go to “HBA Fatal Event Logged PD map” on page 168.
7			**X**	Go to “HBA Fatal Event Logged PD map” on page 168.
8			**X**	Go to “HBA Fatal Event Logged PD map” on page 168.
9		**X**	**X**	Go to “HBA Fatal Event Logged PD map” on page 168.
* When inspecting the event log, look for devices that consistently go offline and come back online before suspecting the component.				
Note: In these diagrams, the term *concentrator* refers to either a switch or a managed hub.				

Controller Fatal Event Logged PD map 1

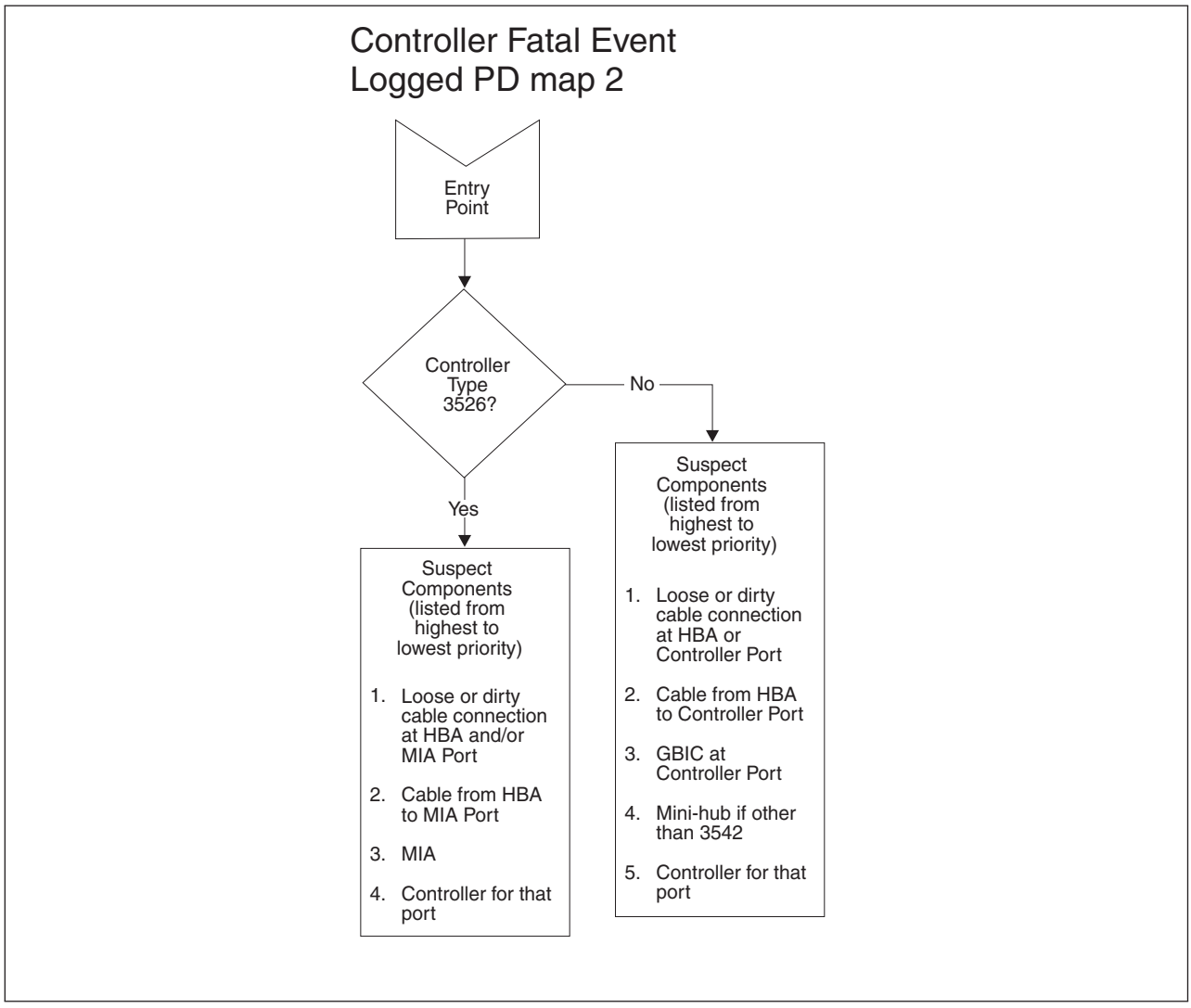
From: “Intermittent PD table - Controller” on page 163.



To see Controller Fatal Event Logged PD map 2, go to “Controller Fatal Event Logged PD map 2”.

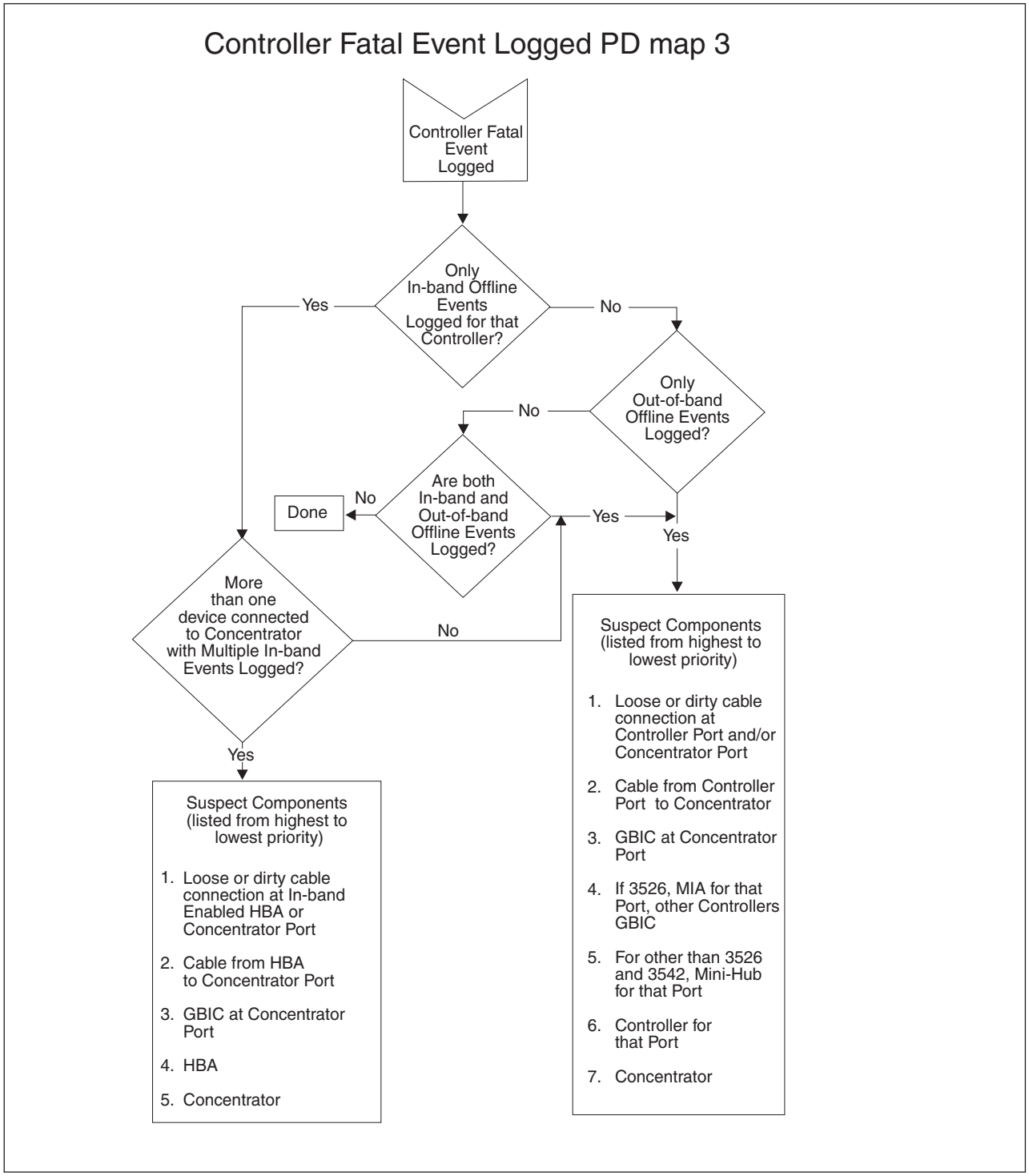
Controller Fatal Event Logged PD map 2

From: “Controller Fatal Event Logged PD map 1” on page 165.



Controller Fatal Event Logged PD map 3

From: “Intermittent PD table - Controller” on page 163; “Controller Fatal Event Logged PD map 1” on page 165.

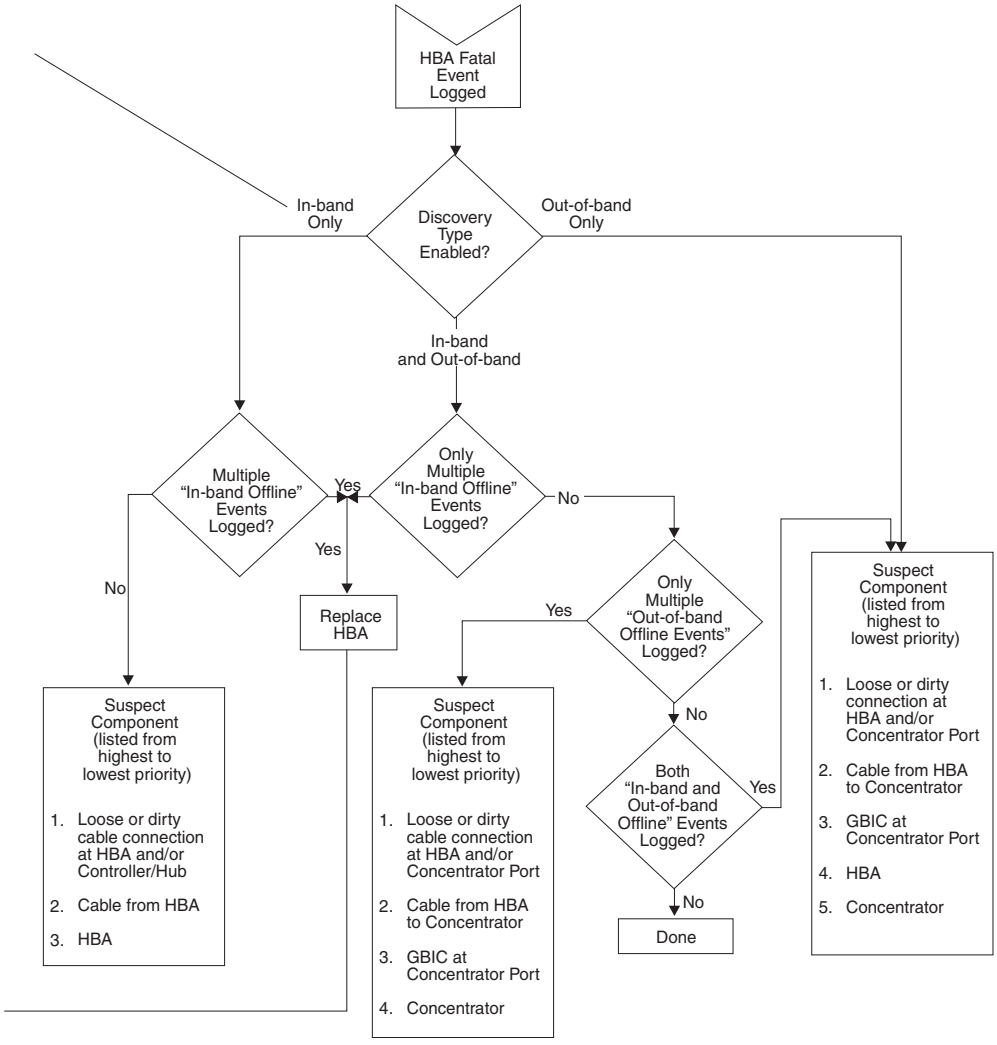


HBA Fatal Event Logged PD map

From: “Intermittent PD table - Host bus adapter” on page 163.

HBA Fatal Event Logged PD map

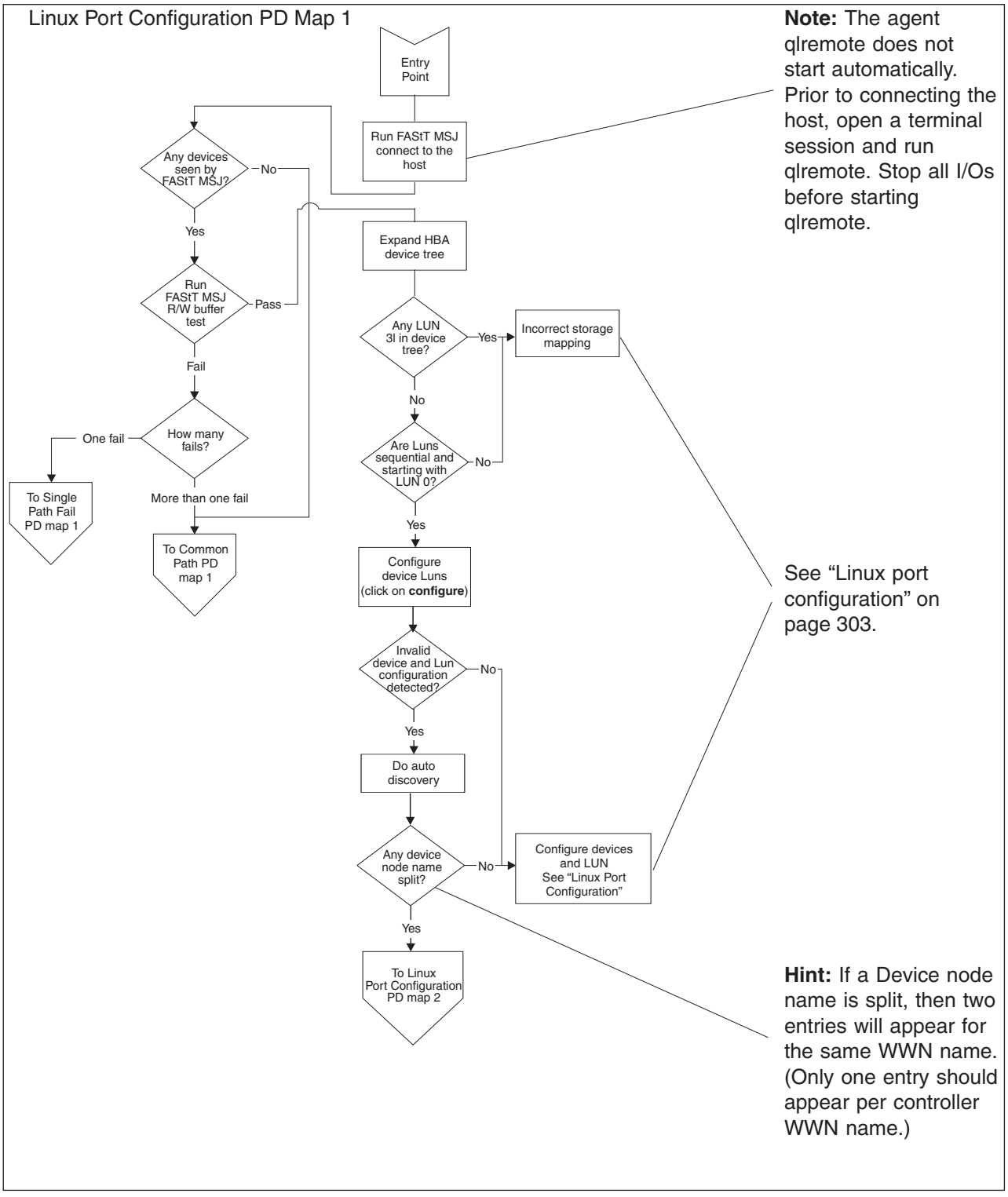
Hint: SANavigator displays in-band discovered SAN as a loop topology.



Hint: All devices connected to this HBA will also show Connection Offline.

Linux Port Configuration PD map 1

From: “Specific problem areas” on page 134.



To see Single Path Fail PD map 1, see “Single Path Fail PD map 1” on page 150.

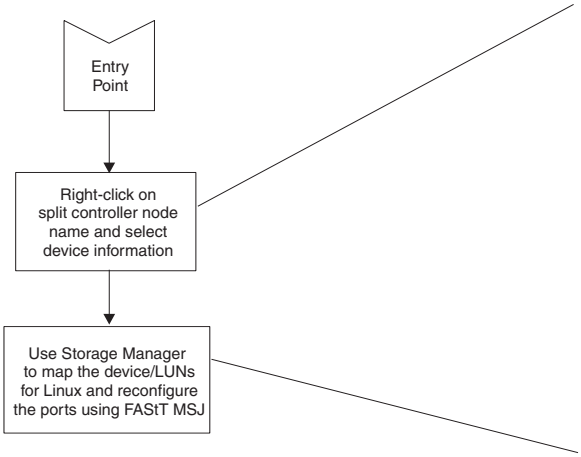
To see Common Path PD map 1, see “Common Path PD map 1” on page 152.

To see Linux Port Configuration PD map 2, see “Linux Port Configuration PD map 2” on page 171.

Linux Port Configuration PD map 2

From: “Linux Port Configuration PD map 1” on page 169

Linux Port Configuration PD Map 2



Hint: Right click on the Host icon in the HBA Tree and select “Adapter Persistent Configuration Data . . .” The Adapter(s) WWNN will be displayed. Record this information as it will be required by FAStT Storage Manager to map your storage to the Linux OS.

Additional information: See “Linux port configuration” on page 303.

To see Single Path Fail PD map 1, see “Single Path Fail PD map 1” on page 150.

Chapter 18. Introduction to FAStT MSJ

This chapter introduces the IBM Fibre Array Storage Technology Management Suite Java (FAStT MSJ) and includes background information on SAN environments and an overview of the functions of FAStT MSJ.

Note: Read the README file, located in the root directory of the installation CD, or refer to the IBM Web site at http://www.ibm.com/pc/support for the latest installation and user information about FAStT MSJ.

SAN environment

In a typical Storage Area Network (SAN) environment, a system might be equipped with multiple host bus adapters (HBAs) that control devices on the local loop or on the fabric.

In addition, a single device can be visible to and controlled by more than one HBA. An example of this is dual-path devices used in a primary/failover setup.

In a switched or clustering setup, more than one system can access the same device; this type of configuration enables storage sharing. Sometimes in this scenario, a system must access certain LUNs on a device while other systems control other LUNs on the same device.

Because SAN has scalable storage capacity, you can add new devices and targets dynamically. After you add these new devices and targets, they need to be configured.

A SAN can change not only through the addition of new devices, but also through the replacement of current devices on the network. For device hot-swapping, old devices sometimes need to be removed and new devices need to be inserted in the removed slots.

In such a complicated environment where there is hot-swapping of SAN components, some manual configuration is required to achieve proper installation and functionality.

Overview of the IBM FAStT Management Suite

FAStT MSJ is a network-capable application that can connect to and configure remote systems. FAStT MSJ helps you configure IBM Fibre Channel HBAs in a SAN environment. FAStT MSJ uses ONC remote procedure calls (RPC) for network communication and data exchange. The networking capability of FAStT MSJ enables centralized management and configuration of the entire SAN.

Note: The diagnostic functions of FAStT MSJ are available for all supported operating systems. The configuration functions are available for Linux operating systems only. IBM FAStT Storage Manager provides management capability for Microsoft Windows-based platforms.

With FAStT MSJ, you can use the following four types of operations to configure devices in the system:

Disable (unconfigure) a device on a host bus adapter
When a device is set as unconfigured by the utility, it is not recognized by the HBA and is inaccessible to that HBA on that system.

Enable a device
This operation adds a device and makes it accessible to the HBA on that system.

Designate a path as an alternate for preferred path
When a device is accessible from more than one adapter in a system, you can assign one path as the preferred path and the other path as the alternate path. If the preferred path fails, the system switches to the alternate path to ensure that data transfer is not interrupted.

Replace a removed device with a new inserted device
In a hot-plug environment, the HBA driver does not automatically purge a device that has been physically removed. Similarly, it does not delete a device that is no longer accessible because of errors or failure. Internally, the driver keeps the device in its database and marks it as invisible.

The HBA driver adds a new device to the database, even if the device is inserted into the same slot as the removed device.

FAStT MSJ provides the function to delete the removed device's data from the driver's database and to assign the inserted device the same slot as the one that it replaces.

FAStT MSJ system requirements

The FAStT MSJ application consists of two components:

- FAStT MSJ client interface
- Host agent

Each component has different system requirements depending on the operating system.

FAStT MSJ client interface

FAStT MSJ, which is written in Java, should run on any platform that has a compatible Java VM installed. The minimum system requirements for FAStT MSJ to run on all platforms are as follows:

- A video adapter capable of 256 colors
- At least 64 MB of physical RAM; 128 MB is preferred. Running with less memory might cause disk swapping, which has a negative effect on performance.
- 30 MB of free disk space

Platform-specific requirements for the FAStT MSJ client interface are as follows:

- Linux x86
  - RedHat Linux 7.1 (preferred configuration)
  - PII 233MHz (preferred minimum)
- Microsoft Windows 2000 and Windows NT
  - Pentium III processor 450 MHz or greater
- Novell NetWare
  - Pentium III processor 450 MHz or greater

Note: If multiple Network Interface Cards (NICs) are present in the system, the FAStT MSJ client will broadcast to the first IP address subnet based on the binding order. Therefore, ensure that the NIC for the local subnet is first in the binding order. If this is not done, the diagnostics might not run properly and remote connection might not occur. See the Readme file in the release package for more information.

Host agent

Host agents are platform-specific applications that reside on a host with IBM HBAs attached. The minimum system requirements for an agent to run on all platforms are as follows:

- An IBM FAStT MSJ-supported device driver (see release.txt in the release package for a list of supported device driver versions for each platform)
- At least 8 MB of physical RAM
- 2 MB of free disk space

Platform-specific requirements for the FAStT MSJ host agents are as follows:

- Linux x86—Agent runs as a daemon
- Microsoft Windows NT or Windows 2000—Agent runs as a Windows NT service
- Novell NetWare installation prerequisites

  Be sure you have the following items before installing the QLremote NetWare Agent:
  - NetWare Client software (from Novell) on the Windows NT or Windows 2000 client
  - NWLink IPX/SPX-compatible transport or TCP/IP transport network protocols

    Note: The TCP/IP transport must be loaded to communicate with the FAStT MSJ agent.
  - NWLink NetBios
  - Drive letter mapped to the root of the SYS volume of the NetWare server. By default, the NetWare Client maps to sys\system or sys\public; however, you must set the root of SYS volume by assigning a drive letter to sys:\.

    Note: You must be logged on as an administrator to map server drive letters.
  - On the NetWare Server—NetWare 5.1 server with service pack 2 or later

Installing and getting started

This section contains procedures for installing FAStT MSJ and for using the application.

Initial installation options

FAStT MSJ supports stand-alone and network configurations. Install the software appropriate for your configuration. See Table 54 on page 176 for details.

Note: The same version of FAStT MSJ must be installed on all systems.

Table 54. Configuration option installation requirements

Configuration	Software Requirements
Stand-alone system: This system monitors host bus adapters locally.	FAStT MSJ GUI Plus one of the following: • FAStT MSJ Windows NT or Windows 2000 agent • FAStT MSJ Linux agent
Networked system: This system monitors host bus adapters locally and monitors remote systems on the network. Host agents are required for remote connection (see ″Host agent system″ following).	FAStT MSJ GUI Plus one of the following: • FAStT MSJ Windows NT or Windows 2000 agent • FAStT MSJ Linux agent
Client system: This system monitors host bus adapters only on remote systems on the network.	FAStT MSJ GUI Host agents (see requirements for host agent system)
Host agent system: The host bus adapters on this system are remotely monitored only from other systems on the network.	One of the following: • FAStT MSJ NT4/2000 agent • FAStT MSJ NetWare 5.x agent • FAStT MSJ Linux agent

Installing FAStT MSJ

The FAStT MSJ installer is a self-extracting program that installs the FAStT MSJ application and related software.

Notes:

1. If you have a previous version of FAStT MSJ installed, uninstall the previous version of FAStT MSJ before installing FAStT MSJ.
2. You cannot install the FAStT MSJ agent directly on a NetWare server; you must install the agent on a system connected to the NetWare server. The Netware server must have a drive mapped to a system running Windows 2000 or Windows NT.

Perform the following steps to install FAStT MSJ on the system or the NetWare server:

1. Access the FAStT MSJ installer by doing one of the following:
   - If installing FAStT MSJ from a CD, click the **IBM FAStT MSJ** folder on the CD.
   - If installing FAStT MSJ from the IBM Web site, go to the page from which you can download FAStT MSJ (this URL is listed in the README file).
2. From the CD folder or the folder in which you saved the FAStT MSJ installer, select the appropriate install file by doing one of the following:
   - For Windows 2000, Windows NT, and NetWare, double-click the FAStTMSJ_install.exe file.

     Note: For NetWare, save to the system drive mapped to the NetWare server.
   - For Red Hat Linux, do the following:

a. Open a shell.
b. Change to the directory that contains the FAStT MSJ installer that you downloaded in Step 1.
c. At the prompt, type `sh ./FAStTMSJ_install.bin`, where `install` is the FAStT MSJ installer file.

   InstallAnywhere prepares to install FAStT MSJ. The Installation Introduction window is displayed.

3. Click **Next**. The Choose Product Features window is displayed. The window differs, depending on whether you are installing on a system running Windows 2000, Windows NT, or Red Hat Linux.
4. Do one of the following to install the software appropriate to your configuration:
   - For a system running Windows 2000 or Windows NT, click one of the following preconfigured installation sets, then click **Next**.
     – Click **GUI and NT Agent** if the system running Windows 2000 or Windows NT will monitor host bus adapters on this system and remote systems on the network.
     – Click **GUI** if the system will monitor host bus adapters only on remote systems on the network.
     – Click **NT Agent** if the host bus adapters on the system running Windows 2000 or Windows NT will be remotely monitored only from other systems on the network.
     – Click **NetWare 5.x Agent** if the host bus adapters on this NetWare 5.x system will be remotely monitored only from other systems on the network.
   - For Red Hat Linux systems, click one of the following preconfigured installation sets, then click **Next**.
     – Click **GUI** if the system will monitor host bus adapters only on remote systems on the network.
     – Click **Linux Agent** if the host bus adapters on this system running Red Hat Linux will be remotely monitored only from other systems on the network.
     – Click **GUI and Linux Agent** if this system running Red Hat Linux will monitor host bus adapters on this system and on remote systems on the network.
   - For other configuration installation sets, click **Customize** to create a customized installation set. The Choose Product Components window is displayed. The window differs depending on whether you are installing on a system running Windows 2000, Windows NT, or Red Hat Linux. Perform the following steps to create a custom installation set:
     a. In the **Feature Set** list-box, click **Custom Set**.
     b. Select from the following components:
        – For a system running Windows 2000 or Windows NT:
          - **GUI**
          - **NT Agent**
          - **NetWare 5.x Agent**
          - **Help**
        – For a system running Red Hat Linux:
          - **GUI**
          - **Linux Agent**

- **Help**

c. Click **Next**. The Important Information window is displayed.

5. Read the information, then click **Next.**

   Note: Information in the README file supplied with the installation package takes precedence over the information in the Important Information window.

   The Choose Install Folder window is displayed.

6. Do one of the following:

   Note: For NetWare, click the drive mapped to the NetWare server.

   - To select the default destination location displayed in the window, click **Next**.

     The default location for a system running Windows 2000 or Windows NT is C:\Program Files\IBM FAStT Management Suite\.

     The default location for a system running Red Hat Linux is /root/IBM_FAStT_MSJ.

   - To select a location other than the default, click **Choose**, click the desired location, and click **Next**.
   - To reselect the default location after selecting a different location, click **Restore Default Folder**, and click **Next**.

7. If you are installing on a Windows platform, the Select Shortcut Profile Location window is displayed. Do one of the following:
   - To select the all users profile to install the application program group and shortcuts, select the **All Users Profile** radio button, and click **Next**.
   - To select the current users profile to install the application program group and shortcuts, select the **Current Users Profile** radio button, and click **Next**.
8. If you are installing on a NetWare system, the Novell NetWare Disk Selection window is displayed. A list of the autodetected, mapped NetWare drives on the subnet is displayed in the following format: *drive*, *server name*, *server IP address*.
   a. Click the drives on which to install the NetWare agent. Each drive must be a NetWare drive mapped on the system running Windows 2000 or Windows NT. You can select drives by clicking one or more autodetected drives from the list or by typing the drive letter corresponding to the drive you want to use.
   b. Click **Next**. The Installing Components window is displayed. Subsequent windows inform you that the installation is progressing. When installation is complete, the Install Complete window is displayed.
9. Click **Done**.
10. Customize the FAStT MSJ application and set your security parameters. See “Security” on page 183 for details.

Uninstalling FAStT MSJ

You must exit the FAStT MSJ application before uninstalling FAStT MSJ. Make sure you uninstall the NetWare agent from the Windows 2000 or Windows NT drive mapped to the Novell NetWare server when installing FAStT MSJ.

Perform the following steps to uninstall FAStT MSJ:

1. Start the FAStT MSJ Uninstaller:

- On a system running Windows 2000 or Windows NT, click **Start** -> **Programs** -> **IBM FAStT MSJ** -> **FAStT MSJ Uninstaller**.
- On a system running Red Hat Linux:
  a. Change to the directory where you installed FAStT MSJ. For example, type:
     ```
     cd /usr
     ```
  b. Type the following to run the InstallAnywhere Uninstaller:
     ```
     ./FAStT_MSJ_Uninstaller
     ```

  The InstallAnywhere Uninstaller window is displayed with IBM FAStT Management Suite Java Vx.x.xx as the program to be uninstalled.

2. Click **Uninstall**. The InstallAnywhere Uninstaller - Component List window lists the components to be uninstalled. A message displays informing you that the uninstaller is waiting 30 seconds for the agent to shut down. Wait while the uninstaller removes the components. The InstallAnywhere Uninstaller - Uninstall Complete window informs you that the uninstall is complete.
3. Click **Quit**.
4. If any items are not successfully uninstalled, repeat the uninstallation instructions to remove them.
5. Restart the system.

Getting started

FAStT MSJ enables you to customize the GUI and agent. After you install FAStT MSJ and set your initial parameters, these components activate each time you start the application.

Starting FAStT MSJ

This section describes how to start FAStT MSJ on systems running Windows and Linux.

Windows 2000 or Windows NT: On a system running Windows 2000 or Windows NT, double-click the **FAStT MSJ** icon on your desktop if you selected to create the icon during installation (see Figure 64), or click **Start** -> **Programs**-> **IBM FAStT MSJ** -> **FAStT MSJ**.

Figure 64. FAStT MS Icon

The FAStT MSJ main window opens.

Red Hat Linux: On a system running Red Hat Linux, perform the following steps to start the FAStT MSJ:

1. Ensure that you are in a graphical user environment.
2. Open a command terminal.
3. Change to the usr directory in which the IBM FAStT MSJ application is installed by typing `cd /usr`.
4. Type `./FAStT_MSJ`. The FAStT MSJ main window opens.

FAStT MSJ main window

The IBM Management Suite Java-HBA View window (hereafter referred to as the FAStT MSJ main window) is displayed after you start FAStT MSJ. See Figure 65.

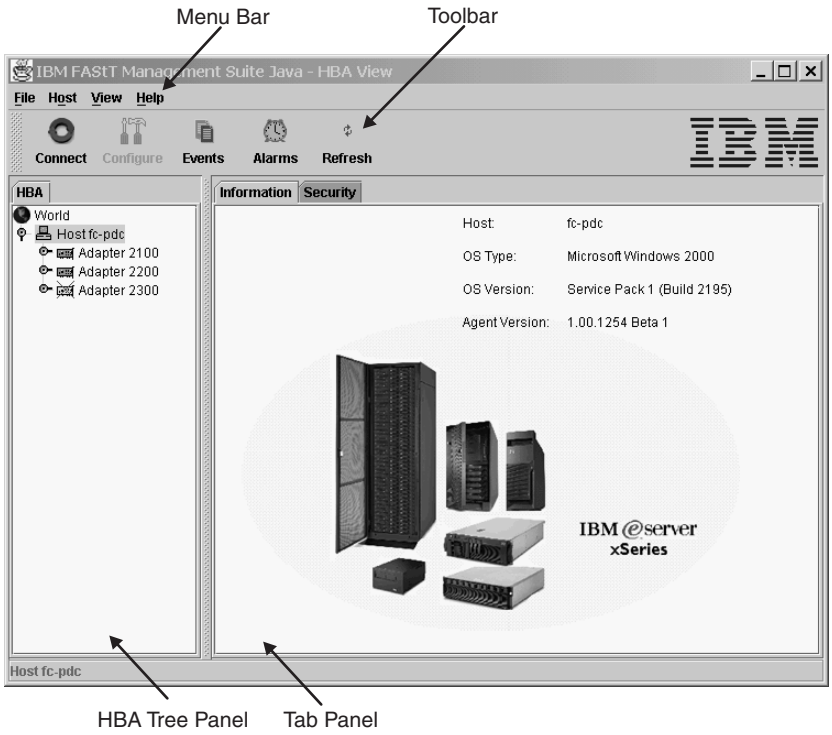


Figure 65. FAStT MSJ Main Window

The window consists of the following sections:

- Menu bar
- Toolbar
- HBA tree panel
- Tab panel

Basic features overview

This section lists FAStT MSJ features and contains general information needed to run FAStT MSJ on any supported platform.

Features

FAStT MSJ enables you to do the following:

- Set FAStT MSJ options
- Connect to hosts
- Disconnect from a host
- View extensive event and alarm log information
- Use host-to-host SAN configuration policies
- Configure port devices
- Use LUN Level configuration

- Watch real-time to see when failovers occur with the Failover Watcher
- Control host-side agent operations, including setting the host agent polling interval
- Review host adapter information, including:
  - General information
  - Statistics
  - Information on attached devices
  - Attached device link status
- Perform adapter functions, including:
  - Configure adapter NVRAM settings
  - Execute fibre channel diagnostics (read/write and loopback tests)
  - Perform flash updates on an adapter
  - Perform NVRAM updates on an adapter
- Manage configurations
  - Save configurations for offline policy checks and SAN integrity
  - Load configurations from file if host is offline for policy checks and SAN integrity
- Confirm security

Options

To configure FAStT MSJ, click **View** -> **Options**. The Options window opens.

The Options window has four sections and two buttons:

- Event Log
- Alarm Log
- Warning Displays
- Configuration Change Alarm
- **OK** (save changes) and **Cancel** (discard changes) buttons

The Options window functions are described in the following sections.

Event log

Event log information includes communication and file system errors. FAStT MSJ stores the event entries in the events.txt file. You can log informational and warning events.

You can set the maximum size of the event log to be in the range of 20 to 200 event entries; the default is 20 events. When the maximum size of the event log is exceeded, old entries are automatically deleted to provide space for new entries.

Alarm log

When FAStT MSJ communicates with a host, FAStT MSJ continually receives notification messages from the host indicating changes directly or indirectly made on adapters. Messages regarding status, configuration, and NVRAM changes are logged. FAStT MSJ stores these alarm messages in the alarms.txt file.

You can set the maximum size of the alarm log to be in the range of 20 to 200 event entries; the default is 200 entries. When the maximum size of the alarm log is exceeded, old entries are automatically deleted to provide space for new entries.

Warning displays

FAStT MSJ displays additional warning dialogs throughout the application. By default, the Warning Displays option is enabled. To disable the display of warning dialogs, clear the **Enable warning displays** check box in the Options window.

Configuration change alarm

FAStT MSJ tries to keep current the devices and the LUNs that the adapter displays. During cable disconnects, device hotplugs, or device removal, configuration change alarms are generated to keep the GUI current. You can control the way FAStT MSJ handles configuration change alarms with the Configuration Change Alarm option. You can choose from the following options:

- Apply Configuration Changes Automatically

  When a configuration change alarm is detected by the GUI, the application disconnects the host and reconnects to get the new configuration automatically.
- Confirm Configuration Change Applies (default setting)

  When a configuration change alarm is detected by the GUI, the application displays a window that the user clicks **Yes** or **No** to refresh the configuration for the specified host.
- Ignore Configuration Changes

  With this setting, a configuration change alarm detected by the GUI is ignored. For the configuration to be updated, a manual disconnect and connect of the host must be performed.

Note: You can refresh the configuration by selecting the desired host and clicking the **Refresh** button on the toolbar or by right-clicking the desired host and clicking **Refresh** on the pop-up menu.

Connecting to hosts

There are two ways to connect to hosts in a network:

- Manually
- Automatically with the Broadcast function

For multi-homed or multiple IP hosts, FAStT MSJ tries to ensure that a specified host is not loaded twice into the recognized host tree. If a particular host has multiple interfaces (NICs), each with its own IP address, and proper name-resolution-services are prepared, the host will not be loaded twice into the tree. Problems can occur when one or more IPs are not registered with a host.

A blinking heart indicator (blue pulsating heart icon) indicates that the connection between the client and remote agent is active for this test.

Manual connection

Perform the following steps to manually connect to a host.

1. From the FAStT MSJ main window, click the **Connect** button or click **Connect** from the **Host** menu.

   The Connect to Host window is displayed.
2. Type in the host name, or select the host you want to connect to from the drop-down list. You can use the computer IP address or its host name. If the computer you want to connect to is the computer on which FAStT MSJ is running, select **localhost** from the drop-down list. To delete all user-entered host names from the drop-down list, click **Clear**.
3. After you have selected or typed the host name, click **Connect** to initiate the connection.

If the connection attempt fails, an error message is displayed that indicates the failure and potential causes. If the connection is successfully established, the host's name and its adapters are shown on the HBA tree.

Click **Cancel** to stop the connection process and return to the main window.

Broadcast connections

FAStT MSJ can auto-connect to all hosts running an agent in a network. For auto-connect to function properly, ensure that the **Broadcast** setting is enabled. To enable auto-connect, select the **Auto Connect** check box from the **Host** menu. To disable auto-connect, clear the **Auto Connect** check box.

Note: If multiple NICs (Network Interface Cards) are present in the system, the FAStT MSJ client will broadcast to the first IP address subnet based on the binding order. Therefore, ensure that the NIC for the local subnet is first in the binding order. If this is not done, the diagnostics might not run properly and remote connection might not occur. See the Readme file in the release package for more information.

Disconnecting from a host

Perform the following steps to disconnect from a host:

1. From the FAStT MSJ main window HBA tree, click the host that you want to disconnect from.
2. Click **Host -> Disconnect**.

   When a host is disconnected, its entry in the HBA tree is removed.

Polling interval

You can set polling intervals on a per-host basis to retrieve information. The polling interval setting can be in the range from 1 second to 3600 seconds (one hour). Perform the following steps to set the polling interval:

1. Click the host in the HBA tree in the FAStT MSJ main window.
2. Click **Host -> Polling**. The Polling Settings - target window is displayed.
3. Type the new polling interval and click **OK**.

Security

FAStT MSJ protects everything written to the adapter or adapter configuration with an agent-side password. You can set the host agent password from any host that can run the FAStT MSJ GUI and connect to the host agent.

When a configuration change is requested, the Security Check window is displayed to validate the application-access password. Type the application-access password for confirmation.

To change the host agent password, select a host by clicking it in the HBA tree. The Information/Security tab panels are displayed. Click the Security tab to display the Security panel.

The security panel is divided into two sections: Host Access and Application Access.

Host access

The Host Access section verifies that the host user login and password has administrator or root privileges before an application access is attempted. The login and password values are the same as those used to access the computer.

Login A host user account with administrator or root-level rights.

Password
The password for the host user account.

Application access

The Application Access section enables you to change the FAStT MSJ host agent password. To change the password, type information into the following fields:

Old password
The current application-access password for the host. The original default password is **config**. Change it immediately to a new password.

New password
The new application-access password for the host.

Verify Password
The new application-access password for host verification.

The Help menu

From the FAStT MSJ **Help** menu, you can specify the location of the browser to launch when help is requested by a user. You can also view FAStT MSJ version information.

The **Help** menu contains the following items:

- **Set Browser Location**

  Click this item to display the Browser Location window (see the following figure). Type the file path of the browser that FAStT MSJ will launch when a user requests help, or click **Browse** to find the file location.
- **Browse Contents**

  Click this item to access FAStT MSJ help.
- **About**

  Click this item to view information about FAStT MSJ, including the current FAStT MSJ version number.

Diagnostics and utilities

The diagnostic and utility features of FAStT MSJ enable you to do the following:

- View event and alarm log information
- Review host adapter information
  - View general information
  - View statistics
  - View information on attached devices
  - View attached device link status
  - View adapter NVRAM settings
- Perform adapter functions, including:
  - Configure adapter NVRAM settings
  - Perform NVRAM updates on an adapter
  - Perform flash updates on an adapter
  - Execute Fibre Diagnostics (read/write and loopback tests)
- Manage configurations
  - Save configurations for offline policy checks and SAN integrity
  - Load configurations from file if host is offline for policy checks and SAN integrity

Viewing logs

FAStT MSJ records an extensive set of information to the event and alarm logs. The logs are saved as text files (alarms.txt and events.txt) in the folder where FAStT MSJ is installed. FAStT MSJ can parse and view these logs in a window. To view these logs, click **Event Log** or **Alarm Log** from the **View** menu, or click the appropriate button on the button bar.

Viewing the event log

The event log window displays events relating to FAStT MSJ application operations. New events are displayed in the window as they occur. There are three types of time-stamped event messages:

- Informative - an informative or general information event
- Warning - a non-critical application event
- Error - a critical application event

Click **OK** to close the Event Log window. Click **Clear** to purge all event entries from the log.

Sorting: To sort a column in ascending or descending order, right-click the column header, and click the desired sorting method.

Details: To view an individual event entry, double-click the entry; a separate event details window is displayed. You can navigate individual entries by clicking **Next** or **Previous**.

Viewing the alarm log

The alarm log window displays events that occurred on hosts connected to FAStT MSJ. New alarms are displayed in the window as they occur. Alarm entries have the following properties:

- Time Stamp — The date and time of the logged alarm
- Host Name — The agent host that sent the alarm
- Adapter ID — The host adapter the alarm occurred on
- Application — The type of device that sent the alarm
- Description — The description of the alarm

Click **OK** to close the Alarm Log window. Click **Clear** to purge all alarm entries from the alarm log.

Sorting: To sort a column in ascending or descending order, right-click the column header, and click the desired sorting method.

Colors: When the GUI receives an alarm with a status color other than white (informational), the adapter in the HBA tree with the most severe status blinks until you view the alarm. The following types of alarms are associated with each color:

- Informational: Rows in the table are color coded white.
- Unknown: Rows in the table are color coded blue.
- Warning: Rows in the table are color coded yellow.
- Bad: Rows in the table are color coded red.
- Loop Down: Adapter in the HBA tree is color coded yellow with a red X (see Figure 66 on page 186).

Figure 66. HBA Tree Adapter

Details: To view an individual alarm entry, double-click the entry; the Alarm Details window is displayed. You can navigate individual entries by clicking **Next** and **Previous**.

Viewing adapter information

To view adapter information, click the adapter in the HBA tree. The Information panel displays general information about the selected adapter (see Figure 67).

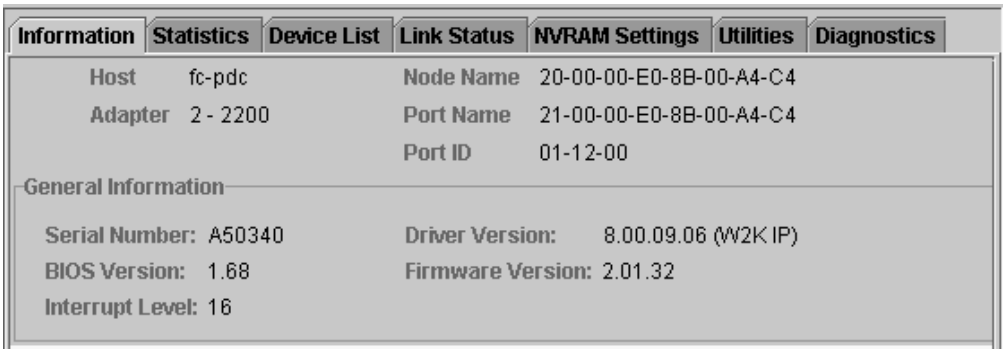


Figure 67. Adapter Information Panel

Viewing adapter statistics

The Statistics panel displays statistical information about the selected adapter (see Figure 68 on page 187).

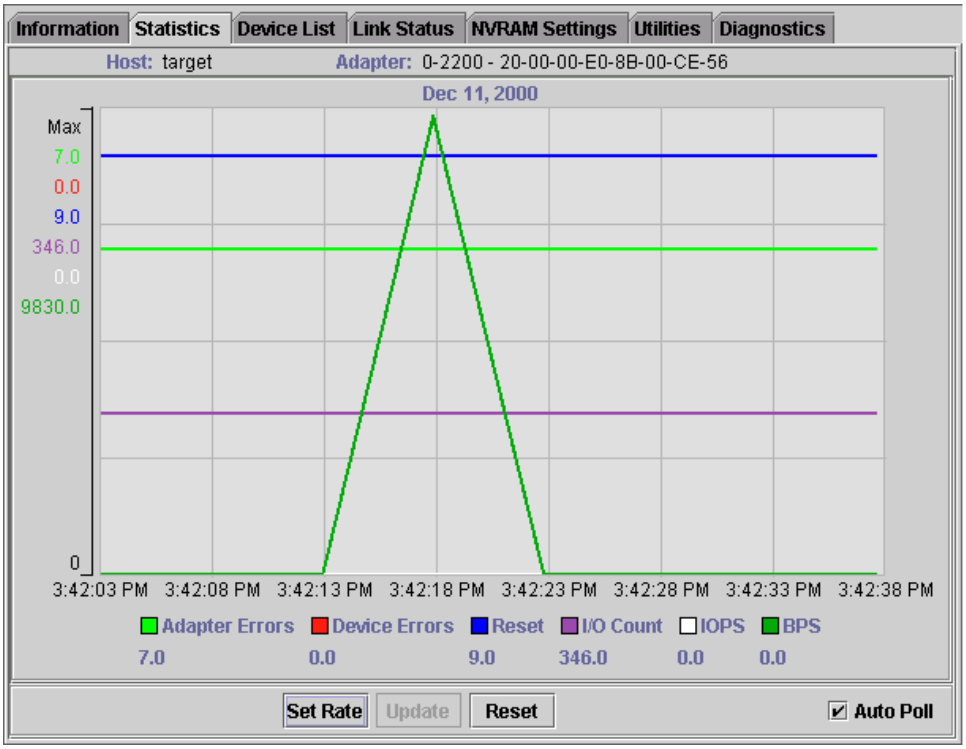


Figure 68. Adapter Statistics Panel

The Statistical panel displays the following information:

- Adapter Errors: The number of adapter errors reported by the adapter device driver.
- Device Errors: The number of device errors reported by the adapter device driver.
- Reset: The number of LIP resets reported by the adapter device driver.
- I/O Count: The total number of I/Os reported by the adapter device driver.
- IOPS (I/O per second): The current number of I/Os per second.
- BPS (bytes per second): The current number of bytes per second processed by the adapter.

Use the buttons and check box at the bottom of the Statistics panel to control sampling:

- **Auto Poll**

  Select this check box to use automatic sampling mode. To use manual mode, clear the check box. If the check box is selected, use **Set Rate** to define the sampling rate.
- **Set Rate**

  Click **Set Rate** to set the polling interval at which the GUI retrieves statistics from the host. The valid range is 5 to 30 seconds.
- **Update**

  Click the **Update** button to retrieve statistics from the host.
- **Reset**

  Click the **Reset** button to reset all statistics to the initial value of 0.

Device list

The Device List panel displays the following information about the devices attached to an adapter connected to a host:

- Host: The name of the host
- Adapter: The ID of the adapter
- Node Name: The node name of the adapter (WWN)
- Port Name: The port name of the adapter
- Path: The path number
- Target: The device ID
- Loop ID: The loop ID of the adapter when operating in loop mode
- Port ID: The port ID of the adapter (the AL-PA if in arbitrated loop environment)
- Vendor ID: ID of the device manufacturer
- Product ID: ID of the device
- Product Revision: Device revision level

Link status

The Link Status panel displays link information for the devices attached to an adapter connected to a host. See Figure 69.

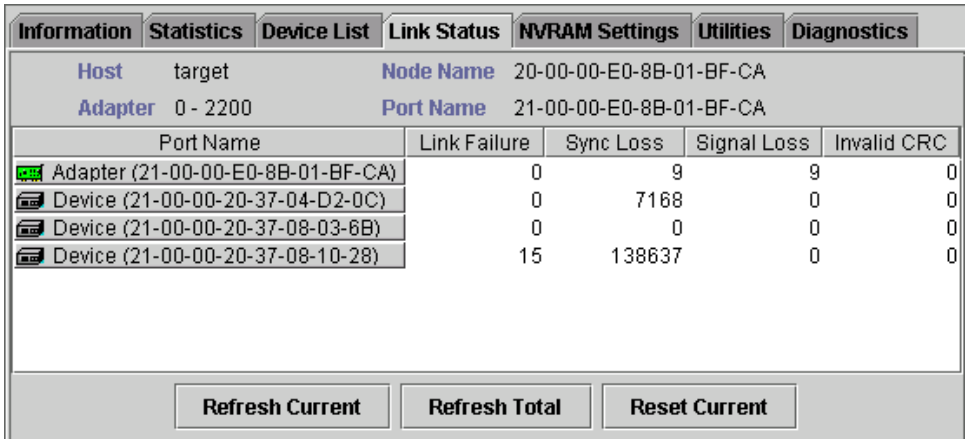


Figure 69. Adapter Link Status Panel

Click the Link Status tab to display the latest adapter link status from the device driver and the status for the adapter and all attached targets.

The first column of the Link Status panel is the World Wide Unique Port Name of the adapter and the attached devices.

The remaining columns display the following diagnostics information about the adapter and devices (see Table 55).

Table 55. Link status table

Diagnostic information	Definition
Link Failure	A loss of word synchronization for more than 100 msec or loss of signal.
Sync Loss	Four invalid transmission words out of eight (FC-PH rules) cause loss of synchronization (synch). Only transitions from in sync to out of sync are counted. Three valid ordered sets in a row are required to reestablish word sync.
Signal Loss	The receiver is not detecting a valid input signal.

Table 55. Link status table (continued)

Diagnostic information	Definition
Invalid CRC	The number of Cyclic Redundancy Check (CRC) errors that were detected by the device.

Use the buttons at the bottom of the panel for the following:

- **Refresh Current**

  Click this button to query the adapter for updated device link statistics since the last refresh.
- **Refresh Total**

  Click this button to query the adapter for cumulative updated device link statistics.
- **Reset Current**

  Click this button to initialize link statistics.

Displaying device information: You can view general device information or a LUN list.

Viewing general device information: To view general information about a device, click the device in the FAStT MSJ main window HBA tree. The Information panel for the device is displayed.

Viewing the LUN List: To display information about LUNs, click the device in the FAStT MSJ main window HBA tree; then, click the **LUN List** tab. The LUN List window is displayed. See Figure 70.

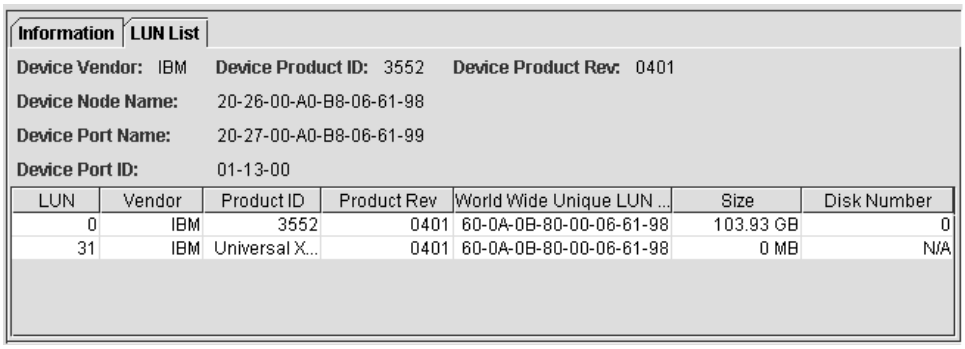


Figure 70. LUN List Window

The following LUN list information is displayed on the LUN List tab:

- LUN: The LUN number
- Vendor: The manufacturer of the LUN
- Product ID: The product ID of the LUN
- Product Rev: The product revision level of the LUN
- World Wide Unique LUN Name: The World wide name of the LUN
- Size: The capacity of the LUN
- Disk Number: The disk number of the LUN

Displaying LUN information: To view general information about a LUN, click the LUN in the FAStT MSJ main window HBA tree; then, click the **Information** tab. The **Information** window for the LUN is displayed.

NVRAM settings

The NVRAM Settings panel displays parameters that are saved in the adapter Non-Volatile RAM (NVRAM).

Note: The NVRAM parameters are preset at the factory. Do not alter them unless an IBM technical-support representative instructs you to do so. Adapter operation might be adversely affected if you enter the wrong parameters.

The NVRAM settings panel controls settings are divided into three categories: Host NVRAM Settings, Advanced NVRAM Settings, and Extended NVRAM Settings. You access sections by clicking an option in the **Select NVRAM** drop-down list. The following sections define the NVRAM parameters and do not necessarily reflect the IBM default values.

Host NVRAM settings

When you click **Host NVRAM Settings** in the **Select NVRAM section** list box, the information shown in Figure 71 is displayed.

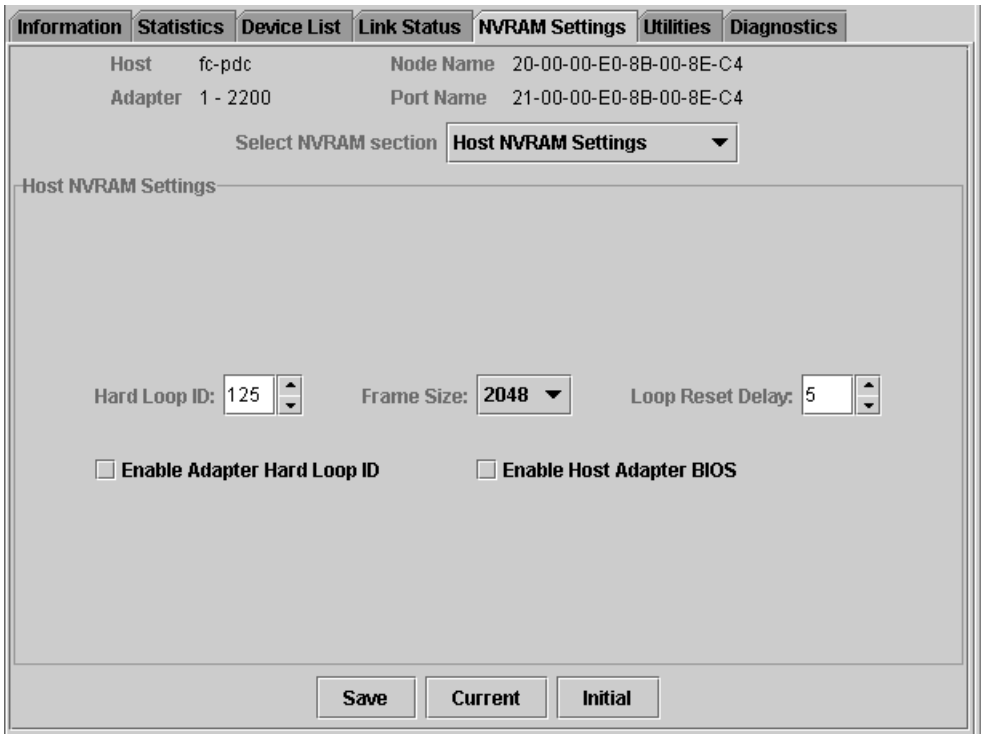


Figure 71. Host NVRAM Settings Panel

The following parameters are available in the Host NVRAM Settings section:

Hard Loop ID
ID used by the adapter when the **Enable Adapter Hard Loop ID** setting is enabled.

Frame Size
Specifies the maximum frame length supported by the adapter. The valid frame sizes are: 512, 1024, and 2048.

Loop Reset Delay
After resetting the loop, the firmware refrains from initiating any loop activity for the number of seconds specified in this setting. The valid delay is 0 to 60 seconds.

Enable Adapter Hard Loop ID
If this setting is enabled, the adapter uses the ID specified in the **Hard Loop ID** setting.

Enable Host Adapter BIOS
When this setting is disabled, the ROM BIOS on the host bus adapter is disabled, freeing space in the system's upper memory. Do not disable this setting if you are booting from a fibre channel disk drive attached to the adapter.

The **Initial** button restores all parameters to the settings used when the system was initially started. The **Current** button restores the updated settings modified by FAStT MSJ. The **Save** button saves the updated NVRAM settings.

Advanced NVRAM settings

When you click **Advanced NVRAM Settings** in the **Select NVRAM section** list box, the information shown in Figure 72 is displayed.

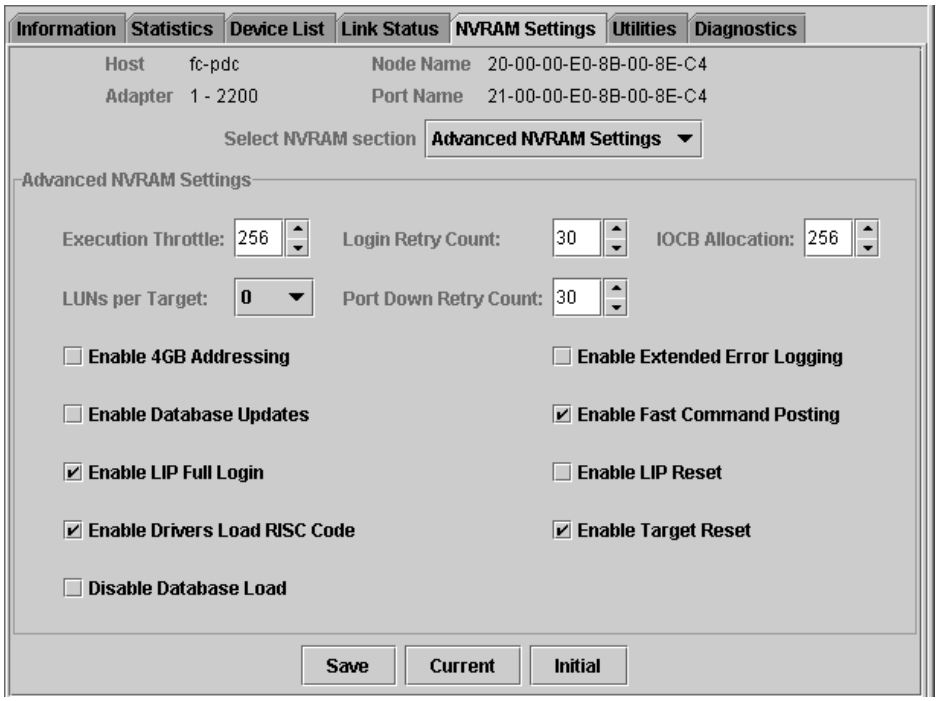


Figure 72. Advanced NVRAM Settings Panel

The following parameters are available in the Advanced NVRAM Settings section:

Execution Throttle
Specifies the maximum number of commands executing on any one port. When a port execution throttle is reached, no new commands are executed until the current command finishes executing. The valid values for this setting are in the range 1 to 256.

Login Retry Count
Specifies the number of retries the adapter uses during a login. This can be a value in the range 0 to 255.

IOCB Allocation
Specifies the maximum number of buffers from the firmware buffer pool to be allocated to any one port. Valid range is 1 to 512.

LUNs per Target
Specifies the number of LUNs per target. Multiple LUN support is typical for Redundant Array of Independent Disk (RAID) boxes that use LUNs to map drives. The valid values for this setting are 0, 8, 16, 32, 64, 128, and 256. If you do not need multiple LUN support, set **LUNs per Target** to 0.

Port Down Retry Count
Specifies the number of times the adapter software retries a command to a port returning port down status. Valid range is 0 to 255.

Enable 4GB Addressing
When enabled, the adapter is notified if the system has more than 4 gigabytes of memory.

Enable Database Updates
When enabled, the adapter device driver saves loop configuration information in the flash (EEPROM) when the system is powered down.

Enable LIP Full Login
When this setting is enabled, the adapter logs in to all ports after a loop initialization process (LIP).

Enable Drivers Load RISC Code
When this setting is enabled, the host adapter uses the RISC firmware that is embedded in the adapter device driver. If this setting is disabled, the adapter device driver loads the latest version of RISC firmware found on the system.

Note: The device driver being loaded must support this setting. If the device driver does not support this setting, the result is the same as disabled regardless of the setting. Leaving this option enabled ensures support of the software device driver and RISC firmware.

Disable Database Load
When enabled, the device database is read from the registry during device driver initialization. When disabled, the device database is created dynamically during device driver initialization. The default value is cleared (Disable Database Load is not enabled).

Note: This option usually applies to Windows NT and Windows 2000 operating environments.

Enable Extended Error Logging
This setting provides additional error and debugging information to the operating system.

Enable Fast Command Posting
When this setting is enabled, command execution time is decreased by minimizing the number of interrupts.

Enable LIP Reset
This setting determines the type of LIP reset that is used when the operating system initiates a bus reset routine. When this setting is enabled,

the adapter device driver initiates a global LIP reset to clear the target drive reservations. When this setting is disabled, the device driver initiates a global LIP reset with full login.

Enable Target Reset
When this setting is enabled, the adapter device driver issues a target reset to all devices on the loop during a SCSI bus reset function call.

Extended NVRAM settings

When you click **Extended NVRAM Settings** in the **Select NVRAM section** list box, the information shown in Figure 73 is displayed.

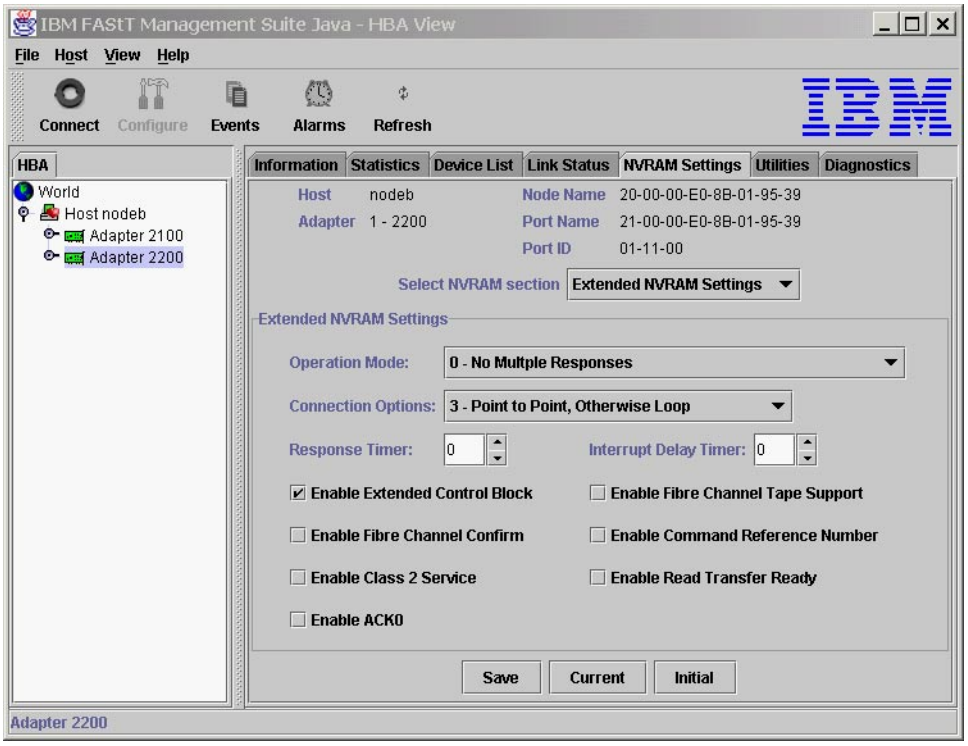


Figure 73. Extended NVRAM Settings Panel

The following parameters are available in the Extended NVRAM Settings section:

Operation mode
Specifies the reduced interrupt operation (RIO) modes (see Table 56). RIO modes enable posting multiple command completions in a single interrupt.

Table 56. Reduced interrupt operation modes

Bit	Description
0	RIO is disabled; enable fast posting by setting the Fast Posting option.
1	Combine multiple responses, 16-bit handles, interrupt the host. The handles are reported by asynchronous event codes 8031h-8035h or the RIO Type 2 IOCB.
2	Combine multiple responses, 32-bit handles, interrupt the host. The handles are reported by asynchronous event code 8020h or 8042h or the RIO Type 1 IOCB.
3	Combine multiple responses, 16-bit handles, delay the host interrupt. The handles are reported by the RIO Type 2 IOCB.

Table 56. Reduced interrupt operation modes (continued)

Bit	Description
4	Combine multiple responses, 32-bit handles, delay the host interrupt. The handles are reported by the RIO Type 1 IOCB.

Connection Options

Defines the type of connection (loop or point-to-point) or connection preference during startup (see Table 57).

Table 57. Connection type and preference

Bit	Description
0	Loop only
1	Point-to-point only
2	Loop preferred, otherwise point-to-point
3	Point-to-point preferred, otherwise loop

Response Timer

Sets the time limit (in 100-microsecond increments) for accumulating multiple responses. For example, if this field is 8, the time limit is 800 microseconds.

Interrupt Delay Timer

Sets the time to wait (in 100-microsecond increments) between accessing a set of handles and generating an interrupt. (An interrupt is not generated when the host updates the queue out-pointer during this period.) For example, if this field is set to 4, then 400 microseconds pass between the DMA operation and the interrupt.

Enable Extended Control Block

This setting enables all extended NVRAM settings. The default is enabled.

Enable Fibre Channel Confirm

This setting is reserved for fibre channel tape support.

Enable Class 2 Service

Select this check box to provide class 2 service parameters during all automatic logins (loop ports). Clear the check box if you do not want to provide class 2 service parameters during automatic logins.

Enable ACK0

Select this check box to use ACK0 when class 2 service parameters are used. Clear this check box to use ACK1.

Enable Fibre Channel Tape Support

Select this check box to enable the firmware to provide fibre channel tape support.

Enable Command Reference Number

This setting is reserved. The default is disabled.

Enable Read Transfer Ready

Select this check box to enable the read transfer ready option (XFR-RDY). The firmware also sends an XPR-RDY IU before transferring read data as a SCSI target.

Utilities

Within the Utilities panel you can perform adapter-level configurations on a host-connected adapter. See Figure 74.

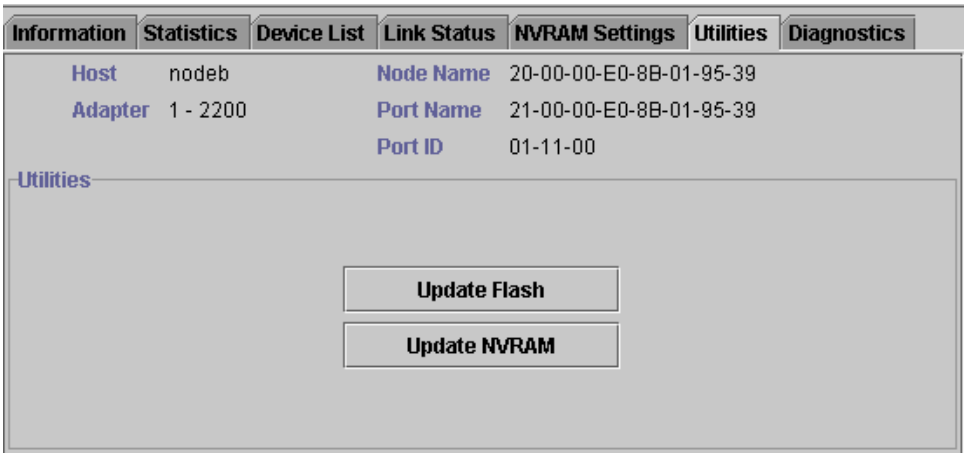


Figure 74. Utilities Panel

Update flash

When you click this button (and the adapter accepts the update), the application prompts for the file name that contains the new flash BIOS. You can obtain this file from the IBM Web site or service personnel. The file name ends with .BIN (for example, QL22ROM.BIN).

After you enter a valid flash file, click **OK** to proceed with the update or click **Cancel** to abort.

When you click **OK**, FAStT MSJ verifies the file name and format of the new file. If the file is valid, the application compares the version of the file with the adapter flash version. If the adapter version is the same or newer than the file flash version, the application asks if you still want to update the flash.

If the update fails, an error message is displayed.

Update NVRAM

When you click this button (and the adapter accepts the update), the application prompts for the file name that contains the new NVRAM. You can obtain this file from the IBM Web site or service personnel. The file name ends with .DAT (for example, NVRM22.DAT).

After you enter a valid NVRAM file, click **OK** to proceed with the update or click **Cancel** to abort.

When you click **OK**, FAStT MSJ verifies the contents of the new file.

If the update fails, an error message is displayed.

Diagnostics

You can perform the loopback and read/write buffer tests using the Diagnostics panel (see Figure 75 on page 196).

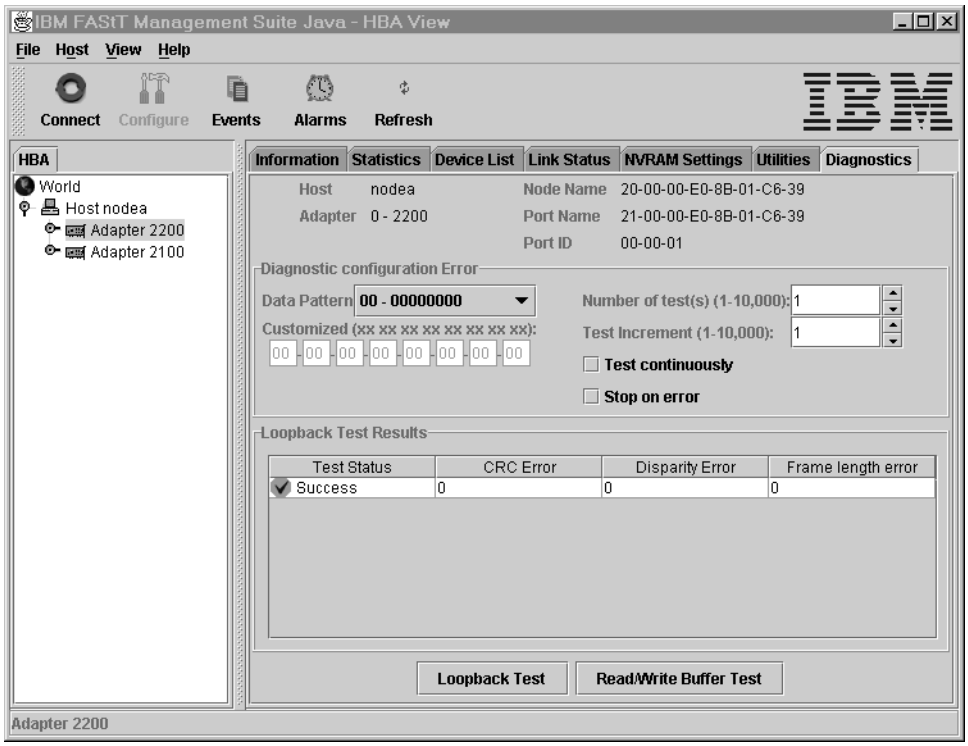


Figure 75. Diagnostics Panel

The loopback test is internal to the adapter. The test evaluates the fibre channel loop stability and error rate. The test transmits and receives (loopback) the specified data and checks for frame CRC, disparity, and length errors.

The read/write buffer test sends data through the SCSI Write Buffer command to a target device, reads the data back through the SCSI Read Buffer command, and compares the data for errors. The test also compares the link status of the device before and after the read/write buffer test. If errors occur, the test indicates a broken or unreliable link between the adapter and the device.

The Diagnostics panel has three main parts:

- Identifying Information

  This part of the panel displays information about the adapter being tested. This information includes:

  – Host
  – Adapter
  – Node Name
  – Port Name
  – Port ID

- Diagnostic Configuration Error

  This part of the panel contains the following testing options:

  Data Pattern

  Sets the test pattern. You can click a data pattern in the list or specify a customized pattern.

To specify a customized pattern, click **Customized** in the list and type the data pattern in hex format (0x00 - 0xFF) into the boxes under **Customized**.

When you select the random pattern from the list, a new random 8-byte pattern is sent to the devices, the adapter, or both (depending on whether you select the loopback or read/write buffer test).

Number of test(s)
Sets the number of tests you want to run. You can run the test for a certain number of times (up to 10,000) or continuously. You can also set the number of test increments per test up to 10,000.

Test continuously
Select this check box to test continuously.

Test Increment
The Test Increment value determines the number of times a test will be run against a particular device (read/write buffer test). For example if the value is set to 10, the read/write buffer test will be run 10 times against that device before moving to the next device in the Device List. The Number of tests parameter determines the total number of tests that will be run.

If you select **Test continuously**, the Test Increment value is set to 125 as the default value. You can increase this value to up to 10,000. While the test is running, a test progress dialog window is displayed. You can cancel the test at any time by clicking the **Stop** button in this window. FAStT MSJ waits until the Test Increment value is reached before stopping. Thus, a large Test Increment value will delay the stop action. The delay is dependent on the number of devices being tested.

Stop on error
Select this check box if you want continuous testing to discontinue when an error is encountered.

- Loopback Test Results

  The Loopback Test Results section displays the results of a test. The first column shows whether the test passed or failed. The remaining columns display error counters.

  For a loopback test, the test result includes the following information: Test Status, CRC Error, Disparity Error, and Frame Length Error.

  For a read/write buffer test, the test result shows the following information: Loop ID/Status, Data Miscompare, Link Failure, Sync Loss, Signal Loss, and Invalid CRC.

  Some devices do not support read/write buffer commands. FAStT MSJ displays the result for these devices as Information (blue) with the `R/W buffer not supported` message in the Data Miscompare column. The test results are sorted in the following order:

  1. Errors
  2. Information
  3. Success

  Notes:

  1. The TotalStorage Fibre Channel Host Bus Adapter (QLA2100) does not support loopback mode. Use only the read/write test for this type of adapter.
  2. A wrap connector and coupler (refer to the README file for the part number) is available to assist in isolating loop problems. When running the loopback

test, you can plug the wrap connector directly into the FAStT host bus adapter to verify whether the adapter is functional. You can then move the wrap connector to other points in the loop (for example, ends of cables, hubs, and so on) to isolate the point of failure.

3. If the read/write buffer test returns the message `The Adapter has no devices attached`, make sure that the HBA is connected to the devices, and click **Refresh**. Detected devices will appear in the HBA tree of the selected host.

Running the diagnostic tests

After you have chosen the loopback and read/write buffer test parameters as described in "Diagnostics" on page 195, click **Loopback Test** or **Read/Write Buffer Test** to run the loopback or read/write buffer test. If displaying warnings is enabled, the warning window shown in Figure 76 is displayed.

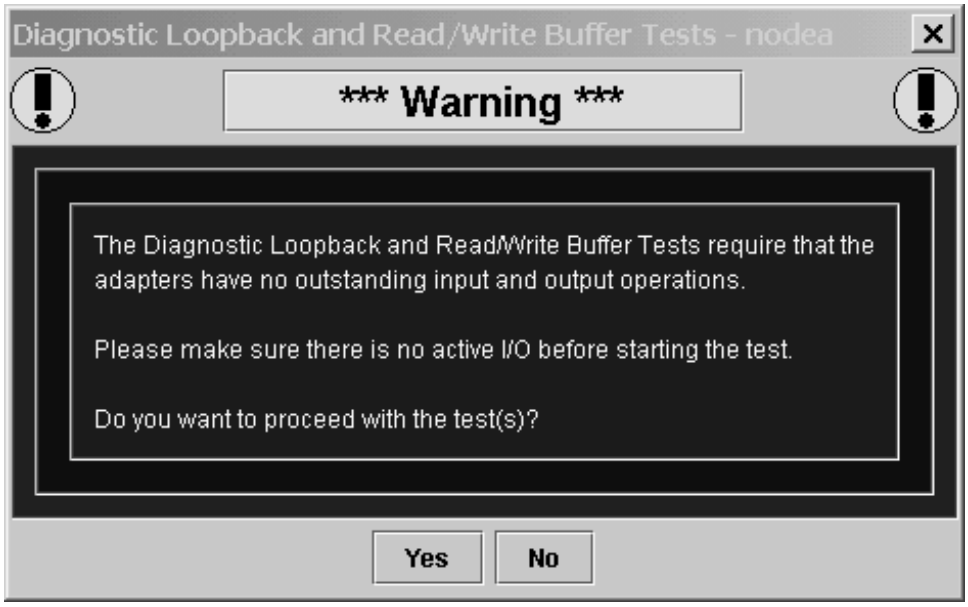


Figure 76. Diagnostic Loopback and Read/Write Buffer Test Warning Window

Note: To disable the warning message, click **View** -> **Options**, and clear the **Enable Warning Messages Displays** check box.

If you selected the **Test continuously** check box or a large value for number of tests or test increments, the Test Progress dialog window is displayed (see Figure 77). Click **Stop** to cancel the test.

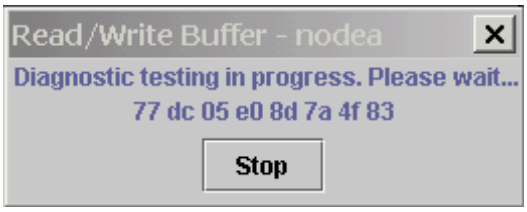


Figure 77. Test Progress Dialog Window

Diagnostic test results

The Test Result section of the Diagnostics panel displays the results of a test (see the following figures). Descriptions of the loopback and read/write test results sections follow.

Loopback test results: The Loopback Test Results section provides the following information:

- Tests Status—whether the test passed or failed. The possible values are:
  - Success—The test passed.
  - Error—CRC, disparity, or frame length errors occurred.
  - Failed—An error occurred when attempting to issue a command.
  - Loop down—The loop is down.
- CRC Error—Number of CRC errors
- Disparity Error—Number of disparity errors
- Frame Length Errors—Number of frame length errors

The Test Status column in Figure 78 shows that the loopback test failed.

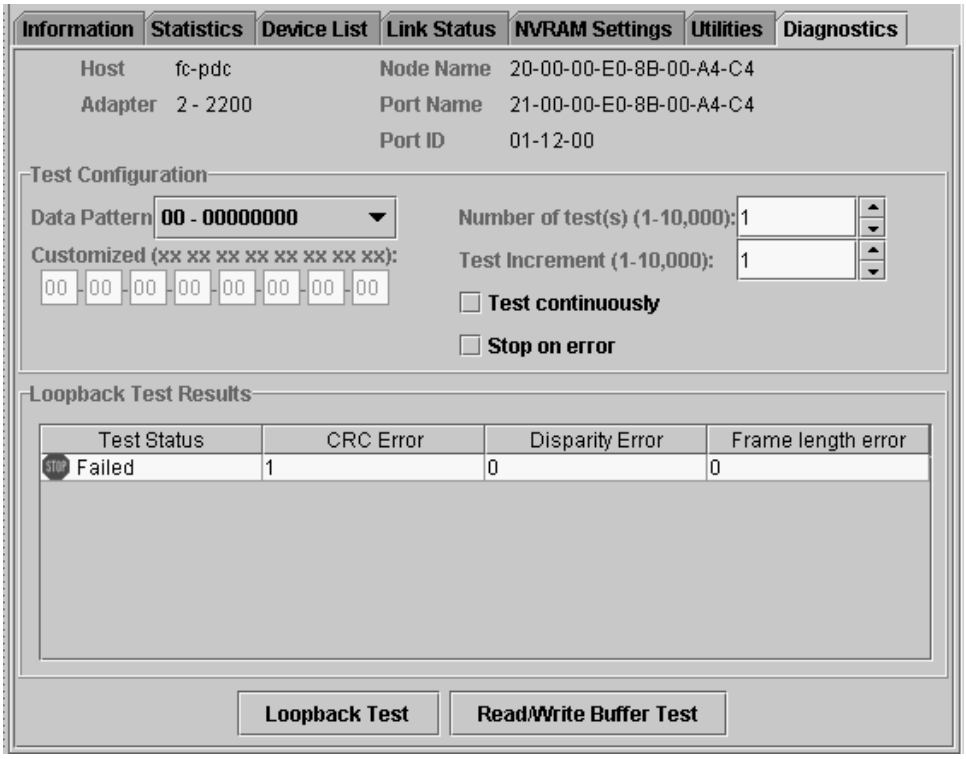


Figure 78. Test Result Section of the Diagnostics Panel

Read/Write Buffer Test Results: The Read/Write Buffer Test Results section provides the following information (see Figure 79 on page 200):

- Loop ID—The loop ID of the adapter when operating in loop mode
- Status—Whether the test passed or failed. The possible values:
  - Success—The test passed.
  - Error—A data miscompare or link status firmware error occurred.
  - Failed—A link status error, SCSI write buffer error, or SCSI read buffer error occurred.

  - Unknown—The target was not present.
  - Unsupported—The device does not support this test.
- Data Miscompare—Type of data miscompare. The possible values:
  - 0 (no data miscompares)
  - Get link status failed
  - Read buffer failed
  - Reserve unit failed
  - Release unit failed
  - R/W buffer not supported
  - Write buffer failed
- Link Failure—Number of link failures
- Sync Loss—Number of sync loss errors
- Signal Loss—Number of signal loss errors
- Invalid CRC—Number of CRCs that were not valid

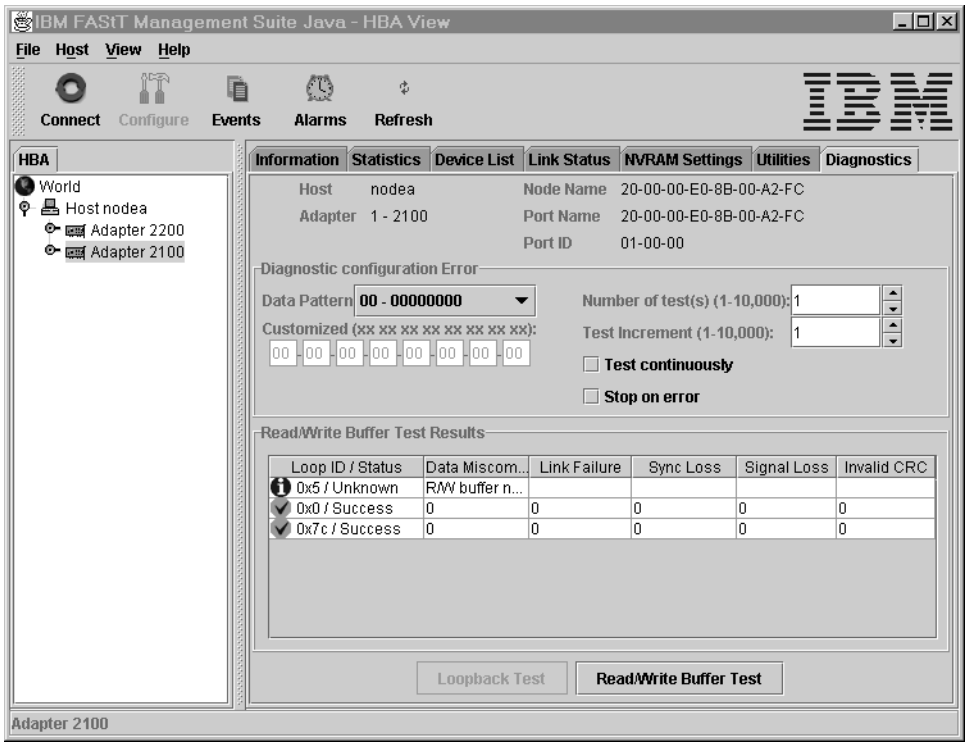


Figure 79. Read/Writer Buffer Test Results Section of the Diagnostics Panel

Saving a configuration to a file

You can save a virtual image of a host that has been configured and might no longer be connected to the network by saving the host configuration to a file. To load the configuration of the host that has been saved, you must first configure and save the host information to a file.

To save the host configuration, click **File -> Save Configuration to File** in the Host Adapter Configuration window.

You are alerted with the information shown in Figure 80.

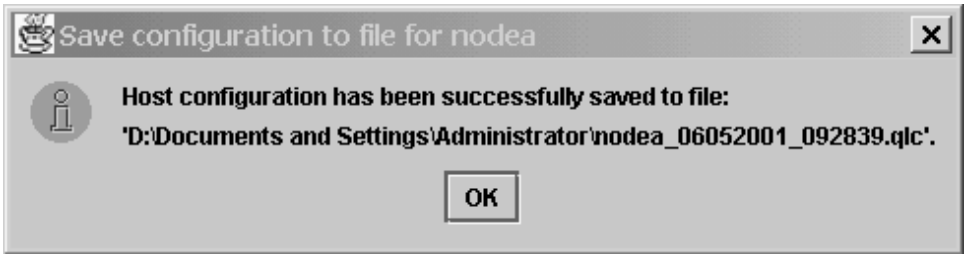


Figure 80. Save Configuration to File Notification Dialog Window

After you have saved the .qlc file, you can load it.

Loading a configuration from a file

After you have saved the host configuration to a file, you can load the configuration. Loading from a file enables you to load a virtual image of a host that has been previously configured and that is no longer connected to the network.

To load a configuration from FAStT MSJ, perform the following steps:

1. Click **Host -> Load from File** in the Host Adapter Configuration window.
2. In the Open window, click the file you want to load, and then click **Open** (see Figure 81).

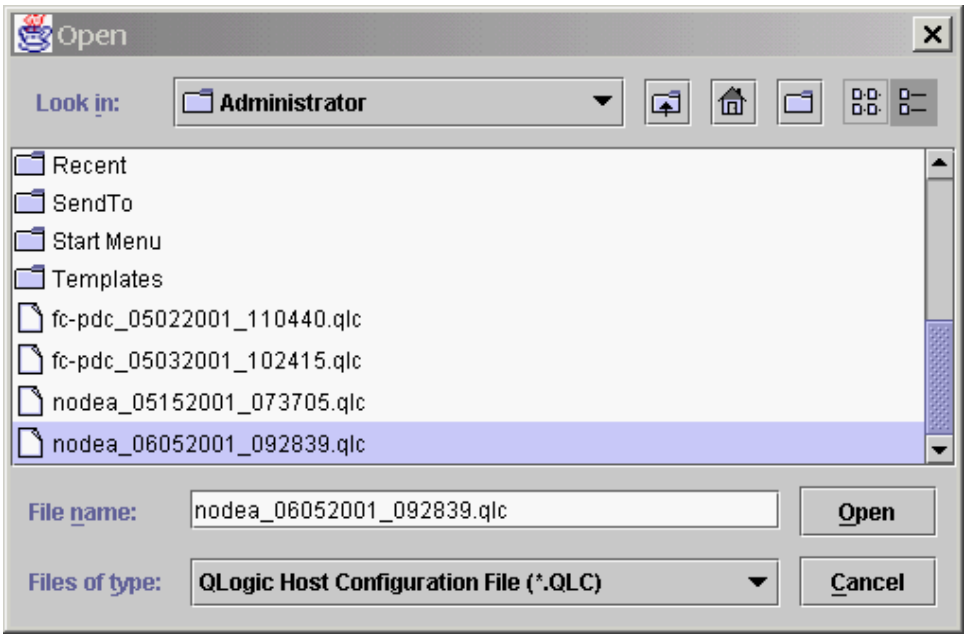


Figure 81. Open Window

After you have loaded the file, the adapters under the newly loaded host will appear in blue in the HBA. Blue adapters indicate that the host was loaded from a file rather than a live host.

Opening a group

Opening the group from a file enables the user to reload all the host information that was previously saved by the Save Group operation. FAStT MSJ will then connect the host and identify any discrepancies between the saved configuration and the newly discovered one.

To open a host configuration, click **File** -> **Open Group** in the **host adapter configuration** window. Select the desired .hst file from the **Open** window. After the file has been opened, the newly loaded host will be connected and displayed in the HBA tree panel.

Saving a group

Saving a Host Group to a file enables the user to save the HBA tree for that host including the device list and configuration settings. This feature also allows a system administrator to create Host files to selectively connect a number of hosts in the same SAN.

To save a host configuration to FAStT MSJ, the host adapter must be configured. Click **File** -> **Save Group** in the host adapter configuration window.

After **Save Group** is selected, the Save window is displayed. Select a file name (for example. Host NodeA.HST) and click **Enter.**

SAN port configuration

This section describes the port configuration function of FAStT MSJ and includes the following information:

- Configuring fibre channel devices
- Configuring LUNs for a device
- Viewing adapter, device, and path information
- Editing persistent configuration data
- Saving and retrieving the host configuration to view from a file
- Using the failover watcher

Note: All of these configuration functions are available for only Linux operating systems.

Configuring fibre channel devices

Perform the following steps to configure fibre channel devices.

1. Do one of the following from the FAStT MSJ main menu.
   - In the HBA tree, click the host or an adapter connected to the host. Click **Configure** on the toolbar.
   - Right-click the host or adapter in the HBA tree. From the pop-up menu, click **Configure**. If FAStT MSJ detects an erroneous port configuration, the following message is displayed. Click **OK** to continue.

     Note: You will see the message shown in Figure 82 on page 203 prior to configuring the ports for the first time.

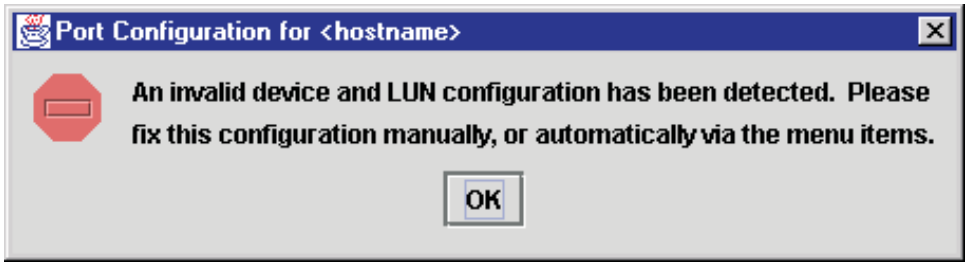


Figure 82. Port Configuration Message Dialog Window

Erroneous port configurations include:

- A device with contradictory visible paths. Only one path can be visible at a time.
- A LUN with contradictory (both disabled and enabled) paths. A configuration is valid when all paths are either enabled or disabled.
- More than one preferred path in the system. Only one path can be preferred at a time.

The Fibre Channel Port Configuration window is displayed (see Figure 83). The host name is displayed in the title bar. The window displays the adapters

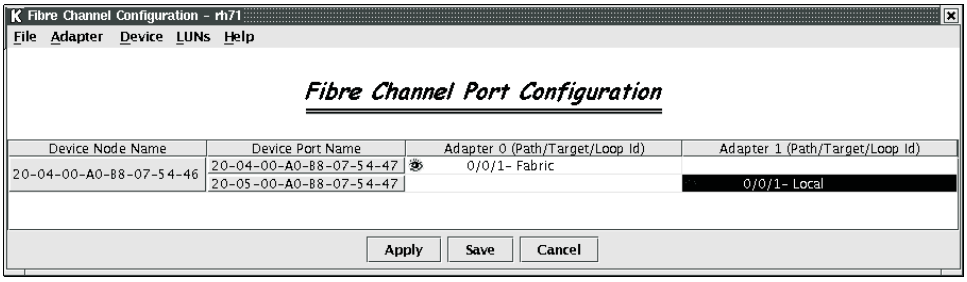


Figure 83. Fibre Channel Port Configuration

and devices in the computer. The following information is displayed.

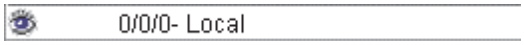
- Device Node Name: World wide device node name
- Device Port Name: World wide device port name
- Adapter n (Path/Target/Loop ID): The adapter cell in the table represents a path (the device is visible to the adapter)

Adapter cell information consists of the following:

– Path: Path number
– Target: Device ID
– Loop ID: Complement of the arbitrated loop_physical address (AL_PA)

The adapter cells are color-coded to represent path information, as follows:

– White with open eye icon: The path is visible to the operating system.



– Black with no icon: The path is hidden from the operating system.

– Gray with stop icon: The device is unconfigured.

– White with no icon: There is no path present.

2. Select the following, as appropriate, from the Fibre Channel Port Configuration window menu.
   - Modify the devices, LUNs, and paths:
     – Editing persistent configuration data (see “Editing persistent configuration data” on page 213)
     – Separating and combining separated device ports (see “Separating and combining separated device ports” on page 205)
     – Auto configuring device paths (see “Automatically configuring device paths” on page 206)
     – Configuring LUNs for a device (see “Configuring LUNs for a device” on page 207)
     – Enabling and disabling LUNs (see “Enabling and disabling all LUNs” on page 206)
     – Load balancing LUN paths on this host (see “Load balancing LUN paths on this host” on page 206)
     – Setting device path visibility (see “Setting device path visibility” on page 207)
   - View information:
     – Adapter information (see “Viewing adapter information” on page 212)
     – Device information (see “Viewing device information” on page 212)
     – Help information. Click **Help** -> **Browse Contents**. The help text for the Fibre Channel Port Configuration window is displayed.
3. The modified configuration set up by FAStT MSJ can be applied to the live system for dynamic updates, or can be saved to the system persistent configuration file. When you save the configuration, the adapter device driver retrieves the data from the persistent configuration file at the next system startup and configures the system accordingly.

Do one of the following:

- Click **Apply** to apply the new configuration. The new configuration is saved to the persistent configuration file; it will be used the next time the system is restarted. The new configuration remains in memory and is displayed after the apply operation completes. If configuration is successful, the message shown in Figure 84 on page 205 is displayed. Click **OK**.

  Note: For Linux operating systems, the applied configuration is only effective after the device driver is unloaded and subsequently reloaded with modprobe.

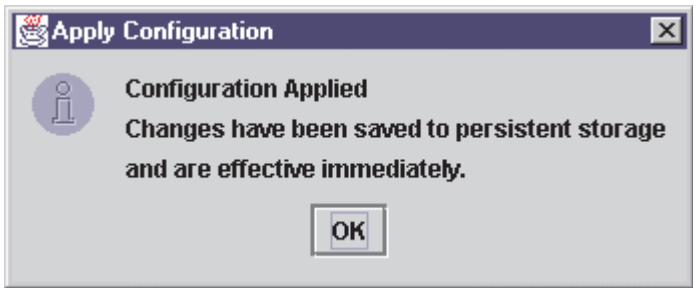


Figure 84. Apply Configuration Dialog Window

- Click **Save** to save the new configuration. The new configuration is saved to the persistent configuration file; it will be used the next time the system is started. The current configuration remains in memory and is redisplayed after the save operation completes.

  If the save was successful, the following message is displayed (see Figure 85). Click **OK**.

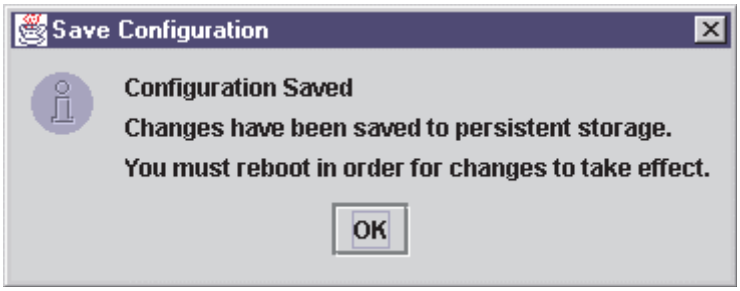


Figure 85. Save Configuration Dialog Window

  If the save failed, the **Save Configuration Failed** message is displayed. The failure is usually caused by communication problems between the GUI and agent. Click **OK**.
- Click **Cancel** on the Fibre Channel Port Configuration window if you do not want to save the configuration changes.

Note: For Linux operating systems, the saved configuration is effective after the device driver is reloaded. Restarting is not required.

Separating and combining separated device ports

Failover and currently active paths are usually configured based on the device (as represented by the device node name). This method allows for adapter level and port failover. You can, however, separate a device into two devices based on a port (by device port name), where each device has a subset of paths. This allows only for adapter level failover.

Forcing separate devices: Perform the following steps to divide a device with two ports into two distinct devices based on the port. Click **Edit** -> **Force Separate Devices**, or right-click the device node name and click **Force Separate Devices**.

Combining separated devices: Perform the following steps to combine two devices with the same device node name (separated based on their port name) back into one device based on the device node name:

1. Click the device node name in the Fibre Channel Port Configuration window.

2. Click **Edit** -> **Combine Separated Devices**, or right-click the **Device Node Name** and click **Combine Separated Devices**.

Automatically configuring device paths

The **Auto Configure** option configures all device paths for the selected host to the default values. The default path for each device is the first available path as visible, with the other paths hidden. This option prompts for the automatic configuration of LUNs associated with these devices.

Perform the following steps to configure the device paths, and optionally the LUN paths, on this host to default values.

1. From the Fibre Channel Port Configuration window, click **Tools** -> **Auto Configure**. The system prompts whether you also want to use default LUN configurations.
2. Click **Yes** to change the current LUN configurations to the default values. Click **No** to keep the current LUN configuration settings.

Enabling and disabling all LUNs

Perform the following steps to configure all LUNs attached to devices on this host as enabled or disabled.

1. From the Fibre Channel Port Configuration window, click **Tools** -> **Enable LUNs**.
2. Do one of the following:
   - Click **Enable All** to configure all LUNs as enabled.
   - Click **Disable All** to configure all LUNs as disabled.
   - Click **Inverse State** to enable currently disabled LUNs and disable currently enabled LUNs.

Load balancing LUN paths on this host

The **Load Balance** option configures all LUN paths on this host to use system resources most efficiently. The LUNs are staggered between the adapters for load distribution. You can configure all LUNs or only LUNs that are enabled.

Perform the following steps to configure LUNs on this host:

1. From the Fibre Channel Port Configuration window, click **Tools** -> **Load Balance**.
2. Do one of the following:
   - Click **Enabled LUNs Only** to configure only enabled LUNs for load balancing across the paths within this device. When you click this option for a device with no enabled LUNs, the message shown in Figure 86 is displayed. Click **OK**.

Figure 86. Enabled LUNs Only Warning Dialog Window

- Click **All LUNs** to configure all LUNs for load balancing across the paths within this device.

Setting device path visibility

Perform the following steps to set device path visibility to the operating system.

Note: There must be one visible path for the operating system to see the device.

1. In the Fibre Channel Port Configuration window, right-click the cell in the Adapter n column that contains the adapter name.
2. From the pop-up menu, click one of the following options:
   - Click **Set Visible** to set this path as visible to the operating system during the start process.
   - Click **Set Hidden** to set this path as not visible to the operating system during the start process but used in failover conditions.
   - Click **Set Unconfigured** to set this path as not visible to the operating system. The path is not used in failover conditions. If setting the path has caused the LUNs associated with this device to have an invalid configuration, the error message shown in Figure 87 is displayed.

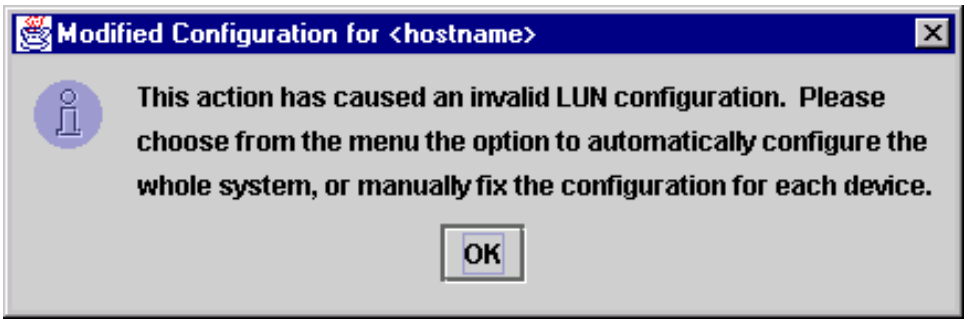


Figure 87. Modified Configuration Error Dialog Window

This problem is usually the result of changing the configuration state of a device. You must modify the LUN configuration for this device before you can save or apply the configuration.

Configuring LUNs for a device

Perform the following steps to configure individual LUNs for a selected device:

1. In the Fibre Channel Port Configuration window, right-click the cell in the Device Node Name or Device Port Name column that contains the device name.
2. From the pop-up menu, click **Configure LUNs**.
   - If FAStT MSJ detects an erroneous LUN configuration, the message shown in Figure 88 on page 208 is displayed. Click **OK** to continue.

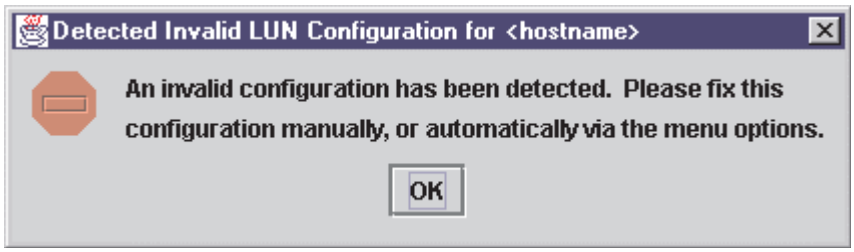


Figure 88. Detected Invalid LUN Configuration Error Dialog Window

Erroneous LUN configurations include:

- A LUN with both enabled and disabled paths. All paths must be either enabled or disabled.
- Too many preferred paths in the system. Only one path can be preferred at a time.

- If FAStT MSJ detects an erroneous SAN cloud configuration, the message shown in Figure 89 is displayed.

Figure 89. Detected Invalid SAN Cloud Dialog Window

Change this configuration before continuing; FAStT MSJ cannot manage erroneous SAN configurations. Click **OK** to continue.

The LUN Configuration window for the device is displayed (see Figure 90). The title displays the host name and world wide device node name. The table

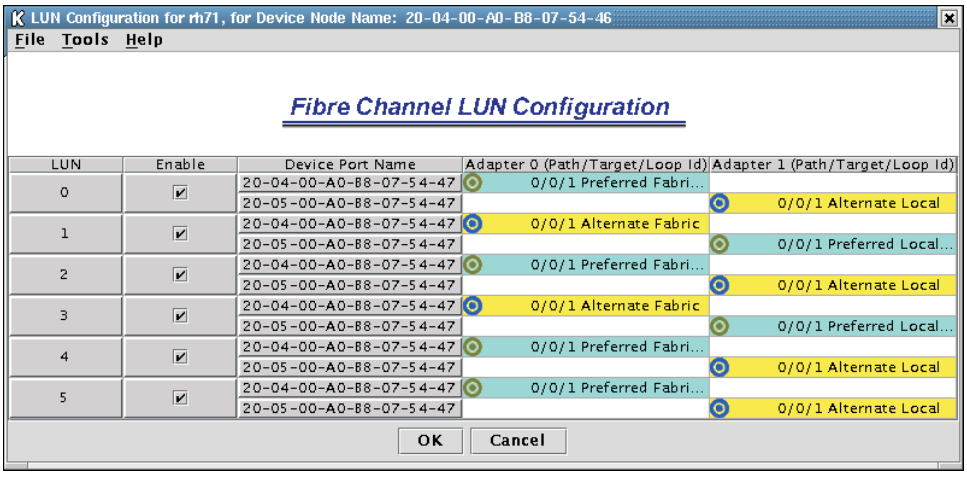


Figure 90. LUN Configuration Window

displays the following information:

- LUN: LUN number
- Enable: Whether the LUN is enabled

- Device Port Name: World wide device port name
- Adapter n (Path/Target/Loop ID): The adapter cell in the table represents a path (the device is visible to the adapter)

Adapter cell information consists of the following:

- Path: Path number
- Target: Device ID
- Loop ID: Loop IDs are 7-bit values that represent the 127 valid AL_PA addresses.
- Path type: Preferred or Alternate, and Current

The adapter cells are color-coded to represent path information, as follows:

- Cyan with green bull's-eye: The preferred path to the LUN.

- Yellow with blue bull's-eye: An alternate path to the LUN.

- Gray with Stop icon: This is an unconfigured device.

- White with no icon: There is no path present.

3. Click the following, as appropriate, from the LUN Configuration window menu:
   - Modify the LUNs and paths for this device:
     - Auto configuring LUN paths (see "Automatically configuring LUN paths" on page 210)
     - Load balancing LUN paths on this device (see "Load balancing LUN paths on this device" on page 210)
     - Configuring a LUN path using the default (see "Configuring a LUN path using the default" on page 211)
     - Enabling and disabling all LUNs (see "Enabling and disabling all LUNs" on page 206)
     - Enabling and disabling individual LUNs (see "Enabling and disabling individual LUNs" on page 211)
     - Setting LUN path failover (see "Setting LUN path failover" on page 211)
   - View information:
     - Adapter information (see "Viewing adapter information" on page 212)
     - Device information (see "Viewing device information" on page 212)
     - Path information (see "Viewing path information" on page 213)
   - Help information. Click **Help** -> **Browse Contents**. The help text for the LUN Configuration window is displayed.
4. Click **OK** to save the changes until you exit the Fibre Channel Port Configuration window; then, review the configuration changes (see Step 3). If FAStT MSJ detects an erroneous LUN configuration while saving the configuration, the Auto LUN Configuration at Exit for <*hostname*> window is displayed (see Figure 91 on page 210).

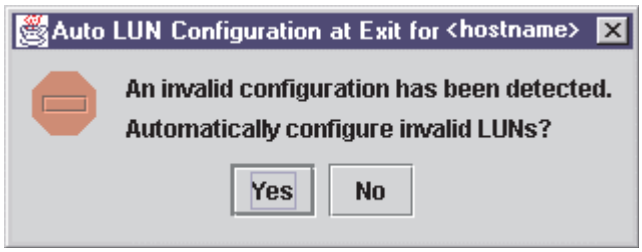


Figure 91. Auto LUN Configuration at Exit Dialog Window

Do one of the following:

- Click **Yes** if you want the software to configure the invalid LUNs with the default paths. The confirmation message shown in Figure 92 is displayed. Click **OK**.

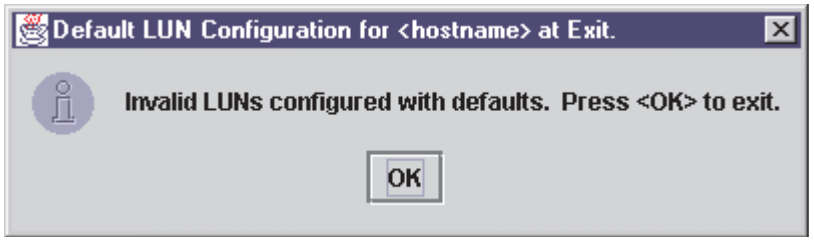


Figure 92. Invalid LUNs Configured with Defaults Error Dialog Window

- Click **No** if you do not want to configure the invalid LUNs. The configuration changes you made are not saved.
- Click **Cancel** if you do not want to apply the configuration changes.

Automatically configuring LUN paths

The **Auto Configure** option configures all LUN paths for the selected device to the default values. The default path for each LUN is the first available preferred path, with the other paths as alternates. From the LUN Configuration window **Tools** menu, click **Auto Configure** to configure the LUN paths on this device to the default values.

Load balancing LUN paths on this device

The **Load Balance** option configures all LUN paths on this device to use system resources most efficiently. The LUNs are staggered between the devices to provide load distribution. You can configure all LUNs or only LUNs that are enabled. Perform the following steps to configure the LUNs on this device:

1. From the LUN Configuration window **Tools** menu, click **Load Balance**.
2. Do one of the following:
   - Click **Enabled LUNs Only** to configure only those LUNs enabled for load balancing across the paths within this device. If you clicked this option for a device with no enabled LUNs, the message shown in Figure 93 on page 211 is displayed. Click **OK**.

Figure 93. Enabled LUNs Configuration Error Dialog Window

- Click **All LUNs** to configure all LUNs for load balancing across the paths within this device.

Configuring a LUN path using the default

Perform the following steps to configure a LUN paths to the default values for LUN failover, with the first configured path as preferred and all other paths as alternate.

Note: This option is available only if the LUN is enabled and there are at least two available paths.

1. For the LUN you want to configure, right-click in the LUN, Enable, or Device Port Name column.
2. From the pop-up menu, click **Configure Path Using Default**.

Enabling and disabling all LUNs

Perform the following steps to configure all LUNs attached to this device as either enabled or disabled.

1. In the LUN Configuration window, right-click the **Enable** heading.
2. From the pop-up menu, click one of the following:
   - **Enable All LUNs** to configure all LUNs as enabled
   - **Disable All LUNs** to configure all LUNs as disabled
   - **Inverse State** to enable currently disabled LUNs and disable currently enabled LUNs

Enabling and disabling individual LUNs

To configure a specific LUN as enabled or disabled, in the LUN Configuration window Enable column do one of the following:

- Select the **Enable** check box to configure the LUN as enabled.
- Clear the **Enable** check box to configure the LUN as disabled.

Setting LUN path failover

Perform the following steps to set a LUN path as the preferred or alternate path in a failover condition. You can also click the preferred or alternate path as the currently active path.

Perform the following steps to set LUN path failover:

1. In the LUN Configuration window, right-click the cell for the device in the Adapter n column.
2. From the pop-up menu, click one of the available options.
   - Click **Set LUN to Preferred** to set the alternate path as the preferred path in a failover condition.
   - Click **Set LUN to Alternate** to set the preferred path as the alternate path in a failover condition.

- Click **Set Path to Current** to set this preferred or alternate path as the currently active path.

Notes:

1. You can set the path of an enabled LUN only. A LUN path can be set as either preferred or alternate (but not as unconfigured) if the device path is configured as hidden or visible.
2. You can use the failover watcher to view the failover settings for a selected host and set the preferred or alternate LUN path as the currently active path (see "Using the failover watcher" on page 215).

Viewing adapter, device, and path information

You can view adapter, device, and path information in the Fibre Channel Port Configuration and LUN Configuration windows. In the LUN Configuration window, you can also view LUN information. See "Diagnostics and utilities" on page 184 for information about viewing host, adapter, device, and LUN information from the tab panel.

Viewing adapter information

Perform the following steps in the Fibre Channel Port Configuration and LUN Configuration windows to view adapter information.

1. Right-click the Adapter n column heading to display information about a specific adapter. The Adapter Information window is displayed. This window lists the following information:
   - Number: Adapter number
   - Type: Type of board. 2200 indicates a QLA22xx
   - Serial Number: Serial number of the adapter
   - Driver Version: Version of the adapter driver on the host that controls the adapter
   - Firmware Version: Version of the adapter firmware on the host that controls the adapter
   - BIOS Version: BIOS version on the adapter
   - PCI Slot Number: PCI slot number assigned by the host
   - Node Name: World wide adapter node name
   - Port Name: World wide adapter port name
   - Total Number of Devices: Number of devices attached to the adapter
2. Click **OK** to close the Adapter Information window.

Viewing device information

Perform the following steps in the Fibre Channel Port Configuration and LUN Configuration windows to view device information.

1. To display information for a device node, do one of the following:
   - In the Fibre Channel Port Configuration window, right-click a cell in either the Device Node Name or Device Port Name column.
   - In the LUN Configuration window, right-click a cell in the LUN, Enable, or Device Port Name column.

   The Device Information window is displayed. This window lists the following information:
   - Product Identification: Product ID of the device
   - Product Vendor: Device manufacturer
   - Product Revision: Device revision level

- Path: Path number
- Target: Device number
- LUN: The first LUN attached to the device
- Loop ID: Loop IDs are 7-bit values that represent the 127 valid AL_PA addresses.
- Port ID: Port ID of the selected device's port
- Node Name: Click World wide node name of the device
- Port Name: World wide port name of the selected device's port

  Note: If the Device Node Name was selected, all the device's port names are displayed.
- Number of LUN(s): Number of LUNs attached to the device

2. Click **OK** to close the Device Information window.

Viewing path information

Perform the following steps to view path information in the LUN Configuration window.

1. Right-click the cell for the device in the Adapter n column. The Path Information window is displayed for the path.

The following information is displayed:

- Device Node Name: World wide node name of the device
- Device Port Name: World wide port name of the selected device's port
- LUN: LUN number
- Device Port ID: Port ID of the selected device's port
- Vendor ID: Device manufacturer
- Product ID: Product ID of the device
- Product Revision: Device revision level
- For the Preferred Path and Alternate Path sections:
  - Adapter Number: Number of the adapter
  - Path ID: Path number
  - Target ID: Device ID

2. Click **OK** to close the Path Information window.

Editing persistent configuration data

When you select **Persistent Configuration Data**, the current configuration data is displayed if a configuration exists. You can do the following:

- Click **Adapter Persistent Configuration** to delete the persistent configuration data for an adapter and its devices and LUNs (see "Deleting adapter persistent configuration data").
- Click **Device Persistent Configuration** to delete the persistent configuration data for a device and its LUNs (see "Deleting device persistent configuration data" on page 214).

Deleting adapter persistent configuration data

Perform the following steps to delete the persistent configuration data for an adapter, its devices, and LUNs.

1. Do one of the following:
   - From the FAStT MSJ main window, right-click the host or adapter in the HBA tree. In the resulting pop-up menu, click **Adapter Persistent Configuration Data**.

- From the Fibre Channel Port Configuration window **Adapter** menu, click **Adapter Persistent Configuration Data**.

The Fibre Persistent Configuration Editor window is displayed (see Figure 94). For each adapter connected to the host, the current persistent configuration editor

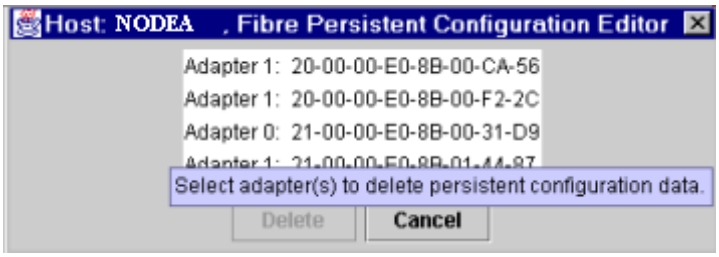


Figure 94. Fibre Persistent Configuration Editor Window

lists the adapter number and its world wide port name.

2. Do one of the following to delete one or more entries:
   - Click the adapter entries that you want to delete.
   - Click **Delete** to remove the entries.

     The Security Check window is displayed. Enter the password, and click **OK**.

     Note: Changes made to the persistent configuration are final. If you do not want the changes, reconfigure the host (see "Configuring fibre channel devices" on page 202).

Deleting device persistent configuration data

Perform the following steps to delete the persistent configuration data for a device and its LUNs.

1. Do one of the following.
   - From the FAStT MSJ main window, right-click the device or LUN in the HBA tree. In the resulting pop-up menu, click **Device Persistent Configuration Data**.
   - From the Fibre Channel Port Configuration window, click **Device** -> **Device Persistent Configuration Data**.

   The Device Persistent Configuration Editor window is displayed.
   For each device connected to the adapter, the current persistent configuration editor displays the device number and its world wide port name.
2. Do the following to delete one or more entries:
   a. Click the device entries that you want to delete.
   b. Click **Delete** to remove the entries. The Security Check window is displayed.
   c. Type the password and click **OK**.

   Note: Changes made to the persistent configuration are final. If you do not want the changes, reconfigure the host (see "Configuring fibre channel devices" on page 202).

Saving and printing the host configuration file

You can save the host configuration file and then view a virtual image of the host. The file name includes the host name, date saved, and time saved. See "Saving a configuration to a file" on page 200 for details.

To print a device and LUN configuration, perform the following steps:

1. From the FAStT MSJ main window, do one of the following:
   a. In the HBA tree, click the host (or adapter connected to the host).
   b. Do one of the following:
      - Click **Configure** on the toolbar.
      - Right-click the host (or adapter) in the HBA tree. From the resulting pop-up menu, click **Configure**.

The Fibre Channel Port Configuration window is displayed.

2. Click **File** -> **Print**.
3. Select the printer and print the configuration.

Using the failover watcher

The failover watcher enables you to view the failover settings for a selected host and set a preferred or alternate LUN path as the currently active path.

Note: See “Setting LUN path failover” on page 211 for more information.
Perform the following steps to view or modify the failover information.

1. In the FAStT MSJ main window HBA tree, click the host for which you want to view failover information.
2. Do one of the following:
   - Click **Host** -> **Current Path**.
   - Right-click the host in the HBA tree. From the pop-up menu, click **Current Path**. The HBA ViewFailover window is displayed (see Figure 95).

   The identifying information is displayed:

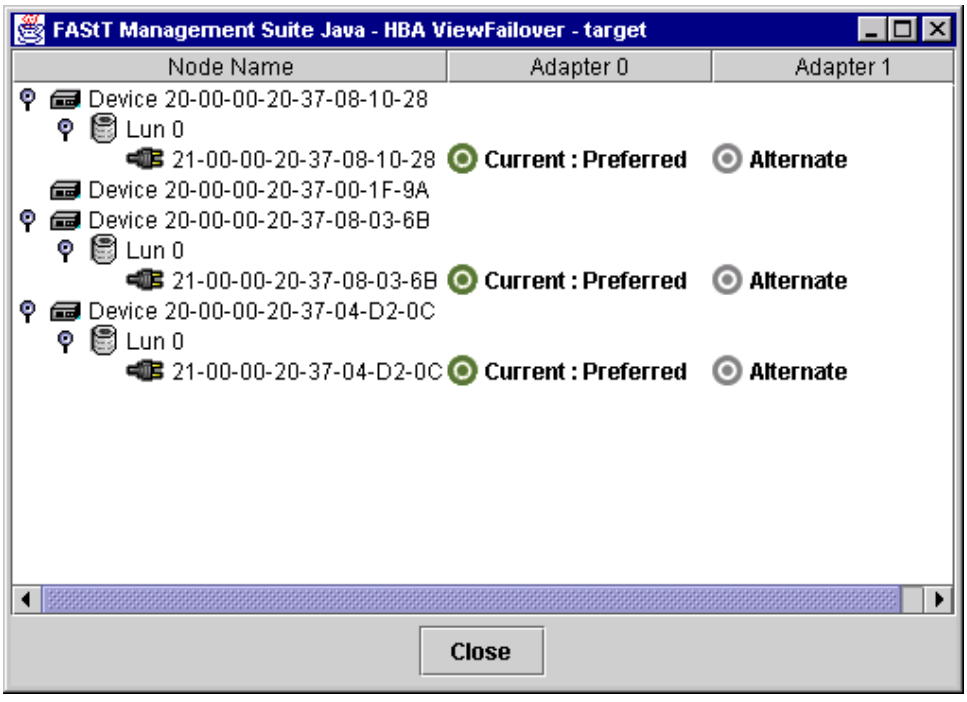


Figure 95. HBA View Failover Window

- **Host**

  The title displays the host name.

The failover information is displayed:

- **Node Name**

  Listing of the devices and LUNs.

  – Devices

    World wide device port name of the devices.

  – LUNs

    LUNs are listed under the devices to which they are connected. Includes the LUN number and world wide LUN port name.

- **Adapters**

  Lists the adapters connected to the host and specifies their path status:

  – Preferred

  – Alternate

  Path status:

  – Green bull's-eye and **Current**: currently active

  – Gray bull's-eye: not active

  – Red bull's-eye: preferred path that is not active

3. To set the path of a device as currently active, do the following:
   a. Right-click the path status in the Adapter column.
   b. In the pop-up menu, click **Set Current**. The bull's-eye changes to green and the word *Current* is displayed.

Chapter 19. Introduction to SANavigator

This chapter provides an overview of the functions of SANavigator. Please refer to the User manual (PDF format) located in the SANavigator install folder to learn more about the features of SANavigator.

SANavigator management software provides easy, centralized management of your SAN, and quick access to device configuration applications. The complete SAN is displayed graphically, so administrators of all levels can manage networks with ease.

Operating in a SAN environment

SANavigator enables you to easily monitor and manage your SAN through the following features:

1. **Discovery**

   SANavigator uses TCP/IP (out-of-band) and fibre channel (in-band) to establish contact with a large number of SAN devices, gather embedded information, and then depict it all graphically. SANavigator discovers the devices attached to your SAN. It then presents a visual map of devices and their interconnections, enabling you to identify any problem components in the map.

2. **Launching Device Applications and Utilities**

   You can launch applications and utilities such as IBM FAStT Storage Manager and IBM FAStT MSJ from SANavigator by right-clicking on the respective devices. A pop-up menu will be displayed to allow you to select the applications as well as link to the IBM Fibre Channel Solution Support web site.

3. **Monitoring**

   SANavigator generates events and messages about the status of devices and their respective properties. SANavigator's self-monitoring event logging and messaging feature enables you to stay informed about the current state of the SAN.

4. **Reporting**

   SANavigator enables you to generate, view, and print reports.

New features of SANavigator 3.1

Version 3.1 has significantly enhanced the capability of SANavigator. It includes the following new features:

- Remote Discovery Connector enabling you to In-Band manage remote hosts from a local Management Station. In previous versions In-Band management was possible only on the system where the SANavigator Server was installed and where the HBAs were located.
- Login/Logout function that enables you to log in or out of a SANavigator server without closing the application.
- Customizable topology views. You can now select to view a single Fabric or all Fabrics. You can also customize the Device List (show/hide/relocate columns on device list).
- Improved user administration function.
- Auto-detection of topology overload.
- Detachable and scalable mini map to allow a more user-customized desktop.
- Latency graphs to monitor performance.

- An improved GUI

System requirements

The following are the minimum requirements for SANavigator:

- Windows operating systems (NT SP 6a and Windows 2000 Professional, Enterprise Server, and Advanced Server)
  - 700 MHz Intel Pentium III and up
  - CD-ROM
  - 512 MB RAM
  - Disk Space: 150 MB
  - VGA - 256 colors or greater
- Linux operating systems (Red Hat 7.2)
  - 700 MHz Intel Pentium III and up
  - 512 MB RAM
  - Disk Space: 150 MB
  - VGA - 256 colors or greater

Installing SANavigator and getting started

This section contains instructions for installing SANavigator on your system.

You can install SANavigator as a client, a server, both client and server, or as a Remote Discovery Connector. The major benefit of using the Client/Server feature is that a SAN running on a server can have a number of clients working simultaneously on the same SAN. Each client can monitor what all other clients are doing, whether across the room or halfway around the world. Each client can access all servers for which it is authorized. Clients can set personal preferences; preferences are saved locally.

You install the Remote Discovery Connector on Host(s) that you want to In-Band manage remotely. In addition the Host(s) must have the HBA API library installed.

Note: When performing any SANavigator install or uninstall, be sure that no part of the application (client, server, or Remote Discovery Connector) is running. This could cause a variety of problems, including a system crash.

You can install SANavigator from a CD or by downloading from the Web.

Note: Always uninstall any prior version of SANavigator before installing a new version.

Windows installation and uninstallation

This section describes how to install SANavigator for Windows from both a CD and from the web as well as how to uninstall the software.

Note: To further enhance the SANavigator discovery engine, install the HBA API library. This library is automatically installed by the IBM FAStT HBA Driver install package (driver version 8.1.5.60 and above). The API library enables you to discover your SAN through the fibre channel medium in addition to the Fabric network.

Installing from a CD

To install SANavigator for Windows from a CD, do the following:

1. Insert the SANavigator CD that came with your FAStT Storage Server into the CD-ROM drive.

   If you have autorun enabled, the install begins automatically. If you do not have autorun enabled, run the setup.exe application file in the Windows folder.

   Follow the instructions presented by the InstallShield wizard.
2. If you want to install a SANavigator client only, clear the **SANavigator Client and Server** check box in the Select Components and Destination window and select **Client**. If you want this machine to be remotely In-Band managed, select the Remote Discovery Connector. You will skip installation steps that are not required.

   Follow the instructions presented by the InstallShield wizard for the remainder of the installation.
3. Review the Readme_ibm.txt file (located in the root directory of the CD).

Installing from a Web download

To download SANavigator for Windows, go to the IBM Solution Support Web site http://www.ibm.com/pc/support. A link to SANavigator's website is available to download the IBM version of SANavigator. You will need to have your FAStT Storage Server model number and serial number available.

To install SANavigator from the Web, do the following:

1. After extracting the zip file, run the setup.exe application file in the Windows folder.

   Follow the instructions presented by the InstallShield wizard.
2. If you want to install a SANavigator client only, clear the **SANavigator Client and Server** check box in the Select Components and Destination window and select **Client**. If you want this Host to be remotely In-Band managed, select the Remote Discovery Connector. This will skip installation steps that are not required.

   Follow the instructions presented by the InstallShield wizard.
3. Review the Readme file (located on the IBM Solution Support Web site).

Uninstalling SANavigator

Note: Before uninstalling SANavigator, the SANavigator Server needs to be terminated. Make sure that no other client is using the server prior to ending the process. To terminate the server and client, click **Server** -> **Shutdown** from the menu bar. A dialog is displayed asking you to confirm the Shutdown and whether or not you want to also exit the client. If you do not uncheck the ″Shutdown Client also″ box, both the Client and Server (on the local machine) will be terminated provided no other remote clients are running.

Click **Start -> Program -> SANavigator -> Uninstall SANavigator** to begin the uninstall process. You are presented with three choices:

- Reinstall - SANavigator will be reinstalled. All SAN files are retained.
- Partial Uninstall - Retain Data and Preference Files - SANavigator will be uninstalled, but all SAN files are retained.
- Full Uninstall SANavigator will be uninstalled and all SAN files are deleted.

In order to retain access to your previous SAN files, be sure to reinstall SANavigator in the same location that the software was previously installed.

If you must reinstall in a new location, be sure to move your SAN files from the old install directory to the new directory.

Note: SANavigator 3.1 allows you to import and open SAN files that were created using version 2.7. See “Starting SANavigator server and client” on page 223for additional information.

Linux installation and uninstallation

This section describes how to install SANavigator for Linux from both a CD and from the web as well as how to uninstall the software.

Note: To further enhance the SANavigator discovery engine, install the HBA API library. This library is part of the IBM FAStT HBA Driver install package (version 6.0 and above). The API library enables you to discover your SAN through the fibre channel medium in addition to the Fabric network. Review the Readme_ibm.txt file located in the Linux/Redhat folder on the CD for additional information.

Installing from a CD

To install SANavigator for Linux from a CD, do the following:

1. Insert the SANavigator CD that came with your FAStT Storage Server into the CD-ROM drive.
2. Login as root.
3. From the Linux\Redhat directory on the CD, copy the .bin file (for example, SANav31irh.bin) to your temp directory.
4. Start the installer (./temp/SANav31irh.bin or sh ./temp/SANav31irh.bin)
5. Follow the on-screen instructions.
6. If you want to install a SANavigator client only, clear the **SANavigator Client and Server** check box in the Select Components and Destination window and Select **Client**. If you want this machine to be remotely In-Band managed select the **Remote Discovery Connector**. You will skip installation steps that are not required.

   Follow the instructions presented by the Installer for the remainder of the installation.
7. Review the Readme_ibm.txt file located in the Linux/Redhat folder on the CD for additional information.

Installing from a Web download

To download SANavigator for Linux, go to the IBM Solution Support Web site http://www.ibm.com/pc/support. A link to SANavigator’s website is available to download the IBM version of SANavigator. You will need to have your FAStT Storage Server model number and serial number available. See the Readme file on the IBM web site.

To install SANavigator from the Web, do the following:

1. Download the bin file from the SANavigator web site.
2. Open a terminal session in the GUI.
3. From the directory where you stored the bin file, do the following at the prompt:

   ```
   sh SANav31irh.bin
   ```

   or

   ```
   ./SANav31irh.bin
   ```
4. Wait for the introduction window to open.

5. Follow the instructions presented by the Installer.
6. If you want to install a SANavigator client only, clear the SANavigator **Client and Server** check box in the Select Components and Destination window and Select **Client**. If you want this machine to be remotely In-Band managed select the Remote Discovery Connector. You will skip installation steps that are not required.

   Follow the instructions presented by the Installer for the remainder of the installation.
7. Review the Readme file (located on the IBM Solution Support Web site).

Uninstalling SANavigator

Note: Before uninstalling SANavigator, the SANavigator Server needs to be terminated. Make sure that no other client is using the server prior to ending the process. To terminate the Server and Client click **Server -> Shutdown** from the menu bar. A dialog is displayed asking you to confirm the Shutdown and whether or not you want to also exit the client. If you do not uncheck the **Shutdown Client also** box, both the Client and Server (on the local machine) will be terminated provided that no other remote clients are running.

To begin uninstalling, do the following:

1. Open a terminal session in the GUI.
2. From the /usr/ directory, do the following at the prompt:

   ```
   sh Uninstall_SANavigator
   ```

   or

   ```
   ./Uninstall_SANavigator
   ```

   Note: Uninstall instructions assume that SANavigator was installed using the default selections.
3. Wait for the introduction window to open.
4. Follow the instructions presented by the Uninstaller.

You are presented with two choices:

- Partial uninstall

  Retain Data and Preference Files - SANavigator will be uninstalled, but all SAN files are retained.
- Full uninstall

  Delete all files - SANavigator will be uninstalled and all SAN files are deleted.

In order to retain access to your previous SAN files, be sure to reinstall SANavigator in the same location that the software was previously installed.

If you must reinstall in a new location, be sure to move your SAN files from the old install directory to the new directory.

Note: SANavigator 3.1 allows you to import and open SAN files that were created using version 2.7. See “Starting SANavigator server and client” on page 223 for additional information.

SANavigator Help

SANavigator help enables you to find subjects listed in the online table of contents or to search for specific keywords. The SANavigator documents are divided into three parts: HelpSet files, User Manual, and Reference Manual. All are listed in the table of contents and all are searched when you use the Find feature.

You can print the entire contents of the User Manual from the PDF file UserManual.pdf located in the SANavigator folder\directory.

For detailed information on how to use any of the following SANavigator features, start SANavigator and open the online help. Help topics are grouped as follows:

- **Reference**

  The Physical Map
  Use the Physical Map to display your SAN topology, devices, and their connections.

  The Mini Map
  Use the Mini Map to view your entire SAN domain and to move within that view.

  Device Tree/List
  The Device Tree/List displays a list of all discovered devices and their properties.

  Event Log
  The Event Log displays SAN events.

- **Tasks**

  - Configuring Your SAN for Best SANavigator Performance Monitoring (Premium feature)
  The configuration of your SAN can affect the functionality and performance of SANavigator.

  - Compatibility with Other Applications
  SANavigator is designed to operate smoothly with other Enterprise applications and network monitoring programs. Because SANavigator has fully configurable SNMP trap listening and forwarding functions, it can act as a primary or secondary network manager.

  - Log-in and Log-out to/from a SAN

  - Discovering Your SAN
  SANavigator uses a unique process to discover devices on your SAN.

  - Monitoring Your SAN
  SANavigator provides three methods of monitoring your SAN devices: Physical Map, Event Log, and Event Notification.

  - Monitoring the Performance of Your SAN (Premium feature)
  SANavigator provides animated, real-time performance information. You can set thresholds and be notified when they are exceeded.

  - Planning a New SAN (Premium feature)
  SANavigator provides the means to graphically plan and evaluate a new SAN.

  - Setting Up E-Mail Notification
  Configure event notification so you can receive messages when events you want to know about occur.

- Exporting Maps and Information

You can import or export SANavigator SAN files, performance data, Physical Map, Device Tree, or reports. This process is very useful when transmitting files to your support center or when capturing network status at local or remote locations.

- **Glossary**

  Many SAN-specific names and terms are described. See “Glossary” on page 463.

Starting SANavigator server and client

This section provides instructions for starting SANavigator in Windows and Linux operating systems.

Starting in Windows

To start both the SANavigator Server and Client in Windows, do one of the following:

- Click **Start -> Programs -> SANavigator x.x -> SANavigator**.
- Double-click the SANavigator x.x desktop icon.

To start the SANavigator Client in Windows, do one of the following:

- Click **Start -> Programs -> SANavigator x.x -> SANavigator Client**.
- Double-click the SANavigator x.x desktop icon.

If you installed the Remote Discovery Connector on a remote Host, click **Start -> Programs -> SANavigator Remote Discovery**. Although the process starts, no user interface is displayed.

Note: To run Remote Discovery Connector, the server must be configured. See “Setting up SANavigator Remote Discovery Connection for in-band management of remote hosts” on page 300 and the online help provided.

Further problem determination information can be found on the IBM Support Website.

Starting in Linux

To start both the SANavigator Server and Client in Linux, open a terminal session and do the following:

Enter the following from the /usr directory:

```
sh SANavigator
```

or

```
./SANavigator
```

To start the SANavigator Client in Linux, open a terminal session and do the following:

Enter the following from the /usr directory:

```
sh SANavClient
```

or

```
./SANavClient
```

If you installed the Remote Discovery Connector on a remote Host, open a terminal session and enter the following from the /user directory:

```
sh SANavRemote start
```

or

```
./SANavRemote start
```

To stop the process, enter the following:

```
sh SANavRemote stop
```

or

```
./SANavRemote stop
```

Note: To run Remote Discovery Connector, the server must be configured. See "Setting up SANavigator Remote Discovery Connection for in-band management of remote hosts" on page 300 and the online help provided.

Further problem determination information can be found on the IBM Support Website.

Configuration wizard

The first time SANavigator is started the Welcome Wizard is displayed. The Wizard allows you to configure SANavigator.

Import Data and Settings

This dialog allows you to select whether or not you want to import SANavigator version 2.7 data and settings into this new version. If you select **Yes** enter the location (path) where the exported .zip files are located.

Note: You need to export the SAN files from a 2.7 SANavigator session before uninstalling 2.7. When uninstalling the older version make sure that you select **Partial Uninstall** so that the SAN files are preserved.

SANavigator Server Name

SANavigator servers are given a name. The name helps you identify different servers. SANavigator automatically assigns the OS Network Identification computer name to the server as a default.

SANavigator Administrator

Users are identified and validated in SANavigator by a User ID and Password. In this dialog, enter your User ID and Password information.

SANavigator Win32 Service

If you run SANavigator as a Win32 service, you can log off the network without closing SANavigator. Click the check box to run SANavigator as a Service.

Note: Running SANavigator as a Win32 service is not recommended unless you are familiar with Win32 service behavior.

SANavigator Server License

This dialog allows you to enter the license key. Once entered, a summary of the server configuration is displayed as well as the features that were enabled by the license key.

To register SANavigator, do one of the following:

If you have an Internet connection, you can register on the Registration window. The completion of all fields is required for registration. Free web email addresses are not accepted.

If you do not have an Internet connection, the Registration window contains contact information. Your new license key will be emailed to you. Follow the instructions in the email to enter the license key in the application after it is running.

Note: The license key is required to enable the premium features. These include the following:

- SAN Planning
- SAN Performance Monitoring
- Zoning
- Policy Engine
- Greater than 32 Switch Ports
- Greater than five clients

Premium Features are available for a trial period of 30 days.

Initial discovery when client and server are on one computer

When you start SANavigator, the Login SAN dialog box is displayed. The Network Address field contains ″localhost″. If SANavigator detected the server, the informational message ″Server Available″ is displayed on the bottom left of the dialog box. The **Server Name** field contains the name of the local hardware server.

To perform initial discovery when the client and server are on the same computer:

1. Type the user ID and the password specified during the SANavigator configuration. Select ″Save Password″ if you want to save the Password.
2. Click **OK**. SANavigator automatically conducts an out-of-band discovery on your local subnet and displays any SAN devices it finds.

Initial discovery when client and a server are on different computers

When you start the SANavigator Client to connect to a remote SANavigator Server the Log-in SAN dialog box is displayed. You can enter the IP address of the remote Host in the Network Address field. If SANavigator connected to the remote server the informational message ″Server Available″ is displayed on the bottom left of the dialog box. To perform initial discovery when the client and server are on different computers:

1. Enter the IP address in the Network Field
2. Type the user ID and the password for the Server on the remote Host
3. Click **OK**. The SANavigator Client gathers the topology information from the remote Server and automatically displays the SAN devices discovered by the remote Server.

Viewing an existing SAN

To view a discovered SAN on an existing server, click Log-in. The Log-in SAN dialog box is displayed.

1. Type the IP address of the server in the Network Address field and click **OK**.
2. Type the user ID and password. Click **OK**. The SAN is discovered and displayed.

Setting up a new discovery

To set up a new discovery, do the following:

1. If the Discover Setup dialog box is not open, click **Discover -> Setup**.
2. Click the **General** tab and verify that **Out-Of-Band** is selected.
3. Click the **Out-of-Band** tab.
4. Review entries in the Selected Subnets and Selected Individual Addresses tables. Click any entries you do not want to discover now, and move them back to the Available Addresses table by clicking the appropriate arrow button.
5. To add new addresses to the Available Addresses table click **Add**; the Domain Information dialog box is displayed.
6. Type a description of the IP subnet where your SAN devices are located in the **Description** field.
7. Type the **IP Address** and **Subnet Mask** of a device (for example, a switch) on the SAN you want to discover.
8. Click **OK** to return to the Discover Setup dialog box.
9. In the Available Addresses table, click the address you entered and use the arrow button to move the address to the Selected Subnets table on the right.
10. If you want to enable In-band discovery, check the In-Band box in the General Tab dialog and select the available HBA(s). If no HBA is available, make sure the HBA API library has been installed. See “In-band discovery” on page 233.
11. Click **OK** to save the settings and to begin the discovery process.

SANavigator main window

The SANavigator main window, shown in Figure 96 on page 227, is displayed when you start SANavigator. By using the drop-down menus on the top of the window, you issue commands to the SANavigator software. To see how each command works, click the menu, note the name of the command, and search for the command in the help.

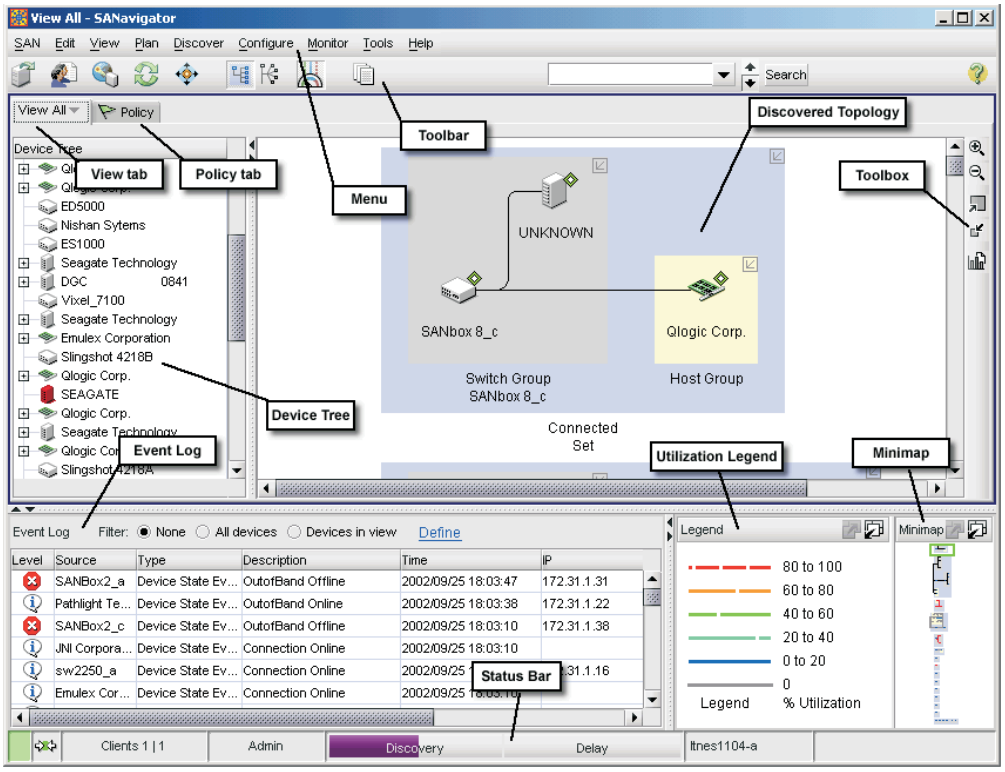


Figure 96. SANavigator Main Window

The desktop consists of five sections.

Physical Map

The Physical Map displays your SAN topology, devices, and their connections. For more information, see “Physical Map” on page 235.

Mini Map/Utilization panel

Use the Mini Map to view your entire SAN domain and to move within that view. For more information, see “Mini Map and Utilization Legend” on page 239.

The Utilization legend is displayed when the Utilization option is selected in the **View -> Connection** menu. It depicts the percent of the data bandwidth that is utilized when I/O’s are in progress. This is a Premium feature.

Event Log

The Event Log displays SAN events. For more information, see “Event Log” on page 240.

Device Tree/List

The Device Tree/List displays a list of all discovered devices and their properties. For more information, see “Device List” on page 241.

Working with SAN files

From the **SAN** menu, you can do the following:

- Log in to a new SAN
- Log out of an existing SAN
- Shutdown SANavigator
- Work with user information

- Export a SAN
- Import a SAN
- Plan a new SAN
- Open an existing SAN

These tasks are described in the following sections.

Log in to a new SAN

To log into a new SAN, do the following:

1. Click **SAN -> Log in** The Log in SAN dialog box appears.
2. The SANavigator application automatically discovers and opens the local SAN when you log in.
3. The server's address displays in the Network Address field. You can specify a new address by typing it in the field, or selecting one from the list.

   Note: In version 3.1, localhost is the default value. The SANavigator application automatically determines your local IP address and uses that value as your local host address. If you had previously connected to another IP address, you can select localhost from the Network Address drop down field.
4. Enter your user ID and password.
5. Select whether you want the SANavigator application to remember your password for the next time you log in.
6. Click **OK**. SANavigator will perform out-of- band discovery on your local subnet and display any SAN devices it finds.

Log out from a current SAN

To log into a different server, you must first log out of the current server.

Select **Log out** from the SAN menu. You will be logged out of the current server. Selecting **Shutdown** shuts down the SANavigator server and client.

Change user information

Click **SAN -> SANavigator -> Users** to open the SANavigator Server Users dialog box, where you can add, delete, or change user information. In the Add User dialog, you can set access to any of the following levels of permission:

None User has no server access. Use this level to restrict access without deleting a user's account, or when a user only needs to receive email.

Browse
User can view almost all information, but cannot make changes to or configure SAN devices.

Admin

User has access to all SANavigator functions.

You can also determine whether a user receives email notifications of events by doing the following:

1. Select the **Enable check box** (located under the Email column).
2. Click **Filter** to set the parameters for email notification.
3. Click **Setup** to open the Event Notification Setup dialog box.

You enable all user management on a single dialog box. See SANavigator Server Users in the help file for specific instructions about adding, defining, and removing users.

Notes:

1. Two users cannot have the same ID.
2. Each user's email address and preferences for event notification are stored with the user's account.
3. All user actions are logged into either the SAN log file or the server log file.
4. You cannot delete all users. There must always be at least one user.

Remote access

A SANavigator server can be accessed by multiple clients. The Remote Access menu function allows you to control whether or not you want multi-client connections, or select which client is permitted to connect to your server.

From the SAN menu, select **SANavigator Server -> Remote Access**. The Remote Access dialog is displayed.

Remote Access Dialog

Allow remote management sessions. Select this option to allow remote management sessions.

Maximum number of remote sessions. Select the number of remote sessions you want to allow.

Allow Any network address to connect. Select to allow any network address to connect.

Only network addresses below to connect. Select to allow only the network addresses specified below to connect.

All network addresses EXCEPT those below to connect. Select to allow all network addresses except those you specify.

Add button. Click to add network addresses.

Remove button. Click to remove network addresses.

Server Properties

Click **SAN -> Properties** to open the Server Properties dialog box. You can use the Name field to change the name of your server. The dialog box displays information about the server that the client is currently logged onto.

Name

Name assigned by the user to the portion of the SANavigator program acting as a server. This property can be set by users with administrative privileges. This name need not correspond to any other names, including the host name.

IP Address

Determined by the machine that the SANavigator server program is running on.

Subnet Mask

Determined by the machine that the SANavigator server program is running on.

Java VM Version
Version of the Java Runtime Environment that is currently running the SANavigator server that you are talking to.

Java VM Vendor
Vendor of the Java Runtime Environment that is currently running the SANavigator server that you are talking to.

Java VM Name
Name of the Java Runtime Environment that is currently running the SANavigator server that you are talking to.

OS Architecture
The SANavigator determines the hardware architecture if available.

OS Name and Version
The SANavigator determines the operating system and its version if available.

Region
The SANavigator server program determines the geographical region of your operating system.

Time Zone
The SANavigator server program determines the world time zone of your server.

Free Memory
Unused memory within the total memory.

Total Memory
Total memory assigned to your Java Runtime Environment.

Exporting a SAN

This feature enables you to capture the current state of a SAN and, at a later time, ″replay″ the SAN in your SANavigator machine or in a remote system that has SANavigator installed. This is useful in providing a view of the SAN to allow for remote diagnosis of problems. The following items are exported when you click **SAN -> Export**:

- SAN files: These are XML files that define your SAN.
- Physical Map: The Physical Map is exported to a JPEG file.
- Device List: The Device List is exported to a tab-delimited text file.
- Performance Data (Premium feature): This file contains the performance information that was gathered during the SAN monitoring.

All of these files are automatically zipped when you select the **Save to Disk** check box in the Export dialog box. A folder is generated that contains three files. See the following example:

```
san011107105249
san011107105249.zip
san011107105249.jpeg
san011107105249.txt
```

All three files can also be emailed by selecting the Mail To dialog box. (You need to have configured your system for email).

Importing a SAN

Click **SAN -> Import** to import a previously exported SAN into any SANavigator system. This enables you to see the exported SAN, including any problems that were present at the time of the capture.

In the Import dialog box, either type the SAN file name (for example, san011107105249.zip) or click **Browse** to search for the file.

The SAN is displayed with a time stamp, giving the date and time of capture in the background. At this point, discovery is disabled until you enable it. If this is the system from which the SAN was exported, the discovery detects any changes from the exported SAN to the current view of the SAN.

Caution: Turning on discovery will replace the currently discovered SAN with the imported data. Only one SAN can be viewed or saved at a time.

Planning a new SAN (premium feature)

You can plan a New SAN or use the current topology as the basis for a planned SAN. You can add, remove, arrange and connect planned devices to help you envision the SAN before implementing it.

1. From the SAN menu, select New Plan (or CTRL+N). The New Plan dialog box displays.
2. In the New Plan field, enter a name for the new plan.
3. Select whether you want to start with a discovered topology or start with an empty plan.
4. Click **OK**. The plan displays.

Opening an existing plan

Perform the following steps to open an existing plan

1. From the SAN menu, select **Open Plan**. The Open Plan dialog box is displayed.
2. Select a plan from the Open Plan list.
3. Click **OK**. The plan will be displayed.

Configuring your SAN environment

Two aspects of your SAN configuration can affect the functionality and performance of SANavigator: LAN configuration and SNMP configuration.

LAN configuration and integration

SANavigator relies on LAN connectivity with the SAN devices to gather information about the devices and connectivity of the SAN. LAN connectivity implies the following:

- All switches, hubs, and bridges have been configured with valid and specific IP addresses.
- The devices are properly cabled and integrated into a functional LAN topology.
- The computer where SANavigator runs has access to the LAN and to the IP addresses of the SAN devices.

SNMP configuration

SNMP is a communications protocol used to remotely monitor, configure, and control network systems. SANavigator acts as a network manager and generates requests and processes responses from SAN devices. SANavigator also listens for event reports or traps from SAN devices.

Subnet discovery

There are two methods of subnet discovery that you can use in your SAN environment:

- Broadcast
- Sweep

The Broadcast method of discovery is the most efficient discovery method, and it is the default method. However, a network administrator can disable this method on the network router. If broadcasting has been disabled on a network, and SANavigator has been configured to block the broadcast method, no devices will be discovered.

The Sweep method of discovery enables SANavigator to broadcast a request to all the devices on a network simultaneously; this improves SNMP communication efficiency. When broadcasting is disabled, sending the request to each device on the network (sweeping) is the only method available to discover SAN devices across an entire subnet. However, sweeping an entire network can take half an hour or more. If broadcast has been disabled, the best method of discovery is to type the individual IP addresses of the SAN devices into the selected individual addresses area of the Configure Discovery dialog box. This method produces good results without unnecessarily waiting for responses from every IP address in the subnet, especially for IP addresses where no devices are present. However, there might be times when a full subnet sweep produces valuable diagnostic information about the configuration of a network or a device.

Trap configuration

In addition to the request–response cycle of communication, SAN devices can generate event reports or SNMP traps. Most network devices can be configured to send their traps to port 162 on one or two IP addresses. By default, SANavigator listens for SNMP traps on port 162 and lists the traps in the Event Log. To make traps visible in the SANavigator Event Log, configure the SAN devices to send their trap event notices to the IP address of the computer running SANavigator. If you want multiple network management applications to receive trap events, refer to the SANavigator help topic Compatibility with Other Applications.

Click **Monitor -> Trap Forwarding** to open the Trap Forwarding dialog box, where you can specify the IP addresses and ports of other computers to which you wish to forward SNMP traps received by SANavigator. If you select the **Enable Trap Forwarding** check box, all traps received by SANavigator are forwarded to the recipients listed in the Selected Recipients table.

Discovering devices with SANavigator

SANavigator is able to discover devices using out-of-band or in-band discovery processes, or both. Out-of-band discovery is required when the SAN configuration contains switches and managed hubs (a Fabric environment). In-band discovery is required when no switch or managed hub is present (that is, when the host bus adapter is connected to a FAStT Storage Server either directly or through an unmanaged hub).

In the Discover dialog box, you can select which of these two processes to use. To enhance the discovery of your SAN, it is suggested that you use both processes.

There are two methods for In-band Discovery:

- Local Server (default) - Only HBAs on the local server are discovered through in-band. Any devices on the same subnet (connected through switches) are discovered out-of-band. HBAs from remote hosts cannot be in-band managed from the local machine but are discovered if connected to the Fabric.
- Local Server and Remote Discovery Connector - The local server communicates with the Remote Discovery Connector (SANavRemote.exe) installed in the remote host. A user can now have IB management of the Remote Host from the local machine.

  See “In-band discovery”for additional information.

Out-of-band discovery

SANavigator uses an out-of-band process to discover SAN devices. During discovery, the SANavigator logo on the right side of the menu bar is active. If discovery is turned off, a red circle with a diagonal bar through it appears over the logo.

Familiarize yourself with the information in the help topic Configuring Your SAN before you proceed.

To discover devices on your SAN, use the Out-of-Band tab in the Discover Setup dialog box to select the TCP/IP subnets or individual IP addresses. When you connect to a server and set up discovery, SANavigator performs a discovery of devices on your SAN. At any time during a SANavigator session, you can turn the discovery feature off or back on by clicking **Discover -> Off** or **Discover -> On**, or by clicking the Discovery button.

SANavigator servers can run discovery on only one SAN at a time. If you turn discovery off and another client turns it on, discovery continues to run on the other client. If you turn discovery on, SANavigator issues a message to the other client that you are taking over the discovery process. You need to negotiate with other users about who should use discovery and when.

In-band discovery

In-band discovery requires that the IBM FAStT HBA SNIA API library be installed on your system. This library is part of the IBM FAStT HBA driver installation package. When in-band discovery is enabled from the Discover Setup dialog box (see Figure 97 on page 234), the supported host bus adapters will be displayed in the Available HBAs panel. Select the HBA or HBAs that you want to discover using the in-band process.

Note: In-band discovery is only enabled on the system on which the HBA SNIA API library is installed and where the host bus adapter or adapters reside. Both the local host and a remote host (with the Remote Discovery Connector installed) can be in-band managed. A SANavigator server must be running in order to perform Remote Discovery (for example, the localhost server can be used to connect to the remote host). See “Setting up SANavigator Remote Discovery Connection for in-band management of remote hosts” on page 300 for In-band management of remote hosts.

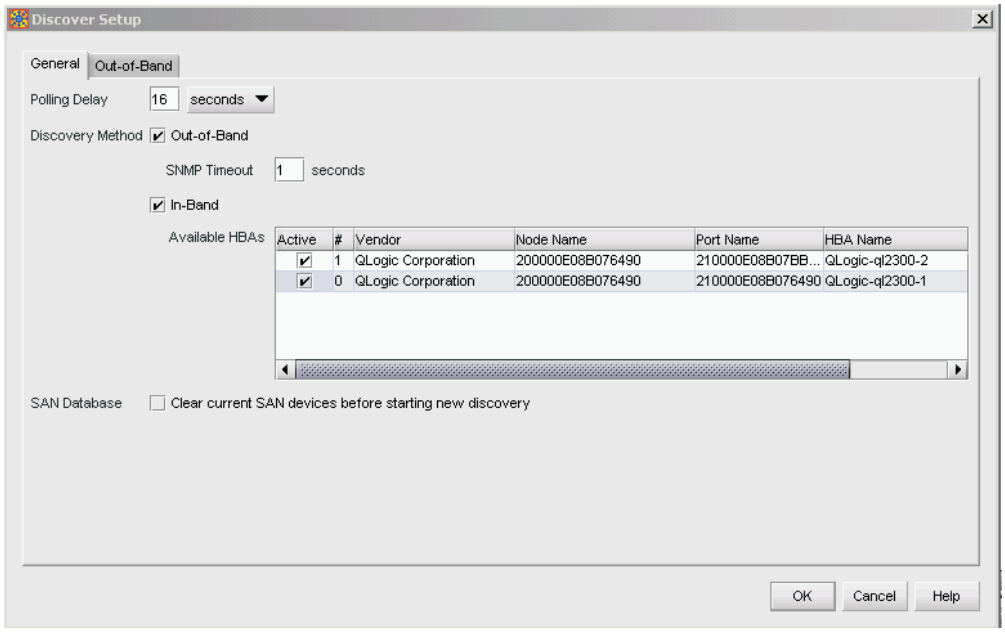


Figure 97. Discover Setup Dialog Window

Discovery indicators

You can determine the discovery method by inspecting the diamonds that are adjacent to the device icons in the physical map. Figure 98 shows the diamond legend.

Tag	Out-of-band	In-Band	Tag	Out-of-band	In-Band
	Present	Not Present		Present	Present
	Failed	Not Present		Present	Failed
	Not Present	Present		Failed	Present
	Not Present	Failed		Failed	Failed

Figure 98. Diamond Legend

SAN database

The SAN database is updated continuously by the discovery engine. Thus, when you change your discovery method, the devices and links that were previously discovered are maintained.

For example, if you had in-band and out-of-band discovery enabled, and you subsequently disabled in-band discovery, all devices and connections that were in-band discovered would be shown in red. You can avoid this by selecting the **Clear Current SAN Devices** check box before starting a new discovery. However, be aware that this will cause any previous configurations to be reset. If you want to keep a copy of the original SAN, export your SAN (see “Exporting a SAN” on page 230).

Community strings

You can either specify custom community strings to communicate with SAN devices or let SANavigator use standard defaults. SNMP protocol enables you to set community strings for both read and write requests. For most SAN devices, the default string for read requests is public, and the default for write requests is private. SANavigator treats custom community strings as secure information, protecting it during entry and encrypting it for storage in the program.

If you have changed the SNMP community strings on your SAN devices, you need to use the Community Strings tab in the Domain Information dialog box to enter your custom strings. SANavigator supports one custom read and one custom write community string per individual IP address or subnet.

Polling timing and SNMP time-out intervals

The polling rate is the delay between successive discovery processes or how long discovery waits for responses from the devices on your SAN. To change the polling rate, click the General tab in the Discover Setup dialog. The polling delay determines the responsiveness of the map in terms of displaying changes in your SAN. Short times (3-10 seconds) give an almost real-time indication of the SAN status. Extended periods reduce network load, but show changes only after each polling period.

If you have a large number of devices, you might want to extend the polling delay so the discovery and mapping processes are completed before another discovery is initiated. Heavy data loads might reduce the responsiveness of SAN devices. You can edit the SNMP time-out interval to provide more time for the devices to respond. (The time setting is for one retry only; SANavigator retries three times for each device.) If SANavigator receives an SNMP trap message, a discovery is initiated immediately.

Note: Short polling delays (less than 10 seconds) might tax the CPU resources, especially on slower processors and in larger SANs.

Monitoring the SAN environment

This section discusses the tools available in SANavigator for monitoring SAN devices:

- Physical Map
- Mini Map
- Event Log
- Device List
- Event Notification

Physical Map

The Physical Map, shown in Figure 99 on page 236, displays devices, their connections, and connection failures. SANavigator discovers devices, displays them on the Physical Map, and monitors communications with the devices. If communication is lost with any device, the device and its connections turn red. For instance, if a device is disconnected from the SAN, its icon turns red and its connections appear red until communications are reestablished with the device or the device is deleted from the map. If a fabric or group is collapsed to an icon and a device in the fabric or group is disconnected from the SAN, the icon appears red. If you click **Delete All** in the **Edit** menu of the desktop, all red devices are deleted.

Note: See “Physical Map” on page 286 for more detailed information about using the Physical Map.

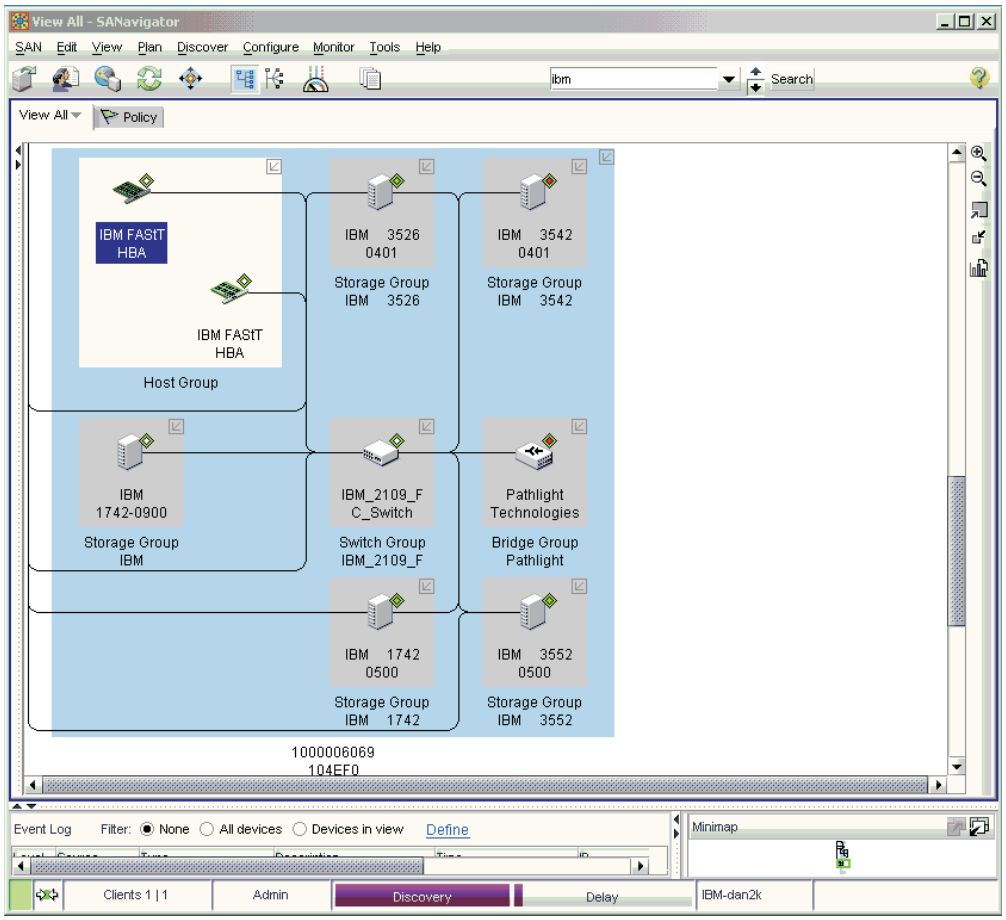


Figure 99. Physical Map

From the Physical map, you can do the following:

- Determine the source and destination of a connection through the Device Tip. The Device Tip, shown in Figure 100 on page 237, pops up when you place the cursor over the selected connection.

  Note: You can disable the Device Tip feature by clicking **View -> Device Tips** and unselecting the Device Tips check box.

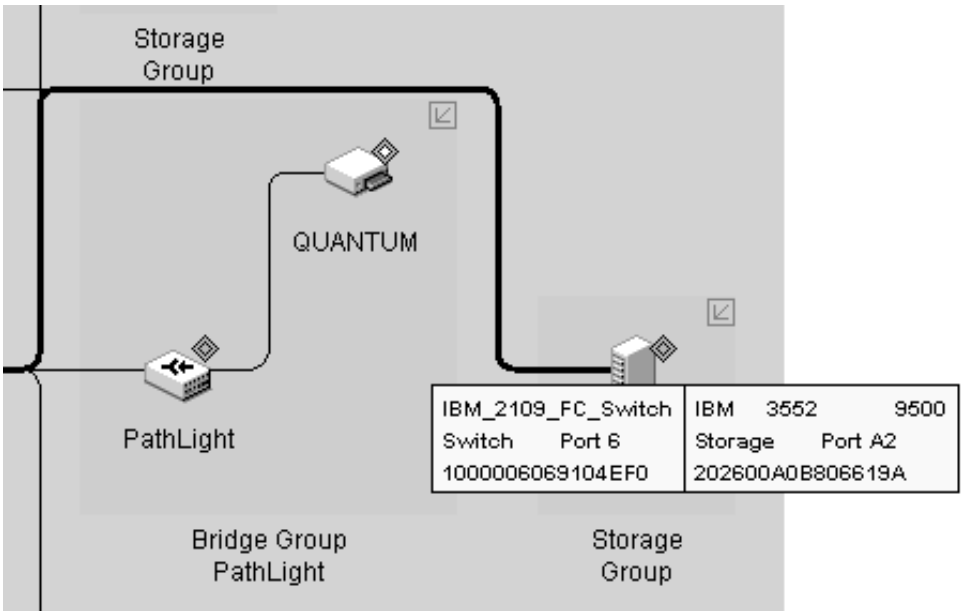


Figure 100. Device Tip

- Expand multi-port devices to show the port assignments. Right-click the device and select **Ports** from the pop-up menu to view the ports. See Figure 101.

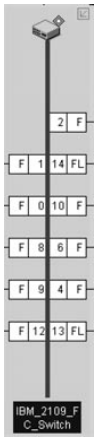


Figure 101. Port Assignments

- Launch device-specific applications and utilities such as the IBM Storage Manager and IBM FAStT MSJ diagnostics. You can also go directly to the IBM Support Web site to access the latest information about IBM FAStT SAN devices, including firmware updates, drivers, and publications. You can also add other applications or tools through the Tools dialog box. Right-click the device and the pop-up menu shown in Figure 102 on page 238 is displayed.

Figure 102. Device Right-click Menu

Click **Setup Tools** to add or modify tools and applications.

Physical Map view buttons

On the right-hand toolbar of the Physical Map, there are five buttons that allow you to view the Physical Map in different formats.

Zoom Buttons

The two buttons with the magnifying glass icon allow you to change the scale of the topology. You can zoom in by clicking on the + magnifying glass button and zoom out by clicking on the - button. You can also scale you topology view on a percentage basis. Select **View->Zoom** in the Menu bar and a pop up menu will be displayed (see Figure 103). Select the desired scaling factor. You can also invoke this menu by right-clicking anywhere outside of the Topology frame and selecting **Zoom** from the pop-up menu.

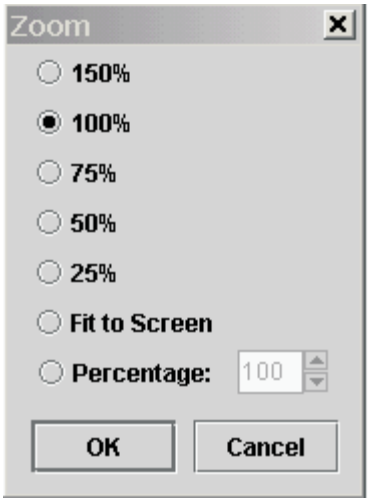


Figure 103. Zoom Dialog Window

Expand/Collapse buttons

You can expand and collapse the topology view by clicking on these buttons. For each click of the Expand button the topology will expand from Fabric Only to Groups Only to All Devices and finally to All Ports. The

Collapse button reverses this sequence. You can also select the **View->Show** in the Menu bar to expand/collapse the map.

Report Button

This last button allows you to generate a report of the Physical Map. See "Generating, viewing, and printing reports" on page 243 for more information.

Mini Map and Utilization Legend

Use the Mini Map to view your entire SAN at a glance and to navigate the more detailed map views. This option can be especially helpful if you have many devices connected to your SAN.

The Mini Map appears in the lower right-hand corner of the SANavigator main window.

To facilitate the navigation of your SAN, the Mini Map displays switches as squares and storage devices as circles. Triangles are reserved for other devices, such as host bus adapters or routers. See Figure 104.

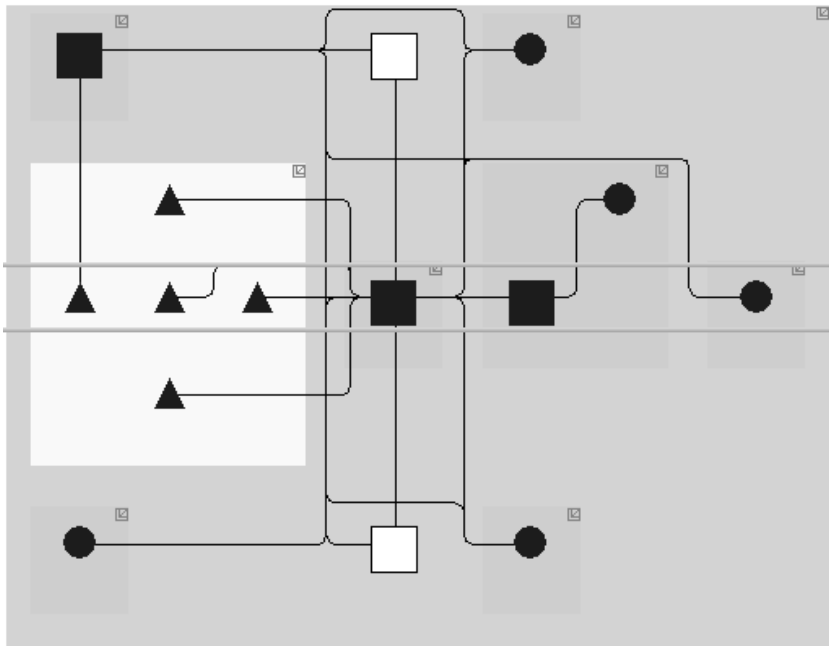


Figure 104. Mini Map

To move within the view of a map, do one of the following:

- Click inside the green-outlined box, which represents the boundaries of the map window, and drag the box to the area you wish to view.
- Click the area in the Mini Map that you wish to view and the green-outlined box will automatically move to that area.

To change the size of the Mini Map, do one of the following:

- Drag the adjoining dividers.
- Click the small triangles on the adjoining dividers.

You can also anchor or float the Mini map to customize your desktop. To float the Mini map and view it in a separate window, click the **Detach** button in the upper right-hand corner of the Minimap. This will detach the Mini Map and place it on the desktop. At this time you can scale the Mini map to the desired size to facilitate navigation of your SAN To return the Mini map to its original location on the SANavigator desktop, click the **Attach** button in the upper right-hand corner of the Mini map or click the **Close** button in the upper right-hand corner of the Mini map. When in the Performance mode (Premium feature), the Utilization legend (shown in Figure 105) is displayed to the left of the Mini Map. The legend displays the percentage ranges indicated by the color of each dashed line in the Physical Map. When I/Os are active, the path of the data flow is displayed in accordance with the bandwidth utilization legend for that path.

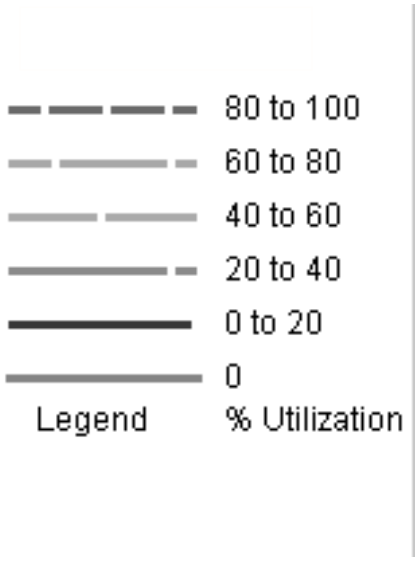


Figure 105. Utilization Legend

In the same manner as the Mini map, the Utilization Legend box can be detached onto the desktop.

Event Log

All configuration actions made by users are listed as events in the Event Log. The Event Log appears in the lower left of the SANavigator main window.

The Event Log lists SNMP trap events and SANavigator server and device events (online, offline, user action, client/server, or performance). The log lists three levels of events:

- Fatal

- Warning

- Information

You can sort the Event Log on any column by clicking on the column header.

You can filter the Event Log to include or exclude specific types and levels of events. Click the **Define** link to define the events you want to display. You can also define which device event log you want displayed depending on the View you selected (see “Physical Map view buttons” on page 238). You can select Devices in view (those on the current Physical Map) or All devices (those in the current Physical Map as well as those in all other Fabric for this SAN).

You can locate in the Physical Map the device logged in the Event Log. Click the device in the log and it will be highlighted automatically on the Physical Map.

If you are experiencing problems with the server, examine the server log for diagnostic information (the default location for the server event log is: `..\SANavigator3.1\Server\Local_Root\SANavigatorEventStorageProvider\event.log`). To examine the event log for the SAN, look at the discovered SAN event log (the default location for the discovered SAN event log is: `\SANavigator3.1\Server\Universe_Home\TestUniverse\_Working\SANavigatorEventStorageProvider\event.log`).

Note: The date and time need to be reasonably accurate on PCs where SANavigator is deployed. If the client and server time differ significantly, there might be problems displaying real-time performance data. Consult your computer’s user manual to see how to set the time and date.

Clearing the Event Log

You can clear the event log by editing the file event.log. This file is located in `\SANavigator3.1\Server\Universe_Home\TestUniverse\_Working\SANavigatorEventStorageProvid`

Caution: You will lose all Event Log information if you delete the content of this file. Make a backup copy of the log file for future reference.

Note: The Event Log shown on the desktop only displays events from the previous 48 hours. The file event.log includes information before this period.

Device Tree

The Device Tree, located on the **View** tab of the desktop, displays the names and properties of all discovered devices and ports. The Device Tree is a quick way to look up device and port information, including serial numbers and IP addresses. To display the Device Tree, select the **View** tab on the SANavigator desktop.

You can sort the Device Tree by clicking a column heading.

The Device Tree can be expanded into a Device List by clicking the expand/contract arrows on the separator bar (or by the use the F9 function key)

Device List

The Device List displays a list of all discovered devices and their properties. To display the Device List, select the **Device List** tab in the upper portion of the main

SANavigator display. A table appears with rows listing all devices and columns listing the following information for each device:

- Label
- System Name
- Device Type
- WW Name
- IP Address
- FC Address
- Vendor
- Model
- Serial Number
- Fabric Name
- Port Count
- Firmware
- Status
- Comments
- Text 1
- Text 2
- Text 3
- Text 4

In these last four columns, you can create additional properties, such as physical location, storage capacity, capital cost, and scheduled maintenance.

Note: You can customize the Device List to remove, move and add columns, Perform the following steps:

1. From the View menu, select **Create View**. Enter a name and description for the view.
2. From the Selected Columns list, select the Device List columns you want to move or that you do not want to view.

Editing properties

Editable properties can be edited directly within the device list by double-clicking the field. (A green triangle indicates that a field is editable.) The table is automatically updated with each discovery cycle.

Sorting properties

You can sort the list by clicking on the title bar of the desired column. Each click will cycle through the following sort options: Ascending, Descending, Discovery sequence. You can sort on multiple columns by selecting the desired columns with the Control key pressed.

Locating devices in the Physical Map

With both the Device Tree and the Physical Map being displayed, click a device name in the Device Tree and the device will be highlighted in the Physical Map.

Event Notification

SANavigator receives, monitors, and generates several types of events that it posts to the event log. To receive email when events occur, do the following:

1. Set up event notification to define the mail server, enter the reply to address, and set the frequency that email is sent to users.

2. Create a SANavigator server user for each of the email recipients and ensure their email addresses are correct.
3. Configure an event filter for each recipient so that they are notified only about the events of interest to them.

For more information, refer to the SANavigator Help.

Generating, viewing, and printing reports

SANavigator provides you with the capability to generate, view and print reports. Generated reports are saved in \SANavigator3.1\Server\Reports\ folder. Exported reports are saved in the \SANavigator3.1\Client\Data\ folder.

Generating reports

To generate a report select **Monitor->Reports->Generate** in the Menu bar. The Select Template dialog box is displayed. Select the information you want to include in the report. Click **OK**. SANavigator will begin generating the report. The time to generate a report is dependent on the size of the SAN.

Viewing a report

The Report Viewer is similar to the Java Help Viewer. The left frame displays a tree structure that you can use to navigate through reports. In the Menu bar, select **Monitor->Reports->View**. The SANavigator Reports dialog box is displayed.

Select one of the following options to view a report:

- Report Type

  Reports are grouped according to their report type (for example, ″Performance Data″, ″Plan Evaluation″).
- User

  Reports are grouped according to the user who generated the report.
- Time

  Reports are grouped according to the time and date that the report was generated.

Exporting reports

To export reports, first select **Export** from the SAN menu. The Export dialog box will display a list of file types that can be exported along with their sizes.

Note: Report files will be zipped for convenient e-mail and disk transfer. The zip file name will be preceded with ″rep″, followed by the export's time stamp (for example, rep010904115344.zip). Report files will be in standard HTML format.

Next, perform the following steps to export reports:

1. From the Export To list, select one of the following options:
   - Disk

     Saves the exported files to the disk on: ...\ SANavigator3.1\Client\Data\
   - E-mail

     Mails the exported files as an e-mail attachment directly from the application
   - Database

     Not available when exporting reports

2. Select the **Reports** option, then click **Select Reports**. The Selects Reports dialog box is displayed.
   a. Select the desired reports. To select multiple files, make sure the folders are fully expanded and press CTRL while selecting the reports.
   b. Click **OK**.
3. On the Export dialog box, click **OK**. To export to more than one destination, click **Apply** after configuring each option to save the changes.
4. Click **OK** when you are finished.

Deleting a report

To delete a generated report, do the following:

1. Browse to the ...\SANavigator2.x\Client\Reports\ folder.
2. Select the files or folders you want to delete.

   Note: Images associated with a report will be stored in a folder that has the same name as the report.
3. Delete the files.

Printing a report

In the SANavigator Reports dialog box, click the **Show in Browser** button. In the Internet browser window, select **Print** from the File menu.

Note: Set up the printer to print in landscape format to ensure that all information fits on the page.

Device properties

Use the Device Properties dialog box (see Figure 106 on page 245) to view and edit the properties of a device. You can change the device type when the device is not directly discovered. Devices that are not directly discovered are usually reported to SANavigator by other SAN devices (such as a switch). However, some discovered properties are editable. The vendor can be discovered, but it is always still editable.

CAUTION:
Changing the Vendor field of a device will disable the auto-launch of applications for that device.

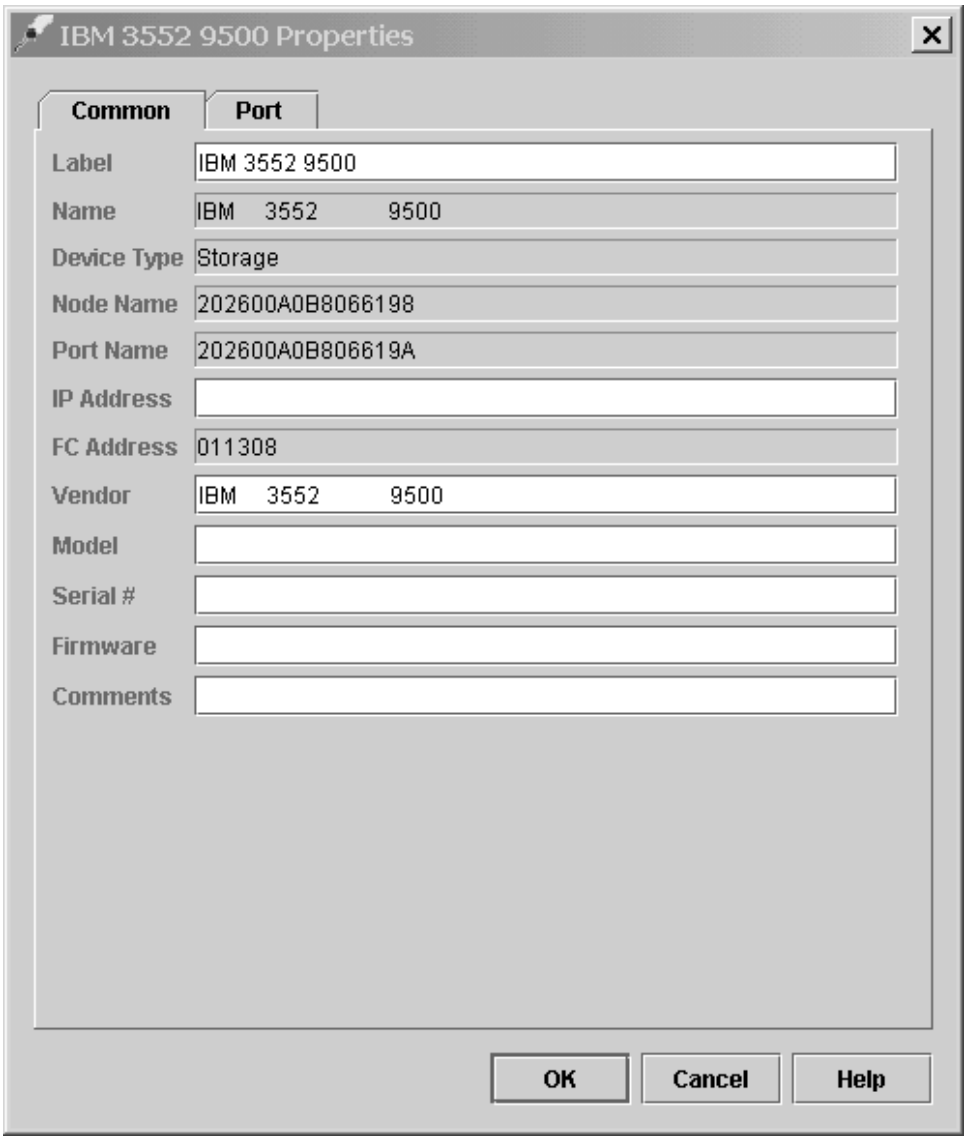


Figure 106. Device Properties Window

Note: The vendor name in the Properties dialog box must match the vendor name in the Device Application command in order to launch applications.

To display device properties, right-click the device's icon in the Physical Map panel and click **Properties** in the pop-up menu or select the device and click **Edit -> Properties**. A dialog box appears with up to three tabs at the top: **Common**, **Adapter**, and **Port**.

Note: The Adapter and Port tabs are available only if In-Band discovery is performed; their properties cannot be edited.

Discovery troubleshooting guide

If the SANavigator tool is having difficulty discovering your SAN, or if you received an error message, there might be one of several problems. This section lists the most common problems and offers solutions for how to correct them. The list begins with the simplest problems and moves on to more complex ones.

- **Problem:** *Discovery is turned off.*

  Solution: Click **Discover -> On** from the desktop window.
- **Problem:** *Discovery not enabled.*

  Solution: Do the following:

  1. Click **Discover -> Setup** from the desktop menu bar.
  2. Click the **General** tab on the Discover Setup dialog box.
  3. Select the **Out-of-Band Discovery** check box or the **In-Band Discovery** check box, or both.
  4. Click **OK**.
- **Problem:** *HBAs are not active for In-Band Discovery.*

  Solution: Do the following:

  1. Click **Discover -> Setup** from the desktop window.
  2. Click the **General** tab on the Discover Setup dialog box.
  3. Select the **In-Band Discovery** check box.
  4. Click the **Active** column for each HBA you would like to discover.
  5. Click **OK**.

     Note: If you cannot set in-band discovery on, check to see whether the HBA API library has been installed. Click **Start -> Settings -> Control Panel -> Add/Remove Programs** and look for the Qlogic SAN/Device Management entry in the program list.
- **Problem:** *Server not found or server not available.*

  Solution: Verify that the server IP address is present and correct in the Out-of-band panel of the Discovery Set Up dialog box. All SAN devices should be on the same subnet as the server. If the server has multiple Network Interface Cards (NICs), then include their IP address in the Out-of-band panel.

  Note: Firewalls might prevent server discovery.
- **Problem:** *Switches not connected to LAN.*

  Solution: Check your physical cables and connectors.
- **Problem:** *Unable to detect tape devices attached to a SAN Data Gateway Router.*

  Solution: Verify that the SAN Data Gateway Router is connected to the network and that its IP address is set to the same subnet as your server.
- **Problem:** *No subnets or addresses selected.*

  Solution: Do the following:

  1. Click **Discover -> Setup** from the desktop window.
  2. Click the **Out-of-Band** tab on the Discover Setup dialog box.
  3. Click the subnet or individual address you would like to discover in the Available Addresses pane.
  4. Click the right arrow (>) to move your choice to the Selected Subnets pane, or to the Selected Individual Addresses pane.
  5. Click **OK**.
- **Problem:** *The wrong IP addresses are selected.*

  Solution: Do the following:

  1. Click **Discover -> Setup** from the desktop window.
  2. Click the **Out-of-Band** tab on the Discover Setup dialog box.

3. Verify that the IP addresses in the Selected Subnets and Selected Individual Addresses panes are the correct current addresses for your SAN.
4. Click **OK**.

- **Problem:** *The wrong community strings are selected.*

  Solution: Do the following:

  1. Click **Discover -> Setup** from the desktop window.
  2. Click the **Out-of-Band** tab on the Discover Setup dialog box.
  3. Select an IP address.
  4. Click **Change**.
  5. Make your community strings selection.
  6. Click **OK**.

- **Problem:** *Broadcast request is blocked by routers.*

  Solution: Depending upon the information available about the required IP addresses, choose one of the following three solutions to this problem:

  – If you know the IP addresses and the addresses are not listed in the Available Addresses pane:
    1. Click **Discover -> Setup** from the desktop window.
    2. Click the **Out-of-Band** tab on the Discover Setup dialog box.
    3. Click **Add**.
    4. Type the required data in the dialog box.
    5. Click **OK**. Repeat as needed until all your addresses are available.
    6. Select the IP Addresses you want to discover in the Available Addresses pane.
    7. Click the right arrow (>) to move your choices to the Selected Individual Addresses pane.
    8. Click **OK**.

  – If you know the IP addresses and the addresses are listed in the Available Addresses pane:
    1. Click **Discover -> Setup** from the desktop window.
    2. Click the **Out-of-Band** tab on the Discover Setup dialog box.
    3. Select the IP Addresses you would like to discover in the Available Addresses pane.
    4. Click the right arrow (>) to move your choices to the Selected Individual Addresses pane.
    5. Click **OK**.

  – If you do not know the specific IP addresses:
    1. Click **Discover -> Setup** from the menu of the desktop window.
    2. Click the **Out-of-Band** tab on the Discover Setup dialog box.
    3. Click the **Method** column for the selected subnet in the Selected Subnets pane and choose **Sweep**.
    4. Click **OK**.

       The sweep method significantly increases your discovery time.

- **Problem:** *Discovery time is excessive.*

  Solution 1: Do the following:

  1. Click **Discover -> Setup** from the desktop window.
  2. Click the **Out-of-Band** tab on the Discover Setup dialog box.

3. Click the **Method** column in the Selected Subnets pane and choose **Broadcast**.
4. Click **OK**.

Solution 2: In most cases, decreasing the SNMP time-out will decrease the discovery time.

- **Problem:** *The server doesn't seem to be starting.*

  Action: Examine the server log (\SANavigator2.x\Server\Data\SANs\server.log) for diagnostic information.

Chapter 20. PD hints — Common path/single path configurations

You should be referred to this chapter from a PD map or indication. If this is not the case, see Chapter 16, “Problem determination starting points”, on page 131.

After you have read the relevant information in this chapter, return to “Common Path PD map 1” on page 152.

In Figure 107, the HBA, HBA-to-concentrator cable, and the port used by this cable are on the common path to all storage. The other cables and ports to the controllers are on their own paths so that a failure on them does not affect the others. This configuration is referred to as single path.

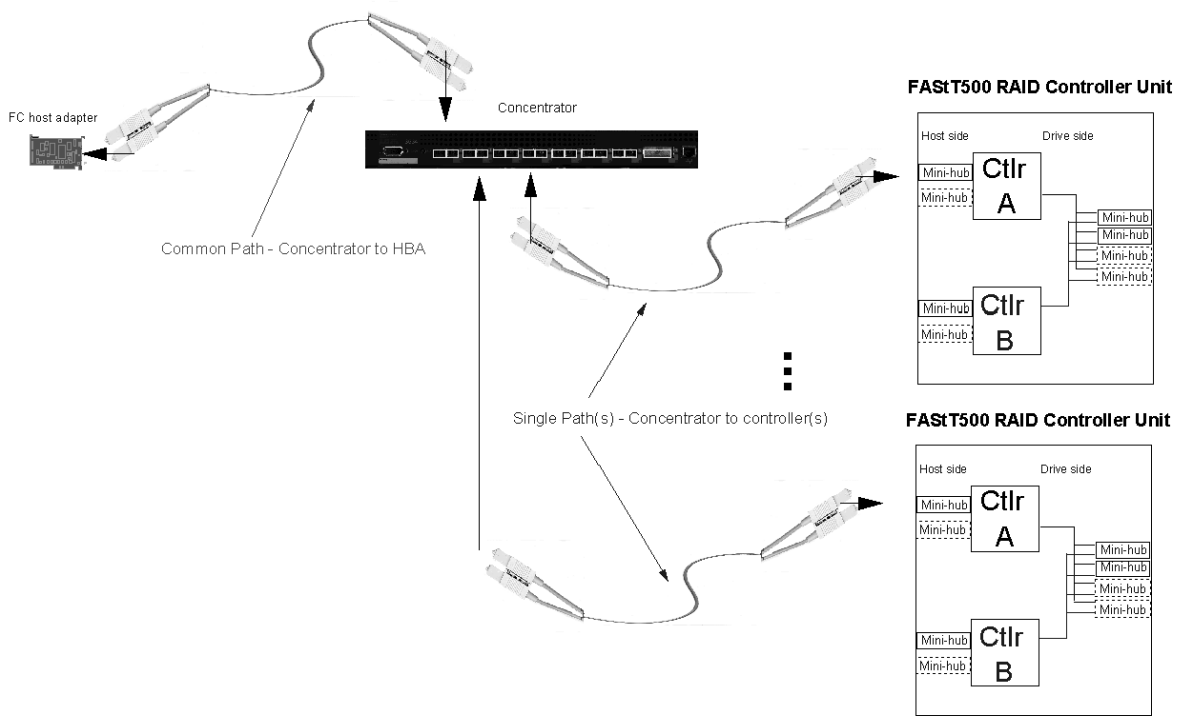


Figure 107. Common Path Configuration

Chapter 21. PD hints — RAID controller errors in the Windows NT event log

You should be referred to this chapter from a PD map or indication. If this is not the case, see Chapter 16, “Problem determination starting points”, on page 131.

After you have read the relevant information in this chapter, return to “RAID Controller Passive PD map” on page 139.

This chapter presents general guidelines that explain the errors can appear in an event log and what actions to perform when these errors occur.

Note: If you have a system running on Windows NT 4.0, the driver is listed as SYMarray. If you have a system running on Windows 2000, the driver is listed as RDACFLTR.

Common error conditions

- **Getting a series of SYMarray event ID 11s in the Windows NT event log**

  Open and review the event log. A series of event ID 11s generally indicates a number of bus resets and might be caused by a bad host bus adapter or a bad cable.
- **Getting a series of SYMarray event ID 11s and 18s in the Windows NT event log**

  Open and review the event log. A series of event ID 11s generally indicates LIPs (Loop resets). This generally indicates a bad fibre path. It could be an indication of a problem with a GBIC, an MIA, or an adapter.

  Event ID 18s indicate that RDAC failed a controller path. The fault will most likely be a component in the fibre path, rather than the controller.
- **Getting a series of SYMarray event ID 15s in the Windows NT event log**

  This error is undocumented. A series of event ID 15s indicates that the link is down. The problem is generally within the Fibre path.

Event log details

In addition to reviewing the SYMplicity Storage Manager log, you can choose to review the Windows NT event log, which is viewed in a GUI environment (see Figure 108). To open the event log, click **Start -> Programs -> Administrative Tools -> Event Viewer**.

Date	Time	Source	Category	Event	User
2/22/99	4:35:25 AM	symarray	None	11	N/A
2/21/99	11:34:35 PM	symarray	None	11	N/A
2/18/99	12:47:45 AM	SNMP	None	1001	N/A

Figure 108. Event Log

Table 58 on page 252 lists the most common, but not necessarily the only, event IDs encountered in a SYMarray (RDAC) event.

Table 58. Common SYMarray (RDAC) event IDs

Event	Microsoft Label Identifier	Description
9	IO_ERR_TIMEOUT	The device %s did not respond within timeout period.
11	IO_ERR_CONTROLLER_ERROR	Driver detected controller failure.
16	ERR_INVALID_REQUEST	The request is incorrectly formatted for%1.
18	IO_LAYERED_FAILURE	Driver beneath this layer failed.
389	STATUS_IO_DEVICE_ERROR	The I/O device reported an I/O error.

Event ID 18 is a special case. SYMarray uses event ID 18 to designate a failed controller path. (The controller on the physical path is the failed controller.) All LEDs on the controller are usually lit when a failure occurs. This does not necessarily mean that the controller is defective, but rather that a component along the path to the controller is generating errors. Possible problem components include the host adapter, fibre cable, GBIC, hub, and so on.

In a multi-node cluster with multiple event ID 18s, the earliest log entry most likely initiated the original controller failure. The event ID 18s on other nodes were most likely responses to the original failure and typically contain an SRB status of (0x0a - SCSI Selection Timeout). Check the system date and time stamp for synchronization to validate which entry occurred first. To review an entry in the Event Viewer, perform the following steps:

1. Double-click the entry you wish to review.
2. Select the **Words** radio button to convert the bottom text from bytes to words. See Figure 109.

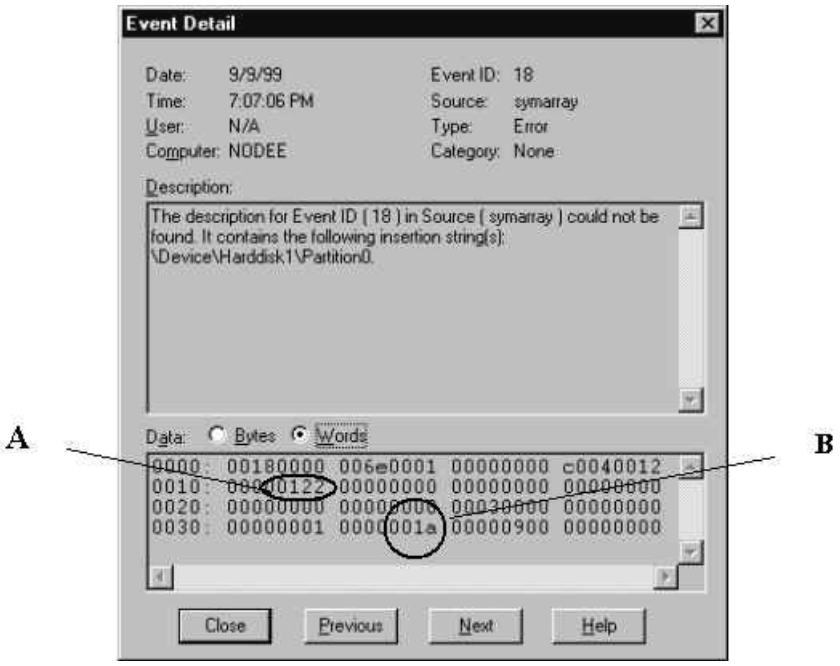


Figure 109. Event Detail

A. The last 4 digits (2 bytes) in this field indicate the unique error value. In this example, the error value shown indicates a Controller Failover Event.

B. For Event ID 18, this offset represents the SCSI operation that was attempted when the failover event took place.

Table 59. Unique Error Value - Offset 0x0010

Unique Error Value - Offset 0x0010			
Value	**Meaning**	**Value**	**Meaning**
100	Media Error (check condition)	110	Device Not Ready (check condition)
101	Hardware Error (check condition)	111	No Sense (check condition)
102	Recovered Error (check condition)	112	Unrecognized Sense Key
103	Default - Controller Error	113	Error being returned to system which would otherwise not be logged
105	Command Aborted or Timed Out	114	SCSI Release Configuration Error, Multiple paths to the same controller
106	Phase Sequence Error	115	SCSI Reserve Configuration Error, Multiple paths to the same controller
107	Request Flushed	116	The driver has discovered more paths to a controller than are supported (four are supported)
108	Parity Error or Unexpected Bus Free	117	The driver has discovered devices with the same WWN but different LUN numbers
109	SCSI Bus Error Status (busy, queue full, and so on)	122	Controller Failover Event (alternate controller/path failed)
10a	Bus Reset	123	A path to a multipath controller has failed
10e	Aborted Command (check condition)	124	A controller failover has failed
10f	Illegal Request (check condition)	125	A Read/Write error has been returned to the system

The example shown in Figure 110 is a recovered drive timeout error on drive 2, 1.

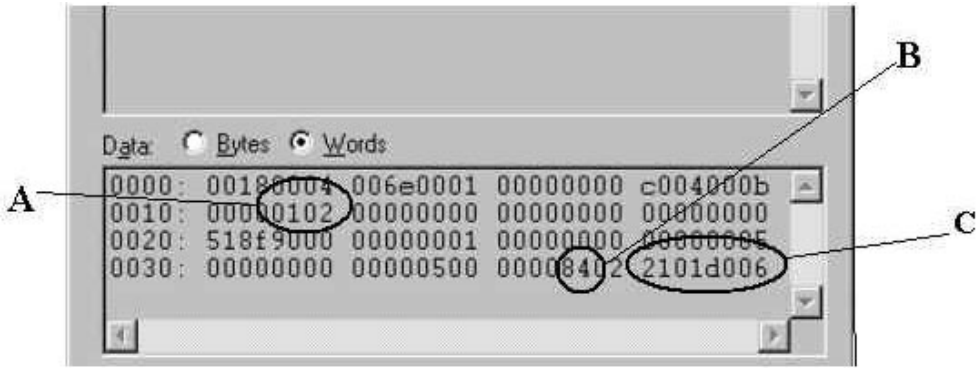


Figure 110. Unique Error Value Example

A. This error indicates (according to the error codes listed in Table 59) a recovered error.

B. This bit indicates validity of the following word. A number 8 means field C is a valid sense key. A number other than 8 means that field C is not valid and should be disregarded.

C. This word represents the FRU code, SCSI sense key, ASC and ASCQ.

ffkkaaqq –			
ff = FRU code	kk = SCSI sense key	aa = ASC	qq = ASCQ

Sense Key table

Table 60 lists Sense Key values and descriptions.

Table 60. Sense Key table

SENSE KEY	DESCRIPTION
0x00	No Sense
0x01	Recovered Error
0x02	Not Ready
0x03	Medium Error
0x04	Hardware Error
0x05	Illegal Request
0x06	Unit Attention
0x07	Data Protect (Not Used)
0x08	Blank Check (Not used)
0x09	Vendor Specific (Not used)
0x0A	Copy Aborted (Not used)
0x0B	Aborted Command
0x0C	Equal (Not used)
0x0D	Volume Overflow (Not used)
0x0E	Miscompare
0x0F	Reserved (Not used)

ASC/ASCQ table

This section lists the Additional Sense Codes (ASC) and Additional Sense Code Qualifier (ASCQ) values returned by the array controller in the sense data. SCSI-2 defined codes are used when possible. Array-specific error codes are used when necessary, and are assigned SCSI-2 vendor-unique codes 80 through FFH. More detailed sense key information can be obtained from the array controller command descriptions or the SCSI-2 standard.

Codes defined by SCSI-2 and the array vendor-specific codes are shown in Table 61. The sense keys most likely to be returned for each error are also listed in the table.

Table 61. ASC/ASCQ values

ASC	ASCQ	Sense Key	Description
00	00	0	No Additional Sense Information The controller has no sense data available for the requesting host and addressed logical unit combination.

Table 61. ASC/ASCQ values (continued)

ASC	ASCQ	Sense Key	Description
04	01	2	Logical Unit is in the Process of Becoming Ready The controller is executing its initialization functions on the addressed logical unit. This includes drive spinup and validation of the drive and logical unit configuration information.
04	02	2	Logical Unit Not Ready, Initializing Command Required The controller is configured to wait for a Start Stop Unit command before spinning up the drives, but the command has not yet been received.
04	04	2	Logical Unit Not Ready, Format In Progress The controller previously received a Format Unit command from an initiator, and is in the process of executing that command.
04	81	2	Storage Module Firmware Incompatible - Manual Code Synchronization Required
04	A1	2	Quiescence Is In Progress or Has Been Achieved
0C	00	4	Unrecovered Write Error Data could not be written to media due to an unrecoverable RAM, battery, or drive error.
0C	00	6	Caching Disabled Data caching has been disabled due to loss of mirroring capability or low battery capacity.
0C	01	1	Write Error Recovered with Auto Reallocation The controller recovered a write operation to a drive and no further action is required by the host. Auto reallocation might not have been used, but this is the only standard ASC/ASCQ that tells the initiator that no further actions are required by the driver.
0C	80	4, (6)	Unrecovered Write Error Due to Non-Volatile Cache Failure The subsystem Non-Volatile cache memory recovery mechanisms failed after a power cycle or reset. This is possibly due to some combination of battery failure, alternate controller failure, or a foreign controller. User data might have been lost.
0C	81	4, (6)	Deferred Unrecoverable Error Due to Memory Failure Recovery from a Data Cache error was unsuccessful. User data might have been lost.
11	00	3	Unrecovered Read Error An unrecovered read operation to a drive occurred and the controller has no redundancy to recover the error (RAID 0, degraded RAID 1, degraded mode RAID 3, or degraded RAID 5).
11	8A	6	Miscorrected Data Error - Due to Failed Drive Read A media error has occurred on a read operation during a reconfiguration operation. User data for the LBA indicated has been lost.

Table 61. ASC/ASCQ values (continued)

ASC	ASCQ	Sense Key	Description
18	02	1	Recovered Data - Data Auto Reallocated The controller recovered a read operation to a drive and no further action is required by the host. Auto reallocation might not have been used, but this is the only standard ASC/ASCQ that tells the initiator that no further actions are required by the driver.
1A	00	5	Parameter List Length Error A command was received by the controller that contained a parameter list and the list length in the CDB was less than the length necessary to transfer the data for the command.
20	00	5	Invalid Command Operation Code The controller received a command from the initiator that it does not support.
21	00	5	Logical Block Address Out of Range The controller received a command that requested an operation at a logical block address beyond the capacity of the logical unit. This error could be in response to a request with an illegal starting address or a request that started at a valid logical block address and the number of blocks requested extended beyond the logical unit capacity.
24	00	5	Invalid Field in CDB The controller received a command from the initiator with an unsupported value in one of the fields in the command block.
25	00	5	Logical Unit Not Supported The addressed logical unit is currently unconfigured. An Add LUN operation in the Logical Array Mode Page must be executed to define the logical unit before it is accessible.
26	00	5	Invalid Field in Parameter List The controller received a command with a parameter list that contained an error. Typical errors that return this code are unsupported mode pages, attempts to change an unchangeable mode parameter, or attempts to set a changeable mode parameter to an unsupported value.
28	00	6	Not Ready to Ready Transition The controller has completed its initialization operations on the logical unit and it is now ready for access.
29	00	6	Power On, Reset, or Bus Device Reset Occurred The controller has detected one of the above conditions.
29	04	6	Device Internal Reset The controller has reset itself due to an internal error condition.
29	81	(6)	Default Configuration has been Created The controller has completed the process of creating a default logical unit. There is now an accessible logical unit that did not exist previously. The host should execute its device scan to find the new logical unit.
29	82	6	Controller Firmware Changed Through Auto Code Synchronization The controller firmware has been changed through the Auto Code Synchronization (ACS) process.

Table 61. ASC/ASCQ values (continued)

ASC	ASCQ	Sense Key	Description
2A	01	6	Mode Parameters Changed The controller received a request from another initiator to change the mode parameters for the addressed logical unit. This error notifies the current initiator that the change occurred. This error might also be reported in the event that Mode Select parameters changed as a result of a cache synchronization error during the processing of the most recent Mode Select request.
2A	02	6	Log Parameters Changed The controller received a request from another initiator to change the log parameters for the addressed logical unit. This error notifies the current initiator that the change occurred. This error is returned when a Log Select command is issued to clear the AEN log entries.
2F	00	6	Commands Cleared by Another Initiator The controller received a Clear Queue message from another initiator. This error is to notify the current initiator that the controller cleared the current initiators commands if it had any outstanding.
31	01	1, 4	Format Command Failed A Format Unit command issued to a drive returned an unrecoverable error.
32	00	4	Out of Alternates A Re-assign Blocks command to a drive failed.
3F	01	(6)	Drive micro-code changed
3F	0E	6	Reported LUNs data has changed Previous LUN data reported using a Report LUNs command has changed (due to LUN creation or deletion or controller hot-swap).

Table 61. ASC/ASCQ values (continued)

ASC	ASCQ	Sense Key	Description
3F	8N	(6)	Drive No Longer Usable The controller has set a drive to a state that prohibits use of the drive. The value of N in the ASCQ indicates the reason why the drive cannot be used. 0 - The controller set the drive state to ″Failed - Write failure″ 1 - Not used 2 - The controller set the drive state to ″Failed″ because it was unable to make the drive usable after replacement. A format or reconstruction error occurred. 3 - Not used 4 - Not used 5 - The controller set the drive state to ″Failed - No response″ 6 - The controller set the drive state to ″Failed - Format failure″ 7 - The controller set the drive state to ″User failed via Mode Select″ 8 - Not used 9 - The controller set the drive state to ″Wrong drive removed/replaced″ A - Not used B - The controller set the drive state to ″Drive capacity < minimum″ C - The controller set the drive state to ″Drive has wrong block size″ D - The controller set the drive state to ″Failed - Controller storage failure″ E - Drive failed due to reconstruction failure at Start of Day (SOD)
3F	98	(6)	Drive Marked Offline Due to Internal Recovery Procedure An error has occurred during interrupted write processing causing the LUN to transition to the Dead state. Drives in the drive group that did not experience the read error will transition to the Offline state (0x0B) and log this error.
3F	BD	(6)	The controller has detected a drive with Mode Select parameters that are not recommended or which could not be changed. Currently this indicates the QErr bit is set incorrectly on the drive specified in the FRU field of the Request Sense data.
3F	C3	(6)	The controller had detected a failed drive side channel specified in the FRU Qualifier field.
3F	C7	(6)	Non-media Component Failure The controller has detected the failure of a subsystem component other than a disk or controller. The FRU codes and qualifiers indicate the faulty component.
3F	C8	(6)	AC Power Fail The Uninterruptible Power Source has indicated that ac power is no longer present and the UPS has switched to standby power.
3F	C9	(6)	Standby Power Depletion Imminent The UPS has indicated that its standby power source is nearing depletion. The host should take actions to stop IO activity to the controller.

Table 61. ASC/ASCQ values (continued)

ASC	ASCQ	Sense Key	Description
3F	CA	(6)	Standby Power Source Not at Full Capability The UPS has indicated that its standby power source is not at full capacity.
3F	CB	(6)	AC Power Has Been Restored The UPS has indicated that ac power is now being used to supply power to the controller.
3F	D0	(6)	Write Back Cache Battery Has Been Discharged The controllers battery management has indicated that the cache battery has been discharged.
3F	D1	(6)	Write Back Cache Battery Charge Has Completed The controllers battery management has indicated that the cache battery is operational.
3F	D8	(6)	Cache Battery Life Expiration The cache battery has reached the specified expiration age.
3F	D9	(6)	Cache Battery Life Expiration Warning The cache battery is within the specified number of weeks of failing.
3F	E0	(6)	Logical Unit Failure The controller has placed the logical unit in a Dead state. User data, parity, or both can no longer be maintained to ensure availability. The most likely cause is the failure of a single drive in non-redundant configurations or a second drive in a configuration protected by one drive. The data on the logical unit is no longer accessible.
3F	EB	(6)	LUN marked Dead due to Media Error Failure during SOD An error has occurred during interrupted write processing causing the LUN to transition to the Dead state.

Table 61. ASC/ASCQ values (continued)

ASC	ASCQ	Sense Key	Description
40	NN	4, (6)	Diagnostic Failure on Component NN (0x80 - 0xFF) The controller has detected the failure of an internal controller component. This failure might have been detected during operation as well as during an on-board diagnostic routine. The values of NN supported in this release of the software are as follows: 80 - Processor RAM 81 - RAID Buffer 82 - NVSRAM 83 - RAID Parity Assist (RPA) chip or cache holdup battery 84 - Battery Backed NVSRAM or Clock Failure 91 - Diagnostic Self Test failed non-data transfer components test 92 - Diagnostic Self Test failed data transfer components test 93 - Diagnostic Self Test failed drive Read/Write Buffer data turnaround test 94 - Diagnostic Self Test failed drive Inquiry access test 95 - Diagnostic Self Test failed drive Read/Write data turnaround test 96 - Diagnostic Self Test failed drive Self Test
43	00	4	Message Error The controller attempted to send a message to the host, but the host responded with a Reject message.
44	00	4, B	Internal Target Failure The controller has detected a hardware or software condition that does not allow the requested command to be completed. If the sense key is 0x04 indicating a hardware failure, the controller has detected what it believes is a fatal hardware or software failure and it is unlikely that a retry would be successful. If the sense key is 0x0B indicating an aborted command, the controller has detected what it believes is a temporary software failure that is likely to be recovered if retried.
45	00	1, 4	Selection Time-out on a Destination Bus A drive did not respond to selection within a selection time-out period.
47	00	1, B	SCSI Parity Error The controller detected a parity error on the host SCSI bus or one of the drive SCSI buses.
48	00	1, B	Initiator Detected Error Message Received The controller received an Initiator Detected Error Message from the host during the operation.
49	00	B	Invalid Message Error The controller received a message from the host that is not supported or was out of context when received.
49	80	B	Drive Reported Reservation Conflict A drive returned a status of reservation conflict.

Table 61. ASC/ASCQ values (continued)

ASC	ASCQ	Sense Key	Description
4B	00	1, 4	Data Phase Error The controller encountered an error while transferring data to or from the initiator or to or from one of the drives.
4E	00	B	Overlapped Commands Attempted The controller received a tagged command while it had an untagged command pending from the same initiator or it received an untagged command while it had one or more tagged commands pending from the same initiator.
5D	80	6	Drive Reported PFA (Predicted Failure Analysis) Condition
80	02	1, 4	Bad ASC code detected by Error/Event Logger
80	03	4	Error occurred during data transfer from SRM host.
84	00	4, 5	Operation Not Allowed With the Logical Unit in its Current State The requested command or Mode Select operation is not allowed with the logical unit in the state indicated in byte 76 of the sense data. Examples would be an attempt to read or write a dead logical unit or an attempt to verify or repair parity on a degraded logical unit.
84	06	4	LUN Awaiting Format A mode select has been done to create a LUN but the LUN has not been formatted.
85	01	4	Drive IO Request Aborted IO Issued to Failed or Missing drive due to recently failed removed drive. This error can occur as a result of IOs in progress at the time of a failed or removed drive.
87	00	4	Microcode Download Error The controller detected an error while downloading microcode and storing it in non-volatile memory.
87	08	4	Incompatible Board Type For The Code Downloaded
87	0C	6	Download failed due to UTM LUN number conflict
87	0E	6	Controller Configuration Definition Inconsistent with Alternate Controller
88	0A	(6)	Subsystem Monitor NVSRAM values configured incorrectly
8A	00	5	Illegal Command for Drive Access The initiator attempted to pass a command through to a drive that is not allowed. The command could have been sent in pass-thru mode or by attempting to download drive microcode.
8A	01	5	Illegal Command for the Current RAID Level The controller received a command that cannot be executed on the logical unit due to its RAID level configuration. Examples are parity verify or repair operations on a RAID 0 logical unit.
8A	10	5	Illegal Request- Controller Unable to Perform Reconfiguration as Requested The user requested a legal reconfiguration but the controller is unable to execute the request due to resource limitations.
8B	02	B, (6)	Quiescence Is In Progress or Has Been Achieved
8B	03	B	Quiescence Could Not Be Achieved Within the Quiescence Timeout Period
8B	04	5	Quiescence Is Not Allowed

Table 61. ASC/ASCQ values (continued)

ASC	ASCQ	Sense Key	Description
8E	01	E, (6)	A Parity/Data Mismatch was Detected The controller detected inconsistent parity/data during a parity verification.
91	00	5	General Mode Select Error An error was encountered while processing a Mode Select command.
91	03	5	Illegal Operation for Current Drive State A drive operation was requested through a Mode Select that cannot be executed due to the state of the drive. An example would be a Delete Drive when the drive is part of a LUN.
91	09	5	Illegal Operation with Multiple SubLUNs Defined An operation was requested that cannot be executed when multiple SubLUNs are defined on the drive.
91	33	5	Illegal Operation for Controller State The requested Mode Select operation could not be completed due to the current state of the controller.
91	36	5	Command Lock Violation The controller received a Write Buffer Download Microcode, Send Diagnostic, or Mode Select command, but only one such command is allowed at a time and there was another such command active.
91	3B	6	Improper LUN Definition for Auto-Volume Transfer mode - AVT is disabled. Controller will operate in normal redundant controller mode without performing Auto-Volume transfers.
91	50	5	Illegal Operation For Drive Group State An operation was requested that cannot be executed due to the current state of the Drive Group.
91	51	5	Illegal Reconfiguration Request - Legacy Constraint Command could not be completed due to Legacy configuration or definition constraints.
91	53	5	Illegal Reconfiguration Request - System Resource Constraint Command could not be completed due to resource limitations of the controller.
94	01	5	Invalid Request Due to Current Logical Unit Ownership
95	01	4	Extended Drive Insertion/Removal Signal The controller has detected the drive insertion/removal signal permanently active.
95	02	(6)	Controller Removal/Replacement Detected or Alternate Controller Released from Reset The controller detected the activation of the signal or signals used to indicate that the alternate controller has been removed or replaced.
98	01	(6)	The controller has determined that there are multiple sub-enclosures with the same ID value selected.
98	02	(6)	Sub-enclosure with redundant ESMs specifying different Tray IDs
98	03	(6)	Sub-enclosure ESMs have different firmware levels

Table 61. ASC/ASCQ values (continued)

ASC	ASCQ	Sense Key	Description
A0	00	(6)	Write Back Caching Could Not Be Enabled The controller could not perform write-back caching due to a battery failure or discharge, Two Minute Warning signal from the UPS, or an ICON failure.
A1	00	(6)	Write Back Caching Could Not Be Enabled - RDAC Cache Size Mismatch The controller could not perform write back caching due to the cache sizes of the two controllers in the RDAC pair not matching.
A4	00	(6)	Global Hot Spare Size Insufficient for All Drives in Subsystem. A defined Global Hot Spare is not large enough to cover all of the drives present in the subsystem. Failure of a drive larger than the Global Hot Spare will not be covered by the Global Hot Spare drive.
A6	00	(6)	Recovered processor memory failure The controller has detected and corrected a recoverable error in processor memory.
A7	00	(6)	Recovered data buffer memory error The controller has detected and corrected a recoverable error in the data buffer memory. Sense bytes 34-36 will contain the count of errors encountered and recovered.
C0	00	4, (6)	The Inter-controller Communications Have Failed The controller has detected the failure of the communications link between redundant controllers.
D0	06	4	Drive IO Time-out The controller destination IO timer expired while waiting for a drive command to complete.
D1	0A	4	Drive Reported Busy Status A drive returned a busy status in response to a command.
E0	XX	4	Destination Channel Error XX = 00 through 07 indicates the Sense Key returned by the drive after a check condition status XX = 10 indicates that a bus level error occurred
E0	XX	6	Fibre Channel Destination Channel Error XX = 20 indicates redundant path is not available to devices XX = 21 indicates destination drive channels are connected to each other Sense Byte 26 will contain the Tray ID. Sense Byte 27 will contain the Channel ID.

FRU code table

A nonzero value in the FRU code byte identifies a field-replaceable unit that has failed or a group of field-replaceable modules that includes one or more failed devices. For some Additional Sense Codes, the FRU code must be used to determine where the error occurred. For example, the Additional Sense Code for SCSI bus parity error is returned for a parity error detected on either the host bus or one of the drive buses. In this case, the FRU field must be evaluated to determine whether the error occurred on the host channel or a drive channel.

Because of the large number of replaceable units possible in an array, a single byte is not sufficient to report a unique identifier for each individual field-replaceable unit. To provide meaningful information that will decrease field troubleshooting and problem resolution time, FRUs have been grouped. The defined FRU groups and their descriptions are listed in Table 62.

Table 62. FRU codes

FRU code	Title	Description
0x01	Host Channel Group	A FRU group consisting of the host SCSI bus, its SCSI interface chip, and all initiators and other targets connected to the bus.
0x02	Controller Drive Interface Group	A FRU group consisting of the SCSI interface chips on the controller that connect to the drive buses.
0x03	Controller Buffer Group	A FRU group consisting of the controller logic used to implement the on-board data buffer.
0x04	Controller Array ASIC Group	A FRU group consisting of the ASICs on the controller associated with the array functions.
0x05	Controller Other Group	A FRU group consisting of all controller-related hardware not associated with another group.
0x06	Subsystem Group	A FRU group consisting of subsystem components that are monitored by the array controller, such as power supplies, fans, thermal sensors, and ac power monitors. Additional information about the specific failure within this FRU group can be obtained from the additional FRU bytes field of the array sense.
0x07	Subsystem Configuration Group	A FRU group consisting of subsystem components that are configurable by the user, on which the array controller will display information (such as faults).
0x08	Sub-enclosure Group	A FRU group consisting of the attached enclosure devices. This group includes the power supplies, environmental monitor, and other subsystem components in the sub-enclosure.
0x09-0x0F	Reserved	
0x10-0xFF	Drive Groups	A FRU group consisting of a drive (embedded controller, drive electronics, and Head Disk Assembly), its power supply, and the SCSI cable that connects it to the controller; or supporting sub-enclosure environmental electronics. The FRU code designates the channel ID in the most significant nibble and the SCSI ID of the drive in the least significant nibble. **Note:** Channel ID 0 is not used because a failure of drive ID 0 on this channel would cause an FRU code of 0x00, which the SCSI-2 standard defines as no specific unit has been identified to have failed or that the data is not available.

Chapter 22. PD hints — Configuration types

You should be referred to this chapter from a PD map or indication. If this is not the case, see Chapter 16, “Problem determination starting points”, on page 131.

After you have read the relevant information in this chapter, return to the “Configuration Type PD map” on page 138.

To simplify a complicated configuration so that it can be debugged readily, reduce the configuration to subsets that can be used to build the larger configuration. This process yields two basic configurations. (The type of RAID controller is not material; FAStT500 is shown in the following examples.)

Type 1 configuration

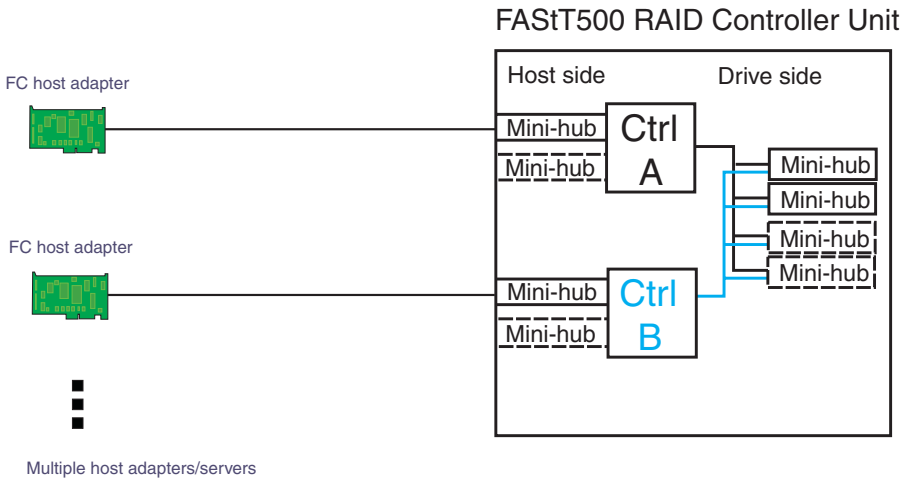


Figure 111. Type 1 Configuration

The identifying features of a type 1 configuration (as shown in Figure 111) are:

- Host adapters are connected directly to mini hubs of Controller A and B, with one or more host adapters per system
- Multiple servers can be connected, but without system-to-system failover (no MSCS)
- Uses some type of isolation mechanism (such as partitions) between server resources

Type 2 configuration

The type 2 configuration can occur with or without hubs and switches, as shown in Figure 112 and Figure 113.

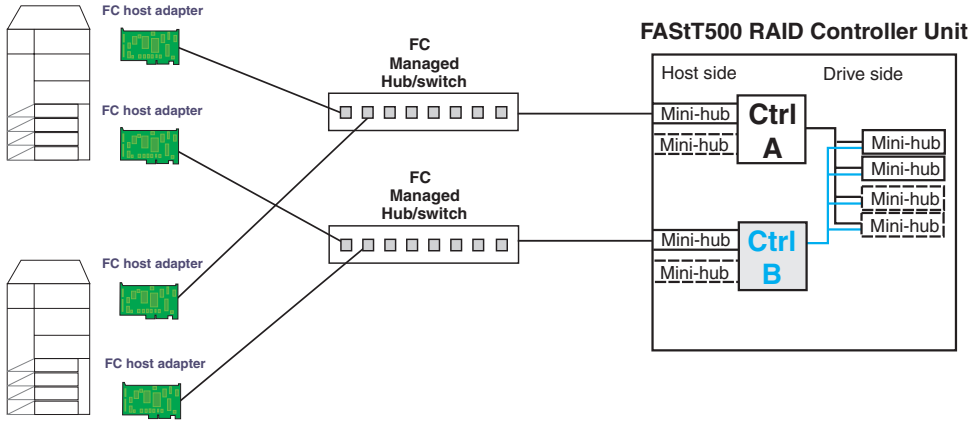


Figure 112. Type 2 Configuration - With Hubs

The identifying features of a type 2 configuration are:

- Multiple host adapters are connected for full redundancy across systems having failover support such as MSCS
- Host adapters are connected either directly to mini hubs or through managed hubs or switches (2 GBIC ports per mini hub are possible)
- A redundant path to mini hubs can be separated using optional mini hubs, as shown in the following figure in red (vs. the green path)

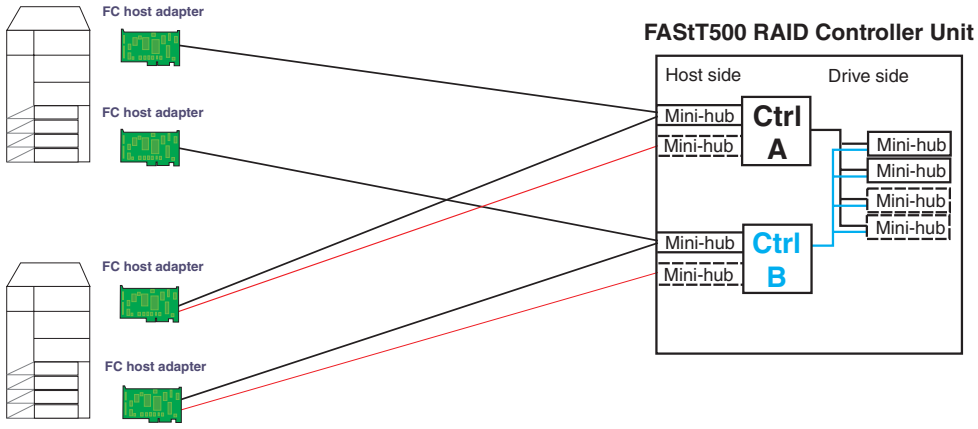


Figure 113. Type 2 Configuration - Without Hubs

Diagnostics and examples

In a type 1 configuration there are no externally managed hubs or switches to aid in debugging. The diagnostic tools available are FAStT MSJ (from the host adapter end), the `sendEcho` command (from the RAID controller end), and SANavigator (with in-band management). If you intend to diagnose a failed path while using the alternate path for production, be sure that you are familiar with the tools and the loop connections so that the correct portion is being exercised and you do not unplug anything in the active path.

For a type 2 configuration, use the features of the switches and managed hubs and the capability of MSCS to isolate resources from the bad or marginal path before beginning debug activities. Switches and managed hubs allow a view of log information that shows what problems have been occurring, as well as diagnostics that can be initiated from these managed elements. Also, a type 2 configuration has the capability to have more than one RAID controller unit behind a switch or managed hub. In the diagnostic maps, the switches and managed hubs are referred to generically as *concentrators*. Figure 114 shows a type 2 configuration with multiple controller units.

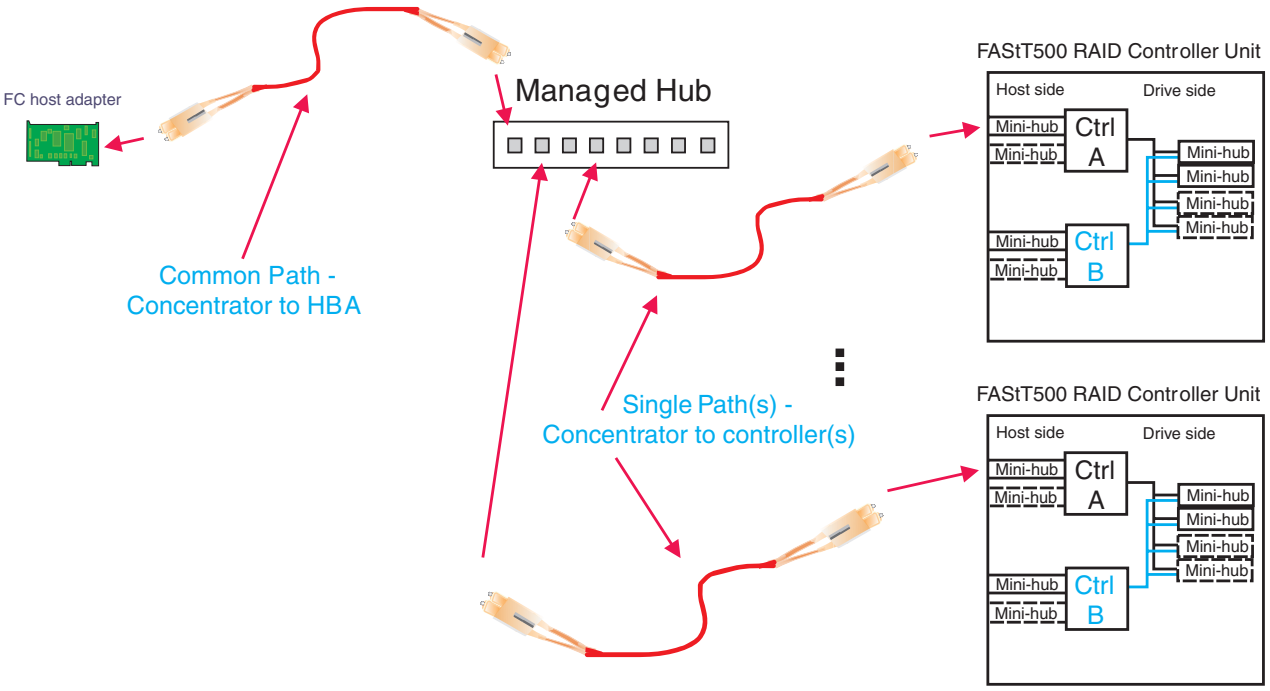


Figure 114. Type 2 Configuration with Multiple Controller Units

You can also use SANavigator to identify and isolate Fibre Path and device problems. SANavigator discovery for a configuration without concentrators requires that the HBA API Library be installed on the server where SANavigator is installed and in which the HBAs are located. This is referred to as in-band management.

For configurations with concentrators, the concentrator (a switch, hub, or router) must be connected to the same sub-network (through Ethernet) as the server in order for SANavigator to discover the devices. This is referred to as out-of-band management.

Both in-band and out-of-band management can be enabled for a particular SAN configuration. It is strongly suggested that you enable both management methods.

Debugging example sequence

An example sequence for debugging a type 2 MSCS configuration is shown in the following sequence of figures.

Multiple server pairs can be attached to the switches (using zoning or partitioning for pair isolation) or combinations of type 1 and type 2 configurations. Break the larger configuration into its smaller subelements and work with each piece separately. In this way you can remove the good path and leave only the bad path, as shown in the following sequence.

1. One controller is passive. In the example shown in Figure 115, controller B is passive.

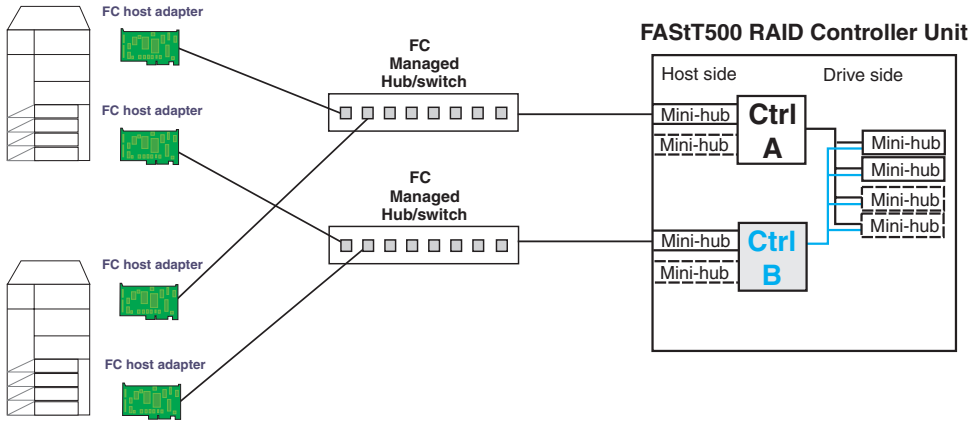


Figure 115. Passive Controller B

2. All I/O is flowing through controller A. This yields the diagram shown in Figure 116 for debugging.

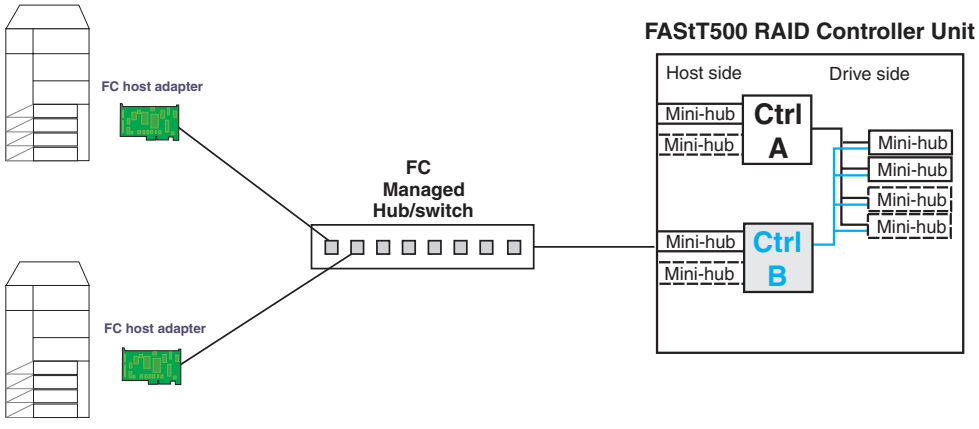


Figure 116. All I/O Flowing Through Controller A

3. To see more clearly what is involved, redraw the configuration showing the path elements in the loop, as shown in Figure 117 on page 269.

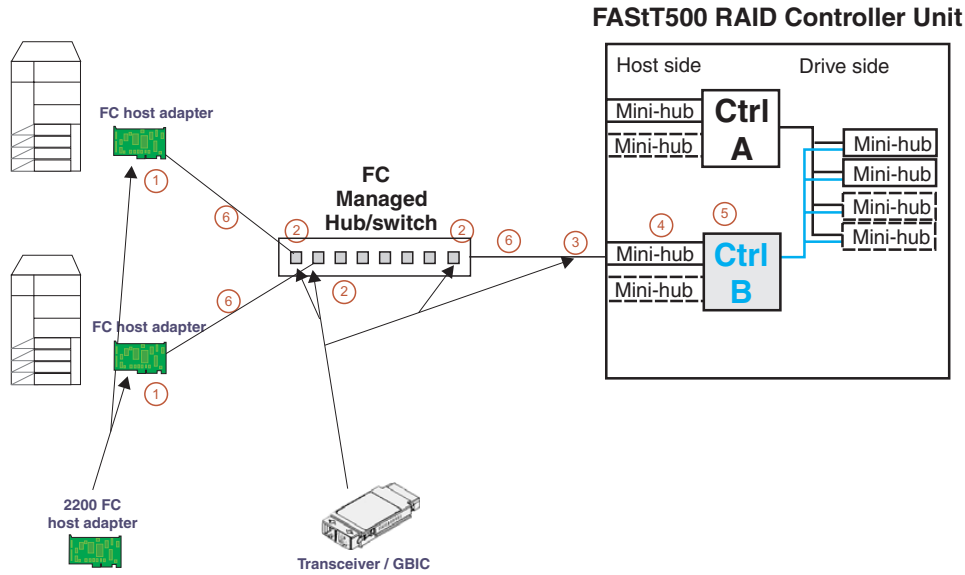


Figure 117. Path Elements Loop

The elements of the paths shown in Figure 117 are as follows:

1. Host adapter with optical transceiver
2. Optical transceiver in managed hub or GBIC in switch
3. GBIC in controller mini hub
4. Mini hub
5. RAID controller
6. Optical cables

Chapter 23. PD hints — Passive RAID controller

You should be referred to this chapter from a PD map or indication. If this is not the case, see Chapter 16, “Problem determination starting points”, on page 131.

After you have read the relevant information in this chapter, return to “RAID Controller Passive PD map” on page 139.

Use the SM client to view the controller properties of the passive controller, which appears as a dimmed icon.

As shown in Figure 118, right-click the dimmed controller icon and click **Properties**.

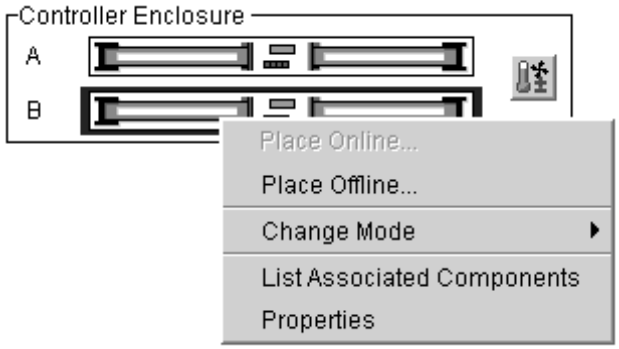


Figure 118. Controller Right-click Menu

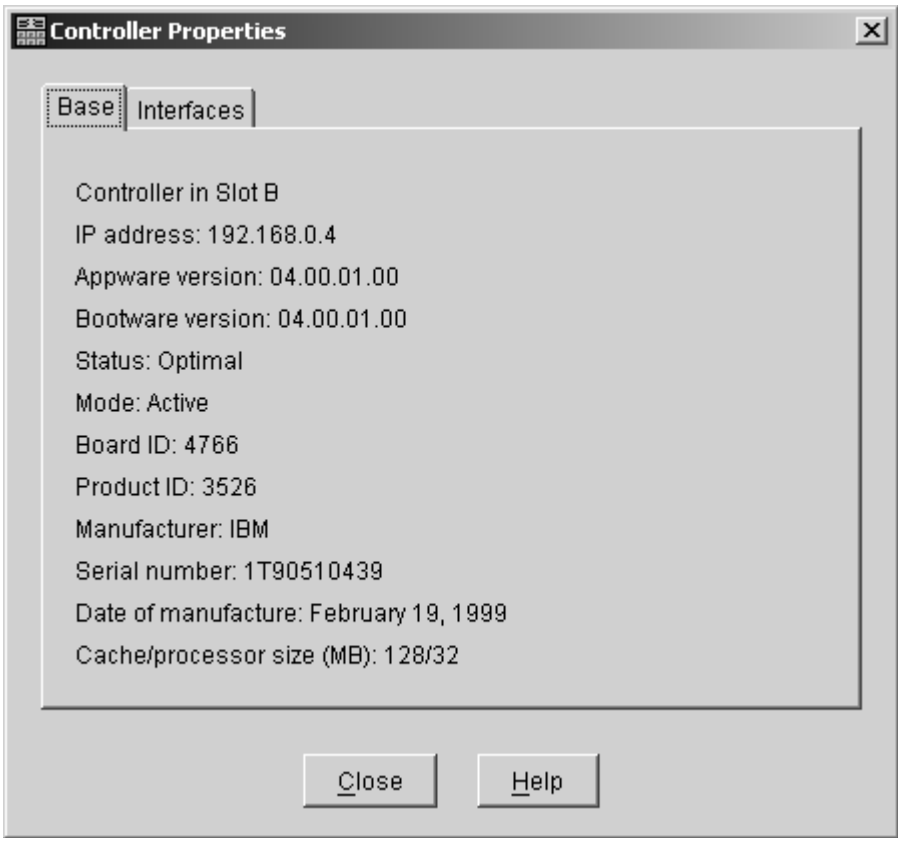


Figure 119. Controller Properties Window

If the Controller Properties view (shown in Figure 119) of the dimmed controller icon does not include a message about it being cached, then the controller is passive. Return to the PD map at the page that referred you here (“RAID Controller Passive PD map” on page 139) and continue.

If the Controller Properties information cannot be retrieved, then call IBM Support.

Perform the following steps when you encounter a passive controller and want to understand the cause:

1. Check the controller LEDs to verify that a controller is passive and to see which controller is passive.
2. Look on the system event viewer of the server to find the SYMarray event ID 18. When you find it, write down the date, time, and SRB status. (The SRB status is found in offset x3A in the Windows NT event log. For an example of offset x3A, see the fourth row, third column of the figure on page 252.)
3. If multiple servers are involved, repeat step 2 for each server.
4. Look for the first event ID 18 found in step 2. The SRB status provides information as to why the failure occurred but is valid only if the high order bit is on (8x, 9x, Ax).
5. Check the history of the event log looking for QL2200/QL2100 events. These entries will give further clues as to whether the fibre loop was stable or not.
   - SRB statuses of 0x0d, 0x0e, and 0x0f point to an unstable loop. (To find the value, discard the high order ″valid″ bit. For example, 8d yields an SRB status of 0d.)
   - QL2200/2100 events of 80110000, 80120000 indicate an unstable loop.

6. If an unstable loop is suspected, diagnose the loop using the fibre path PD aids (see “Fibre Path PD map 1” on page 148).
7. If the diagnosis in step 6 does not reveal the problem, then the adapter and the controller might be the cause. If you determine that the adapter and controller caused the problem, then reset all fibre components on the path and retest.
8. If fibre cabling can be rearranged, swap the adapter cabling so that the adapter communicating to controller A is now connected to controller B (and vice-versa).

   Note: *Do not* do this in a system that is still being used for business. It is useful for bring-up debug.
9. When the problem is resolved, set the controller back to active and rebalance logical drives.
10. If the problem occurred as the result of an I/O condition, then rerun and determine whether the failure reoccurs.

Note: If the failure still occurs, then you need to perform further analysis, including the use of the serial port to look at loop statuses. The previous steps do not include consideration of switches or managed hubs. If these are included, then see “Hub/Switch PD map 1” on page 143 for helpful tools.

Chapter 24. PD hints — Performing sendEcho tests

You should arrive at this chapter from a PD map or indication. If this is not the case, see Chapter 16, “Problem determination starting points”, on page 131.

After you have read the relevant information in this chapter, return to “Single Path Fail PD map 1” on page 150.

The 3526 controllers use MIA copper-to-optical converters, while the 3542, 3552, and 1742 controllers use GBICs. There are times when these devices, and their corresponding cable mediums, need to be tested to insure that they are functioning properly.

Note: Running the loopback test for a short period of time might not catch intermittent problems. It might be necessary to run the test in a continuous loop for at least several minutes to track down intermittent problems.

Setting up for a loopback test

This section describes how to set up for a loopback test.

Loopback test for MIA or mini hub testing

1. Remove the fiber-optic cable from the controller MIA or mini hub.
2. Depending on whether you are working with a 3526, 3552, or 1742 controller, do one of the following:
   a. For a Type 3526 RAID controller, install a wrap plug to the MIA on controller A. See Figure 120.

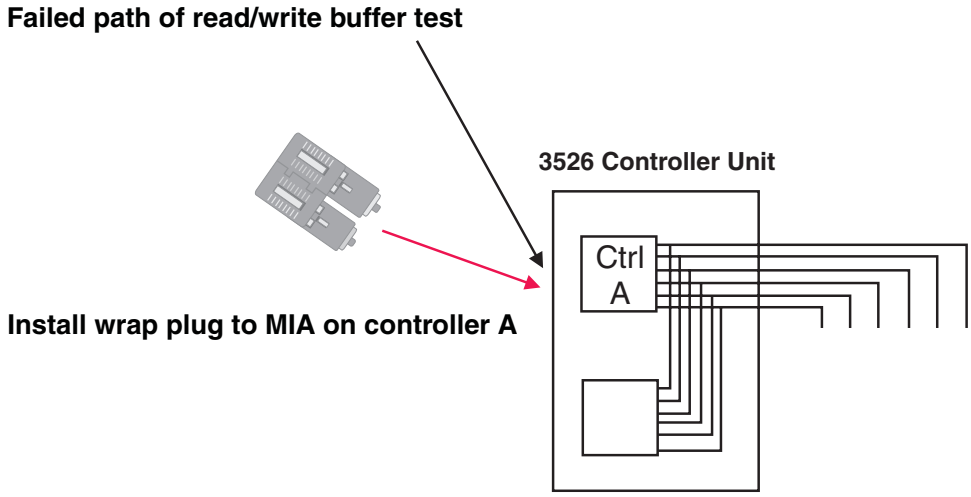


Figure 120. Install Wrap Plug to MIA on Controller A

   b. For a Type 3552 or 1742 controller, install a wrap plug to the GBIC in the mini hub on controller A. See Figure 121 on page 276.

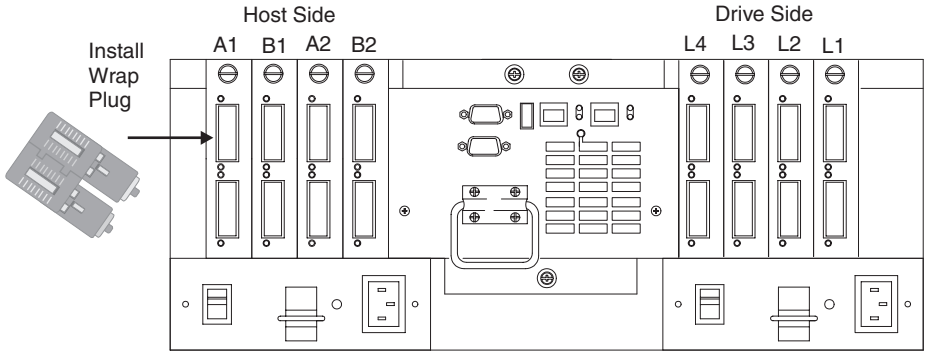


Figure 121. Install Wrap Plug to GBIC in Mini Hub on Controller A

3. Go to the appropriate Loopback Test section (either “Running the loopback test on a 3526 RAID controller” or “Running the loopback test on a FAStT200, FAStT500, or FAStT700 RAID controller” on page 277).

Loopback test for optical cable testing

1. Detach the remote end of the optical cable from its destination.
2. Plug the female-to-female converter connector from your kit onto the remote end of the optical cable.
3. Insert the wrap plug from your kit into the female-to-female converter. See Figure 122.

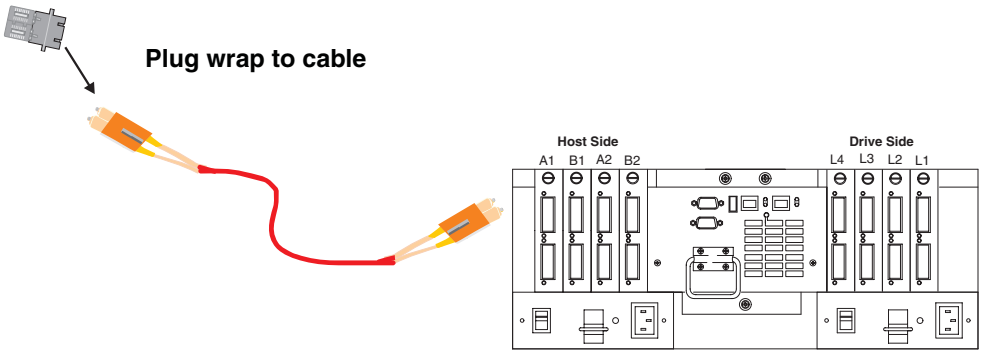


Figure 122. Install Wrap Plug

4. Go to the appropriate loopback test section (either “Running the loopback test on a 3526 RAID controller” or “Running the loopback test on a FAStT200, FAStT500, or FAStT700 RAID controller” on page 277).

Running the loopback test on a 3526 RAID controller

1. In the controller shell, type the following: `fc 5`
2. From the output, write down the AL_PA (Port_ID) for this controller.
3. Type the command `isp sendEcho,<AL_PA>,<# of iterations>`

   It is recommended that you use **50 000** for `# of iterations`. A value of **-1** will run for an infinite number of iterations. Message output to the controller shell is generated for every 10 000 frames sent.
4. Type the command `stopEcho` when tests are complete.

Running the loopback test on a FAStT200, FAStT500, or FAStT700 RAID controller

1. In the controller shell, type the following command: `fcAll`
2. From the output, write down the AL_PA (Port_ID) for the channel to be tested.
3. Type the command `fcChip=X` where X=the chip number for the loop to be tested.
4. Type the command `isp sendEcho,<AL_PA>,<# of iterations>`

   It is recommended that you use **50 000** for `# of iterations`. A value of **-1** will run for an infinite number of iterations. Message output to the controller shell is generated for every 10 000 frames sent.
5. Type the command `stopEcho` when tests are complete.

If the test is successful, then you will receive the following message:

```
Echo accept (count n)
```

If you receive the following message:

```
Echo timeout interrupt: interrupt ... end echo test
```

or if you receive nonzero values after entering the command `isp sendEcho`, then there is still a problem. Continue with the “Single Path Fail PD map 1” on page 150.

Chapter 25. PD hints - Tool hints

You should be referred to this chapter from a PD map or indication. If this is not the case, refer back to Chapter 16, “Problem determination starting points”, on page 131.

This chapter contains hints in the following PD areas:

Determining the configuration

Use FAStT MSJ to determine what host adapters are present and where they are in the systems, as well as what RAID controllers are attached and whether they are on Fabric (switches) or loops. Alternately, you can click **Control Panel->SCSI adapters** in Windows NT or **Control Panel -> System -> Hardware -> Device Manager -> SCSI and RAID Controllers** in Windows 2000.

Figure 123 shows the FAStT MSJ window for a configuration with two 2200 host adapters. When only the last byte of the Port ID is displayed, this indicates that the connection is an arbitrated loop.

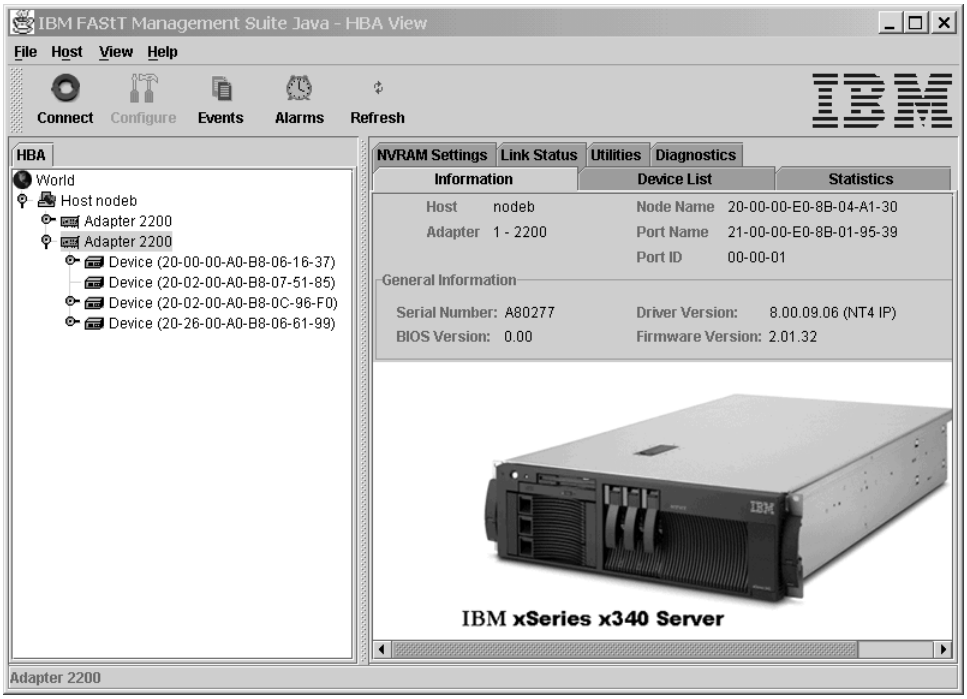


Figure 123. FAStT MSJ Window - Two 2200 Host Adapters

A different configuration is shown in Figure 124, which shows a 2200 adapter. Its World Wide Name is 20-00-00-E0-8B-04-A1-30 and it has five devices attached to it. When the first two bytes of the Port ID are displayed (and they are other than 00), the configuration is Fabric (switch).

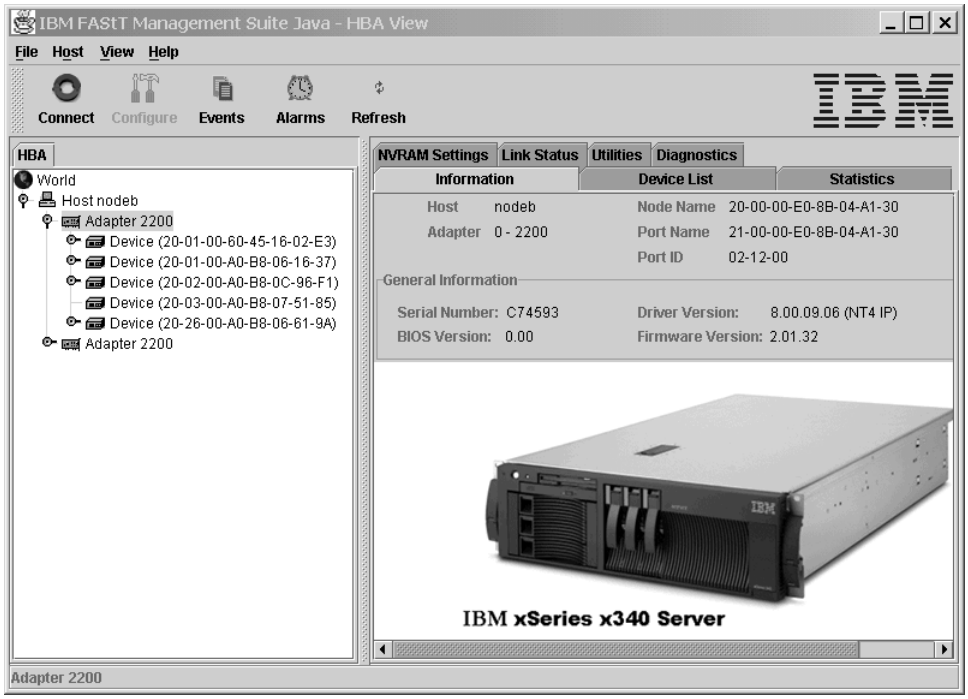


Figure 124. FAStT MSJ Window - One 2200 Host Adapter

As shown in Figure 125 on page 281, if you select one of the devices beneath a host adapter, you find that it is a controller in a 3526 controller unit.

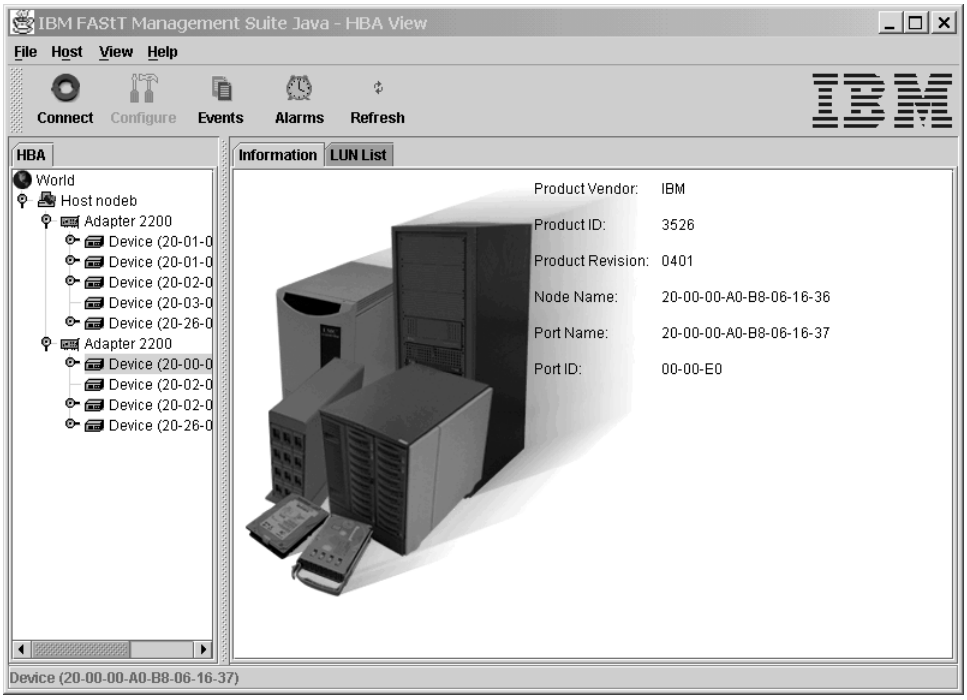


Figure 125. 3526 Controller Information

Boot-up delay

In Windows operating systems, an extended start-up delay indicates that Windows is not finding the expected configuration that is in its registry. In Linux operating systems, the delay might also be caused by an incorrectly configured storage subsystem (see “Linux port configuration” on page 303 for hints on troubleshooting this problem.)

The delay in the Windows operating system can be caused by several things, but the following example shows what typically happens when a fibre channel cable connecting a host adapter to the storage has failed (a failed cable is broken so that no light makes it through the cable).

Bluescreen example (Windows NT):

Note: The following example describes boot-up delay symptoms in a Windows NT operating system. In the Windows 2000 operating system, the Windows 2000 Starting Up progress bar would be frozen. To retrieve the SCSI information in Windows 2000, use the Computer Management dialog (right-click **My Computer** and select **Manage**.)

1. Windows NT comes up to the blue screen and reports the first two lines (version, number of processors, and amount of memory). Windows NT takes a very long time to start. The SCSI Adapters applet in the Control Panel displays the window shown in Figure 126 for the 2100:

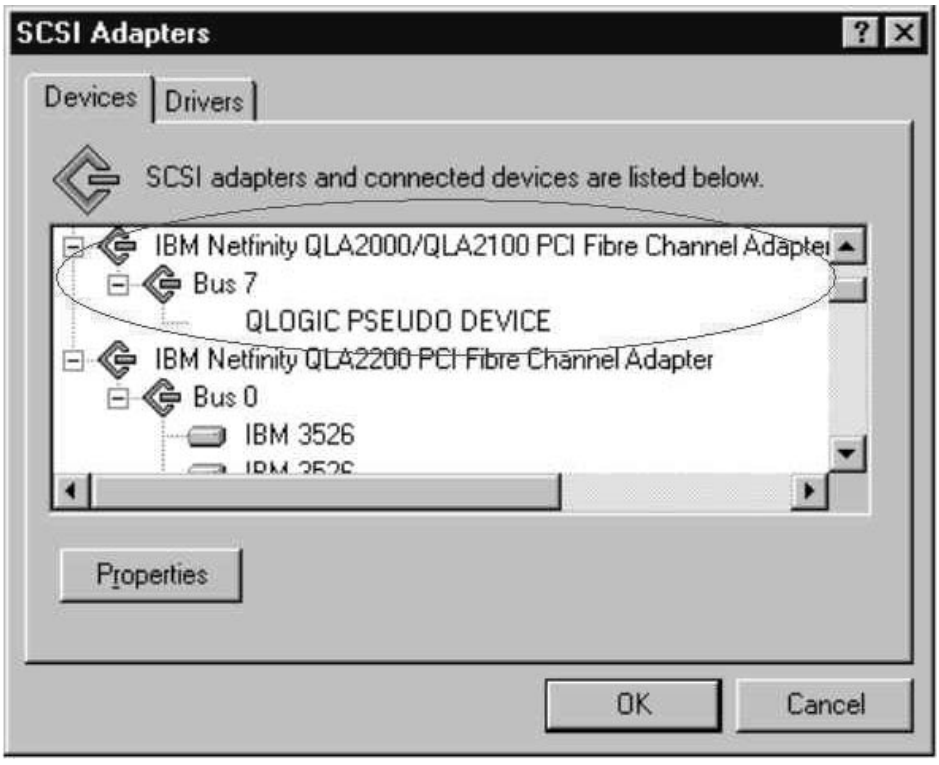


Figure 126. SCSI Adapters

There are no other devices; there should have been a Bus 0 with 21 of the IBM 3526s and one IBM Universal Xport. Note the 2100 DD shows up as started in the Drivers tab here and in the Control Panel Devices applet.

2. WINDISK is started. It takes longer than normal to start (and there is a particularly long pause at the 100% mark) and then reports the message shown in Figure 127.

Figure 127. Disk Administrator Information Dialog

3. Because disks were balanced across the two RAID controllers before the error occurred, every other disk shows in the Disk Administrator as off-line, and the partition information section is grayed out, showing the following:

   ```
   Configuration information not available
   ```

   The drive letters do not change for the drives (they are sticky, even though they are set only for boot drive). Because the cable to RAID controller A is the failed cable, it was Disk 0, Disk 2, and so on, that are missing. See Figure 128.

Figure 128. Disk Administrator

4. **If Done:** Return to “Boot-up Delay PD map” on page 141.

Controller units and drive enclosures

In Figure 129 (an EXP500 fibre channel drive enclosure), there are two loops in the box. The ESM on the left controls one loop path and the ESM on the right controls another loop path to the drives. This box can be used with the 3552, 3542, and 1742 Controller Units.

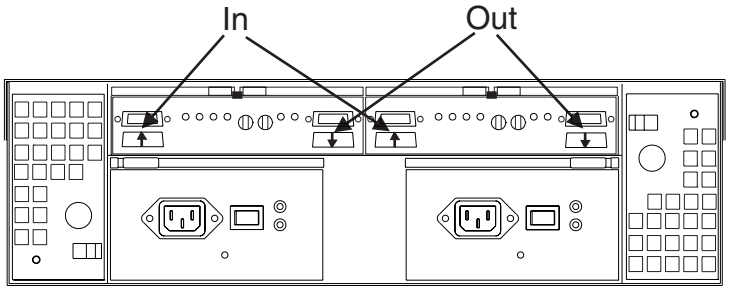


Figure 129. EXP500 Fibre Channel Drive Enclosure

Note: In the previous figure, the connections for the GBICs are labeled as In and Out. This designation of the connections is for cabling routing purposes only, as all Fibre cables have both a transmit fiber and receive fiber in them. Any connection can function as either output or input (transmitter or receiver).

Figure 130 shows the locations of the controller connections in a FAStT500 or FAStT700 Fibre Channel controller unit.

Note: In Figure 130, a FAStT500 controller unit is shown.

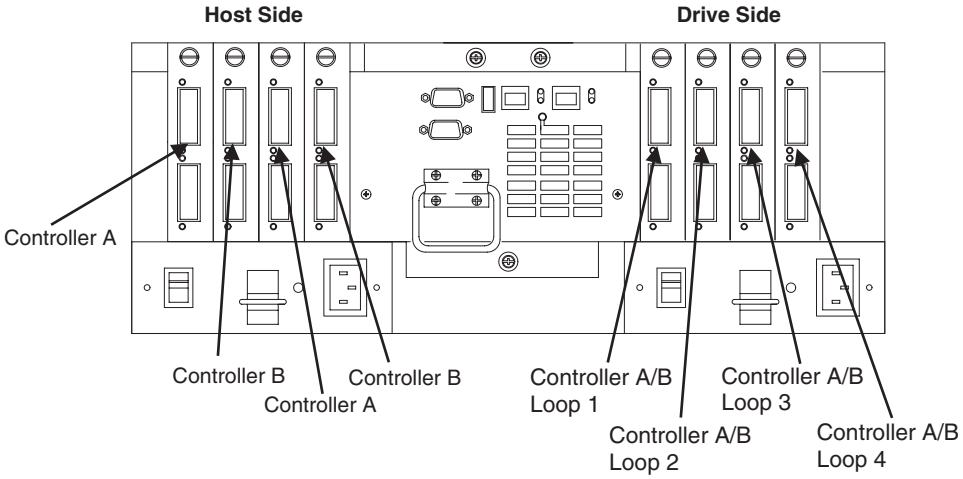


Figure 130. FAStT500 Controller Connection Locations

Figure 131 on page 285 shows the locations of the controller units in a FAStT200 Fibre Channel controller and drive enclosure unit.

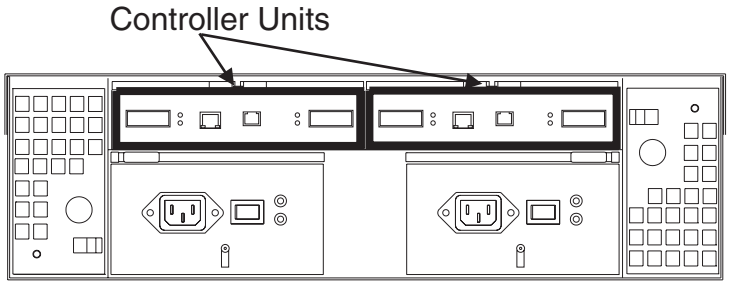


Figure 131. FAStT200 Fibre Channel Controller Unit Locations

Figure 132 shows a configuration containing both controllers. It uses GBICs for the connection but does not have the mini hub feature of the 3552. There is a place for a single host to attach to each controller without using an external concentrator. The other connection on each is used to attach more drives using EXP500 enclosures.

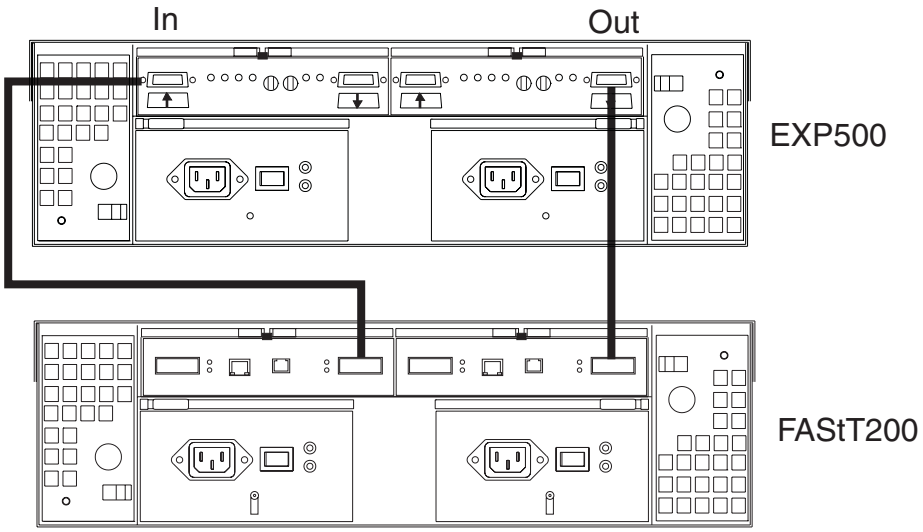


Figure 132. EXP500 and FAStT200 Configuration

SANavigator discovery and monitoring behavior

This section provides examples and commentary explaining the use and interpretation of the SANavigator Physical Map and Event Log.

For more information about using SANavigator, see Chapter 19, “Introduction to SANavigator”, on page 217.

Physical Map

To simplify management, devices are displayed in groups. Groups are shown with background shading and are labeled appropriately. You can expand and collapse groups to easily view a large topology. See Figure 133.

This section describes the groups shown on a typical SANavigator representation of a SAN. The following map shows devices bundled into four types of groups: Host, Switch, Storage, and Bridge.

Note: In version 2.7, SANavigator displayed the SAN topology as one single fabric. In version 3.x, each switch (and associated devices) is shown as an individual Fabric. If the switches are connected through ISL (Inter-Switch Link), then SANavigator will display the topology as a single fabric and assign the WWNN of one of the switches to the fabric.

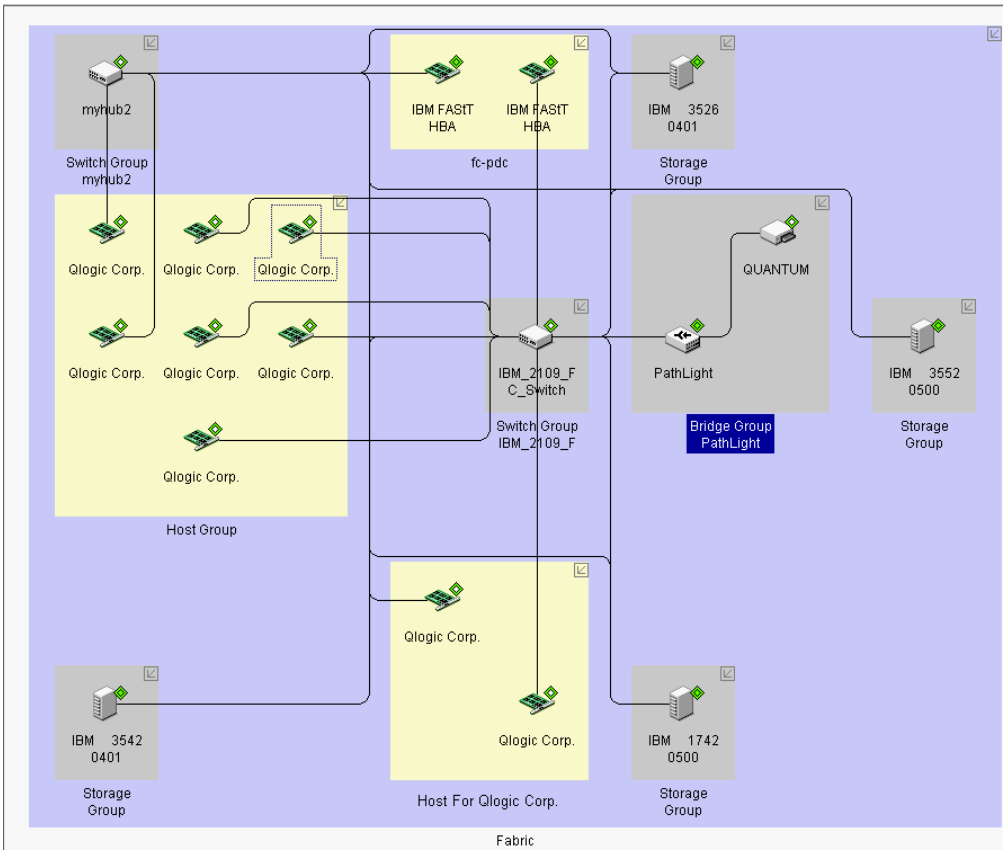


Figure 133. SANavigator Physical MAP

The four types of groups displayed in this Physical Map are:

- **Host Groups**

  Three host groups are shown in this map: Host, Host For Qlogic Corp., and fc-pdc.

  The unassigned host bus adapters are contained within one group (Host). At the time this map was captured, the discovered HBAs were not associated with their respective servers.

  If a discovered server has identical HBA types (for example, two 2200s or two 2310s), then SANavigator reconciles these HBAs into their respective servers and assigns the HBA name (for example ″Host For Qlogic Corp.″) as the name of the server. This is shown in the second group on the topology (Server Host For Qlogic Corp.). This type of automatic association is valid only for Windows operating systems.

  Instructions are provided for changing the name of the server and assigning HBAs to other servers in “Associating unassigned HBAs to servers” on page 288.

  HBAs can also be associated automatically to the system on which they reside provided that in-band management for that system is enabled. A new feature of SANavigator 3.x is the ability to perform in-band management of remote hosts from a local management station. The local SANavigator server communicates with the Remote Discovery Connector (SANavRemote.exe) installed on the remote host. You need to choose Remote Discovery Connector when installing SANavigator on the remote Host.

  This method of Discovery requires that the HBA API library be installed on the system (local or remote or both). It is shown in the third group on the topology (Host fc-pdc). The inner and outer diamonds for each of the HBAs are green; this indicates that both in-band and out-of band discovery have occurred and are still active.

- **Switch Group**

  This group represents the switches that are required for SANavigator to perform out-of-band management. You can expand the switch icon to expose the ports by right-clicking the icon and selecting **Port** from the pop-up menu.

  Note: If switches or managed hubs are present, then out-of-band management must be enabled.

- **Storage Groups**

  These groups represent the FAStT Storage Servers or other storage devices. You can expand the Storage Server to expose the ports by right-clicking the icon and selecting **Port** from the pop-up menu.

  Both inner and outer diamonds for each of the Storage Servers are green; this indicates that both in-band and out-of-band discovery have occurred and are still active. The in-band discovery is accomplished by the HBAs in the fc-pdc server and is only applicable to that server.

- **Bridge Group**

  The SAN Data Gateway router, like the IBM 2103-R03, is displayed as a Bridge Group. The Physical Map shown in this section shows a PathLight SAN Router connected to port 14 of a switch. The discovery diamond adjacent to the router shows that the router was discovered through both in-band and out-of-band discovery methods.

  Attached to the router is a Quantum Tape Library. Its discovery diamond shows that it was discovered only through out-of-band discovery. The out-of-band discovery was achieved because the router Ethernet port was connected to the SAN sub-network. Like the Storage Groups, fc-pdc is the only server in this SAN that can in-band manage the router.

Associating unassigned HBAs to servers

You can associate unassigned HBAs to their respective systems. To do this, you need to know in which system they reside and the HBA World Wide Node name. After you have this information, right-click anywhere in the Host Group box and select **Servers** from the pop-up menu.

Figure 134 shows the Server\HBA assignment dialog box. The left panel shows the unassigned HBAs and the right panel shows those HBAs which were assigned automatically to their servers. Once an HBA is assigned automatically, you cannot remove it from the server tree. You can add additional HBAs to the server tree, but SANavigator does not verify that the HBAs belong to that server.

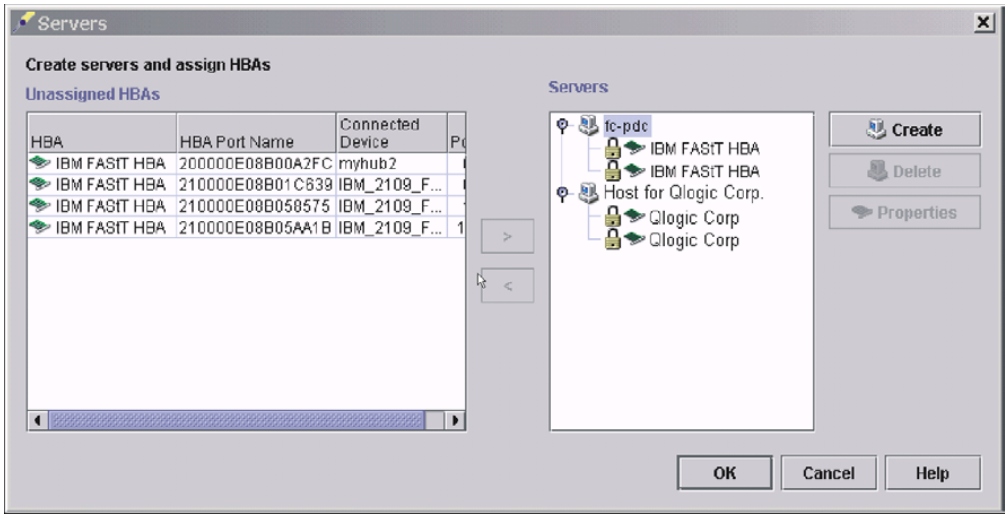


Figure 134. Server \ HBA Assignment Window

Figure 135 on page 289 shows the creation of system Node A with the correct HBAs assigned to it. This was done by clicking **Create**, typing `Node A` in the **Name** field, and then moving the appropriate HBAs to the right panel under the newly created server (select the HBAs to be moved and click the appropriate arrow).

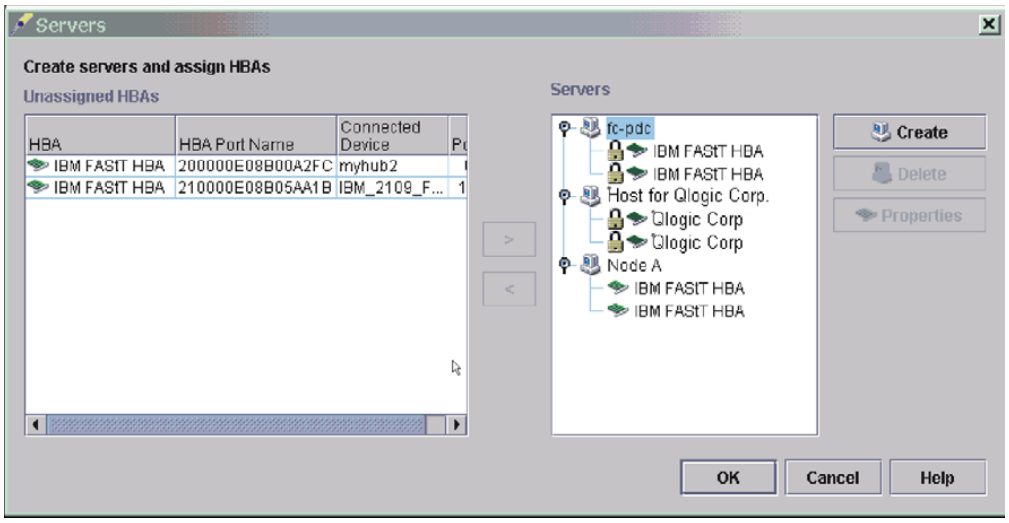


Figure 135. System Node Creation

As shown in Figure 136 on page 290, the Physical Map now displays the following three types of association:

- Server fc-pdc (associated through in-band discovery)
- Server Host For Qlogic Corp. (associated through common HBA type)
- Node A (newly created)

Additional servers can be created because not all HBAs were assigned.

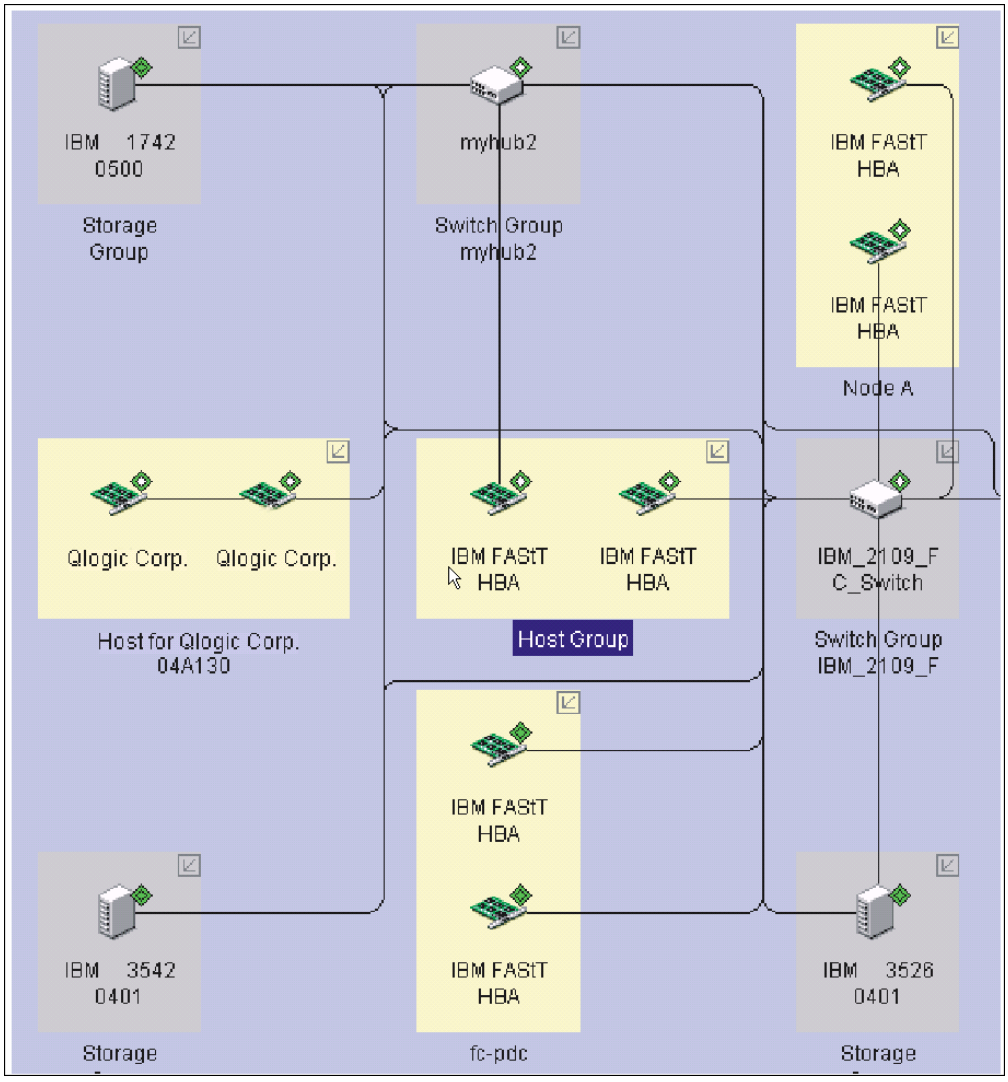


Figure 136. Physical Map Association

Displaying off-line events

Figure 137 shows an example of the SANavigator method for displaying devices that go off-line. The figure shows a FAStT Fibre Channel HBA connected to port 2 of a switch. The discovery diamond adjacent to the HBA shows that it was discovered through out-of-band (outer diamond is present).

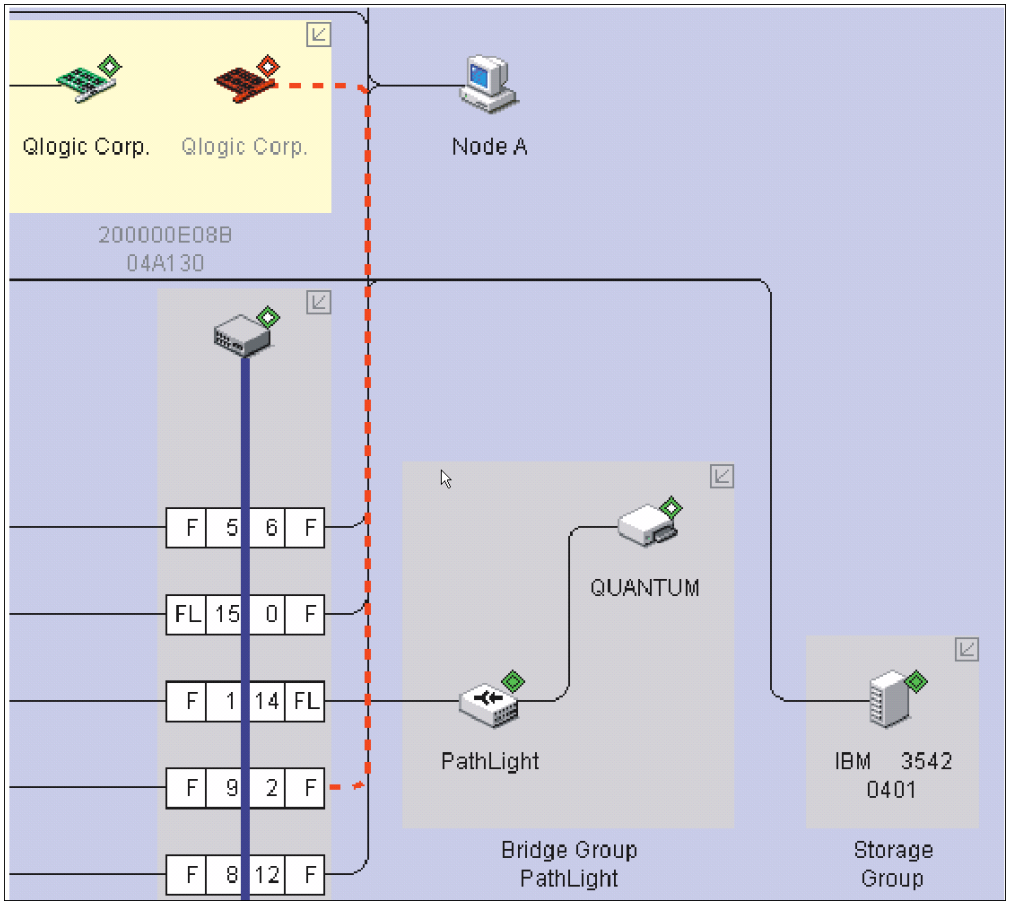


Figure 137. Offline HBA

In the scenario shown in Figure 137, a problem has occurred that caused the HBA to go off-line. Note the HBA discovery diamond. The outer diamond is red and the inner diamond is clear (indicating no in-band management). The HBA icon and the connecting line to the port are also red, indicating that there is no communication through the out-of-band network. The loss of the out-of-band connection was most likely due to a Fibre Path problem.

In this scenario, if in-band discovery had been enabled, then the HBA icon and the inner diamond would have remained green. In this case, the problem probably lies in the Fibre Path between the HBA and the switch; this can be determined because the HBA is still being in-band managed (that is, it is still responding to SCSI commands). The cause of the problem might include the HBA (fibre channel circuitry or transceivers), the cable to the switch, the GBIC for that port, the switch port, or the switch itself.

As this example shows, enabling both discovery methods increases the power of SANavigator to isolate problems. If both diamonds had turned red, the HBA would have most likely been the cause of the problem.

See “Event Log behavior” for additional information on understanding SANavigator’s discovery process.

Exporting your SAN for later viewing (Import)

Exporting a SAN is useful when SAN problems are encountered and your Technical Support organization (level 2 for example) asks you to provide them with the SAN database to facilitate troubleshooting the failure. Chapter 19, “Introduction to SANavigator”, on page 217 provides information on how to Export/Import SANs.

In addition, Export/Import is the method by which you save your SAN in version 3.x. In previous versions, SANs could be saved as SAN files (Save, Save as...). This is no longer available in 3.x.

Event Log behavior

The tables in this section describe the SANavigator Event Log and associated GUI behavior when problems are encountered relating to the Fibre Path, controllers, host bus adapters, and storage servers.

A discovery diamond is displayed adjacent to each device in the Physical Map. Figure 138 shows the discovery diamond legend.

Tag	Out-of-band	In-Band	Tag	Out-of-band	In-Band
	Present	Not Present		Present	Present
	Failed	Not Present		Present	Failed
	Not Present	Present		Failed	Present
	Not Present	Failed		Failed	Failed

Figure 138. Discovery Diamond Legend

Table 63 displays the Event Log behavior for problems involving host bus adapters.

Table 63. SANavigator Event Log Behavior matrix for host bus adapters

	If the problem is in the Fibre Path, then the indicator is ...	**If the problem is the HBA, then the indicator is ...**
Out-of-band discovery		
Event Log entries (fatal events)		
Log entry #1	HBA - Out-of-band off-line	HBA - Out-of-band off-line
Log entry #2	Concentrator port for that HBA - Connection off-line	Concentrator port for that HBA - Connection off-line
Log entry #3	HBA - Connection off-line	HBA - Connection off-line
Physical Map		
HBA outer diamond	Red	Red
HBA inner diamond	Clear (no in-band)	Clear (no in-band)
HBA connection line	Red	Red
HBA icon	Red	Red
Out-of-band and in-band discovery		
Event Log entries (fatal events)		
Log entry #1	HBA - Out-of-band off-line	HBA - Out-of-band off-line
Log entry #2	Concentrator port for that HBA - Connection off-line	Concentrator port for that HBA - Connection off-line
Log entry #3	HBA - Connection off-line	HBA - Connection off-line
Log entry #4	All devices detected by HBA - In-band off-line	HBA - In-band off-line
Log entry #5		All devices detected by HBA - In-band off-line
Log entry #6		All devices detected by HBA - Connection off-line
Physical Map		
HBA outer diamond	Red	Red
HBA inner diamond	Green	Red
HBA connection line	Red	Red
HBA icon	Normal	Red
In-band discovery*		
Event Log entries (fatal events)		
Log entry #1	All devices detected by HBA - In-band off-line	HBA - In-band off-line
Log entry #2	All devices detected by HBA - Connection off-line	HBA - Connection off-line
Log entry #3	HBA - Connection off-line (if connected to switch)	All devices detected by HBA - In-band off-line
Log entry #4		All devices detected by HBA - Connection off-line
Physical Map		

Table 63. SANavigator Event Log Behavior matrix for host bus adapters (continued)

	If the problem is in the Fibre Path, then the indicator is ...	**If the problem is the HBA, then the indicator is ...**
HBA outer diamond	Clear (no out-of-band)	Clear (no out-of-band)
HBA inner diamond	Green	Red
HBA connection line (or lines)	Red (if connected to switch)	Red
HBA icon	Normal	Red
* The HBA inner diamond remains Green (for Fibre Path problems) or Red (for bad HBAs or In-band disabled).		

Notes:

1. The log entry sequence is based on the time events were logged; your sequence might differ from this table.
2. The term *concentrator* refers to a switch or managed hub.
3. You can determine the supported and configured link speed of the HBA by looking at the HBA Properties Port tab. The Device Tip also shows this information.
4. When in-band discovery is enabled, the HBA names will be displayed as IBM FAStT HBA (for 2200 and above HBA types). If this does not occur make sure you are running the latest drivers. Otherwise, suspect that the HBA is not an IBM part number.

Table 64 displays the Event Log behavior for problems involving controllers in the Fibre Path.

Table 64. SANavigator Event Log Behavior matrix for controllers

	If the problem is in the Fibre Path to one or more (but not all) controller ports, then the indicators are ...	**If the problem is in the Fibre Path to all controller ports, or if the Storage Server is not discovered, then the indicators are ...**
Out-of-band discovery		
Event Log entries (fatal events)		
Log entry #1	Concentrator port for that controller port - Connection off-line	Concentrator ports for that Storage Server - Connection off-line
Log entry #2	Controller port - Connection off-line	Storage Server - Out-of-band off-line **Note:** Ignore Port WWN
Log entry #3		Controller ports - Connection off-line
Physical Map		
Storage Server outer diamond	Green	Red
Storage Server inner diamond	Clear (no in-band)	Clear (no in-band)
Connection	Red (for that port)	Red
Storage Server icon	Normal	Red
Out-of-band and in-band discovery		
Event Log entries (fatal events)		
Log entry #1	Concentrator port for that controller port - Connection off-line	Concentrator ports for that Storage Server - Connection off-line
Log entry #2	Controller port - Connection off-line	Controller ports - Connection off-line
Log entry #3	Controller port - In-band off-line	Storage Server - Out-of-band off-line **Note:** Ignore Port WWN
Log entry #4		Storage Server - In-band off-line **Note:** Ignore Port WWN
Physical Map		
Storage Server outer diamond	Green	Red
Storage Server inner diamond	Red	Red
Connection	Red (for that controller port)	Red
Storage Server icon	Normal	Red
In-band discovery*		
Event Log entries (fatal events)		
Log entry #1	Controller Port - Connection off-line	Controller Ports - Connection off-line
Log entry #2	Controller Port - In-band off-line **Note:** Ignore Port WWN	Storage Server - In-band off-line **Note:** Ignore Port WWN
Log entry #3	HBA - Connection off-line (if direct connect to HBA)	
Physical Map		
Storage Server outer diamond	Clear (no out-of-band)	Clear (no out-of-band)
Storage Server inner diamond	Red	Red

Table 64. SANavigator Event Log Behavior matrix for controllers (continued)

	If the problem is in the Fibre Path to one or more (but not all) controller ports, then the indicators are ...	**If the problem is in the Fibre Path to all controller ports, or if the Storage Server is not discovered, then the indicators are ...**
Connection	Red (port to loop)	Red (all ports to loop)
Storage Server icon	Normal	Red
* Devices that are in-band discovered have the inner diamond red. The inner diamond of the HBA that is connected to its respective controller port (or ports if connected to an unmanaged hub) remains Green (for Fibre Path problems) or Red (for bad HBAs or In-band disabled). See Table 63 on page 293.		
Notes: 1. The log entry sequence is based on the time events were logged; your sequence might differ from this table. 2. The term *concentrator* refers to a switch or managed hub.		

Table 65 displays the Event Log behavior for problems involving SAN Data Gateway Routers.

Table 65. SANavigator Event Log Behavior matrix for SAN Data Gateway Routers

	If the problem is in the Fibre Path, then the indicators are ...	**If the problem is in the Ethernet connection to SDG, then the indicators are ...**
Out-of-band discovery (Ethernet connection to Concentrator only)		
Event Log entries (fatal events)		
Log entry #1	SDG - Out-of-band off-line	N/A
Log entry #2	Concentrator port - Connection off-line	N/A
Log entry #3	SDG - Connection off-line	N/A
Physical Map		
SDG outer diamond	Red	N/A
SDG inner diamond	Clear (no in-band)	N/A
Connection	Red	N/A
SDG icon	Red	N/A
Out-of-band discovery (Ethernet connection to SDG and Concentrator)		
Event Log entries (fatal events)		
Log entry #1	SDG - Connection off-line	SDG - Out-of-band off-line
Log entry #2	Concentrator port - Connection off-line	Tape device - Out-of-band off-line
Log entry #3		Tape device - Connection off-line
Log entry #4		SDG - Connection off-line
Physical Map		
SDG outer diamond	Green	Red
SDG inner diamond	Clear	Clear
Concentrator-to-SDG connection	Red	Normal
SDG-to-Tape connection	Normal	Red
SDG icon	Normal	Normal
Tape device outer diamond	Green	Red
Tape device inner diamond	Clear (no in-band)	Clear (no in-band)
Tape device icon	Normal	Red
Out-of-band and in-band discovery (Ethernet connection to Concentrator only)		
Event Log entries (fatal events)		
Log entry #1	SDG - Out-of-band off-line	N/A
Log entry #2	Concentrator port - Connection off-line	N/A

Table 65. SANavigator Event Log Behavior matrix for SAN Data Gateway Routers (continued)

	If the problem is in the Fibre Path, then the indicators are ...	**If the problem is in the Ethernet connection to SDG, then the indicators are ...**
Log entry #3	SDG - Connection off-line	N/A
Log entry #4	SDG - In-band off-line	N/A
Physical Map		
SDG outer diamond	Red	N/A
SDG inner diamond	Red	N/A
Connection	Red	N/A
SDG icon	Red	N/A
Out-of-band and in-band discovery (Ethernet connection to SDG and Concentrator)		
Event Log entries (fatal events)		
Log entry #1	SDG - Connection off-line	SDG - Out-of-band off-line
Log entry #2	Concentrator port - Connection off-line	Tape device - Out-of-band off-line
Log entry #3	SDG - In-band off-line	Tape device - Connection off-line
Log entry #4		SDG - Connection off-line
Physical Map		
SDG outer diamond	Green	Red
SDG inner diamond	Red	Green
Concentrator-to-SDG connection	Red	Normal
SDG-to-Tape connection	Normal	Red
SDG icon	Normal	Normal
Tape device outer diamond	Green	Red
Tape device inner diamond	Clear	Clear
Tape device icon	Normal	Red

Notes:

1. It is not necessary for the SAN Data Gateway (SDG) unit to be connected to the network for it to be discovered by SANavigator. However, if the SDG is not connected to the network, SANavigator will not be able to detect devices attached to the SDG. The devices attached to the SDG are only discovered through the out-of-band method (Ethernet cable plugged to the SDG)
2. The log entry sequence is based on the time events were logged; your sequence might differ from this table.
3. The term *concentrator* refers to a switch or managed hub.

Table 66 describes the conventions for naming FAStT Storage Server ports.

Table 66. FAStT Storage Server Port Naming Convention

Machine Type	Number of Ports	SANavigator Port Naming	Algorithm	Example
3526, 3542	2	A, B	Port A: Last character of the node WWN + 1 Port B: Fourth and last character of the node WWN +1	Node: 20-00-00-A0-B8-06-16-36 Port: 20-00-00-A0-B8-06-16-37 Node: 20-00-00-A0-B8-06-16-36 Port: 20-01-00-A0-B8-06-16-37
3552, 1742	4	A1, B1,A2, B2 (**Note:** The following figure shows the physical locations of these ports.)	Port A1: Last character of the node WWN + 1 Port B1: Fourth and last character of the node WWN +1 Port A2: Last character of the node WWN + 2 Port B2: Fourth character of the node WWN+1 and last character of the node WWN+2	Node: 20-26-00-A0-B8-06-61-98 Port: 20-26-00-A0-B8-06-61-99 Node: 20-26-00-A0-B8-06-61-98 Port: 20-27-00-A0-B8-06-61-99 Node: 20-26-00-A0-B8-06-61-98 Port: 20-26-00-A0-B8-06-61-9A Node: 20-26-00-A0-B8-06-61-98 Port: 20-27-00-A0-B8-06-61-9A

Figure 139 shows the physical locations of the ports described in Table 66.

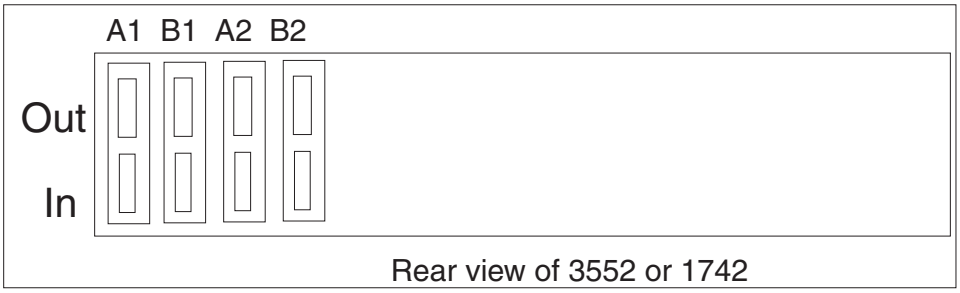


Figure 139. Rear View of 3552 or 1742

Setting up SANavigator Remote Discovery Connection for in-band management of remote hosts

Remote Discovery Connection

In order for Remote Discovery Connection (RDC) to function, install the Remote Discovery Connector on the host that you want to In-band manage remotely. The following modifications to the Deployment Property file on the local machine are required to enable RDC.

Navigate to `$\Program Files\SANavigator3.1\resources\Server` and edit the file Deployment.Properties:

1. Comment out the first two sets of ″com.sanavigator″ and enable the third set, as shown below:
   - Set 1

     ```
     # Use this for conventional discovery by the server
     #com.sanavigator.plugsnpeers.plugs.IContainer = \
     #com.sanavigator.server.plugdiscovery.ClassicDiscoveryContainer
     ```

   - Set 2

     ```
     # Use this for discovery by all peers (remove the # comment char from the
     # next 2 lines, delete or comment the lines above!)
     #com.sanavigator.plugsnpeers.plugs.IContainer = \
     #com.sanavigator.plugsnpeers.peers.rmi.Peer
     ```

   - Set 3

     ```
     # Use this for discovery by server and all peers (remove the # comment char
     # from the next 3 lines, delete or comment the first lines above!)
     com.sanavigator.plugsnpeers.plugs.IContainer = \
     com.sanavigator.server.plugdiscovery.ClassicDiscoveryContainer;\
     com.sanavigator.plugsnpeers.peers.rmi.Peer
     ```

2. You should update the peer (Peer.Properties) file whenever a peer is providing remote discovery information and is not discovered via a broadcast discovery on the default subnet.

   Navigate to `$\Program Files\SANavigator3.1\resources\Server` and edit the file `Peers.Properties. Scroll` about half-way down the file to the section listed below:

   ```
   # Who you gonna call? (in addition to broadcast)
   # HOST:PORT separated by semi-colons
   # Example: PeerAddresses=172.23.2.2:333;fred.sanavigator.com
   PeerAddresses =
   Add each remote peer IP address as follows:
   PeerAddresses=172.31.1.3;172.31.3.5
   ```

   You can also enter the server name followed by the domain as shown above as: `fred.sanavigator.com`. This is just an alternate method to enter the IP addresses.

Configuring Only Peers to Discover (not recommended)

This method will accept in-band and out-of-band discovery information from remote peers only. HBAs in the local server will not be displayed in the Discover Setup dialog box. Out-of-band discovery can still be performed using the local server. The peer file also needs to be updated for peers not discovered via the broadcast method.

Caution: This configuration is not recommended. The local server should be allowed to perform discovery as well.

1. Navigate to `$\Program Files\SANavigator3.1\resources\Server` and edit the file

   `Deployment.Properties`

2. Comment out Set 1 and Set 3 and enable Set 2
   - Set 1

     ```
     # Use this for conventional discovery by the server
     #com.sanavigator.plugsnpeers.plugs.IContainer = \
     #com.sanavigator.server.plugdiscovery.ClassicDiscoveryContainer
     ```

   - Set 2

     ```
     # Use this for discovery by all peers (remove the # comment char from the
     # next 2 lines, delete or comment the lines above!)
     com.sanavigator.plugsnpeers.plugs.IContainer = \
     com.sanavigator.plugsnpeers.peers.rmi.Peer
     ```

   - Set 3

     ```
     # Use this for discovery by server and all peers (remove the # comment char
     # from the next 3 lines, delete or comment the first lines above!)
     #com.sanavigator.plugsnpeers.plugs.IContainer = \
     #com.sanavigator.server.plugdiscovery.ClassicDiscoveryContainer;\
     #com.sanavigator.plugsnpeers.peers.rmi.Peer
     ```

Controller diagnostics

The latest versions of the Storage Manager (7.2 and 8.x) include controller diagnostics. The Diagnostics option enables a user to verify that a controller is functioning properly, using various internal tests. One controller is designated as the Controller Initiating the Test (CIT). The other controller is the Controller Under Test (CUT).

The diagnostics use a combination of three different tests: Read Test, Write Test, and Data Loopback Test. You should run all three tests at initial installation and any time there are changes to the storage subsystem or components that are connected to the storage subsystem (such as hubs, switches, and host adapters).

Note: During the diagnostics, the controller on which the tests are run (CUT) will NOT be available for I/O.

- **Read Test**

  The Read Test initiates a read command as it would be sent over an I/O data path. It compares data with a known, specific data pattern, checking for data integrity and redundancy errors. If the read command is unsuccessful or the data compared is not correct, the controller is considered to be in error and is failed.

- **Write Test**

  A Write Test initiates a write command as it would be sent over an I/O data path (to the Diagnostics region on a specified drive). This Diagnostics region is then read and compared to a specific data pattern. If the write fails or the data compared is not correct, the controller is considered to be in error and is failed and placed off-line. (Use the Recovery Guru to replace the controller.)

- **Data Loopback Test**

  Important: The Data Loopback Test does not run on controllers that have SCSI connections between the controllers and drive (model 3526).

  The Data Loopback Test is run only on controllers that have fibre channel connections between the controller and the drives. The test passes data through each controller's drive-side channel, mini hub, out onto the loop and then back

again. Enough data is transferred to determine error conditions on the channel. If the test fails on any channel, then this status is saved so that it can be returned if all other tests pass.

All test results are displayed in the Diagnostics dialog box status area.

Events are written to the Storage Manager Event Log when diagnostics is started, and when it is has completed testing. These events will help you to evaluate whether diagnostics testing was successful or failed, and the reason for the failure. To view the Event Log, click **View -> Event Log** from the Subsystem Management Window.

Running controller diagnostics

Important: If diagnostics are run while a host is using the logical drives owned by the selected controller, the I/O directed to this controller path is rejected.

Click **Controller -> Run Diagnostics** to run various internal tests to verify that a controller is functioning properly.

1. From the Subsystem Management Window, highlight a controller. Then, either click **Controller -> Run Diagnostics** from the main menu or right-click the controller and click **Run Diagnostics** from the pop-up menu. The Diagnostics dialog box is displayed.
2. Select the check boxes for the diagnostic tests to be run. Choose from the following:
   - Read Test
   - Write Test
   - Data Loopback Test
3. To run the Data Loopback Test on a single channel, select a channel from the drop- down list.
4. Select a Data Pattern file for the Data Loopback Test. Select **Use Default Data Pattern** to use the default Data Pattern or **Use Custom Data Pattern file** to specify another file.

   Note: A custom Data Pattern file called diagnosticsDataPattern.dpf is provided on the root directory of the Storage Manager folder. This file can be modified, but the file must have the following properties to work correctly for the test:
   - The file values must be entered in hexadecimal format (00 to FF) with one space ONLY between the values.
   - The file must be no larger than 64 bytes in size. (Smaller files will work but larger files will cause an error.)
5. Click the **Run** button. The Run Diagnostics confirmation dialog box is displayed.
6. Type yes in the text box, and then click **OK**.

   The selected diagnostic tests begin. When the tests are complete, the Status text box is updated with test results. The test results contain a generic, overall status message, and a set of specific test results. Each test result contains the following information:
   - Test (Read/Write/Data Loopback)
   - Port (Read/Write)
   - Level (Internal/External)
   - Status (Pass/Fail)

7. Click **Close** to exit the dialog box.

   Important: When diagnostics are completed, the controller should automatically allow data to be transferred to it. However, if there is a situation where data transfer is not re-enabled, highlight the controller and click **Data Transfer -> Enable**.

Linux port configuration

Linux operating systems do not currently make use of the IBM FAStT Storage Manager to configure their associated Storage Subsystems. Instead, use FAStT MSJ to perform Device and LUN configuration on Linux operating systems. However, the Storage Manager is used to map the FAStT storage servers' logical drives to the appropriate operating system (in this case, Linux). The following sections provide you with hints on how to correctly configure your storage for the Linux operating system.

FAStT Storage Manager hints

Use the Storage Manager to map the desired logical drives to Linux storage. Refer to the *Storage Manager User's Guide* for instructions. Note the following:

- Host ports for the Linux host are defined as Linux. See Chapter 29, "Heterogeneous configurations", on page 331 for more information.
- The Access LUN (LUN 31, also called the UTM LUN) is not present. FAStT MSJ will typically display the following messages when attempting to configure the storage and LUN 31 is detected:
  - `An invalid device and LUN configuration has been detected`
  - `Non-SPIFFI compliant device(s) have been separated (by port names)`

    Note: The Device node name (FAStT Storage Server World Wide Node name) should appear once in the FAStT MSJ Fibre Channel Port Configuration dialog (see the figure following Step 5 on page 304) for both device ports. The Device port names reflect the FAStT Storage Server controller Port World Wide Node names. If the Device node name is split (that is, if the Device node name is shown once for each Port name), then an invalid configuration is present. Check the storage mapping once more using the FAStT Storage Manager.
- LUNs are sequential and start with LUN 0.
- Prior to configuration, all LUNs are assigned to the controller that is attached to the first HBA.
- Both storage controllers must be active. Failover is only supported in an ACTIVE/ACTIVE mode.

Linux system hints

After you have properly mapped the storage, you will also need to configure the Linux host. Refer to the HBA driver README file for instructions on how to configure the driver to allow for Failover support.

Make sure the HBAs that are installed in your systems are of the same type and are listed in the modules.conf file in the /etc/ directory. Add the following options string to allow more than 1 LUN to be reported by the driver:

```
options scsi_mod max_scsi_luns=32
```

This is what you might see in the modules.conf file:

```
alias eth1 eepro100
alias scsi_hostadapter aic7xxx
alias scsi_hostadapter1 qla2200
alias scsi_hostadapter2 qla2200
options scsi_mod max_scsi_luns=32
```

FAStT MSJ

FAStT MSJ is used to configure the driver for failover. See Chapter 18, “Introduction to FAStT MSJ”, on page 173 for installation instructions and to familiarize yourself with this application.

Configuring the driver with FAStT MSJ

To configure the driver, launch FAStT MSJ and do the following:

1. Open a new command window and type `qlremote`; then press Enter. This will run qlremote agent in this command window.
2. Open a new command window and run /usr./FAStT_MSJ
3. Select CONNECT.
4. Enter the IP address of the server or select LOCALHOST.
5. Select CONFIGURE. You will then be presented with the Fibre Channel Port Configuration dialog (see Figure 140).

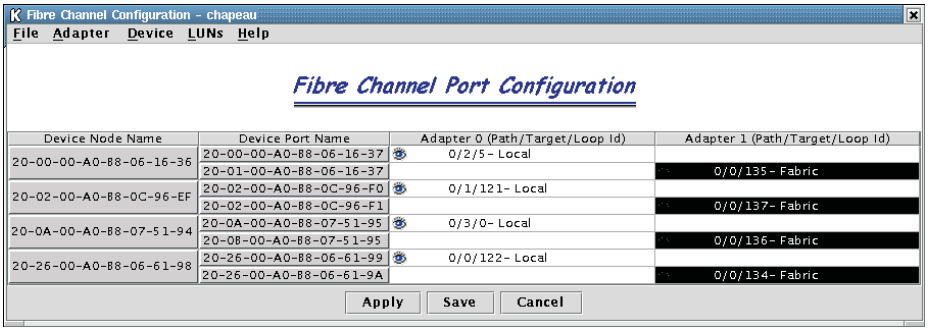


Figure 140. Fibre Channel Port Configuration

6. Right-click the Device node name.
7. Click **Configure LUNs**. The LUN Configuration window opens (see Figure 141).

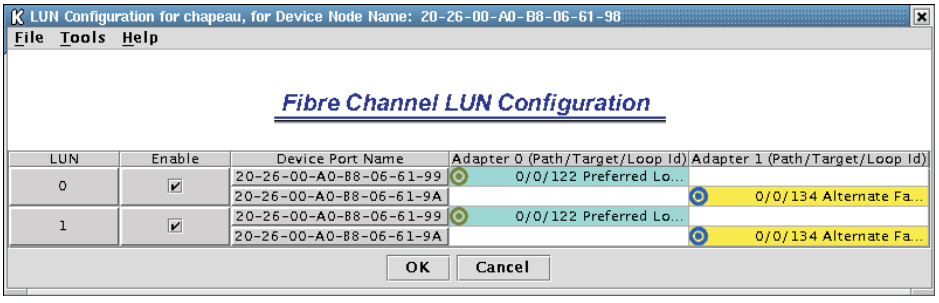


Figure 141. LUN Configuration

8. Click **Tools -> Automatic Configuration**.
9. Click **Tools -> Load Balance**.

Your configuration should then look similar to Figure 142, which shows the preferred and alternate paths alternating between the adapters.

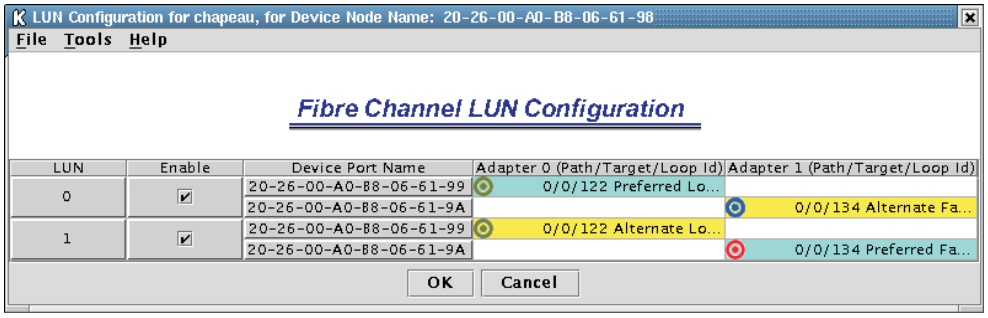


Figure 142. Preferred and Alternate Paths Between Adapters

10. Click **OK**.
11. Click **Apply** or **Save**.
12. This will save the configuration into the etc/modules.conf file. Verify that the option string reflecting the new configuration was written to that file. The string should look like this:

```
options qla2300 ConfigRequired=1 ql2xopts=scsi-qla00-adapter
port=210000e08b05e875\;scsi-qla00-tgt-000-di-00-node=202600a0b8066198\;scsi-
qla00-tgt-000-di-00-port=202600a0b8066199\;scsi-qla00-tgt-000-di-00-
preferred=ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffd\;scsi
-qla00-tgt-000-di-00-control=00\;scsi-qla00-tgt-001-di-00-
node=200200a0b80c96ef\;scsi-qla00-tgt-001-di-00-port=200200a0b80c96f0\;scsi-
qla00-tgt-001-di-00-
preferred=ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff\;scsi
-qla00-tgt-001-di-00-control=00\;scsi-qla00-tgt-002-di-00-
node=200000a0b8061636\;scsi-qla00-tgt-002-di-00-port=200000a0b8061637\;scsi-
qla00-tgt-002-di-00-
preferred=ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff\;scsi
-qla00-tgt-002-di-00-control=00\;scsi-qla00-tgt-003-di-00-
node=200a00a0b8075194\;scsi-qla00-tgt-003-di-00-port=200a00a0b8075195\;scsi-
qla00-tgt-003-di-00-
preferred=ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff\;scsi
-qla00-tgt-003-di-00-control=00\;scsi-qla01-adapter-port=210000e08b058275\;scsi-
qla01-tgt-001-di-01-node=200200a0b80c96ef\;scsi-qla01-tgt-001-di-01-
port=200200a0b80c96f1\;scsi-qla01-tgt-001-di-01-control=80\;scsi-qla01-tgt-003-
di-01-node=200a00a0b8075194\;scsi-qla01-tgt-003-di-01-
port=200b00a0b8075195\;scsi-qla01-tgt-003-di-01-control=80\;scsi-qla01-tgt-002-
di-01-node=200000a0b8061636\;scsi-qla01-tgt-002-di-01-
port=200100a0b8061637\;scsi-qla01-tgt-002-di-01-control=80\;scsi-qla01-tgt-000-
di-01-node=202600a0b8066198\;scsi-qla01-tgt-000-di-01-
port=202600a0b806619a\;scsi-qla01-tgt-000-di-01-
preferred=0000000000000000000000000000000000000000000000000000000000000002\;scsi
-qla01-tgt-000-di-01-control=80\;
```

FAStT MSJ Hints

Following are hints for using FAStT MSJ to configure Linux ports:

- FAStT MSJ does not automatically launch the agent qlremote. If you are unable to connect the host or hosts, make sure that you have started qlremote.
- Any time a change is made to your storage (for example, if LUNs are added or removed), you must kill qlremote (Ctrl + C), unload your HBA driver, and then re-load it.
  - To unload: modprobe -r qla2x00
  - To load: modprobe qla2x00
  - To restart: qlremote

You will then need to run FAStT MSJ to perform failover configuration.

- Do not mix HBA types. For example, qla2200 must be matched with another qla2200.
- If you replace an HBA, make sure you change the mapping in the FAStT Storage Manager to point to the WWN name for the new adapter. You will then need to reconfigure your storage.

Chapter 26. PD hints — Drive side hints and RLS Diagnostics

You should be referred to this chapter from a PD map or indication. If this is not the case, refer back to Chapter 16, “Problem determination starting points”, on page 131.

This chapter contains hints in the following PD areas:

- “Drive side hints”
- “Read Link Status (RLS) Diagnostics” on page 316

Drive side hints

When there is a drive side (device side) issue, looking at SM often helps to isolate the problem. Figure 143 shows the status of drive enclosures attached to the RAID controller unit. Notice that the windows show that enclosure path redundancy is lost. This is an indication that a path problem exists between the controllers and one or more drive enclosures.

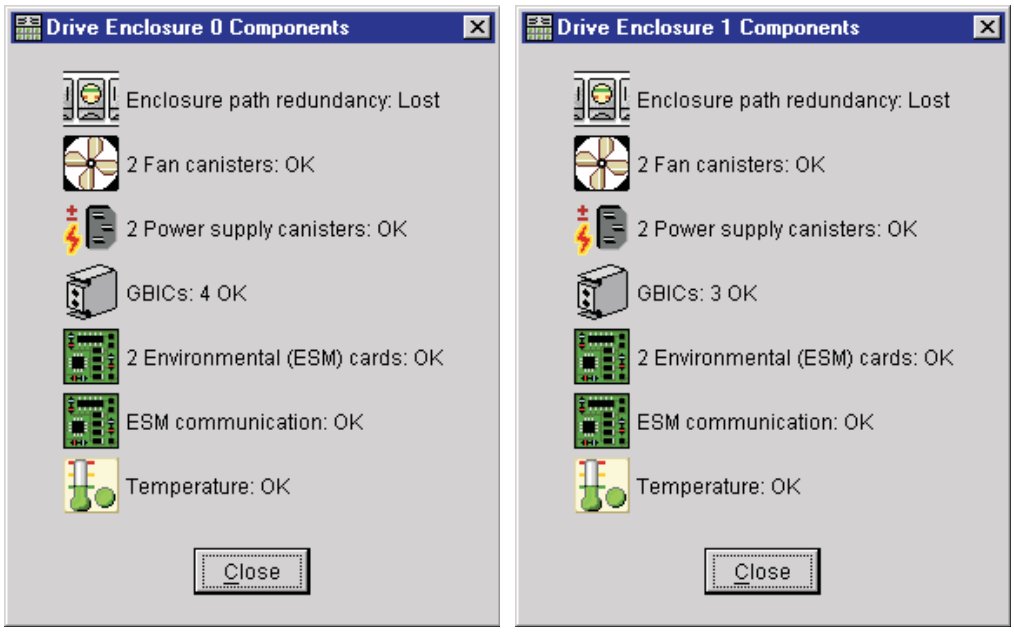


Figure 144 on page 308 shows that an ESM has failed.

Figure 143. Drive Enclosure Components

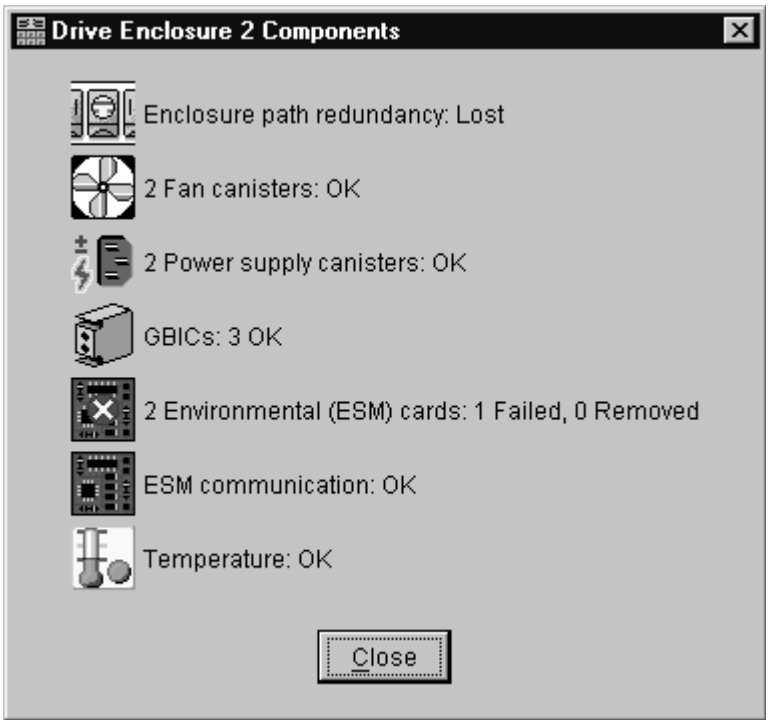


Figure 144. Drive Enclosure Components - ESM Failure

When an ESM has failed, go to the Recovery Guru for suggestions on resolving the problem. See Figure 145 on page 309.

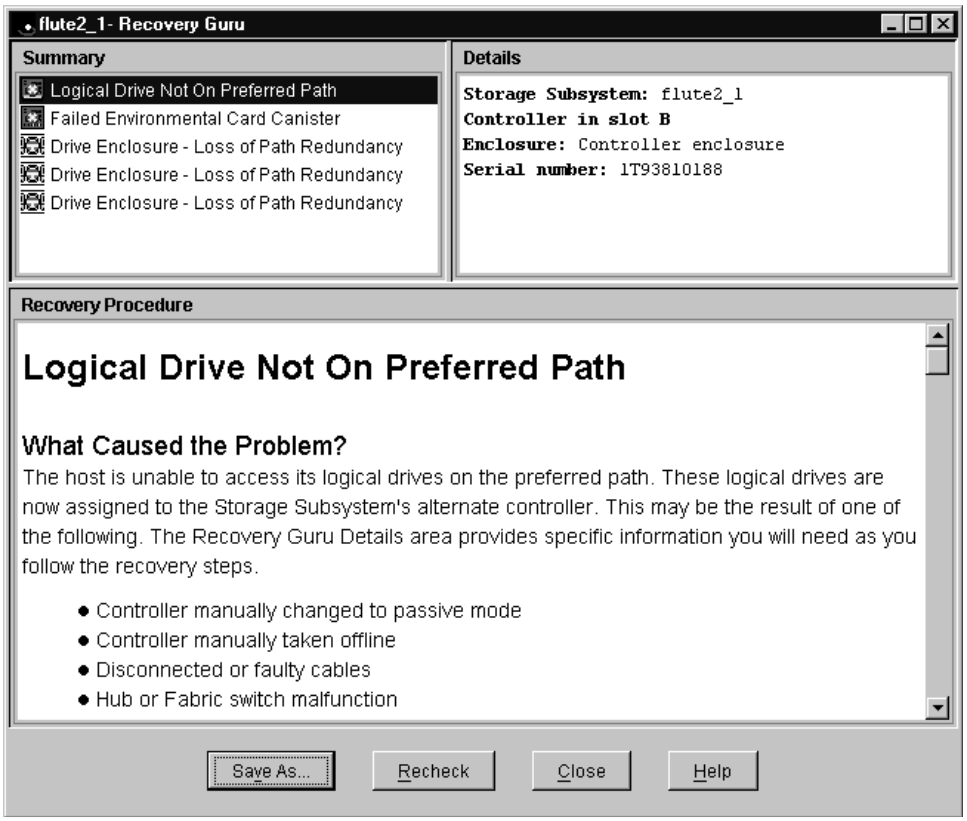


Figure 145. Recovery Guru

In the Recovery Guru window, the message `Logical drive not on preferred path` does not necessarily pertain to the current problem. The drive could have been moved to the other controller and not moved back. The loss of redundancy and the failed ESM are what is important.

Note: Figure 146 on page 310 also shows the message `Failed or Removed Power Supply Cannister`. However, this message is not significant here because the power supply was removed for purposes of illustration.

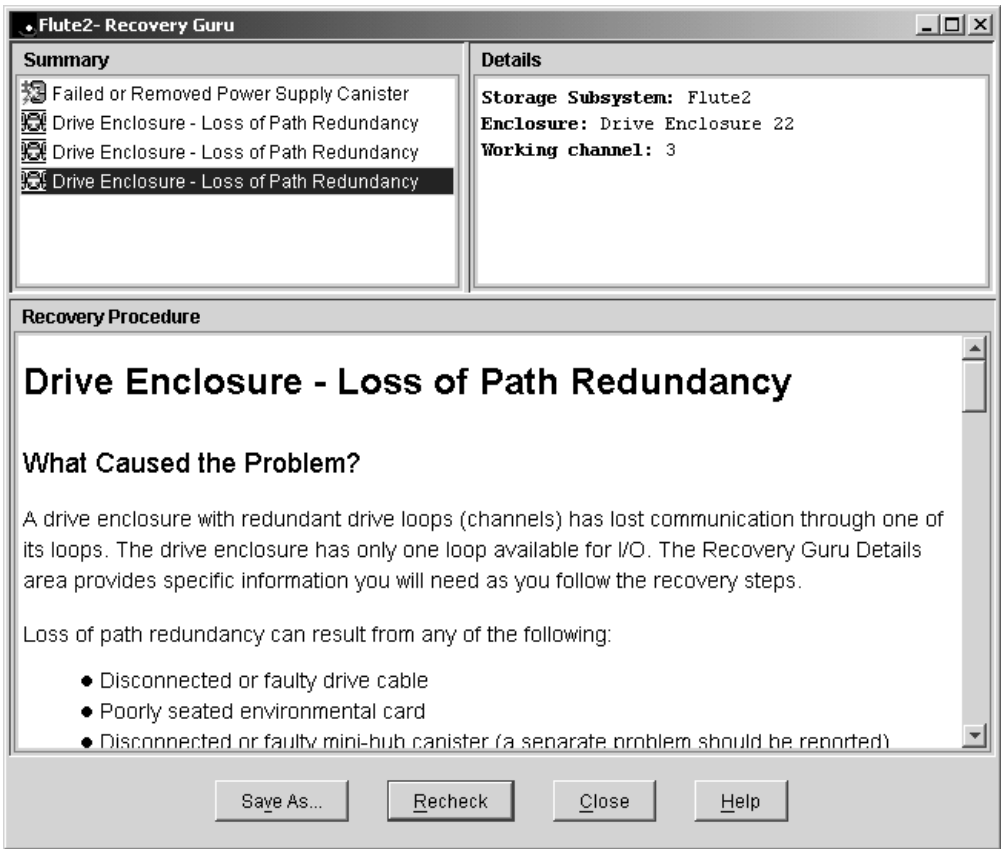


Figure 146. Recovery Guru - Loss of Path Redundancy

Use the following indicators for drive side problems.

- **FAStT200:**
  - Fault light per controller (1 on single controller model and 2 on redundant)
  - Loop bypass per controller (1 or 2)
  - Link status per GBIC port (2) per controller (2 or 4)
- **FAStT500 or FAStT700: (mini hubs)**
  - Fault
  - Loop bypass
  - Link status
- **EXP500:**
  - Fault per ESM (2)
  - Loop bypass per GBIC port per ESM (4)
  - Link status per ESM (2)

Troubleshooting the drive side

Always ensure that you are working on the loop side that is no longer active. Unplugging devices in a loop that is still being used by the host can cause loss of access to data.

To troubleshoot a problem in the drive side, use the following procedure:

1. Disconnect the cable from the loop element that has the bypass indicator light on. See Figure 147.

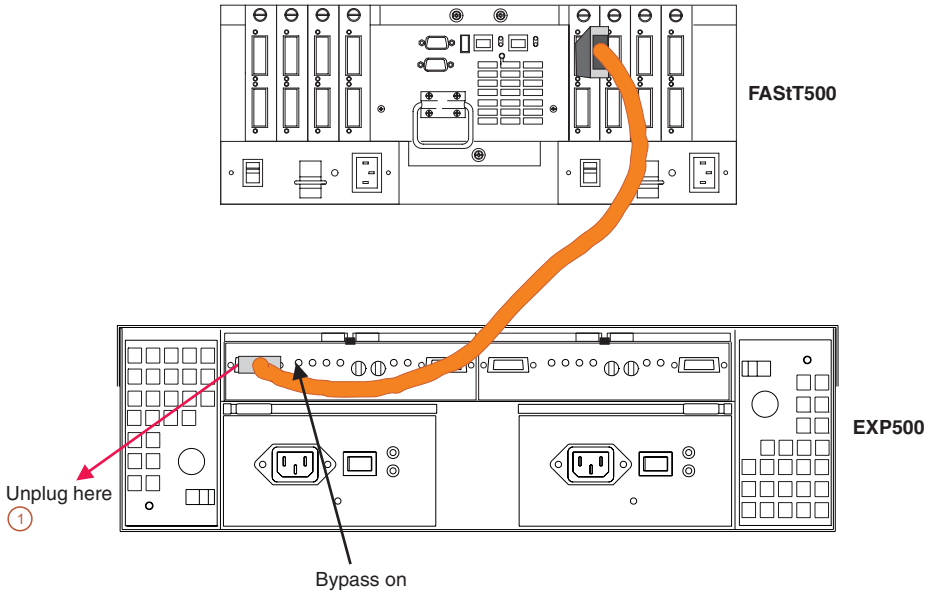


Figure 147. Disconnect Cable from Loop Element

2. Insert a wrap plug in the element from which you disconnected the cable. See Figure 148.
   a. Is the bypass light still on? Replace the element (for example, a GBIC). The procedure is complete.

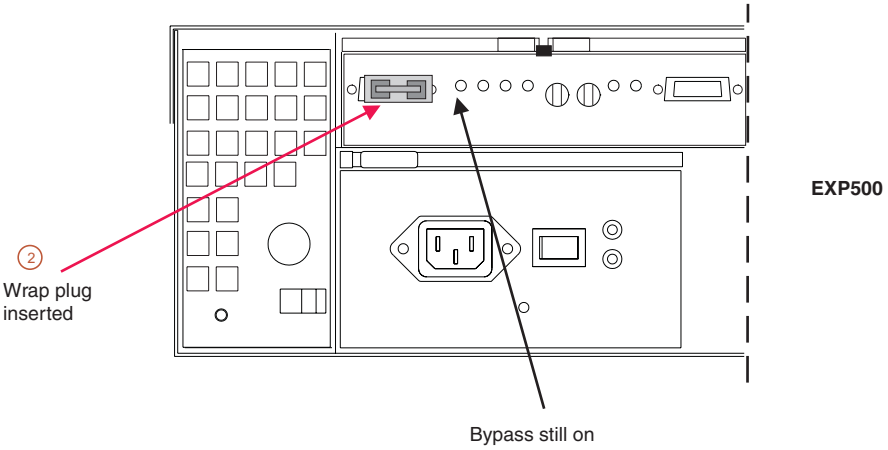


Figure 148. Insert Wrap Plug

   b. If the bypass light is now out, then this element is not the problem. Continue with step 3.
3. Reinsert the cable. Then unplug the cable at the other end.
4. Insert a wrap plug with an adapter onto the cable end. See Figure 149 on page 312.
   a. Is the bypass light still on? Replace the cable. The procedure is complete.

b. If the bypass light is now out, then this element is not the problem. Continue with step 5.

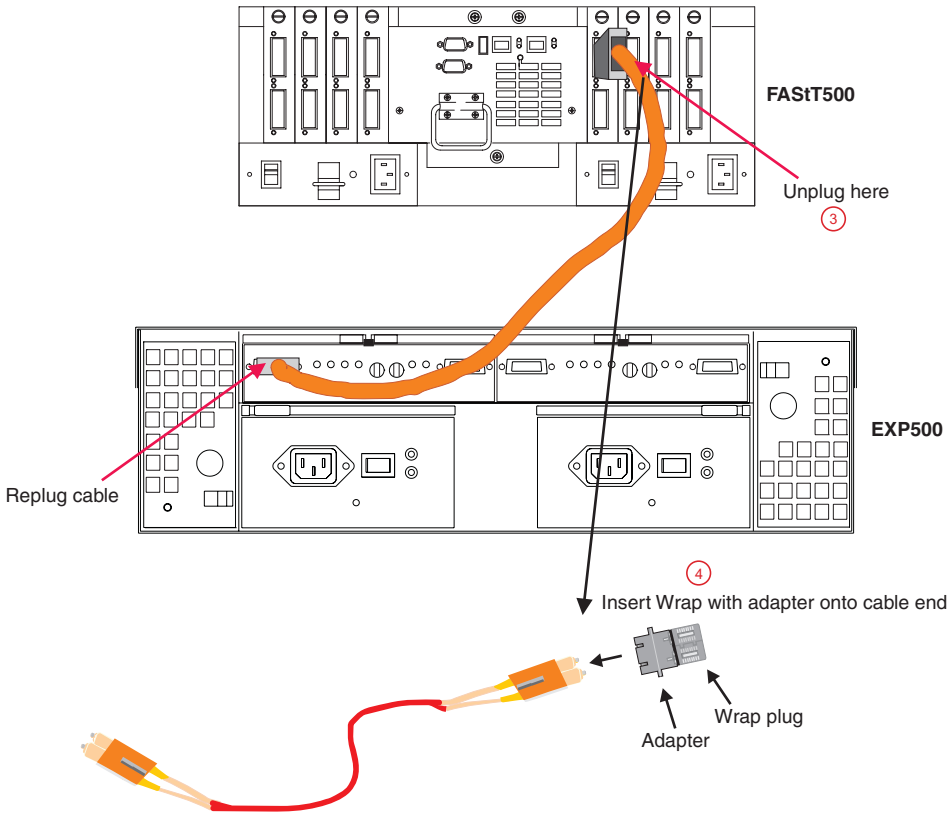


Figure 149. Insert Wrap with Adapter on Cable End

5. As was shown in step 4, insert the wrap plug into the element from which the cable was removed in step 3. See Figure 150 on page 313.
   a. Is the bypass light still on? Replace the element (for example, a GBIC). The procedure is complete.
   b. If the bypass light is now out, then this element is not the problem. In this fashion, keep moving through the loop until everything is replugged or until there are no more bypass or link down conditions.

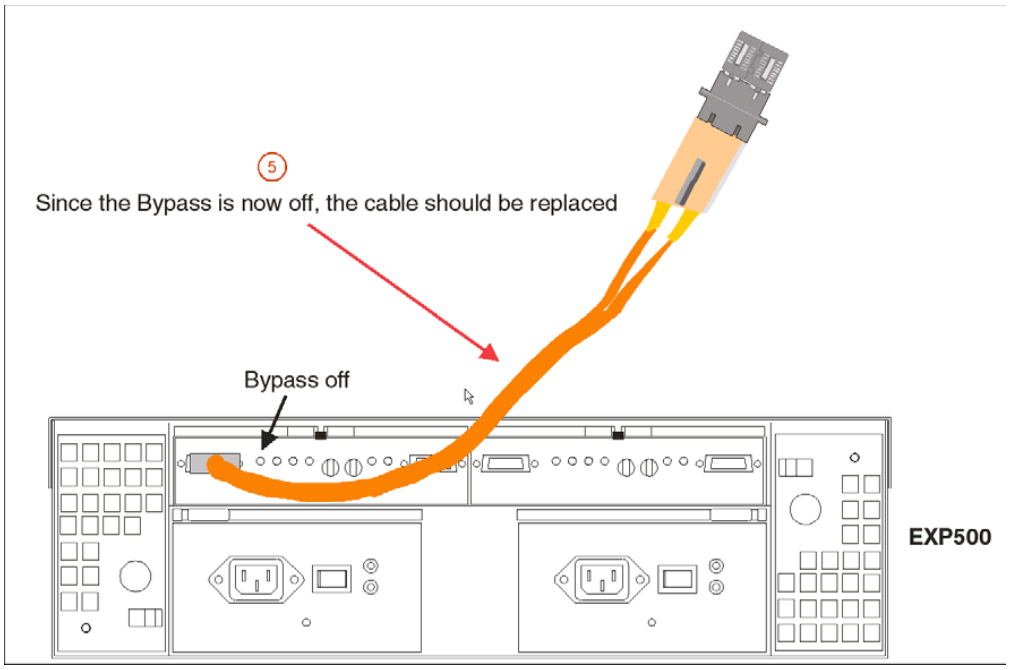


Figure 150. Insert Wrap Plug into Element

Indicator lights and problem indications

The following figures show the indicator lights for each unit on the device side (for the mini hub, the host side is also shown). The table following each figure shows the normal and problem indications.

FAStT500 RAID controller

Figure 151 on page 314 shows the mini hub indicator lights for the FAStT500 RAID controller.

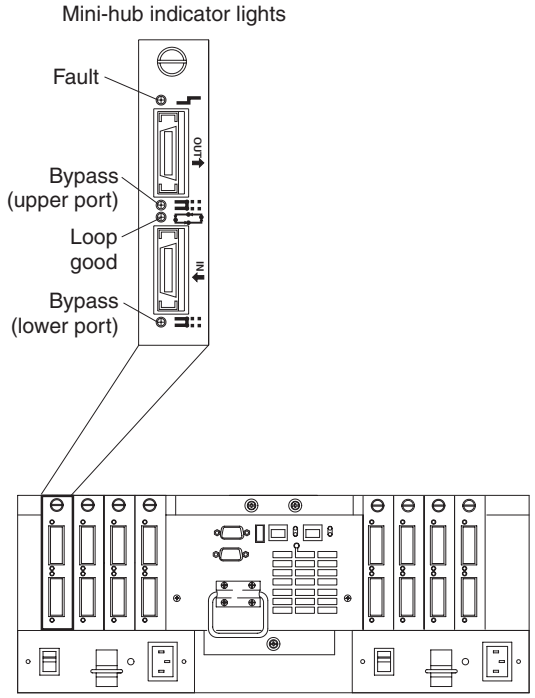


Figure 151. FAStT500 RAID Controller Mini Hub Indicator Lights

Table 67. FAStT500 mini hub indicator lights

Icon	Indicator Light	Color	Normal Operation	Problem Indicator	Possible condition indicated by the problem indicator
	Fault	Amber	Off	On	Mini hub or GBIC has failed. **Note:** If a host-side mini hub is not connected to a controller, this fault light is always on.
	Bypass (upper port)	Amber	Off	On	• Upper mini hub port is bypassed • Mini hub or GBIC has failed, is loose, or is missing • Fiber-optic cables are damaged **Note:** If the port is unoccupied, the light is on.
	Loop good	Green	On	Off	• The loop is not operational • Mini hub has failed or a faulty device might be connected to the mini hub • Controller has failed **Note:** If a host-side mini hub is not connected to a controller, the green light is always off and the fault light is always on.
	Bypass (lower port)	Amber	Off	On	• Lower mini hub port is bypassed • Mini hub or GBIC has failed, is loose, or is missing • Fiber-optic cables are damaged **Note:** If the port is unoccupied, the light is on.

FAStT EXP500 ESM

Figure 152 shows the indicator lights for the FAStT EXP500 ESM.

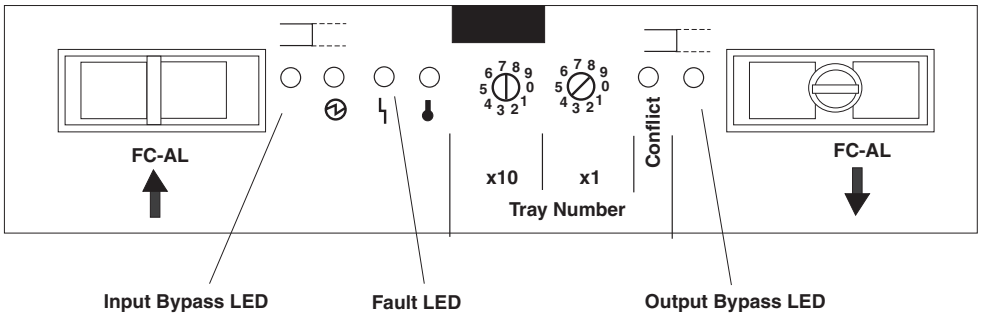


Figure 152. FAStT EXP500 ESM Indicator Lights

Table 68. EXP500 ESM indicator lights

Icon	Indicator Light	Color	Normal Operation	Problem Indicator	Possible condition indicated by the problem indicator
	Fault	Amber	Off	On	ESM failure **Note:** If fault is on, both In and Out should be in bypass.
	Input Bypass	Amber	Off	On	Port empty • Mini hub or GBIC has failed, is loose, or is missing • Fiber-optic cables are damaged • No incoming signal detected
	Output Bypass	Amber	Off	On	• Port empty • Mini hub or GBIC has failed, is loose, or is missing • Fiber-optic cables are damaged • No incoming signal detected, is loose, or is missing

FAStT200 RAID controller

Figure 153 on page 316 shows the controller indicator lights for a FAStT200 controller.

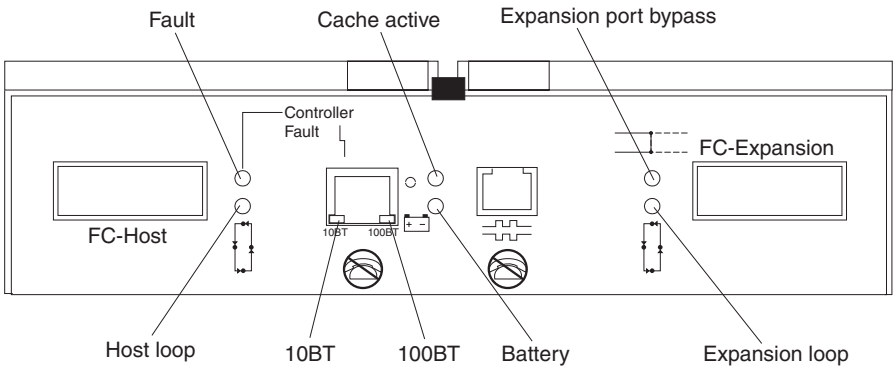


Figure 153. FAStT200 Controller Indicator Lights

Table 69. FAStT200 controller indicator lights

Icon	Indicator Light	Color	Normal Operation	Problem Indicator	Possible condition indicated by the problem indicator
	Fault	Amber	Off	On	The RAID controller has failed
	Host Loop	Green	On	Off	• The host loop is down, not turned on, or not connected • GBIC has failed, is loose, or not occupied • The RAID controller circuitry has failed or the RAID controller has no power.
	Expansion Loop	Green	On	Off	The RAID controller circuitry has failed or the RAID controller has no power.
	Expansion Port Bypass	Amber	Off	On	• Expansion port not occupied • FC cable not attached to an expansion unit • Attached expansion unit not turned on • GBIC has failed, FC cable or GBIC has failed in attached expansion unit

Read Link Status (RLS) Diagnostics

A fibre channel loop is an interconnection topology used to connect storage subsystem components and devices. The IBM FAStT Storage Manager (version 8.x) software uses the connection between the host machine and each controller in the storage subsystem to communicate with each component and device on the loop.

During communication between devices, Read Link Status (RLS) error counts are detected within the traffic flow of the loop. Error count information is accumulated over a period of time for every component and device including:

- Drives
- ESMs
- Fibre channel ports

Error counts are calculated from a baseline, which describes the error count values for each type of device in the fibre channel loop. Calculation occurs from the time when the baseline was established to the time at which the error count information is requested.

The baseline is automatically set by the controller. However, a new baseline can be set manually through the Read Link Status Diagnostics dialog box. For more information, see “How to set the baseline” on page 318.

Overview

Read Link Status error counts refer to link errors that have been detected in the traffic flow of a fibre channel loop. The errors detected are represented as a count (32-bit field) of error occurrences accumulated over time. The errors help to provide a coarse measure of the integrity of the components and devices on the loop.

The Read Link Status Diagnostics dialog box retrieves the error counts and displays the controllers, drives, ESMs, and fibre channel ports in channel order.

By analyzing the error counts retrieved, it is possible to determine the components or devices within the fibre channel loop which might be experiencing problems communicating with the other devices on the loop. A high error count for a particular component or device indicates that it might be experiencing problems, and should be given immediate attention.

Error counts are calculated from the current baseline and can be reset by defining a new baseline.

Analyzing RLS Results

Analysis of the RLS error count data is based on the principle that the device immediately ″downstream″ of the problematic component should see the largest number of Invalid Transmission Word (ITW) error counts.

Note: Because the current error counting standard is vague about when the ITW count is calculated, different vendors’ devices calculate errors at different rates. Analysis of the data must take this into account.

The analysis process involves obtaining an ITW error count for every component and device on the loop, viewing the data in loop order, and then identifying any large jumps in the ITW error counts. In addition to the ITW count, the following error counts are displayed in the Read Link Status Diagnostics dialog box:

Error Count Type	Definition of error
Link Failure (LF)	When detected, link failures indicate that there has been a failure within the media module laser operation. Link failures might also be caused by a link fault signal, a loss of signal or a loss of synchronization.
Loss of Synchronization (LOS)	Indicates that the receiver cannot acquire symbol lock with the incoming data stream, due to a degraded input signal. If this condition persists, the number of Loss of Signal errors increases.
Loss of Signal (LOSG)	Indicates a loss of signal from the transmitting node, or physical component within the fibre channel loop. Physical components where a loss of signal typically occurs include the gigabit interface connectors, and the fibre channel fibre optic cable.
Primitive Sequence Protocol (PSP)	Refers to the number of N_Port protocol errors detected, and primitive sequences received while the link is up.
Link Reset Response (LRR)	A Link Reset Response (LRR) is issued by another N_Port in response to a link reset.

Error Count Type	Definition of error
Invalid Cyclic Redundancy Check (ICRC)	Indicates that a frame has been received with an invalid cyclic redundancy check value. A cyclic redundancy check is performed by reading the data, calculating the cyclic redundancy check character, and then comparing its value to the cyclic check character already present in the data. If they are equal, the new data is presumed to be the same as the old data.

If you are unable to determine which component or device on your fibre channel loop is experiencing problems, save the RLS Diagnostics results and forward them to IBM technical support for assistance.

Running RLS Diagnostics

To start RLS Diagnostics, select the storage subsystem from the Subsystem Management Window; then, either click **Storage Subsystem -> Run Read Link Status Diagnostics** from the main menu or right-click the selected subsystem and click **Run Read Link Status Diagnostics** from the pop-up menu. The Read Link Status Diagnostics dialog box is displayed, showing the error count data retrieved. The following data is displayed:

Devices
A list of all the devices on the fibre channel loop. The devices are displayed in channel order, and within each channel they are sorted according to the devices position within the loop.

Baseline Time
The date and time of when the baseline was last set.

Elapsed Time
The elapsed time between when the Baseline Time was set, and when the read link status data was gathered using the Run option.

ITW The total number of Invalid Transmission Word (ITW) errors detected on the fibre channel loop from the baseline time to the current date and time. ITW might also be referred to as the Received Bad Character Count.

Note: This is the key error count to be used when analyzing the error count data.

LF The total number of Link Failure (LF) errors detected on the fibre channel loop from the baseline time to the current date and time.

LOS The total number of Loss of Synchronization (LOS) errors detected on the fibre channel loop from the baseline time to the current date and time.

LOSG The total number of Loss of Signal (LOSG) errors detected on the fibre channel loop from the baseline date to the current date and time.

PSP The total number of Primitive Sequence Protocol (PSP) errors detected on the fibre channel loop from the baseline date to the current date and time.

ICRC The total number of Invalid Cyclic Redundancy Check (ICRC) errors detected on the fibre channel loop, from the baseline date to the current date and time.

How to set the baseline

Error counts are calculated from a baseline (which describes the error count values for each type of device in the fibre channel loop), from the time when the baseline was established to the time at which the error count information is requested.

The baseline is automatically set by the controller; however, a new baseline can be set manually through the Read Link Status Diagnostics dialog box using the following steps:

Note: This option establishes new baseline error counts for ALL devices currently initialized on the loop.

1. Click **Set Baseline**. A confirmation dialog box is displayed.
2. Click **Yes** to confirm baseline change. If the new baseline is successfully set, a success message is displayed indicating that the change has been made.
3. Click **OK**. The Read Link Status Diagnostics dialog box is displayed.
4. Click **Run** to retrieve the current error counts.

How to interpret results

To interpret RLS results, do the following:

1. Open the Read Link Status Diagnostics dialog box.
2. Review the ITW column in the Read Link Status Diagnostics dialog box and identify any unusual increase in the ITW counts.

   Example:

   The following shows the typical error count information displayed in the Read Link Status Diagnostics dialog box. In this example, the first screen displays the values after setting the baseline. The RLS diagnostic is run a short while later and the result shows an increase in error counts at Controller B. This is probably due to either the drive right before (2/9), or more likely the ESM (Drive enclosure 2).

   Figure 154 shows the RLS Status after setting the baseline.

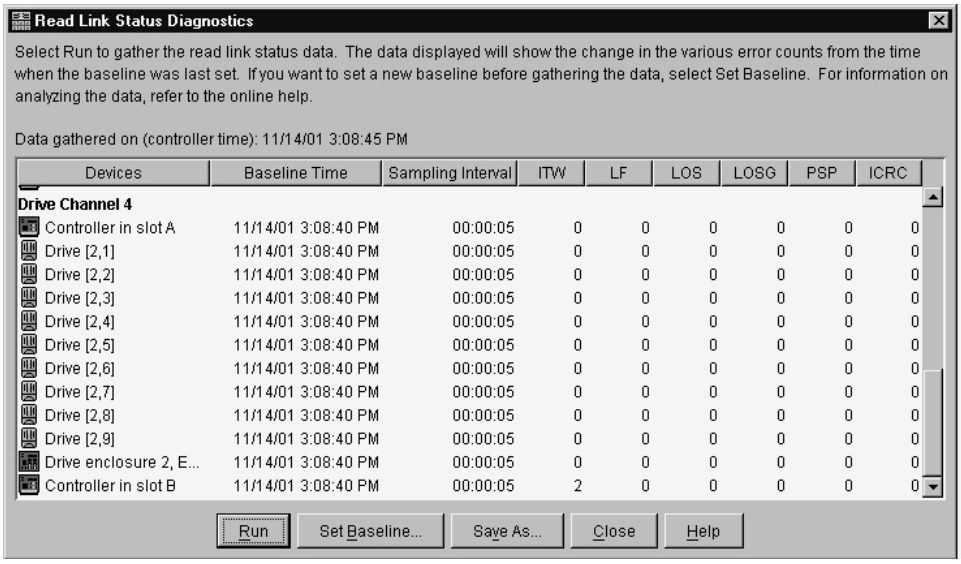


Figure 154. RLS Status After Setting Baseline

Figure 155 on page 320 shows the RLS Status after running the diagnostic.

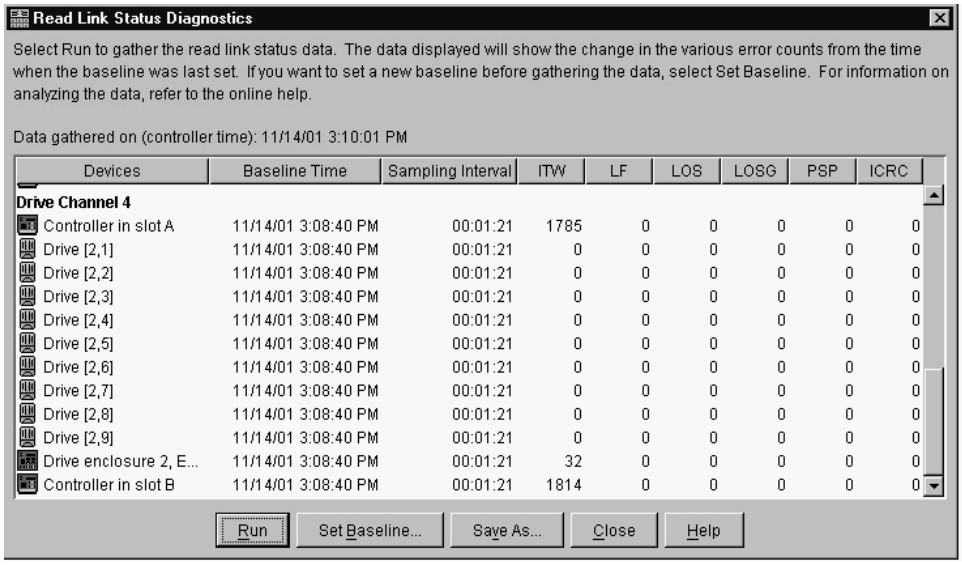


Figure 155. RLS Status After Diagnostic

Note: This is only an example and is not applicable to all situations.
Important: Because the current error counting standard is vague about when the ITW error count is calculated, different vendor's devices calculate at different rates. Analysis of the data must take this into account.

3. Click **Close** to return to the Subsystem Management Window, and troubleshoot the problematic devices. If you are unable to determine which component is problematic, save your results and forward them to IBM technical support.

How to save Diagnostics results

For further troubleshooting assistance, save the Read Link Status results and forward them to technical support for assistance.

1. Click **Save As**. The Save As dialog box is displayed.
2. Select a directory and type the file name of your choice in the **File name** text box. You do not need to specify a file extension.
3. Click **Save**. A comma-delimited file containing the read link status results is saved.

Chapter 27. PD hints — Hubs and switches

You should be referred to this chapter from a PD map or indication. If this is not the case, refer back to Chapter 16, “Problem determination starting points”, on page 131.

After you have read the relevant information in this chapter, return to the PD map that directed you here, either “Hub/Switch PD map 2” on page 145 or “Common Path PD map 2” on page 153.

Unmanaged hub

The unmanaged hub is used only with the type 3526 controller. This hub does not contain any management or debugging aids other than the LEDs that give an indicator of port up or down.

Switch and managed hub

The switch and managed hub are used with the type 3552, 3542, and 1742 controllers. The following sections describe tests that can be used with the switch and managed hub.

Running crossPortTest

The `crossPortTest` verifies the intended functional operation of the switch and managed hub by sending frames from the transmitter for each port by way of the GBIC or fixed port and external cable to another port’s receiver. By sending these frames, the `crossPortTest` exercises the entire path of the switch and managed hub.

A port can be connected to any other port in the same switch or managed hub, provided that the connection is of the same technology. This means that ShortWave ports can only be connected to ShortWave ports; LongWave ports can be connected only to LongWave ports.

Note: An error condition will be shown for any ports that are on the switch or managed hub but that are not connected. If you want more information on the `crossPortTest` and its options, see the Installation and Service Guide for the switch or managed hub you are using.

To repeat the results in the following examples, run the tests in online mode and with the `singlePortAlso` mode enabled. The test will run continuously until your press the Return key on the console being used to perform Ethernet connected management of the switch or managed hub.

To run, the test must find at least one port with a wrap plug or two ports connected to each other. If one of these criteria is not met, the test results in the following message in the telnet shell:

```
Need at least 1 port(s) connected to run this test.
```

The command syntax is `crossPortTest <nFrames>, <0 or 1>` where `<nFrames>` indicates the number of frames to run.

With `<nFrames>` set to 0, the test runs until you press Return.

With the second field set to 0, no single port wrap is allowed and two ports must be cross connected. Figure 156 shows the preferred option, which works with either wrap or cross connect. Figure 157 on page 323 shows the default parms, which work only with cross connect.

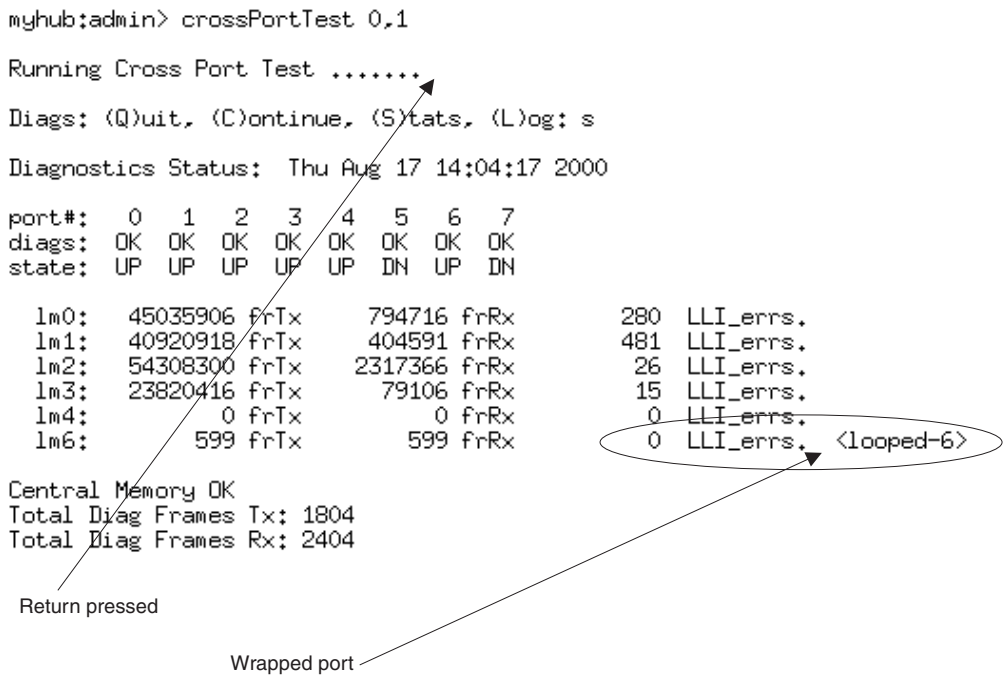


Figure 156. Cross Port Test - Wrap or Cross Connect

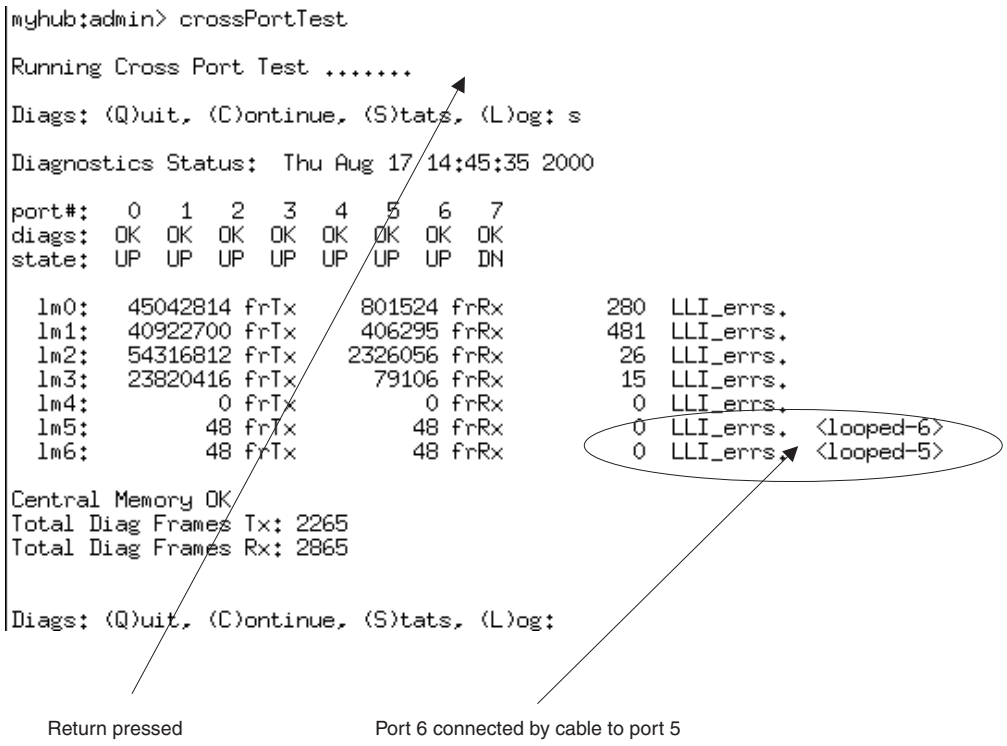


Figure 157. Cross Port Test - Cross Connect Only

Alternative checks

In some rare cases, you might experience difficulty in locating the failed component after you have checked a path. This section gives alternative checking procedures to help resolve the problem.

Some of these checks require plugging and unplugging components. This could lead to other difficulties if, for instance, a cable is not plugged back completely. Therefore, when the problem is resolved, you should perform a path check to make sure that no other problems have been introduced into the path. Conversely, if you started with a problem and, after the unplugging and replugging, you end up at a non-failing point in the PD maps without any repairs or replacement, then the problem was probably a bad connection. You should go back to the original check, such as FAStT MSJ, and rerun the check. If it now runs correctly, you can assume that you have corrected the problem (but it is a good idea to keep checking the event logs for further indications of problems in this area).

Figure 158 on page 324 shows a typical connection path.

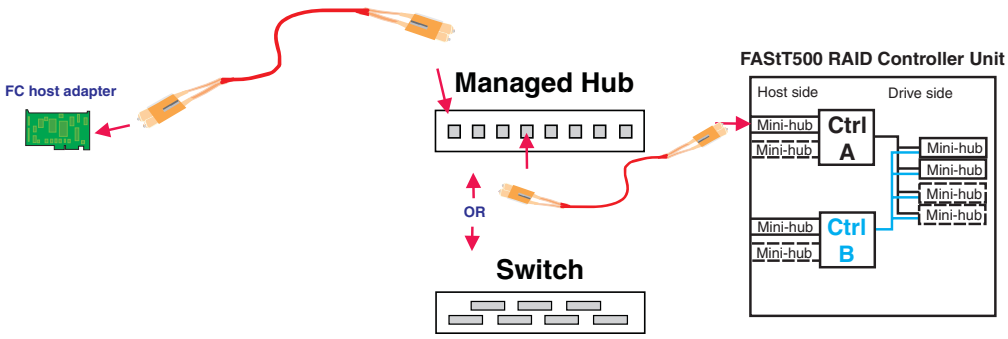


Figure 158. Typical Connection Path

In the `crossPortTest`, data is sourced from the managed hub or switch and travels the path outlined by the numbers 1, 2, and 3 in Figure 159. For the same path, the `sendEcho` function is sourced from the RAID controller and travels the path 3, 2, 1. Using both tests when problems are hard to find (for example, if the problems are intermittent) offers a better analysis of the path. In this case, the duration of the run is also important because enough data must be transferred to enable you to see the problem.

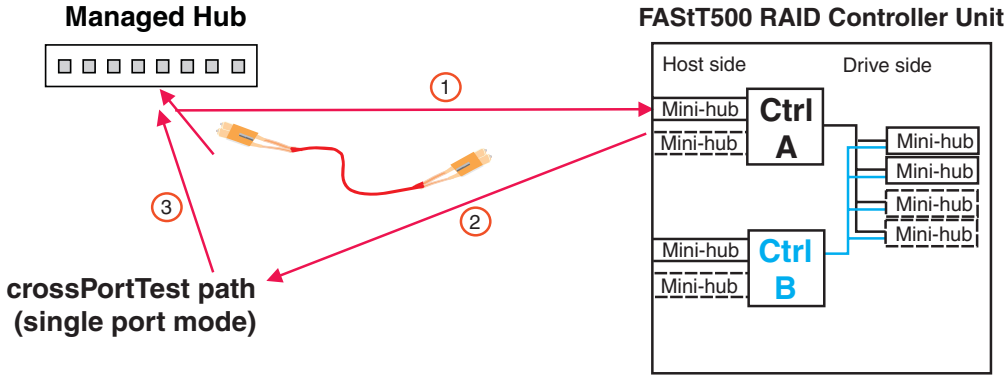
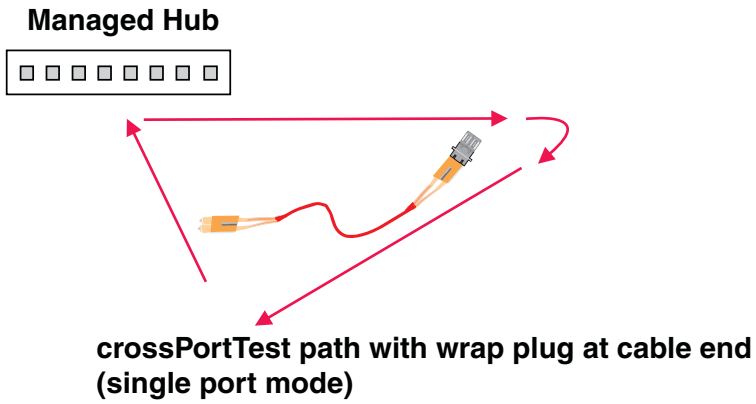


Figure 159. crossPortTest Data Path

Running crossPortTest and sendEcho path to and from the controller

In the case of wrap tests with the wrap plug, there is also dual sourcing capability by using `sendEcho` from the controller or `crossPortTest` from the managed hub or switch. Figure 160 on page 325 shows these alternative paths.



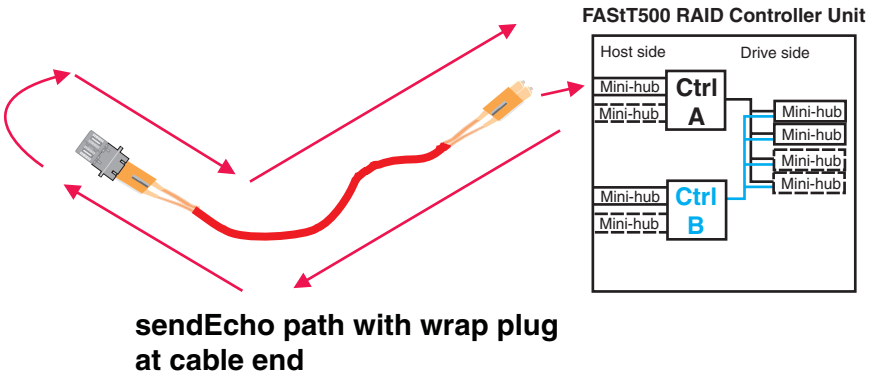


Figure 160. sendEcho and crossPortTest Alternative Paths

Chapter 28. PD hints — Wrap plug tests

You should be referred to this chapter from a PD map or indication. If this is not the case, refer back to Chapter 16, “Problem determination starting points”, on page 131.

After you have read the relevant information in this chapter, return to “Single Path Fail PD map 1” on page 150.

The following sections illustrate the use of wrap plugs.

Running sendEcho and crossPortTest path to and from controller

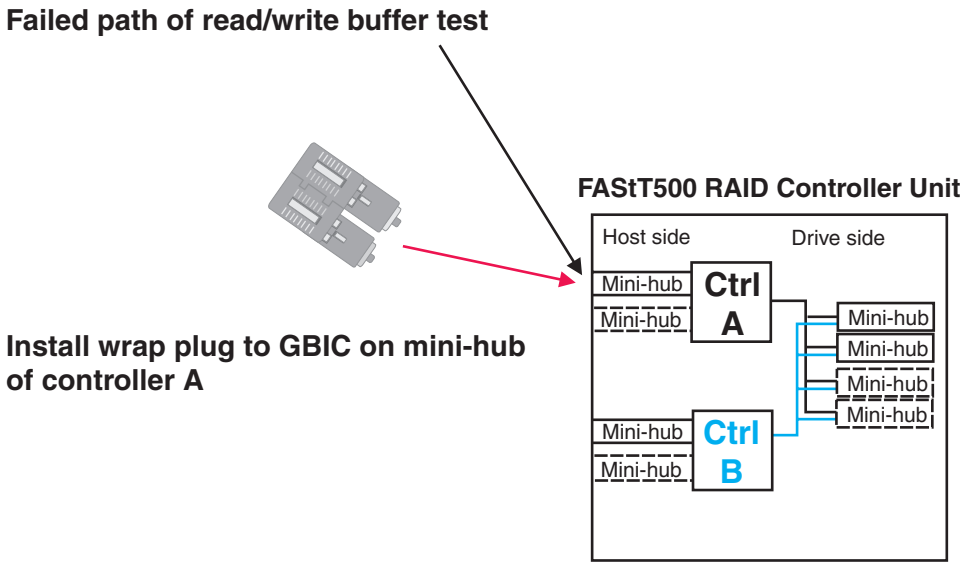


Figure 161. Install Wrap Plug to GBIC

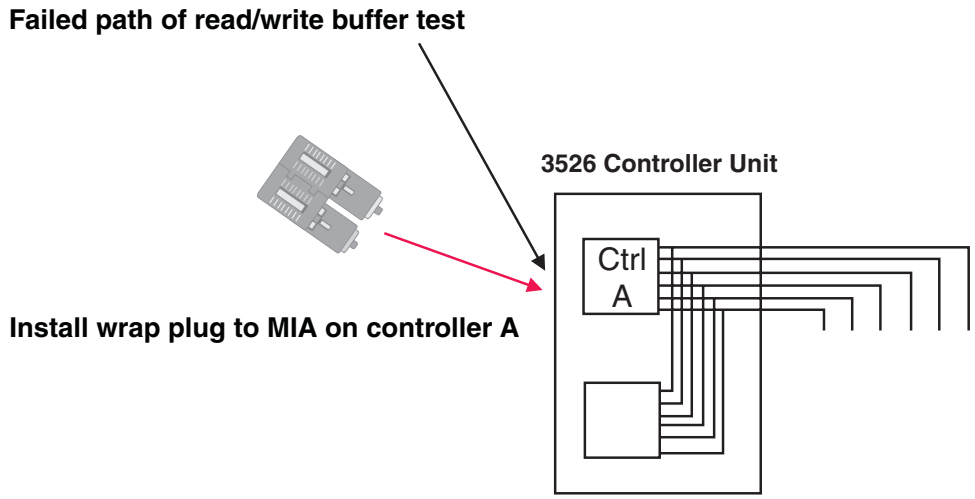


Figure 162. Install Wrap Plug to MIA

Alternative wrap tests using wrap plugs

There is dual sourcing capability with wrap tests using wrap plugs. Use `sendEcho` from the controller or `crossPortTest` from the managed hub or switch. See "Hub/Switch PD map 1" on page 143 for the information on how to run the `crossPortTest`. Figure 163 shows these alternative paths.

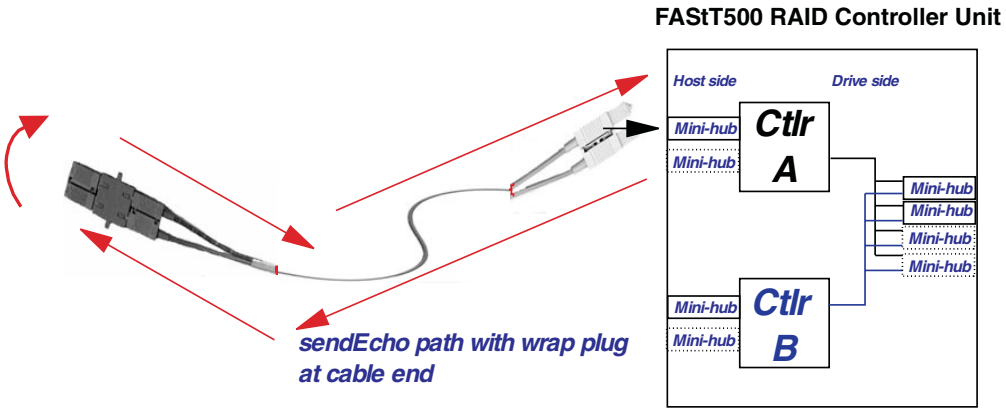


Figure 163. sendEcho Path

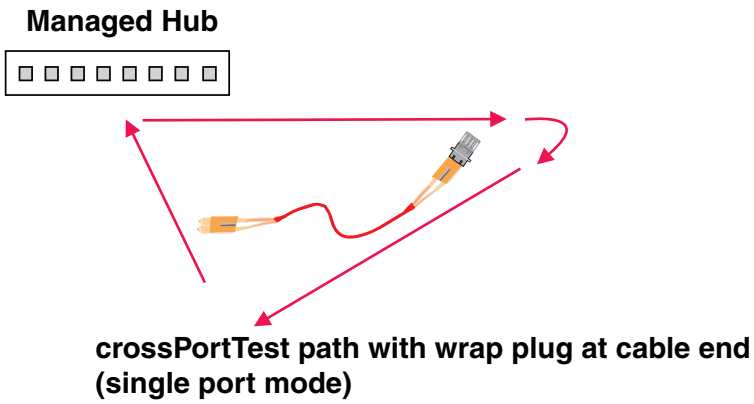


Figure 164. crossPortTest Path

Chapter 29. Heterogeneous configurations

You should be referred to this chapter from a PD map or indication. If this is not the case, refer back to Chapter 16, “Problem determination starting points”, on page 131.

The FAStT Storage managers (version 7.x and 8.xx) provide the capability to manage storage in an heterogeneous environment. This does introduce increased complexity and the potential for problems. This chapter shows examples of heterogeneous configurations and the associated configuration profiles from the FAStT Storage Manager. These examples can assist you in identifying improperly configured storage by comparing the customer’s profile with those supplied, assuming similar configurations.

It is very important that the Storage Partitioning for each host be assigned the correct host type (see Figure 165). If not, the host will not be able to see its assigned storage. The host port identifier that you assign a host type to is the HBA WW node name.

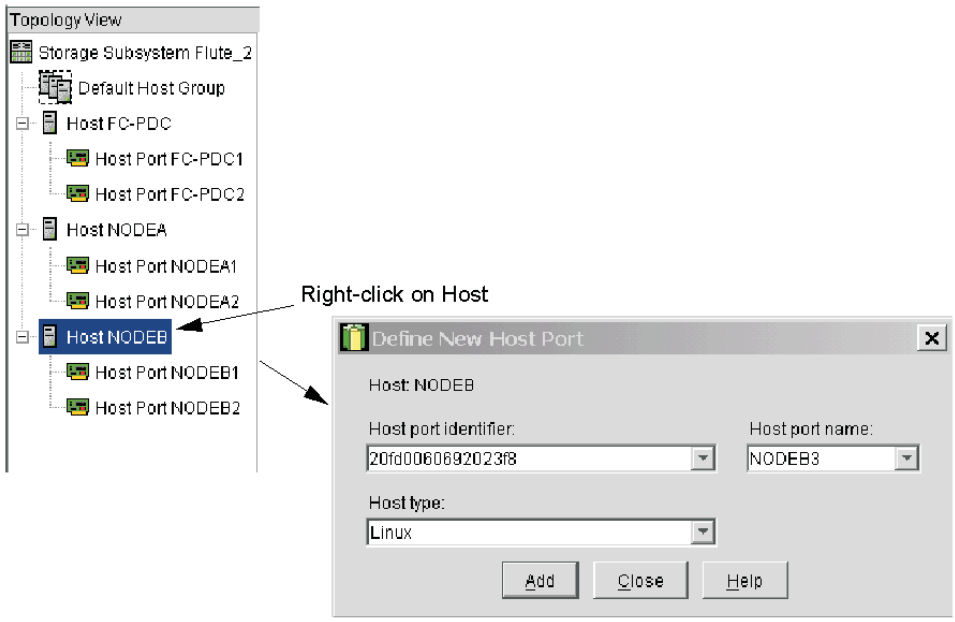


Figure 165. Host Information

Configuration examples

Following are examples of heterogeneous configurations and the associated configuration profiles for Storage Manager Version 7.10 and above. For more detailed information, refer to the Storage Manager Concept guides for your respective SM version.

Windows cluster

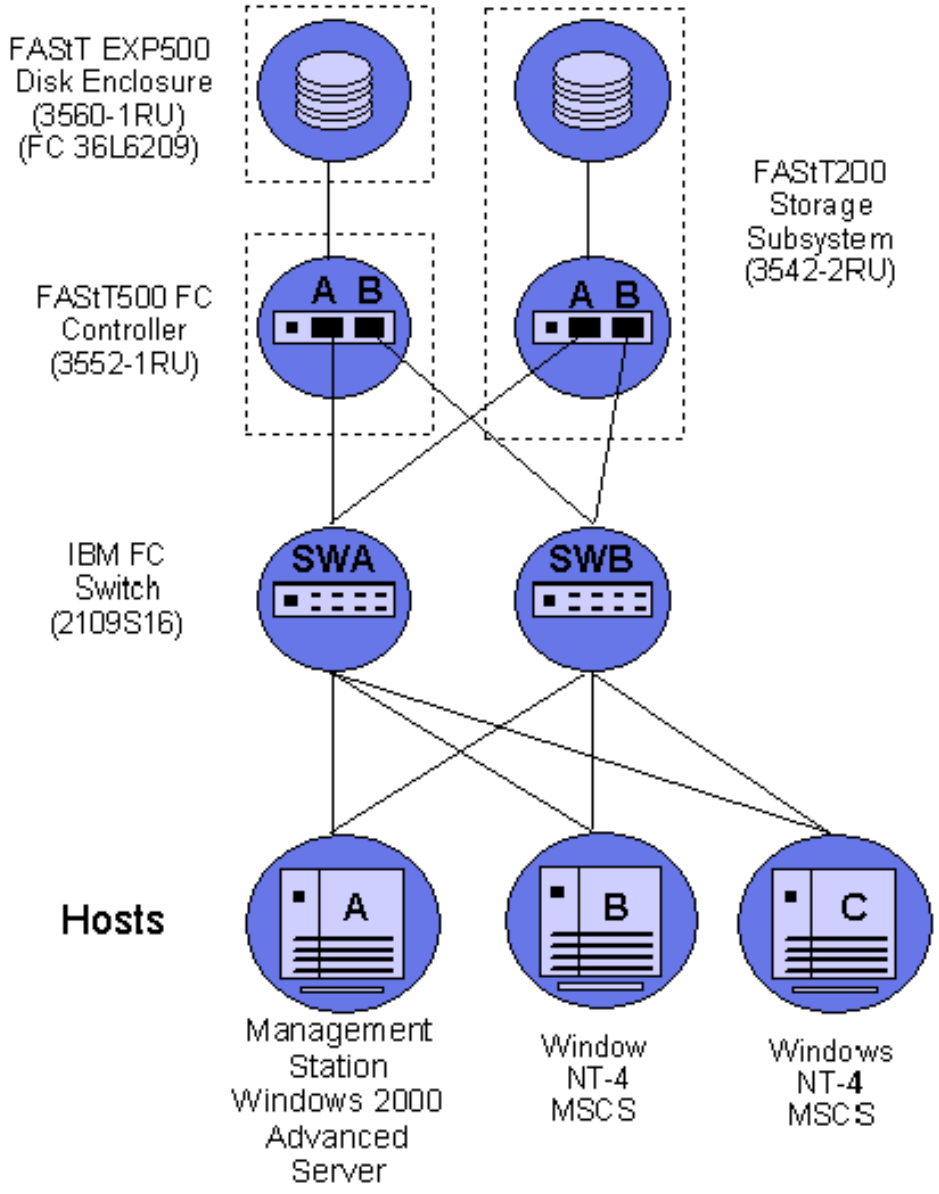


Figure 166. Windows Cluster

Table 70. Windows Cluster configuration example

	Network Management Type	Partition	Storage Partitioning Topology
Host A	Client Direct attached	Windows 2000 AS	Host Port A1 Type=Windows 2000 Non-Clustered Host Port A2 Type=Windows 2000 Non-Clustered
Host B	Host Agent Attached	Windows NT Cluster	Host Port B1 Type=Windows Clustered (SP5 or later) Host Port B2 Type=Windows Clustered (SP5 or later)

Table 70. Windows Cluster configuration example (continued)

	Network Management Type	Partition	Storage Partitioning Topology
Host C	Host Agent Attached	Windows NT Cluster	Host Port C1 Type=Windows Clustered (SP5 or higher) Host Port C2 Type=Windows Clustered (SP5 or higher)

Heterogeneous configuration

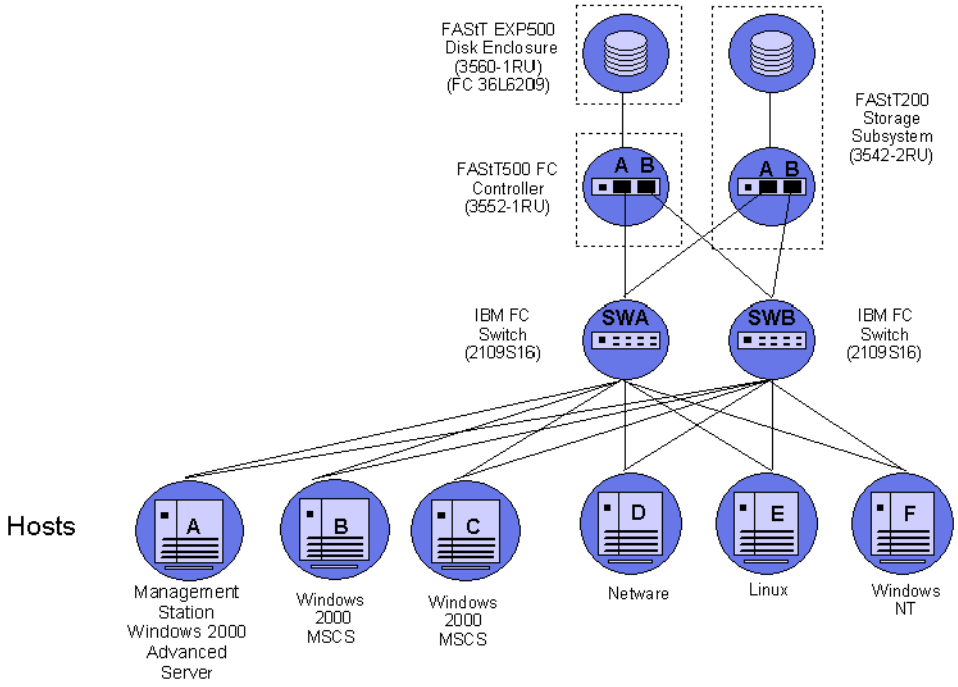


Figure 167. Heterogeneous Configuration

Table 71. Heterogeneous configuration example

	Network Management Type	Partition	Storage Partitioning Topology
Host A	Client Direct attached	Windows 2000 AS	Host Port A1 Type=Windows 2000 Non-Clustered Host Port A2 Type=Windows 2000 Non-Clustered
Host B	Host Agent Attached	Windows 2000 Cluster	Host Port B1 Type=Windows Clustered Host Port B2 Type=Windows Clustered
Host C	Host Agent Attached	Windows 2000 Cluster	Host Port C1 Type=Windows Clustered Host Port C2 Type=Windows Clustered
Host D	Host Agent Attached	Netware	Host Port D1/ Type=Netware Host Port D2/Type=Netware

Table 71. Heterogeneous configuration example (continued)

	Network Management Type	Partition	Storage Partitioning Topology
Host E	Host Agent Attached	Linux	Host Port E1/ Type=Linux Host Port E2/Type=Linux
Host F	Host Agent Attached	Windows NT	Host Port F1/Type=Windows NT Host Port F2/ Type=Windows NT

Chapter 30. Using IBM Fast!UTIL

This chapter provides detailed configuration information for advanced users who want to customize the configuration of the following adapters:

- IBM Fibre Channel Adapter (FRU 01K7354)
- IBM FAStT Host Adapter (FRU 09N7292)
- IBM FAStT FC2-133 (FRU 24P0962) and FC2-133 Dual Port (FRU 24P8053) Host Bus Adapters

For more information about these adapters, see Chapter 3, “Fibre Channel PCI Adapter (FRU 01K7354)”, on page 13, Chapter 4, “IBM FAStT Host Adapter (FRU 09N7292)”, on page 15, and Chapter 5, “IBM FAStT FC2-133 (FRU 24P0962) and IBM FAStT FC2-133 Dual Port (FRU 24P8053) Host Bus Adapters”, on page 19.

You can configure the adapters and the connected fibre channel devices using the Fast!UTIL utility.

Starting Fast!UTIL

To access Fast!UTIL, press Ctrl+Q (or Alt+Q for 2100) during the adapter BIOS initialization (it might take a few seconds for the Fast!UTIL menu to appear). If you have more than one adapter, Fast!UTIL prompts you to select the adapter you want to configure. After changing the settings, Fast!UTIL restarts your system to load the new parameters.

Important: If the configuration settings are incorrect, your adapter will not function properly. Do not modify the default configuration settings unless you are instructed to do so by an IBM support representative or the installation instructions. The default settings are for a typical Microsoft Windows installation. Refer to the adapter driver README for the appropriate operating system for required NVRAM setting modifications for that operating system.

Fast!UTIL options

This section describes the Fast!UTIL options. The first option on the **Fast!UTIL Options** menu is **Configuration Settings**. The settings configure the fibre channel devices and the adapter to which they are attached.

Note: If your version of Fast!UTIL has settings that are not discussed in this section, then you are working with down-level BIOS or non-supported BIOS. Update your BIOS version.

Host Adapter settings

You can access this option from the **Configuration Settings** menu in Fast!UTIL by selecting **Host Adapter Settings**. The current default settings for the host adapters are described in this section.

Note: All settings for the IBM Fibre Channel Adapter (FRU 01K7354) are accessed from the **Host Adapter Settings** menu option (see Table 72 on page 336). The FAStT Host Adapter (FRU 09N7292) and the FAStT FC2-133 Adapters (FRU 24P0962, 24P8053) offer additional settings available from the **Advanced Adapter Settings** menu option (see Table 73 on page 336 and Table 74 on page 336). Any settings for the Fibre Channel Adapter (FRU

01K7354) not described in this section are described in “Advanced Adapter settings” on page 337.

Table 72. IBM Fibre Channel Adapter (FRU 01K7354)host adapter settings

Setting	Options	Default
Host adapter BIOS	Enabled or Disabled	Disabled
Enable LUNs	Yes or No	Yes
Execution throttle	1 - 256	256
Drivers load RISC code	Enabled or Disabled	Enabled
Frame size	512, 1024, 2048	2048
IOCB allocation	1-512 buffers	256 buffers
Loop reset delay	0-15 seconds	8 seconds
Extended error logging	Enabled or Disabled	Disabled
Port down retry count	0-255	30

Table 73. FAStT Host Adapter (FRU 09N7292)host adapter settings

Setting	Options	Default
Host adapter BIOS	Enabled or Disabled	Disabled
Frame size	512, 1024, 2048	2048
Loop reset delay	0-15 seconds	5 seconds
Adapter hard loop ID	Enabled or Disabled	Enabled
Hard loop ID	0-125	125

Table 74. FAStT FC2-133 Adapters(FRU 24P0962, 24P8053)host adapter settings

Setting	Options	Default
Host adapter BIOS	Enabled or Disabled	Disabled
Frame size	512, 1024, 2048	2048
Loop reset delay	0-60 seconds	5 seconds
Adapter hard loop ID	Enabled or Disabled	Enabled
Hard loop ID	0-125	125
Spin up delay	Enabled or Disabled	Disabled

Host adapter BIOS: When this option is set to Disabled, the ROM BIOS code on the adapter is disabled, freeing space in upper memory. This setting must be enabled if you are starting from a fibre channel hard disk that is attached to the adapter. The default is Disabled.

Frame size: This setting specifies the maximum frame length supported by the adapter. The default size is 2048. If you are using F-Port (point-to-point) connections, the default is best for maximum performance.

Loop reset delay: After resetting the loops, the firmware does not initiate any loop activity for the number of seconds specified in this setting. The default is 5 seconds.

Adapter hard loop ID: This setting forces the adapter to use the ID specified in the Hard loop ID setting. The default is Enabled. (For FAStT Host Adapter [FRU 09N7292)] and FAStT FC2-133 Adapters [FRU 24P0962, 24P8053] only.)

Hard loop ID: When the adapter hard loop ID is set to Enabled, the adapter uses the ID specified in this setting. The default ID is 125.

Spin up delay: When this setting is Enabled, the BIOS code waits up to five minutes to find the first drive. The default is Disabled.

Note: Adapter settings and default values might vary, based on the version of BIOS code installed for the adapter.

Selectable Boot settings

You can access the **Selectable Boot Settings** option from the **Configuration Settings** menu. When this option is set to Enabled, you can select the node name from which you want to start up (boot). When this option is set to Enabled, the node will start from the selected fibre channel hard disk, ignoring any IDE hard disks attached to your server. When this option is set to Disabled, the Boot ID and Boot LUN parameters have no effect.

The BIOS code in some new systems supports selectable boot, which supersedes the Fast!UTIL selectable boot setting. To start from a fibre channel hard disk attached to the adapter, select the attached fibre channel hard disk from the system BIOS menu.

Note: This option applies only to disk devices; it does not apply to CDs, tape drives, and other nondisk devices.

Restore Default settings

You can access this option from the **Configuration Settings** menu. It restores the adapter default settings.

Note: The default NVRAM settings are the adapter settings that were saved the last time an NVRAM update operation was executed from the BIOS Update Utility program (option U or command line /U switch). If the BIOS Update Utility program has not been used to update the default NVRAM settings since the adapter was installed, the factory settings are loaded.

Raw NVRAM data

This option displays the adapter nonvolatile random access memory (NVRAM) contents in hexadecimal format. This is a troubleshooting tool; you cannot modify the data.

Advanced Adapter settings

You can access this option from the **Configuration Settings** menu by selecting **Advanced Adapter Settings**. The current default settings for the adapter are described in this section.

Note: The **Advanced Adapter Settings** menu option is available only for the FAStT Host Adapter (FRU 09N7292) (see Table 75 on page 338) and the FAStT FC2-133 Adapters (FRU 24P0962, 24P8053) (see Table 76 on page 338). All settings for the IBM Fibre Channel Adapter (FRU 01K7354) are accessed from the **Host Adapter Settings** menu option.

Table 75. FAStT Host Adapter (FRU 09N7292) advanced adapter settings

Setting	Options	Default
Execution throttle	1-256	256
Fast command posting	Enabled or Disabled	Enabled
>4GByte addressing	Enabled or Disabled	Disabled
LUNs per target	0, 8, 16, 32, 64, 128, 256	0
Enable LIP reset	Yes or No	No
Enable LIP full login	Yes or No	Yes
Enable target reset	Yes or No	Yes
Login retry count	0-255	30
Port down retry count	0-255	30
Drivers load RISC code	Enabled or Disabled	Enabled
Enable database updates	Yes or No	No
Disable database load	Yes or No	No
IOCB allocation	1-512 buffers	256 buffers
Extended error logging	Enabled or Disabled	Disabled

Table 76. FAStT FC2-133 Adapters(FRU 24P0962, 24P8053) advanced adapter settings

Setting	Options	Default
Execution throttle	1-256	256
>4GByte addressing	Enabled or Disabled	Disabled
LUNs per target	0, 8, 16, 32, 64, 128, 256	0
Enable LIP reset	Yes or No	No
Enable LIP full login	Yes or No	Yes
Enable target reset	Yes or No	Yes
Login retry count	0-255	30
Port down retry count	0-255	30
IOCB allocation	1-512 buffers	256 buffers
Extended error logging	Enabled or Disabled	Disabled

Execution throttle: This setting specifies the maximum number of commands executing on any one port. When a port reaches its execution throttle, Fast!UTIL does not run any new commands until the current command is completed. The valid options for this setting are 1 through 256. The default (optimum) is 256.

Fast command posting: This setting decreases command execution time by minimizing the number of interrupts. The default is Enabled for the FAStT Host Adapter (FRU 09N7292).

>4GByte addressing: Enable this option when the system has more than 4 GB of memory available. The default is Disabled.

LUNs per target (for IBM Fibre Channel Adapter [FRU 01K7354]): This setting specifies the number of LUNs per target. Multiple logical unit number (LUN) support is typically for redundant array of independent disks (RAID) enclosures that use LUNs to map drives. The default is 8. For Netware, set the number of LUNs to 32.

LUNs per target (for FAStT Host Adapter [FRU 09N7292] and FAStT FC2-133 Adapters [FRU 24P0962, 24P8053]): This setting specifies the number of LUNs per target. Multiple logical unit number (LUN) support is typically for redundant array of independent disks (RAID) enclosures that use LUNs to map drives. The default is 0. For Netware, set the number of LUNs to 32.

Enable LIP reset: This setting determines the type of loop initialization process (LIP) reset that is used when the operating system initiates a bus reset routine. When this option is set to **Yes**, the device driver initiates a global LIP reset to clear the target device reservations. When this option is set to **No**, the device driver initiates a global LIP reset with full login. The default is **No**.

Enable LIP full logon: This setting instructs the ISP chip to log into all ports after any LIP. The default is Yes.

Enable target reset: This setting enables the device drivers to issue a Target Reset command to all devices on the loop when a SCSI Bus Reset command is issued. The default is Yes.

Login retry count: This setting specifies the number of times the software tries to log in to a device. The default is 30 retries.

Port down retry count: This setting specifies the number of times the software retries a command to a port that is returning port-down status. The default is 30 retries.

Drivers load RISC code: When this option is set to Enabled, the adapter uses the RISC firmware that is embedded in the software device driver. When this option is set to Disabled, the software device driver loads the RISC firmware found in the adapter BIOS code. The default is Enabled.

Note: To load the embedded device driver software, the device driver being loaded must support this setting. If the device driver does not support this setting, the result is the same as if this option is set to Disabled, regardless of the setting. Leaving this option enabled ensures a certified combination of software device driver and RISC firmware.

Enable database updates: When this option is set to Enabled, the software can save the loop configuration information in flash memory as the system powers down. The default is No.

Disable database load: When this option is set to Enabled, the device database is read from the Registry during driver initialization. When this option is set to Disabled, the device database is created dynamically during device driver initialization. The default is No.

Note: This option usually applies to the Windows NT and Windows 2000 operating system environments.

IOCB allocation: This option specifies the maximum number of buffers from the firmware buffer pool that are allocated to any one port. The default setting is 256 buffers.

Extended error logging: This option provides additional error and debugging information to the operating system. When this option is set to Enabled, events are

logged into the Windows NT Event Viewer or Windows 2000 Event Viewer (depending on the environment you are in). The default is Disabled.

Extended Firmware settings

You can access this option from the **Configuration Settings** menu by selecting **Extended Firmware Settings**. The current default settings for the host adapter are listed in Table 77 and are described in this section.

Note: The **Extended Firmware Settings** menu option is available only for the FAStT Host Adapter (FRU 09N7292) and the FAStT FC2-133 Adapters (FRU 24P0962, 24P8053). Extended firmware settings are not available for the IBM Fibre Channel Adapter (FRU 01K7354).

Table 77. Extended firmware settings for FAStT Host Adapter (FRU 09N7292) and FAStT FC2-133 Adapters(FRU 24P0962, 24P8053)

Setting	Options	Default
RIO operation mode	0, 5	0
Connection Options [for FAStT Host Adapter (FRU 09N7292)]	0, 1, 2, 3	3
Connection Options [for FAStT FC2-133 Adapters (FRU 24P0962, 24P8053)]	0, 1, 2	2
Fibre channel tape support	Enabled or Disabled	Disabled
Interrupt delay timer	0-255	0
Data rate [for FAStT FC2-133 Adapters (FRU 24P0962, 24P8053) only]	0, 1, 2	2

RIO operation mode: This setting specifies the reduced interrupt operation (RIO) modes, if supported by the software device driver. RIO modes enable posting multiple command completions in a single interrupt (see Table 78). The default is 0.

Table 78. RIO operation modes for FAStT Host Adapter (FRU 09N7292) and FAStT FC2-133 Adapters(FRU 24P0962, 24P8053)

Option	Operation mode
0	No multiple responses
5	Multiple responses with minimal interrupts

Connection options: This setting defines the type of connection (loop or point-to-point) or connection preference (see Table 79). The default is 3 for the FAStT Host Adapter (FRU 09N7292) or 2 for the FAStT FC2-133 Adapters (FRU 24P0962, 24P8053).

Table 79. Connection options for FAStT Host Adapter (FRU 09N7292) and FAStT FC2-133 Adapters(FRU 24P0962, 24P8053)

Option	Type of connection
0	Loop only
1	Point-to-point only
2	Loop preferred; otherwise, point-to-point

Table 79. Connection options for FAStT Host Adapter (FRU 09N7292) and FAStT FC2-133 Adapters(FRU 24P0962, 24P8053) (continued)

Option	Type of connection
3 (for FAStT Host Adapter [FRU 09N7292] only)	Point-to-point; otherwise, loop

Fibre channel tape support: This setting is reserved for fibre channel tape support. The default is Disabled.

Interrupt delay timer: This setting contains the value (in 100-microsecond increments) used by a timer to set the wait time between accessing (DMA) a set of handles and generating an interrupt. The default is 0.

Data rate (for FAStT FC2-133 Adapters [FRU 24P0962, 24P8053] only): This setting determines the data rate (see Table 80). When this field is set to 2, the FAStT FC2-133 Adapters determines what rate your system can accommodate and sets the rate accordingly. The default is 2.

Table 80. Data rate options for FAStT FC2-133 Adapters(FRU 24P0962, 24P8053)

Option	Data Rate
0	1 Gbps
1	2 Gbps
2	Auto select

Scan fibre channel devices

Use this option to scan the fibre channel loop and list all the connected devices by loop ID. Information about each device is listed, for example, vendor name, product name, and revision. This information is useful when you are configuring your adapter and attached devices.

Fibre channel disk utility

Attention: Performing a low-level format removes all data on the disk.

Use this option to scan the fibre channel loop bus and list all the connected devices by loop ID. You can select a disk device and perform a low-level format or verify the disk media.

Loopback data test

Use this option to verify the adapter basic transmit and receive functions. A fibre channel loop back connector option must be installed into the optical interface connector on the adapter before starting the test.

Select host adapter

Use this option to select, configure, or view a specific adapter if you have multiple adapters in your system.

ExitFast!UTIL

After you complete the configuration, use the ExitFast!UTIL option to exit the menu and restart the system.

Chapter 31. Storage Manager FAQs

This chapter contains answers to frequently asked questions in the following areas:

Global Hot Spare (GHS) drives

What is a Global Hot Spare?

A Global Hot Spare is a drive within the storage subsystem that has been defined by the user as a spare drive. The Global Hot Spare is to be used in the event that a drive that is part of an array with redundancy (RAID 1, 3, 5 array) fails. When the fail occurs, and a GHS drive is configured, the controller will begin reconstructing to the GHS drive. Once the reconstruction to the GHS drive is complete, the array will be promoted from the Degraded state to the Optimal state, thus providing full redundancy again. When the failed drive is replaced with a good drive, the copy-back process will start automatically.

What is reconstruction and copy-back?

Reconstruction is the process of reading data from the remaining drive (or drives) of an array that has a failed drive and writing that data to the GHS drive. Copy-back is the process of copying the data from the GHS drive to the drive that has replaced the failed drive.

What happens during the reconstruction of the GHS?

During the reconstruction process, data is read from the remaining drive (or drives) within the array and used to reconstruct the data on the GHS drive.

How long does the reconstruction process take?

The time to reconstruct a GHS drive will vary depending on the activity on the array, the size of the failed array, and the speed of the drives.

What happens if a GHS drive fails while sparing for a failed drive?

If a GHS drive fails while it is sparing for another drive, and another GHS is configured in the array, a reconstruction process to another GHS will be done.

If a GHS fails, and a second GHS is used, and both the originally failed drive and the failed GHS drive are replaced at the same time, how will the copy-back be done?

The controller will know which drive is being spared by the GHS, even in the event that the first GHS failed and a second GHS was used. When the original failed drive is replaced, the copy-back process will begin from the second GHS.

If the size of the failed drive is 9Gbyte, but only 3Gbytes of data have been written to the drive, and the GHS is an 18Gbyte drive, how much is reconstructed?

The size of the array determines how much of the GHS drive will be used. For example, if the array has two 9Gbyte drives, and the total size of all logical drives is 18Gbyte, then 9Gbytes of reconstruction will occur, even if only 3Gbytes of data exist on the drive. If the array has two 9Gbyte drives, and the total size of all logical drives is 4Gbytes, then only 2Gbytes of reconstruction will be done to the GHS drive.

How can you determine if a Global Hot Spare (GHS) is in use?

The Global Hot Spare is identified in Storage Manager by the following icon:

If a drive fails, which GHS will the controller attempt to use?

The controller will first attempt to find a GHS on the same channel as the failed drive; the GHS must be at least as large as the configured capacity of the failed drive. If a GHS does not exist on the same channel, or if it is already in use, the controller will check the remaining GHS drives, beginning with the last GHS configured. For example, if the drive at location 1:4 failed, and if the GHS drives were configured in the following order, 0:12, 2:12, 1:12, 4:12, 3:12, the controller will check the GHS drives in the following order, 1:12, 3:12, 4:12, 2:12, 0:12.

Will the controller search all GHS drives and select the GHS drive closest to the configured capacity of the failed drive?

No. The controller will use the first available GHS that is large enough to spare for the failed drive.

Can any size drive be configured as a GHS drive?

At the time a drive is selected to be configured as a GHS, it must be equal or larger in size than at least one other drive in the attached drive enclosures that is not a GHS drive. However, it is strongly recommended that the GHS have at least the same capacity as the target drive on the subsystem.

Can a GHS that is larger than the drive that failed act as a spare for the smaller drive?

Yes.

Can a 9Gbyte GHS drive spare for an 18Gbyte failed drive?

A GHS drive can spare for any failed drive, as long as the GHS drive is at least as large as the configured capacity of the failed drive. For example, if the failed drive is an 18Gbyte drive with only 9Gbyte configured as part of an array, a 9Gbyte drive can spare for the failed drive.

However, to simplify storage management tasks and to prevent possible data loss in case a GHS is not enabled because of inadequate GHS capacity, it is strongly recommended that the GHS have at least the same capacity as the target drive on the subsystem.

What happens if the GHS drive is not large enough to spare for the failed drive?

If the controller does not find a GHS drive that is at least as large as the configured capacity of the failed drive, a GHS will not be activated, and, depending on the array state, the LUN will become degraded or failed.

What action should be taken if all drives in the array are now larger than the GHS drive?

Ideally, the GHS drive will be replaced with a drive as large as the other drives in the array. If the GHS drive is not upgraded, it will continue to be a viable spare as long as it is as large as the smallest configured capacity of at least one of the configured drives within the array.

The previous two questions describe what might happen in this case. It is strongly recommended that you upgrade the GHS to the largest capacity drive.

How many GHS drives can be configured in an array?

The maximum number of GHS drives for Storage Manager versions 7 or 8 is fifteen per subsystem.

How many GHS drives can be reconstructed at the same time?

Controller firmware versions 3.x and older will only allow for one reconstruction process per controller to occur at the same time. An additional requirement is that in order for two reconstruction processes to occur at the same time, the LUNs affected cannot be owned by the same controller. For example, if a drive in LUN_1 and a drive in LUN-4 fail, and both LUNs are owned by Controller_A, then only one reconstruction will occur at a time. However, if LUN-1 is owned by Controller_A, and LUN-4 is owned by Controller_B, then two reconstruction process will occur at the same time. If multiple drives fail at the same time, the others will be queued after the currently-executing reconstruction completes.

Once the GHS reconstruction has started, and the failed drive is replaced, does the reconstruction of the GHS stop?

The reconstruction process will continue until complete, and then begin a copy-back to the replaced drive.

What needs to be done to a GHS drive that has spared for a failed drive after the copy-back to the replaced drive has been completed?

Once the copy-back to the replaced drive is complete, the GHS drive will be immediately available as a GHS. There is no need for the user to do anything.

Does the GHS have to be formatted before it can be used?

No. The GHS drive will be reconstructed from the other drive (or drives) within the LUN that had a drive fail.

What happens if a GHS drive is moved to a drive-slot that is part of LUN, but not failed?

When the GHS drive is moved to a drive-slot that is not failed and is part of a LUN, the drive will be spun up, marked as a replacement of the previous drive, and reconstruction started to the drive.

Can a GHS drive be moved to a drive-slot occupied by a faulted drive that is part of a LUN?

Yes. In this case, the GHS drive will now be identified as a replacement for the failed drive, and begin a copy-back or reconstruction, depending on whether a GHS drive was activated for the faulted drive.

What happens if a GHS drive is moved to an unassigned drive-slot, and the maximum GHS drives are already configured?

Once the maximum number of GHS drives have been configured, moving a GHS drive to an unassigned drive-slot will cause the GHS drive to become an unassigned drive.

What happens if a drive from a LUN is accidentally inserted into a GHS drive slot?

Once a drive is inserted into a slot configured as a GHS, the newly inserted drive will become a GHS, and the data previously on the drive will be lost. Moving drives in or out of slots configured as GHS drives must be done very carefully.

How does the controller know which drive slots are GHS drives?

The GHS drive assignments are stored in the dacStore region of the Sundry drives.

Auto Code Synchronization (ACS)

What is ACS?

ACS is a controller function that is performed during the controller Start-Of-Day (SOD) when a foreign controller is inserted into an array, at which time the Bootware (BW) and Appware (AW) versions will be checked and synchronized if needed.

What versions of FW support ACS?

ACS was first activated in controller FW version 3.0.x, but the LED display was added to controller FW version 03.01.x and later.

How to control if ACS is to occur?

ACS will occur automatically when a foreign controller is inserted, or during a power-on, if bit 1 is set to 0 (zero) and bit 2 is set to 1 (one) in NVSRAM byte offset 0x29. If these bits are set appropriately, the newly inserted controller will check the resident controller BW and AW versions with its own, and if different, will begin the synchronization process.

Bit 1 = 0	Auto Code Synchronization will occur only if the newly inserted controller is a foreign controller (a different controller from the one that was previously in the same slot).
Bit 2 = 1	Enable Automatic Code Synchronization (ACS)

What is a resident controller and what is a foreign controller?

A controller is considered to be resident if it is the last controller to have completed a SOD in that slot and has updated the dacStore on the drives. A foreign controller is one that is not recognized by the array when powered on or inserted.

Example A: In a dual controller configuration that has completed SOD, both controllers are considered to be resident. If the bottom controller is removed, and a new controller is inserted, the new controller will not be known by the array and will be considered foreign, because it is not the last controller to have completed a SOD in that slot.

Example B: In a dual controller configuration that has completed SOD, both controllers are considered to be resident. If controller Y is removed from the bottom slot, and controller Z is inserted into the bottom slot, controller Z will be considered foreign until it has completed the SOD. If controller Z is then removed and controller Y is reinserted, controller Y will be considered foreign because it is not the last controller to have completed the SOD in that slot.

What happens if a single controller configuration is upgraded to dual controller?

If a controller is inserted into a slot that has not previously held a controller since the array was cleared, ACS will not be invoked. This is because there is no previous controller information in the dacStore region to use for evaluating the controller as being resident or foreign.

When will ACS occur?

Synchronization will occur only on power cycles and controller insertion, not on resets. During the power-on, the foreign controller will send its revision levels to the resident controller and ask if ACS is required. The resident controller will check NVSRAM settings and, if ACS is enabled, will then check the revision numbers. A response is then sent to the foreign controller, and if ACS is not required, the foreign controller will continue its initialization. If ACS is required, a block of RPA cache will be allocated in the foreign controller and the ACS process will begin.

Which controller determines if ACS is to occur?

The NVSRAM bits of the resident controller will be used to determine whether synchronization is to be performed. The controller being swapped in will always request synchronization, which will be accepted or rejected based on the NVSRAM bits of the resident controller.

What is compared to determine if ACS is needed?

The entire code revision number will be used for comparison. Both the BW and AW versions will be compared, and, if either are different, both the BW and AW will be erased and rewritten. The number of separate loadable partitions is also compared; if different, the code versions are considered to be different without considering the revision numbers.

How long will the ACS process take to complete?

The ACS process will begin during the Start-Of-Day process, or between 15 and 30 seconds after power-up or controller insertion. The ACS process for Series 3

controller code will take approximately three minutes to complete. As the code size increases, the time to synchronize will also increase. Once ACS is complete, do not remove the controllers for at least three minutes, in case NVSRAM is also synchronized during the automatic reset.

What will happen if a reset occurs before ACS is complete?

It is important that neither of the controllers are reset during the ACS process. If a reset occurs during this process, it is likely that the foreign controller will no longer boot or function correctly, and it might have to be replaced.

Is NVSRAM synchronized by ACS?

NVSRAM synchronization is not part of ACS, but is checked with dacStore on the drives every time the controller is powered on. The synchronization is not with the alternate controller, but with the NVSRAM as written to dacStore for the controller slot. Each controller, slot-A and slot-B, have individual NVSRAM regions within dacStore. The update process takes approximately five seconds, does not require a reset, and synchronizes the following NVSRAM regions: UserCfg, NonCfg, Platform, HostData, SubSys, DrvFault, InfCfg, Array, Hardware, FCCfg, SubSysID, NetCfg, Board.

Note: No LED display will be seen during the synchronization of the NVSRAM.

What is the order of the synchronization?

Both the BW and AW are synchronized at the same time. NVSRAM will be checked and synchronized during the automatic reset following the ACS of the controller code.

Will the controller LEDs flash during ACS?

The function to flash the LEDs during ACS was first enabled in controller Firmware version 03.01.01.01. If the foreign controller has a release prior to 03.01.01.01, the LED display will not be seen during ACS. The controller being updated controls the LED synchronization display.

What is the LED display sequence?

If the foreign controller has a Firmware version equal to or newer than 03.01.01.01, the LEDs will be turned on from right to left, and then turned off left to right. This sequence will continue until the ACS process is complete.

Is a reset required after ACS is complete?

When the ACS process is complete, the controller will automatically reset.

What is the ACS sequence for controllers with AW prior to 03.01.01.01?

If the foreign controller has AW prior to 03.01.01.01, the LED display will not be displayed. In this case, the controllers should not be removed or reset for at least 15 minutes. Once the foreign controller has reset, the controller will be ready for use within two minutes.

Will ACS occur if the controller is cold swapped?

Yes, providing the NVSRAM bits are set to allow ACS to occur.

What happens if both controllers are cold swapped?

If both controllers are cold swapped (that is, if both are foreign), the controller with the higher FW version number will be loaded onto the alternate controller. This is simply a numerical comparison. For example, if controller A is 03.01.01.08, and controller B is 03.01.01.11, then controller A will be upgraded to 03.01.01.11. The NVSRAM will be updated from dacStore.

What sequence of events should be expected during ACS?

If ACS is enabled, the process will begin about 30 seconds after the controller is inserted or powered on. When ACS begins, the SYM1000 and the foreign controller fault lights will begin to flash, and the controller LEDs will begin to turn on one at a time from right to left, then off left to right. This process will continue for approximately three minutes until the ACS process is complete. Once the ACS process is complete, the foreign controller will reset automatically and during the reset, the NVSRAM will be checked, and updated if needed. The entire process will take approximately five minutes to complete.

Storage partitioning

Does the Storage Partitions feature alleviate the need to have clustering software at the host end?

No. Clustering software provides for the movement of applications between hosts for load balancing and failover. Storage Partitions just provides the ability to dedicate a portion of the storage to one or more hosts. Storage partitions should work well with clustering in that a cluster of hosts can be grouped as a Host Group to provide access to the same storage as needed by the hosts in that cluster.

If I have two hosts in a host group sharing the same logical drives, and both hosts trying to modify the same data on the same logical drive, how are conflicts resolved?

This is one of the primary value adds of clustering software. Clustering software comes in two flavors:

- Shared Nothing - In this model, clustered hosts partition the storage between the hosts in the cluster. In this model, only one host at a time obtains access to a particular set of data. In the event load balancing or a server failure dictates, the cluster software manages a data ownership transition of the set of data to another host. Microsoft MSCS is an example.
- Shared Clustering - In this model, clustered hosts all access the same data concurrently. The cluster software provides management of locks between hosts that prevents two hosts from accessing the same data at the same time. Sun Cluster Server is an example.

Note: In the Storage Manager 7.x client, you cannot change the default host type until the Write Storage Partitioning feature is disabled.

How many partitions does the user really get?

By default, the user has one partition always associated with the default host group. Therefore, when the user enables (up to 4) or (up to 8) partitions, they are

technically getting 4 or 8 partitions in addition to the ″default″ partition. However, there is a caveat for leaving any logical drives in the Default Host Group (see next question).

Why wouldn't I use the default host group's partition?

You can potentially run into logical drive/LUN collisions if you replace a host port in a host without using the tools within the Definitions Window to associate the new host port with the host.

Furthermore, there is no read/write access control on logical drives that are located in the same partition. For operating systems running Microsoft Windows, data corruption will occur if a logical drive is mounted on more than two systems without the presence of middleware, such as Cluster Service, to provide read/write access locking.

Example: You have Host 1 mapped to logical drive Fred using LUN 1. There is also a logical drive George, which is still part of the Default Host Group that uses LUN 1. If you replace a host adapter in Host 1 without associating the new host adapter with Host 1, then Host 1 will now have access to logical drive George, instead of logical drive Fred, through LUN 1. Data corruption could occur.

Miscellaneous

What is the best way to identify which NVSRAM file version has been installed on the system when running in the controller?

In Storage Manager, use the profile command. The NVSRAM version is included in the board/controller area.

Alternatively, in the subsystem management window, right-click in the storage subsystem and select **Download -> NVSRAM**. The NVSRAM version is displayed.

When using arrayPrintSummary in the controller shell, what does *synchronized* really mean and how is it determined?

The term *synchronized* in the shell has nothing to do with firmware or NVSRAM. Simply put, *synchronized* usually means the controllers have successfully completed SOD in an orderly manner and have synchronized cache. A semaphore is passed back and forth between the controllers as one or more of the controllers are going through SOD. If this semaphore gets stuck on one controller, or if a controller does not make it through SOD, the controllers will not come up synchronized.

One way the semaphore can get stuck is if a LUN or its cache cannot be configured. In addition, if a controller has a memory parity error, the controllers will not be synchronized. There have been cases where one controller states the controllers are synchronized while its alternate states that they are not. One cause of this is that a LUN might be 'locked' by the non-owning controller; this can sometimes be fixed by turning off bit 3 of byte 0x29 in NVSRAM (Reserve and Release).

Storage Manager shows the nodes in the enterprise window with either IP address or machine name. Why is this not consistent?

Storage Manager tries to associate a name with each host node, but if one is not found, then the IP address is used. The inconsistency occurs because the client software cannot resolve the IP address to a name, or the user has manually added a host node by IP address.

Why do you see shared fibre drives twice during text setup of NT/W2K? The UTM does not seem protected (because you can create/delete the partition).

The UTM is only necessary if the Agent software is installed on a host. If you are direct-attached (network-attached) to a module, you do not need the Agent. This, in turn, means you do not need the UTM LUN. RDAC is what 'hides' the UTM from the host and creates the failover nodes. If RDAC is not installed on an operating system, then the UTM will appear to be a normal disk (either 20 Mbytes or 0 MBytes) to the operating system. However, there is no corresponding data space ″behind″ the UTM; the controller code write-protects this region. The controller will return an error if an attempt is made to write to this non-existent data region. The error is an ASC/ASCQ of 21/00 - Logical block address out of range, in the Event Viewer.

For Linux operating systems, the UTM LUN is not required and should not be present for a Linux Host.

If RDAC is not installed on a host, and NVSRAM offset 0x24 is set to 0, then you will see each LUN twice (once per controller). This is necessary because most HBAs need to see a LUN 0 on a controller in order for the host to come up. You should only be able to format one of the listed devices by using the node name which points to the controller that really owns the disk. You will probably get an error if you try to format a LUN through the node pointing to the non-owning controller. The UTM is ″owned″ by both controllers as far as the controller code is concerned, so you will probably be able to format or partition the UTM on either node.

In short, if RDAC is not installed, the UTM will appear to be a regular disk to the host. Also, you will see each disk twice. In this case, it is up to the user to know not to partition the UTM, and to know which of the two nodes for each device is the true device.

How can you determine from the MEL which node has caused problems (that is, which node has failed the controller)?

You cannot tell which host has failed a controller in a multi-host environment. You need to use the host Event Log to determine which host is having problems.

When RDAC initiates a Path failure and sets a controller to passive, why does the status in the enterprise window of Storage Manager shows the subsystem as optimal?

This is a change in the design from older code which should prove to be a useful support tool once we get used to it. A 'failed' controller which shows as passive in the EMW window, but which has been failed by RDAC, indicates that no hardware problem could be found on the controller. This type of state implies that we have a problem in the path to the controller, not with the controller itself. In short, a bad cable, hub, GBIC, and so on, on the host side is probably why the failover occurred. Hopefully, this will minimize the number of controllers which are mistakenly returned as bad.

(NT/W2K) What is the equivalent for symarray (NT) with Storage Manager W2K?

rdacfltr is the ″equivalent″ of symarray. However, symarray was a class driver, whereas rdacfltr is a Low level filter driver. rdacfltr will report Event 3 (configuration changes) and Event 18 (failover events) information. Any errors which are not of this type (such as check conditions) will be reported by W2K's class driver. These errors will be logged by the (disk) class driver. ASC/ASCQ codes and SRB status information should appear in the same location in these errors. The major difference is this break up of errors in W2K, but the error information should be available under one of these two sources in the Event Log.

Chapter 32. PD hints — MEL data format

After you have read the relevant information in this chapter, return to “RAID Controller Passive PD map” on page 139.

The SM event viewer formats and displays the most meaningful fields of major event log entries from the controller. The data displayed for individual events varies with the event type and is described in “Event descriptions” on page 358. The raw data contains the entire major event data structure retrieved from the controller subsystem. The event viewer displays the raw data as a character string. Fields that occupy multiple bytes might appear to be byte-swapped depending on the host system. Fields that might appear as byte-swapped are noted in Figure 165 on page 331.

	7	6	5	4	3	2	1	0
Byte	Constant Data Fields							
0-7	**(MSB)**	**Sequence Number - *(byte swapped)***						
								(LSB)
8-11	**(MSB)**	**Event Number - *(byte swapped)***						
								(LSB)
12-15	**(MSB)**	**Timestamp - *(byte swapped)***						
								(LSB)
16-19	**(MSB)**	**Location Information - *(byte swapped)***						
		(Channel & Device or Tray & Slot Number)						**(LSB)**
20-23	**(MSB)**	**IOP ID - *(byte swapped)***						
								(LSB)
24-25	**I/O Origin - *(byte swapped)***							
26-27	**Reserved**				**(MSB)**			
	LUN/Volume Number - *(byte swapped)*							**(LSB)**
28	**Controller Number**							
29	**Number of Optional Fields Present (M)**							
30	**Total Length of Optional Field(N)**							
31	**Pad (unused)**							
	Optional Field Data							
32	**Data Length (L)**							
33	**Pad (unused)**							
34 - 35	**Data Field Type - *(byte swapped)***							
36 - 32 + L	**Data** …							
	Last Optional Field Data Entry							

Figure 168. Constant data fields

Constant data fields

The constant data fields are described in the following section.

Sequence Number (bytes 0-7)

The **Sequence Number** field is a 64-bit incrementing value starting from the time the system log was created or last initialized. Resetting the log does not affect this value.

Event Number (bytes 8-11)

The **Event Number** field is a 4-byte encoded value that includes bits for drive and controller inclusion, event priority and the event value. The **Event Number** field is encoded as shown in .

Table 81. Event number field

	7	6	5	4	3	2	1	0
0	Internal Flags		Log Group		Priority			
1	Category				Component			
2	(MSB) Event Value							
3	(LSB)							

Internal Flags

The **Internal Flags** field (see Table 82) is used internally within the controller firmware for events that require unique handling; the host application ignores these values.

Table 82. Internal Flags field

Flag	Value
Mod Controller Number	0x2
Flush Immediate	0x1

Log Group

The **Log Group** field indicates what kind of event is being logged. All events are logged in the system log. The values for the **Log Group** field are as shown in Table 83.

Table 83. Log Group field

Log Group	Value
System Event	0x0
Controller Event	0x1
Drive Event	0x2

Priority

The **Priority** field is defined as shown in Table 84.

Table 84. Priority field

Priority	Value
Informational	0x0
Critical	0x1
Reserved	0x2 - 0xF

Event Group

The **Event Group** field specifies the general category of the event. General types of events that are logged for a given event group are listed after the event group. Event groups are defined as shown in Table 85.

Table 85. Event Group field

Event Group	Value
Unknown	0x0
Error	0x1
Failure	0x2
Command	0x3
Notification	0x4
State	0x5
Host	0x6
General	0x7
Reserved	0x8 - 0xF

Component

The **Component** field is defined as shown in Table 86.

Table 86. Component field

Component	Value
Unknown/Unspecified	0x0
Drive	0x1
Power Supply	0x2
Cooling Element	0x3
Mini hub	0x4
Temperature Sensor	0x5
Channel	0x6
Environmental Services Electronics (ESM)	0x7
Controller Electronics	0x8
Nonvolatile Cache (RPA Cache Battery)	0x9
Enclosure	0xA
Uninterruptible Power Supply	0xB
Chip - I/O or Memory	0xC
Volume	0xD
Volume Group	0xE
I/0 Port CRU	0xF

Timestamp (bytes 12-15)

The **Timestamp** field is a 4-byte value that corresponds to the real-time clock on the controller. The real-time clock is set (using the Start menu) at the time of manufacture. It is incremented every second and started relative to 1 January 1970.

Location Information (bytes 16-19)

The **Location Information** field indicates the Channel/Drive or Tray/Slot information for the event. Logging of data for this field is optional and is zero when not specified.

IOP ID (bytes 20-23)

The IOP ID used by MEL to associate multiple log entries with a single event or I/O. The IOP ID is guaranteed to be unique for each I/O. A valid IOP ID might not be available for certain MEL entries and some events use this field to log other information. The event descriptions indicate whether the IOP ID is being used for unique log information.

Logging of data for this field is optional and is zero when not specified.

I/O Origin (bytes 24-25)

The **I/O Origin** field specifies where the I/O or action originated that caused the event. It uses one of the Error Event Logger defined origin codes shown in Table 87.

Table 87. I/O Origin field

Value	Definition
0	Active Host
1	Write Cache
2	Hot Spare
3	Other Internal

A valid I/O Origin might not be available for certain MEL entries and some events use this field to log other information. The event descriptions indicate whether the I/O Origin is being used for unique log information.

Logging of data for this field is optional and is zero when not specified.

LUN/Volume Number (bytes 26-27)

The **LUN/Volume Number** field specifies the LUN or volume associated with the event being logged.

Logging of data for this field is optional and is zero when not specified.

Controller Number (byte 28)

The **Controller Number** field specifies the controller associated with the event being logged. See Table 88.

Table 88. Controller Number field

Value	Definition
0x00	Controller with Drive side SCSI ID 6 (normally the bottom controller in the subsystem)
0x01	Controller with Drive side SCSI ID 7 (normally the top controller in the subsystem)

Logging of data for this field is optional and is zero when not specified.

Number of Optional Fields Present (byte 29)

The **Number of Optional Fields Present** field specifies the number (if any) of additional data fields that follow. If this field is zero then there is no additional data for this log entry.

Optional Data

The format for the individual **Optional Data** fields is shown in Table 89.

Table 89. Optional data fields

0	Data Length (L)
1-2	Data Field Type
3 L	Data ...

Data Length (byte 32)

The length, in bytes, of the optional field data (including the Data Field Type).

Data Field Type (bytes 34-35)

See “Data field types” on page 427 for the definitions for the various Optional Data fields.

Data (byte 36 — 32 + L)

Optional field data associated with the Data Field Type. This data might appear as byte swapped when using the event viewer.

Event descriptions

The following sections contain descriptions for all events. Note that some events might not be logged in a given release. The critical events are highlighted with a gray shade. The critical events are logged in the Event Log in the Array Management Window of the storage management software. In addition, the critical events are also sent via email, SNMP, or both, depending on the alert notification set-up that the user performed within the Enterprise Management Window of the storage management software.

This section describes the following events and code information:

Destination Driver events

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Channel Failure: **(SYMsm Description - Channel failed)** **Logged when the parallel SCSI destination driver detects a channel failure.**					
Controller (0x1)	**Critical (0x1)**	**Failure (0x2)**	**Chip (0xC)**	**0x1001**	**Device: FRU info** **Origin: FRU info**
Channel Revival: **(SYMsm Description - Channel revived)** **Currently Not Logged.**					
Controller (0x1)	**Informational (0x0)**	**Notification (0x4)**	**Chip (0XC)**	**0x1002**	
Tally Exceeded: **(SYMsm Description - Drive error tally exceeded threshold)** **Currently Not Logged.**					
Drive (0x2)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x1003**	
Open Error: **(SYMsm Description - Error on drive open)** **Currently Not Logged.**					
System (0x0)	**Informational (0x0)**	**Error (0x1)**	**Drive (0x1)**	**0x1004**	
Read Failure: **(SYMsm Description - Drive read failure - retries exhausted)** **Currently Not Logged.**					
Drive (0x2)	**Informational (0x0)**	**Error (0x1)**	**Drive (0x1)**	**0x1005**	
Write Failure: **(SYMsm Description - Drive write failure - retries exhausted)** **Currently Not Logged.**					
Drive (0x2)	**Informational (0x0)**	**Error (0x1)**	**Drive (0x1)**	**0x1006**	
No Memory: **(SYMsm Description - Controller out of memory)** **Logged when memory allocation failed.**					
System (0x0)	**Informational (0x0)**	**Error (0x1)**	**Controller (0x8)**	**0x1007**	**Id: 0: SCSI Device Structure** **1: SCSI_Op NCE Structure** **2: SCSI_Op NCE Structure (non-cache)** **3: SCSI Ops**

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Unsupported Chip: **(SYMsm Description: Unsupported SCSI chip)** **Currently Not Logged.**					
Controller (0x1)	**Informational (0x0)**	**Error (0x1)**	**Chip (0xC)**	**0x1008**	
Memory Parity Error: **(SYMsm Description: Controller memory parity error)** **Logged when a memory parity error is detected by the destination driver.**					
Controller (0x1)	**Informational (0x0)**	**Error (0x1)**	**Controller (0x8)**	**0x1009**	
Drive Check Condition: **(SYMsm Description: Drive returned CHECK CONDITION)** **Logged when the driver was unable to recover the specified device returned a check condition to the driver and driver retries have been exhausted.**					
Drive (0x2)	**Informational (0x0)**	**Error (0x1)**	**Drive (0x1)**	**0x100A**	**Data Field Type: 0x010D**
Destination SOD Error: **(SYMsm Description: Start-of-day error in destination driver)** **Logged when the destination driver can't complete SOD initialization successfully.**					
Controller (0x1)	**Informational (0x0)**	**Error (0x1)**	**Controller (0x8)**	**0x100B**	**Origin: Indicates the structure that couldn't be allocated.** **1: Call to VKI_REBOOT_HOOK failed.** **2: Status byte structure allocation failed** **3: Data_phase_tag_ptrs structure allocation failed** **4: Invalid_Reselect_data structure allocation failed** **Data Field Type: 0x0206**
Destination Hardware Error: **(SYMsm Description: Hardware error on drive side of controller)** **Currently Not Logged.**					
Controller (0x1)	**Informational (0x0)**	**Error (0x1)**	**Controller (0x8)**	**0x100C**	
Destination Timeout: **(SYMsm Description: Timeout on drive side of controller)** **Currently Not Logged.**					
Controller	**Informational**	**Error**	**Controller**	**0x100D**	
Unexpected Interrupt: (SYMsm Description: Unexpected interrupt on controller) Logged due to an unexpected interrupt with no active device on chip.					
Controller (0x1)	Informational (0x0)	Error (0x1)	Controller (0x8)	0x100E	Data Field Type: 0x0201

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Bus Parity Error: **(SYMsm Description: Bus parity error on controller)** **Logged when a Bus Parity error is detected by the destination driver.**					
Controller (0x1)	**Informational (0x0)**	**Error (0x1)**	**Controller (0x8)**	**0x100F**	
Drive PFA: **(SYMsm Description: Impending drive failure (PFA) detected)** **The logged device generated a PFA condition.**					
Controller (0x1)	**Critical (0x1)**	**Error (0x1)**	**Drive (0x1)**	**0x1010**	**None**
Chip Error: **(SYMsm Description: Chip error)** **Currently Not Logged.**					
Controller (0x1)	**Informational (0x0)**	**Error (0x1)**	**Chip (0XC)**	**0x1011**	
Destination Driver: **(SYMsm Description: Destination driver error)** **Logged when the destination driver has an unrecovered error from the drive.**					
Controller (0x1)	**Informational (0x0)**	**Error (0x1)**	**Drive (0x1)**	**0x1012**	**Origin: Contains the low level destination driver internal error.** **Id: Contains the raw error logger error number.**
Destination Diagnostic Failure: **(SYMsm Description: Destination driver level 0 diagnostic failed)** **Logged when destination driver level 0 diagnostics failed for the specified channel.**					
Controller (0x1)	**Informational (0x0)**	**Error (0x1)**	**Controller (0x8)**	**0x1013**	**Id: Contains diagnostic test that failed.** **1: Read/Write registers** **2: 64 byte FIFO** **3: DMA FIFO** **Data Field Type: 0x010B**
Destination Reassign Block: **(SYMsm Description: Destination driver successfully issued reassign blocks command)** **Logged when the destination driver issues a reassign block to the drive due to a write failure.**					
Controller (0x1)	**Informational (0x0)**	**Error (0x1)**	**Controller (0x8)**	**0x1014**	**Origin: Block List**

SCSI Source Driver events

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
SCSIChip: ***(SYMsm Description: SRC driver detected exception on SCSI chip)*** ***Logged when the SRC driver detects an exception condition from the SCSI chip.***					
Controller (0x1)	***Informational (0x0)***	***Error (0x1)***	***Controller (0x8)***	***0x1101***	***Device: Base address of the SCSI chip*** ***Id: Register offset where exception was detected possible values are:*** ***0xC dstat register*** ***0x42 SIST0_REG*** ***0x43 SIST1_REG*** ***Origin: Value of the register***
HostBusReset: ***(SYMsm Description: Host bus reset asserted)*** ***Logged when the source SCSI driver asserts the RESET signal on the host SCSI bus. This is usually done as a response to have a host bus reset propagated to it by the alternate controller in a Wolfpack environment.***					
System (0x0)	***Informational (0x0)***	***Notification (0x4)***	***Controller (0x8)***	***0x1102***	***None***
HostBusResetReceived: ***(SYMsm Description: Host bus reset received)*** ***Logged when a host bus reset was received and the controller is going to propagate it to the alternate controller in a wolf pack environment. Log entries for Host Bus Reset Received and Host Bus Reset should always appear in pairs in the system log.***					
System (0x0)	***Informational (0x0)***	***Notification (0x4)***	***Controller (0x8)***	***0x1103***	***None***
Unknown Interrupt: ***(SYMsm Description: Unknown interrupt)*** ***Logged when the source SCSI driver detects an unknown interrupt.***					
Controller (0x1)	***Informational (0x0)***	***Error (0x1)***	***Controller (0x8)***	***0x1104***	***Device: Base address of the SCSI chip*** ***Origin: Value in the interrupt register.***

Fibre Channel Source Driver events

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
LIP Reset Received: **(SYMsm Description: Fibre channel-LIP reset received)** **Logged when a selective LIP reset (LipPdPs) is received.**					
Controller (0x1)	**Informational (0x0)**	**Error (0x1)**	**Controller (0x8)**	**0x1201**	**Id: Internal Checkpoint Code** **Origin: 0 = Source Side FC**
Target Reset Received: **(SYMsm Description: Fibre channel-TGT reset received)** **Logged when a Target Reset if received.**					
Controller (0x1)	**Informational (0x0)**	**Error (0x1)**	**Controller (0x8)**	**0x1202**	**Id: Internal Checkpoint Code** **Origin: 0 = Source Side FC**
Third Party Logout Reset Received:**(SYMsm Description: Fibre channel-TPRLO reset received)** **Logged when a Third Party Logout with the Global Logout bit set. This is treated as a Target Reset by the controller.**					
Controller (0x1)	**Informational (0x0)**	**Error (0x1)**	**Controller (0x8)**	**0x1203**	**Id: Internal Checkpoint Code** **Origin: 0 = Source Side FC**
Initialization Error: **(SYMsm Description: Fibre channel-driver detected error after initialization)** **Logged when a controller is unable to initialize an internal structure.**					
Controller (0x1)	**Informational (0x0)**	**Error (0x1)**	**Controller (0x8)**	**0x1204**	**Id: Internal Checkpoint Code** **Origin: 0 = Source Side FC**
General Error: **(SYMsm Description: Fibre channel-driver detected error during initialization)** **Logged when an internal error (e.g. unable to obtain memory, unable to send frame) occurs.**					
Controller (0x1)	**Informational (0x0)**	**Error (0x1)**	**Controller (0x8)**	**0x1205**	**Id: Internal Checkpoint Code** **Origin: 0 = Source Side FC**
Link Error Threshold: (SYMsm Description: Fibre channel link errors continue) **Logged when Link Error count exceeds the threshold value after the initial notification.**					
Controller (0x1)	**Informational (0x0)**	**Error (0x1)**	**Channel (0x6)**	**0x1206**	**Dev: Link Error Information** **Id: Internal Checkpoint Code**
Link Error Threshold Critical: (SYMsm Description: Fibre channel link errors-threshold exceeded) **Logged when Link Error count exceeds the threshold the first time.**					
Controller (0x1)	**Critical (0x1)**	**Error (0x1)**	**Channel (0x6)**	**0x1207**	**Dev: Link Error Information** **Id: Internal Checkpoint Code**

Fibre Channel Destination Driver events

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Init Error: (SYMsm Description: Channel initialization error) **Logged when a controller is unable to initialize hardware or an internal structure.**					
Controller (0x1)	**Informational (0x0)**	**Error (0x1)**	**Controller (0x8)**	**0x1500**	**Id: 1 = TachLite 2 = SGB Allocation 3 = Spy SGB Allocation**
Drive Reset: (SYMsm Description: Selective LIP reset issued to drive) **Logged when the fibre channel driver resets a device.**					
Drive (0x2)	Informational (0x0)	Error (0x1)	Drive (0x1)	0x1501	
Alt Controller Reset: (SYMsm Description: Selective LIP reset issued to alternate controller) Logged when the fibre channel driver resets the alternate controller.					
Controller (0x1)	Informational (0x0)	Error (0x1)	Controller (0x8)	0x1502	
Enclosure Reset: (SYMsm Description: Selective LIP reset issued to environmental card (ESM)) Logged when the fibre channel driver resets an enclosure.					
System (0x0)	Informational (0x0)	Error (0x1)	ESM (0x7)	0x1503	
Drive Enable: (SYMsm Description: Loop port enable (LPE) issued to drive) Logged when the fibre channel driver enables a drive.					
Drive (0x2)	Informational (0x0)	Notification (0x4)	Drive (0x1)	0x1504	
Alternate Enclosure Enable: (SYMsm Description: Loop port enable (LPE) issued to alternate controller) Logged when the alternate controller enables an enclosure.					
Controller (0x1)	Informational (0x0)	Notification (0x4)	Controller (0x8)	0x1505	
Enclosure Enable: (SYMsm Description: Loop port enable (LPE) issued to environmental card (ESM)) Logged when the fibre channel driver enables an enclosure.					
System (0x0)	Informational (0x0)	Notification (0x4)	ESM (0x7)	0x1506	
Drive Bypass: (SYMsm Description: Loop port bypass (LPB) issued to drive) Logged when the fibre channel driver bypasses a device.					
Drive (0x2)	Informational (0x0)	Error (0x1)	Drive (0x1)	0x1507	

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Alternate Controller Bypass: **(SYMsm Description: Loop port bypass (LPB) issued to alternate controller)** **Logged when the alternate controller is bypassed by the fibre channel driver.**					
Controller (0x1)	**Informational (0x0)**	**Error (0x1)**	**Controller (0x8)**	**0x1508**	
Enclosure Bypass: **(SYMsm Description: Loop port bypass (LPB) issued to environmental card(ESM))** **Logged when an enclosure is bypassed by the fibre channel driver.**					
System (0x0)	**Informational (0x0)**	**Error (0x1)**	**ESM (0x7)**	**0x1509**	
Drive Missing: **(SYMsm Description: Unresponsive drive (bad AL_PA error))** **Logged when the fibre channel driver detects that a drive is missing.**					
Drive (0x2)	**Informational (0x0)**	**Error (0x1)**	**Drive (0x1)**	**0x150A**	
Alternate Controller Missing: **(SYMsm Description: Unresponsive alternate controller (bad AL_PA error))** **Logged when the fibre channel driver detects that the alternate controller is missing.**					
Controller (0x1)	**Informational (0x0)**	**Error (0x1)**	**Controller (0x8)**	**0x150B**	
Enclosure Missing: **(SYMsm Description: Unresponsive environmental card (ESM) (bad AL_PA error))** **Logged when the fibre channel driver detects that an enclosure is missing.**					
System (0x0)	**Informational (0x0)**	**Error (0x1)**	**ESM (0x7)**	**0x150C**	
Channel Reset: **(SYMsm Description: Channel reset occurred)** **Logged when a fibre channel port is reset.**					
System (0x0)	Informational (0x0)	Notification (0x4)	Channel (0x6)	0x150D	
Loop Diagnostic Failure: **(SYMsm Description: Controller loop-back diagnostics failed)** **Logged when loop or minihub diagnostics detect that the controller is the bad device on the loop.**					
System (0x0)	Critical (0x1)	Notification (0x4)	Controller (0x8)	0x150E	
Channel Miswire: (SYMsm Description: Channel miswire) Logged when two channels are connected with one or more ESMs in between.					
System (0x0)	**Critical (0x1)**	**Error (0x1)**	**Channel (0x6)**	**0x150F**	
ESM Miswire: (SYMsm Description: Environmental card miswire) Logged when two ESMs of the same tray are seen on the same channel.					
System (0x0)	**Critical (0x1)**	**Error (0x1)**	**ESM (0x7)**	**0x1510**	

Channel Miswire Clear: (SYMsm Description: Channel miswire resolved) Logged when the channel miswire is cleared.					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Channel (0x6)**	**0x1511**	
ESM Miswire Clear: (SYMsm Description: Environmental card miswire resolved) Logged when the environmental card miswire is cleared.					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**ESM (0x7)**	**0x1512**	

VDD events

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Repair Begin: **(SYMsm Description: Repair started)** **Logged when a repair operation is started for the specified unit.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume (0xD)**	**0x2001**	**None**
Repair End: **(SYMsm Description: Repair completed)** **Currently Not Logged.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume (0xD)**	**0x2002**	**Data Field Type: 0x0613**
Interrupted Write Begin: **(SYMsm Description: Interrupted write started)** **Currently Not Logged.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume (0xD)**	**0x2003**	
Interrupted Write End: **(SYMsm Description: Interrupted write completed)** **Currently Not Logged.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume (0xD)**	**0x2004**	
Fail Vdisk: **(SYMsm Description: Virtual disk failed - interrupted write)** **Logged when the specified LUN is internally failed.**					
System (0x0)	**Informational (0x0)**	**Failure (0x2)**	**Volume (0xD)**	**0x2005**	**Origin: LBA of the detected failure**
Fail Piece: **(SYMsm Description: Piece failed)** **Currently Not Logged.**					
System (0x0)	**Informational (0x0)**	**Failure (0x2)**	**Drive (0x1)**	**0x2006**	
Fail Piece Delay: **(SYMsm Description: Fail piece delayed)** **Currently Not Logged.**					
System (0x0)	**Informational (0x0)**	**Failure (0x2)**	**Drive (0x1)**	**0x2007**	
DEAD LUN Reconstruction: (SYMsm Description: Failed volume started reconstruction) Currently Not Logged.					
System (0x0)	Informational (0x0)	Notification (0x4)	Drive (0x1)	0x2008	

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
RAID 0 Write Fail: **(SYMsm Description: RAID 0 write failures)** **Currently Not Logged.**					
System (0x0)	**Informational (0x0)**	**Error (0x1)**	**Drive (0x1)**	**0x2009**	
Data Parity Mismatch: **(SYMsm Description: Data/parity mismatch on volume)** **Logged when a data/parity mismatch is detected during data scrubbing.**					
System (0x0)	**Informational (0x0)**	**Error (0x1)**	**Volume (0xD)**	**0x200A**	**Data Field Type: 0x0706**
Unrecovered Deferred Error**: (SYMsm Description: Unrecovered deferred error on volume)** **Currently Not Logged.**					
System (0x0)	**Informational (0x0)**	**Error (0x1)**	**Volume (0xD)**	**0x200B**	
Recovered Error: **(SYMsm Description: Recovered error on volume)** **Currently Not Logged.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume (0xD)**	**0x200C**	
I/O Aborted: **(SYMsm Description: I/O aborted on volume)** **Currently Not Logged.**					
System (0x0)	**Informational (0x0)**	**Error (0x1)**	**Volume (0xD)**	**0x200D**	
VDD Reconfigure: **(SYMsm Description: Virtual disk driver reconfigured)** **Currently Not Logged.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x200E**	
VDD Synchronize Begin: **(SYMsm Description: Cache synchronization started)** **Logged when cache synchronization is begun from an external (to VDD) source.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x200F**	**Data Field Type: 0x0706** **0's in Number of blocks filed indicate entire LUN will be synchronized.**
VDD Synchronize End: (SYMsm Description: Cache synchronization completed) Logged when cache synchronization for the specified unit completes.					
System (0x0)	Informational (0x0)	Notification (0x4)	Controller (0x8)	0x2010	Device: Contains ending error status Origin: Contains buf flags value

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
VDD Purge Begin: **(SYMsm Description: Cache flush started)** **Logged when an operation to flush cache for the specified unit is begun.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x2011**	**None**
VDD Purge End: **(SYMsm Description: Cache flush completed)** **Logged when an operation to flush cache for the specified unit has completed.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x2012**	**None**
VDD Cache Recover: **(SYMsm Description: Unwritten data/parity recovered from cache)** **Logged when unwritten data and parity is recovered from cache at start-of-day or during a forced change in LUN ownership between the controllers.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x2013**	**Origin: Contains the number of cache blocks recovered.**
VDD Error: **(SYMsm Description: VDD logged an error)** **Logged when VDD logs an error.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x2014**	**Data Field Type: 0x0707**
Uncompleted Write Count: **(SYMsm Description: Uncompleted writes detected in NVSRAM at start-of-day)** **Logged at start-of-day when uncompleted writes are detected in NVSRAM.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x2015**	**Origin: Contains the number of uncompleted writes found**
Write Count: **(SYMsm Description: Interrupted writes processed)** **Logged when VDD processes interrupted writes for the specified unit.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x2016**	**Origin: Number of interrupted writes processed.**
Log Write Count: **(SYMsm Description: Interrupted writes detected from checkpoint logs)** **Logged when VDD creates a list of interrupted writes from the data/parity checkpoint logs.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x2017**	**Origin: Number of interrupted writes processed.**
VDD Wait: (SYMsm Description: I/O suspended due to no pre-allocated resources) Logged when an I/O is suspended because of no preallocated resources. This event is logged once per resource.					
System (0x0)	Informational (0x0)	Notification (0x4)	Controller (0x8)	0x2018	Data Field Type: 0x0700 Data: First 4 characters of the resource name.

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
VDD Long I/O: **(SYMsm Description: Performance monitor: I/O's elapsed time exceeded threshold)** **Logged if performance monitoring is enabled and an I/Os elapsed time equal to or exceeds the threshold limit.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x2019**	**Origin: Contains the elapsed time for the I/O** **Device: Contains the threshold value.**
VDD Restore Begin: **(SYMsm Description: VDD restore started)** **Logged at the beginning of a RAID 1 or RAID 5 VDD restore operation.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x201A**	**Data Field Type: 0x0612**
VDD Restore End: **(SYMsm Description: VDD restore completed)** **Logged at the end of a restore operation.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x201B**	**Data Field Type: 0x0613**
VDD Recover Begin: **(SYMsm Description: VDD recover started)** **Logged at the beginning of a RAID 1 or RAID 5 VDD recover operation.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x201C**	**Data Field Type: 0x0617**
VDD Recover End: **(SYMsm Description: VDD recover completed)** **Logged at the end of a recover operation.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x201D**	**Data Field Type: 0x0613**
VDD Repair Begin: **(SYMsm Description: VDD repair started)** **Logged at the beginning of a repair operation.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x201E**	**None**
VDD Repair End: **(SYMsm Description: VDD repair completed)** **Logged at the end of a repair operation.**					
System	**Informational**	**Notification**	**Controller**	**0x201F**	**Data Field Type: 0x0613**
Interrupted Write Fail Piece: (SYMsm Description: Piece failed during interrupted write) Logged when a piece is failed during an interrupted write operation.					
System (0x0)	Informational (0x0)	Notification (0x4)	Controller (0x8)	0x2020	Data Field Type: 0x0612

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Interrupted Write Fail Vdisk: **(SYMsm Description: Virtual disk failed during interrupted write)** **Logged when a virtual disk is failed as part of a interrupted write operation.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x2021**	**Origin: LBA of the LUN that caused the failure.**
Scrub Start: **(SYMsm Description: Media scan (scrub) started)** **Logged when scrubbing is started for the specified unit.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume (0xD)**	**0x2022**	**None**
Scrub End: **(SYMsm Description: Media scan (scrub) completed)** **Logged when scrubbing operations for the specified unit have completed.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume (0xD)**	**0x2023**	**Data Field Type: 0x0618**
Scrub Resume: **(SYMsm Description: Media scan (scrub) resumed)** **Logged when scrubbing operations are resumed for the specified unit.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume (0xD)**	**0x2024**	**None**
Reconstruction Begin: **(SYMsm Description: Reconstruction started)** **Logged when reconstruction operations are started for the specified unit.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume (0xD)**	**0x2025**	**None**
Reconstruction End: **(SYMsm Description: Reconstruction completed)** **Logged when reconstruction operations for the specified unit have completed.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume (0xD)**	**0x2026**	**Data Field Type: 0x0613**
Reconstruction Resume: **(SYMsm Description: Reconstruction resumed)** **Logged when reconstruction operations are resumed for the specified unit.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume (0xD)**	**0x2027**	**None**
Reconstruction Begin: (SYMsm Description: Modification (reconfigure) started) Logged when reconfiguration operations are started for the specified unit.					
System (0x0)	Informational (0x0)	Notification (0x4)	Volume (0xD)	0x2028	None

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Reconfiguration End: **(SYMsm Description: Modification (reconfigure) completed)** **Logged when reconfiguration operations for the specified unit have completed.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume (0xD)**	**0x2029**	**Data Field Type: 0x0613**
Reconfiguration Resume: **(SYMsm Description: Modification (reconfigure) resumed)** **Logged when reconfiguration operations are resumed for the specified unit.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume (0xD)**	**0x202A**	**None**
Parity Scan Begin: **(SYMsm Description: Redundancy check started)** **Logged when parity scan operations are started for the specified unit.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume (0xD)**	**0x202B**	**None**
Parity Scan End: **(SYMsm Description: Redundancy check completed)** **Logged when parity scan operations for the specified unit have completed**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume (0xD)**	**0x202C**	**None**
Parity Scan Resume: **(SYMsm Description: Redundancy check resumed)** **Logged when parity scan operations are resumed for the specified unit.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume (0xD)**	**0x202D**	**None**
Miscorrected Data: **(SYMsm Description: Read drive error during interrupted write)** **Logged when an Unrecoverable Read Error is detected.**					
System (0x0)	Critical (0x1)	Notification (0x4)	Controller (0x8)	0x202E	Origin: LBA of the LUN that caused the failure.
Auto LUN Transfer End: **(SYMsm Description: Automatic volume transfer completed)** **Logged when an auto lun transfer operation has completed.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x202F**	**None**
Format End: (SYMsm Description: Initialization completed on volume) Logged when a volume format has completed.					
System (0x0)	Informational (0x0)	Notification (0x4)	Volume (0xD)	0x2030	None

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Format Begin: **(SYMsm Description: Initialization started on volume)** **Logged when a volume format has begun.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume (0xD)**	**0x2031**	**None**
Format Resume: **(SYMsm Description: Initialization resumed on volume)** **Logged when a volume format has resumed.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume (0xD)**	**0x2032**	**None**
Parity Repair: **(SYMsm Description: Parity reconstructed on volume)** **Logged when parity has been reconstructed on a volume.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume (0xD)**	**0x2033**	**None**
HSTSCANMismatch: **(SYMsm Description: Data/parity mismatch detected on volume)** **Logged when a data/parity mismatch is detected on a volume.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume (0xD)**	**0x2034**	**None**

Cache Manager events

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Late Check In: **(SYMsm Description: Alternate controller checked in late)** **Logged when the alternate controller checked in late.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x2101**	**None**
Mirror Out Of Sync: **(SYMsm Description: Cache mirroring on controllers not synchronized)** **The mirror is out of sync with the alternate controllers mirror.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x2102**	**None**
UPS: **(SYMsm Description: UPS battery is fully charged)** **Currently Not Logged.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**UPS**	**0x2103**	
Synchronize and Purge: **(SYMsm Description: Controller cache synchronization/purge event)** **Currently Not Logged.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x2104**	
Reconfigure Cache: **(SYMsm Description: Controller cache reconfigure event)** **Currently Not Logged.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x2105**	
Set Configuration: **(SYMsm Description: Update requested on controller cache manager's DACSTORE)** **A request to update the cache managers DACSTORE area was received.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x2106**	**None**
Clear Configuration: **(SYMsm Description: Clear requested on controller cache manager's DACSTORE)** **A request to clear the cache manager's DACSTORE area was received.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x2107**	**None**
Cache Manager Errors: (SYMsm Description: Controller cache manager experiencing errors) Currently Not Logged.					
System (0x0)	Informational (0x0)	Notification (0x4)	Controller (0x8)	0x2108	

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
CCM Hardware Mismatch: **(SYMsm Description: Controller cache not enabled - cache sizes do not match)** **Write back cache could not be enabled due to different cache sizes of the controllers in the subsystem. ASC/ASCQ value of 0xA1/0x00 is also logged with this event.**					
System (0x0)	**Critical (0x1)**	**Error (0x1)**	**Controller (0x8)**	**0x2109**	**None**
Cache Disabled Internal: **(SYMsm Description: Controller cache not enabled or was internally disabled)** **Write back cache could not be enabled or was internally disabled. The ASC/ASCQ value of 0xA0/0x00 is also logged with this event.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x210A**	**None**
Cache Synchronize Failed: **(SYMsm Description: Cache between controllers not synchronized)** **Cache synchronization between the controllers failed. The ASC/ASCQ value of 0x2A/0x01 is also logged with this event.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x210B**	**None**
Cache Battery Failure: **(SYMsm Description: Controller cache battery failed)** **Cache battery has failed. ASC/ASCQ of 0x0C/0x00 is also logged with this event.**					
System (0x0)	**Critical (0x1)**	**Notification (0x4)**	**Battery (0x9)**	**0x210C**	**None**
Deferred Error: **(SYMsm Description: Controller deferred error)** **Currently Not Logged.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x210D**	
Cache Data Loss: **(SYMsm Description: Controller cache memory recovery failed after power cycle or reset)** **Logged by cache manager when cache blocks can't be successfully recovered. Companion to an ASC/ASCQ status of 0x0C/0x81.**					
Controller (0x1)	**Critical (0x1)**	**Error (0x1)**	**Controller (0x8)**	**0x210E**	**The LUN and LBA(in Id field) are logged in the event data if they are available. An unavailable LUN is logged as 0xFF. An unavailable LBA is logged as 0. No additional data is logged.**

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Memory Parity Error Detected: **(SYMsm Description: Controller cache memory parity error detected)** **Logged when a memory parity error is detected.**					
Controller (0x1)	**Informational (0x0)**	**Error (0x1)**	**Controller (0x8)**	**0x210F**	**Device:** 0 = **Processor Memory** 1 = **RPA Memory** 2 = **Spectra Double Bit Error** 3 = **Spectra Multi-Bit Error** 4 = **Spectra PCI Error** 5 = **RPA PCI Error**
Cache Memory Diagnostic Fail: **(SYMsm Description: Controller cache memory initialization failed)** **Logged when a persistent RPA Memory Parity error is detected.**					
System (0x0)	**Critical (0x1)**	**Failure (0x2)**	**Controller (0x8)**	**0x2110**	
Cache Task Fail: **(SYMsm Description: Controller cache task failed)** **Currently Not Logged.**					
System (0x0)	**Informational (0x0)**	**Failure (0x2)**	**Controller (0x8)**	**0x2111**	
Cache Battery Good: **(SYMsm Description: Controller cache battery is fully charged)** **Logged when the cache battery has transitioned to the good state.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Battery (0x9)**	**0x2112**	**None**
Cache Battery Warning: **(SYMsm Description: Controller cache battery nearing expiration)** **Logged when the cache battery is within the specified number of weeks of failing. The ASC/ASCQ value of 0x3F/0xD9 is also logged with this event.**					
System (0x0)	**Critical (0x1)**	**Error (0x1)**	**Battery (0x9)**	**0x2113**	
Alternate Cache Battery Good: **(SYMsm Description: Alternate controller cache battery is fully charged)** **Logged when the alternate controller's cache battery has transitioned to the good state.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Battery (0x9)**	**0x2114**	**None**
Alternate Cache Battery Warning: (SYMsm Description: Alternate controller cache battery nearing expiration) Currently Not Logged.					
System (0x0)	Informational (0x0)	Error (0x1)	Battery (0x9)	0x2115	

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Alternate Cache Battery Fail: **(SYMsm Desription: Alternate controller cache battery failed)** **Logged when the alternate controller's cache battery has transitioned to the failed state.**					
System (0x0)	**Informational (0x0)**	**Failure (0x2)**	**Battery (0x9)**	**0x2116**	**None**
CCM Error Cleared: **(SYMsm Description: Controller cache manager error cleared)** **On occasion CCM may log an error prematurely and then clear it later. For example errors may be logged when the alternate controller is removed from the subsystem. If the controller is replaced before a write is done CCM will cancel the errors logged since the controller is replaced and functioning normally.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x2117**	**Id: Contains the event that is being cleared**
Memory Parity ECC Error: **(SYMsm Description: Memory parity ECC error)** **Logged when a memory parity error occurs and information on the error is available.**					
Controller (0x1)	**Informational (0x0)**	**Error (0x1)**	**Controller (0x8)**	**0x2118**	**Data Field Type: 0x0111**
Recovered Data Buffer Memory Error: **(SYMsm Description: Recoverable error in data buffer memory detected/corrected)** **Logged when the controller has detected and corrected a recoverable error in the data buffer memory.**					
Controller (0x1)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x2119**	
Cache Error Was Corrected: **(SYMsm Description: Cache corrected by using alternate controller's cache)** **Logged when the cache manager has corrected using the alternate controller's cache memory.**					
Controller (0x1)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x211A**	**None**

Configuration Manager events

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Mark LUN Optimal: **(SYMsm Description: Volume marked optimal)** **Currently Not Logged.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume (0xD)**	**0x2201**	
Add Vdisk: **(SYMsm Description: Volume added)** **Logged when a LUN is added to the subsystem.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume (0xD)**	**0x2202**	**Data Field Type: 0x0612**
Delete Vdisk: **(SYMsm Description: Volume group or volume deleted)** **Logged when the specified virtual disk is deleted.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume (0xD)**	**0x2203**	**None**
Resume I/O: **(SYMsm Description: I/O is resumed)** **Logged when vdResumeIo is called for specified device.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume (0xD)**	**0x2204**	**None**
Fail Copy Source: **(SYMsm Description: Source drive failed during copy operation)** **Logged when the source drive of a copy type operation fails.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume (0xD)**	**0x2205**	**None**
CFG Reconstruction Device Complete:**(SYMsm Description: Reconstruction completed)** **Logged when CFG manager has completed reconfiguring the specified device successfully.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x2206**	**None**
CFG Copy Device Complete:**(SYMsm Description: Device copy complete)** **Logged when the configuration manager has completed the copy process to the specified device.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume (0xD)**	**0x2207**	**None**
CFG Reconfiguration Setup: (SYMsm Description: Modification (reconfigure) started) Logged by the configuration manager when it has set up the specified unit and device number for reconfiguration and is going to call VDD to start the reconfiguration.					
System (0x0)	Informational (0x0)	Notification (0x4)	Volume (0xD)	0x2208	Data Field Type: 0x0612

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
CFG Reconfiguration: **(SYMsm Description: Modification (reconfigure) completed)** **Logged when the LUN has finished reconfigure process the new LUN state is in origin.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume (0xD)**	**0x2209**	**None**
CFG Copyback Start: **(SYMsm Description: Copyback started)** **Logged when copy task is started.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x220A**	**None**
CFG Copyback Restart: **(SYMsm Description: Copyback restarted)** **Logged when copy task is restarted.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x220B**	**None**
CFG Fail Delayed: **(SYMsm Description: Device failed during interrupted write processing)** **Logged when the specified device or LUN is failed during interrupted write processing. SK/ASC/ASCQ = 0x06/0x3F/0x8E will be reported for the device that is failed. SK/ASC/ASCQ = 0x06/0x3F/0xE0 will be reported for each LUN that is goes dead.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x220C**	**None**
CFG Scrub Enabled: **(SYMsm Description: Media scan (scrub) enabled)** **Logged when the configuration manager enables scrubbing for the specified device.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume (0xD)**	**0x220D**	**Origin: 0 – Scrub & parity check are turned off** **1 - Scrub is enabled** **2 - Parity check is enabled** **3 - Scrub & parity check enabled**
CFG Scrub Start: **(SYMsm Description: Media scan (scrub) started)** **Logged when a scrub operation is started for the specified unit.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume (0xD)**	**0x220E**	**Origin: Actual buf address**
CFG Scrub Complete: (SYMsm Description: Media scan (scrub) completed) Logged when a scrub operation is completed for the specified unit.					
System (0x0)	Informational (0x0)	Notification (0x4)	Volume (0xD)	0x220F	None

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
CFG Restore Begin: **(SYMsm Description: Restore started)** **Logged when cfg manager begins a restore operation on specified unit and device number.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume (0xD)**	**0x2210**	**None**
CFG Restore End: **(SYMsm Description: Restore completed)** **Logged when cfg manager successfully completes a restore operation. If an error occurred during the restore this entry may not appear.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume (0xD)**	**0x2211**	**None**
CFG Parity Scan Restore: **(SYMsm Description: Parity repaired)** **Logged when the configuration manager repairs the parity of specified unit and device.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x2212**	**Origin: Starting LBAs for the LUN**
Zero LUN: **(SYMsm Description: Volume initialized with zeros)** **Logged when zeros are written to the specified LUN.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume (0xD)**	**0x2213**	**Data Field Type: 0x0706**
CFG Copy Sundry: **(SYMsm Description: One or more Sundry regions created)** **Logged when configuration manager creates 1 or more sundry drives.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Unknown (0x0)**	**0x2214**	**Origin: The number of sundry drives created**
CFG Post Fail: **(SYMsm Description: Drive marked failed)** **Logged when configuration manager posts a UA/AEN for a failed drive.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x2215**	
Piece Out of Service (OOS): **(SYMsm Description: Piece taken out of service)** **Logged when the configuration manager take a piece of the specified LUN out of service.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x2216**	**Origin: New LUN state**
Piece Fail: (SYMsm Description: Piece failed) Logged when a piece of specified LUN is failed.					
System (0x0)	Informational (0x0)	Notification (0x4)	Drive (0x1)	0x2217	Origin: Piece number

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Piece Fail Delay: **(SYMsm Description: Piece failed during uncompleted write processing)** **Logged when a piece of specified LUN is failed during uncompleted write processing.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x2218**	**Origin: Piece number**
Piece Removed: **(SYMsm Description: Piece removed from volume)** **Logged when a piece of specified LUN has been removed.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x2219**	**Origin: Piece number**
Piece Replace: **(SYMsm Description: Piece replaced)** **Logged when a piece of specified LUN has been replaced.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x221A**	**Origin: Piece number**
Piece In Service: **(SYMsm Description: Piece placed in service)** **Logged when the configuration manager places a LUN piece in service.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x221B**	**None**
Drive Group Offline: **(SYMsm Description: Volume group placed offline)** **Logged when an entire drive group is placed online the first 16 devices of the drive group are recorded in the data buffer.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume Group (0xE)**	**0x221C**	**Data Field Type: 0x0603**
Drive Group Online: **(SYMsm Description: Volume group placed online)** **Logged when an entire drive group is placed online.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume Group (0xE)**	**0x221D**	**Data Field Type: 0x0603**
LUN Initialized: **(SYMsm Description: Volume group or volume initialized)** **Logged when a LUN has been created.**					
System (0x0)	Informational (0x0)	Notification (0x4)	Volume (0xD)	0x221E	Device: Contains the LUN number initialized
IAF LUN Initialized: (SYMsm Description: Initialization (immediate availability) started or restarted) Logged when an immediate availability LUN has been initialized.					
System (0x0)	Informational (0x0)	Notification (0x4)	Volume (0xD)	0x221F	Device: Contains the LUN number initialized

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
GHS Added: **(SYMsm Description: Hot spare drive added to hot spare list)** **Logged when a drive is added to the global hot spare list.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x2220**	**None**
GHS Removed: **(SYMsm Description: Hot spare drive removed from hot spare list)** **Logged when a drive is removed from the hot spare list.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x2221**	**None**
Change Unit Number: **(SYMsm Description: Logical unit number for volume reassigned)** **Logged when a new rank has a duplicate unit number as an existing LUN.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x2222**	**Origin: New unit number** **LUN: Old unit number**
Duplicate Physical Device: **(SYMsm Description: Duplicate data structure exists for two devices)** **Logged when cfg mgr discovers a duplicate data structure exists for two devices.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x2223**	**Id: Device id of first device** **Device: Device id of second device**
CFG Reconstruction Start: **(SYMsm Description: Reconstruction started)** **Logged when reconstruction is started for the specified device.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x2224**	**None**
CFG Reconstruction Restart: **(SYMsm Description: Reconstruction restarted)** **Logged when reconstruction is restarted for the specified device.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x2225**	**None**
CFG Spin Down: **(SYMsm Description: Drive spun down)** **Logged when the specified drive is spun down.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x2226**	**None**

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Set Device Operational: **(SYMsm Description: Drive marked optimal)** **Logged when the routine cfgSetDevOper (external interface) is called from the shell, by the format command handler, or by the mode select command handler.**					
Drive (0x2)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x2227**	**None**
Delete Device: **(SYMsm Description: Drive deleted)** **Logged when cfgDelDrive (external interface) or cfgDriveDeleted is called. This interface can be called from the shell or mode select command handler.**					
Drive (0x2)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x2228**	**None**
Ctl Fail Drive: **(SYMsm Description: Drive failed by controller)** **Logged when the configuration manager internally fails the device.**					
System (0x0)	**Critical (0x1)**	**Notification (0x4)**	**Drive (0x1)**	**0x2229**	**Origin: Reason for failure** **0x91: Locked Out** **0xA3: User Failed via Mode Select**
Mark Drive GHS: **(SYMsm Description: Hot spare drive assigned)** **Logged when an unassigned drive is specified as a global hot spare.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x222A**	**None**
CFG Cold Replaced: **(SYMsm Description: Drive replaced when Storage Array was turned off)** **Logged when the configuration manager finds a drive that has been cold replaced. i.e. Replaced when the controller & subsystem were powered off.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x222B**	**None**
Device Unassigned: **(SYMsm Description: Drive marked unassigned)** **Logged when a drive is to be marked unassigned, also Logged if an unknown drive that was part of a LUN is to be brought online.**					
Drive (0x2)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x222C**	**None**
Device Fail: **(SYMsm Description: Drive manually failed)** **Logged when cfgFailDrive (external interface) or cfgDriveFailed is called.**					
Device Removed: (SYMsm Description: Mark drive removed) Logged when a drive is to be marked removed.					
Drive (0x2)	Informational (0x0)	Notification (0x4)	Drive (0x1)	0x222E	None

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Device Replace: **(SYMsm Description: Drive marked replaced)** **Logged when a notification is received that a failed drive is to be replaced and that data reconstruction on this device should begin.**					
Drive (0x2)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x222F**	**None**
Device Manager Fail: **(SYMsm Description: Drive failed by device manager)** **Logged when the configuration manager state machine has been called to fail the device. This is an additional event that indicates the configuration manager has determined that processing has to be done in order to fail the device. Appearance of this entry depends on the drive's previous state prior to being failed.**					
Drive (0x2)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x2230**	**Origin: Reason for Failure**
Device Manager Removed: **(SYMsm Description: Drive marked removed)** **Logged when the configuration manager state machine is going to mark a drive removed.**					
Drive (0x2)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x2231**	**None**
Device Manager Removed 1: **(SYMsm Description: Removed drive marked removed)** **Logged when the configuration manager is called to remove a drive that has already been removed.**					
Drive (0x2)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x2232**	**None**
Device Manager Removed 2: **(SYMsm Description: Unassigned drive marked removed)** **Logged when an unassigned drive has been marked as removed by the configuration manager.**					
Drive (0x2)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x2233**	**None**
Device Manager Removed 3: **(SYMsm Description: Reconstructing drive marked removed)** **Logged when a drive has been removed that hasn't finished reconstruction, usually happens when a drive that is waiting for reconstruction to begin is removed.**					
Drive (0x2)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x2234**	**None**
Device Manager Removed 4: (SYMsm Description: Optimal/Replaced drive marked removed) Logged when an optimal or replaced drive has been removed.					
Drive (0x2)	Informational (0x0)	Notification (0x4)	Drive (0x1)	0x2235	None

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Device Manager Copy Done: **(SYMsm Description: Hot spare drive copy completed)** **Logged by the configuration manager state machine when a copy operation has completed on a global hot spare drive.**					
Drive (0x2)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x2236**	**Origin: Internal device flags managed by the configuration manager, definition is unspecified.**
Device Manager Copy Done 1: **(SYMsm Description: Replaced drive completed reconstruction)** **Copy Done: Logged when a replaced drive has finished reconstruction.**					
Drive (0x2)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x2237**	**None**
Device Manager New: **(SYMsm Description: Drive added in previously unused slot)** **Logged when a drive has been inserted in a previously unused slot in the subsystem.**					
Drive (0x2)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x2238**	**None**
Device Manager GHS Unassigned: **(SYMsm Description: Hot spare drive assigned internally)** **Logged when an unassigned drive is marked as a global hot spare internally.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x2239**	**None**
Device Manager Delete: **(SYMsm Description: Drive marked deleted)** **Logged when a drive is to be marked as deleted. Previously the drive was unassigned or failed.**					
Drive (0x2)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x223A**	**None**
Device Manager Replace: **(SYMsm Description: Failed/Replaced drive marked replaced)** **Logged when a failed or replaced drive is marked as replaced.**					
Drive (0x2)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x223B**	**None**
Device Manager Replace 1: **(SYMsm Description: Drive reinserted)** **Logged when a removed optimal drive or replaced drive has been reinserted or when a failed drive is reinserted.**					
Drive (0x2)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x223C**	**Origin: Location where event is logged, value unspecified**
Device Manager Replace 2: (SYMsm Description: Unassigned drive replaced) Logged when an unassigned drive has been replaced.					
Drive (0x2)	Informational (0x0)	Notification (0x4)	Drive (0x1)	0x223 D	Origin: Location where event is logged, value is unspecified

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Device Manager Operational:**(SYMsm Description: Drive marked optimal)** **Logged when a drive has been marked operational.**					
Drive (0x2)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x223E**	**None**
Device Manager Operational:**(SYMsm Description: Partially reconstructed drive marked optimal)** **Logged when a optimal drive that hasn't completed reconstruction is marked operational.**					
Drive (0x2)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x223F**	**None**
Device Manager No DACSTORE Unassigned:**(SYMsm Description: DACSTORE created for unassigned or hot spare drive)** **Logged when an unassigned drive or unassigned global hot spare has no DACSTORE and a DACSTORE has been created.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x2240**	**None**
Device Manager No DACSTORE Fail:**(SYMsm Description: Unassigned drive with no DACSTORE failed)** **Logged when an unassigned drive without a DACSTORE has been failed.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x2241**	**None**
Device Manager No DACSTORE Delete:**(SYMsm Description: Unassigned drive with no DACSTORE deleted)** **Logged when an unassigned drive without a DACSTORE has been deleted.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x2242**	**None**
Device Manager No DACSTORE Remove:**(SYMsm Description: Unassigned drive with no DACSTORE removed)** **Logged when an unassigned drive without a DACSTORE has been removed.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x2243**	**None**
Device Manager Unassigned:**(SYMsm Description: Unknown drive marked unassigned)** **Logged when an unknown drive is marked unassigned.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x2244**	**None**
CFG Scrub Stop: (SYMsm Description: Media scan (scrub) stopped) Logged when a scrub operation is stopped for the specified unit.					
System (0x0)	Informational (0x0)	Notification (0x4)	Volume (0xD)	0x2245	None

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
CFG Scrub Resume: **(SYMsm Description: Media scan (scrub) resumed)** **Logged when a scrub operation is resumed for the specified unit or drive group.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume (0xD)**	**0x2246**	**None**
CFG Unrecovered Interrupted Write: **(SYMsm Description: Data lost on volume during unrecovered interrupted write)** **Logged when a LUN is marked DEAD due to a media error failure during SOD. An error occurred during Interrupted Write processing causing the LUN to transition to the DEAD State. SK/ASC/ASCQ = 0x06/0x3F/0xEB will be offloaded for this error.**					
System (0x0)	**Critical (0x1)**	**Notification (0x4)**	**Volume (0xD)**	**0x2247**	**None**
CFG Unrecovered Write Failure: **(SYMsm Description: Drive failed – write failure)** **Logged when the configuration manager posts an UA/AEN of ASC/ASCQ = 0x3F/0x80 indicating the controller set the drive state to "Failed – Write Failure".**					
System (0x0)	**Critical (0x1)**	**Failure (0x2)**	**Drive (0x1)**	**0x2248**	**Origin: FRU info**
CFG Drive Too Small: **(SYMsm Description: Drive capacity less than minimum)** **Logged when the configuration manager posts an UA/AEN of ASC/ASCQ = 0x3F/0x8B indicating the controller set the drive state to "Drive Capacity < Minimum".**					
System (0x0)	**Critical (0x1)**	**Notification (0x4)**	**Drive (0x1)**	**0x2249**	**Origin: FRU info**
Wrong Sector Size: **(SYMsm Description: Drive has wrong block size)** **Logged when the configuration manager posts an UA/AEN of ASC/ASCQ = 0x3F/0x8C indicating the controller set the drive state to "Drive has wrong blocksize".**					
System (0x0)	**Critical (0x1)**	**Notification (0x4)**	**Drive (0x1)**	**0x224A**	**Origin: FRU info**
Drive Format Failed: **(SYMsm Description: Drive failed-initialization failure)** **Logged when the configuration manager posts an UA/AEN of ASC/ASCQ = 0x3F/0x86 indicating the controller set the drive state to "Failed – Format failure".**					
System (0x0)	**Critical (0x1)**	**Notification (0x4)**	**Drive (0x1)**	**0x224B**	**Origin: FRU info**
Wrong Drive: (SYMsm Description: Wrong drive removed/replaced) Logged when the configuration manager posts an UA/AEN of ASC/ASCQ = 0x3F/0x89 indicating the controller set the drive state to "Wrong drive removed/replaced".					
System (0x0)	Informational (0x0)	Notification (0x4)	Drive (0x1)	0x224C	Origin: FRU info

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Drive No Response: **(SYMsm Description: Drive failed-no response at start of day)** **Logged when the configuration manager posts an UA/AEN of ASC/ASCQ = 0x3F/0x85 indicating the controller set the drive state to "Failed – No Response".**					
System (0x0)	**Critical (0x1)**	**Notification (0x4)**	**Drive (0x1)**	**0x224D**	**Origin: FRU info**
Reconstruction Drive Failed: **(SYMsm Description: Drive failed-initialization/reconstruction failure)** **Logged when the configuration manager posts an UA/AEN of ASC/ASCQ = 0x3F/0x82 indicating the controller set the drive state to "Failed" be it was unable to make the drive usable after replacement.**					
System (0x0)	**Critical (0x1)**	**Failure (0x2)**	**Drive (0x1)**	**0x224E**	**Origin: FRU info**
Partial Global Hot Spare: **(SYMsm Description: Hot spare capacity not sufficient for all drives)** **Logged when a defined Global Hot Spare device is not large enough to cover all of the drives in the subsystem.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x224F**	**None**
LUN Down: **(SYMsm Description: Volume failure)** **Logged when the configuration manager posts an UA/AEN of ASC/ASCQ = 0x3F/0xE0 indicating Logical Unit Failure.**					
System (0x0)	**Critical (0x1)**	**Failure (0x2)**	**Volume (0xD)**	**0x2250**	**None**
CFG Read Failure: **(SYMsm Description: Drive failed - reconstruction failure)** **Logged when the configuration manager posts an UA/AEN of ASC/ASCQ = 0x3F/0x8E indicating that the drive failed due to a reconstruction failure at SOD.**					
System (0x0)	**Critical (0x1)**	**State (0x5)**	**Drive (0x1)**	**0x2251**	**Origin: FRU info**
Fail Vdisk Delayed: **(SYMsm Description: Drive marked offline during interrupted write)** **Logged when the specified device is failed during interrupted write processing. SK/ASC/ASCQ = 0x06/0x3F/0x98 will be offloaded for each failing device.**					
System (0x0)	**Critical (0x1)**	**Notification (0x4)**	**Drive (0x1)**	**0x2252**	**None**
LUN Modified: (SYMsm Description: Volume group or volume modified (created or deleted)) Logged when the configuration manager posts an UA/AEN of ASC/ASCQ = 0x3F/0x0E indicating that previous LUN data reported via a Report LUNs command has changed (due to LUN creation/deletion or controller hot swap.					
System (0x0)	Informational (0x0)	Notification (0x4)	Volume (0xD)	0x2253	None

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Drive Parity Scan Error: **(SYMsm Description: Redundancy (parity) and data mismatch was detected)** **Logged when there is a parity data mismatch encountered during a drive parity scan operation.**					
System (0x0)	**Critical (0x1)**	**Notification (0x4)**	**Volume (0xD)**	**0x2254**	**Origin: Number of mismatches**
Bad LUN Definition: **(SYMsm Description: Volume definition incompatible with ALT mode-ALT disabled)** **Logged when there is an improper LUN definition for Auto-LUN transfer. The controller will operate in normal redundant controller mode without performing Auto-LUN transfers.**					
System (0x0)	**Critical (0x1)**	**Notification (0x4)**	**Volume (0xD)**	**0x2255**	**None**
Copyback Operation Complete: **(SYMsm Description: Copyback completed on volume)** **Logged when copyback is completed on volume.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume (0xD)**	**0x2256**	**None**
Volume Reconfiguration Start: **(SYMsm Description: Modification (reconfigure) started on volume)** **Logged when reconfiguration is started on volume.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume (0xD)**	**0x2257**	**None**
Volume Reconfiguration Completed: **(SYMsm Description: Modification (reconfigure) completed on volume)** **Logged when reconfiguration is completed on volume.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume (0xD)**	**0x2258**	**None**
LUN Initialization Start: **(SYMsm Description: Initialization started on volume)** **Logged when initialization is started on volume.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume (0xD)**	**0x2259**	**None**
Immediate Availability Format Start: **(SYMsm Description: Immediate availability initialization (IAF) started on volume** **Logged when IAF started on volume.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume (0xD)**	**0x225A**	**None**

Hot-swap events

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
HSM Drive Removed: **(SYMsm Description: Hot swap monitor detected drive removal)** **Logged in the system log when the hot swap monitor detects that a drive has been removed from the system.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x2400**	**Device: Number of the removed drive**
HSM Drive Inserted: **(SYMsm Description: Hot swap monitor detected drive insertion)** **Logged in the system log when the hot swap monitor detects that a drive has been inserted in the system.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Drive (0x1)**	**0x2401**	**Device: Number of the inserted drive**
Controller: **(SYMsm Description: Controller inserted or removed)** **Currently Not Logged.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x2500**	
Mode Switch Active: **(SYMsm Description: Controller mode changed to active)** **Currently Not Logged.**					
System (0x0)	**Informational (0x0)**	**State (0x5)**	**Controller (0x8)**	**0x2501**	
Icon Error: **(SYMsm Description: Controller icon chip error)** **Currently Not Logged.**					
System (0x0)	**Informational (0x0)**	**Error (0x1)**	**Controller (0x8)**	**0x2502**	
Mode Switch Active/Passive: **(SYMsm Description: Controller mode changed to passive)** **Logged on successful completion of an Active/Passive mode switch.**					
System (0x0)	**Informational (0x0)**	**State (0x5)**	**Controller (0x8)**	**0x2503**	**Origin: Local and alternate mode information**
Mode Switch Dual Active: **(SYMsm Description: Controller mode changed to active)** **Logged on successful completion of a Dual Active mode switch.**					
System (0x0)	**Informational (0x0)**	**State (0x5)**	**Controller (0x8)**	**0x2504**	**Origin: Local and alternate mode information**
Mode Switch: (SYMsm Description: Controller mode switch occurred) Currently Not Logged.					
System (0x0)	Informational (0x0)	State (0x5)	Controller (0x8)	0x2505	

Start of Day events

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
ACS Download Start: **(SYMsm Description: Automatic controller firmware synchronization started)** **Logged when an ACS Download is started.**					
Controller (0x1)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x2600**	
ACS Download Completed: **(SYMsm Description: Automatic controller firmware synchronization completed)** **Logged after the controller has been rebooted after auto code synchronization has been preformed. An ASC/ASCQ value of 0x29/0x82 is also logged with this event.**					
Controller (0x1)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x2601**	**Origin: Non-zero indicated download failure**
ACS Error: **(SYMsm Description: Automatic controller firmware synchronization failed)** **Logged when auto code synchronization failed.**					
System (0x0)	**Critical (0x1)**	**Error (0x1)**	**Controller (0x8)**	**0x2602**	**Data Field Type: 0x0701**
Default LUN Created: **(SYMsm Description: Default volume created)** **Logged when the default LUN was created at SOD.**					
System (0x0)	**Informational (0x0)**	**State (0x5)**	**Volume (0xD)**	**0x2603**	**None**
Persistent Memory Parity Error: **(SYMsm Description: Persistent controller memory parity error)** **Logged when SOD detects that the persistent memory parity error state has been set.**					
Controller (0x1)	**Informational (0x0)**	**Error (0x1)**	**Controller (0x8)**	**0x2604**	**None**
Start of Day Completed: **(SYMsm Description: Start-of-day routine completed)** **Logged when the controller has completed initialization.**					
Controller (0x1)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x2605**	**None**
RPA Parity Error: **(SYMsm Description: Controller RPA memory parity error detected)** **Logged during ccmInit during start of day if a parity error is found in RPA memory.**					
Controller (0x1)	**Informational (0x0)**	**Error (0x1)**	**Controller (0x8)**	**0x2700**	**Id: Error block** **Device: 1 = RPA Memory**
PCI Parity Error: (SYMsm Description: PCI controller parity error) Currently Not Logged.					
Controller (0x1)	Informational (0x0)	Error (0x1)	Controller (0x8)	0x2701	

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
RPA Unexpected Interrupt: **(SYMsm Description: Controller unexpected RPA interrupt detected)** **Logged when an unexpected RPA Interrupt is detected.**					
Controller (0x1)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x2702**	**Data Field Type: 0x0110**
Recovered Processor DRAM Error: **(SYMsm Description: Recoverable error in processor memory detected/corrected)** **Logged when the controller has encountered recoverable processor DRAM ECC errors (below the maximum threshold).**					
Controller (0x1)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x2703**	

Subsystem Monitor events

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Power Supply: **(SYMsm Description: Power supply state change detected)** **Logged when a power supply changes state.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Power Supply (0x2)**	**0x2800**	**Id: Power Supply Status: 0 = Failed 1 = Good**
On Battery: **(SYMsm Description: Storage Array running on UPS battery)** **Logged when the UPS battery starts to supply power to the subsystem.**					
System (0x0)	**Critical (0x1)**	**Notification (0x4)**	**Battery (0x9)**	**0x2801**	**None**
UPS Battery Good: **(SYMsm Description: UPS battery is fully charged)** **Logged when the UPS battery has charged and transitioned to the good state.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Battery (0x9)**	**0x2802**	**None**
UPS Battery 2 Minute Warning: **(SYMsm Description: UPS battery-two minutes to failure)** **Logged when the UPS battery has transitioned and given the 2 minute warning. The UPS has signaled that it has 2 minutes of power left before failing. The controllers will flush any dirty data in their caches and turn off data caching.**					
System (0x0)	**Critical (0x1)**	**Notification (0x4)**	**Battery (0x9)**	**0x2803**	**None**
Not Used					
				0x2804	
Line State Change: **(SYMsm Description: Controller tray component change detected)** **Logged when a discreet line state change is detected and an AEN is posted. This can either be a good to bad transition or bad to good. This does not include the cache battery line. Cache battery events are logged by the cache manager.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Unknown (0x0)**	**0x2805**	**Data Field Type: 0x0704**
Drive Enclosure: (SYMsm Description: Tray component change) Logged when SSM has detected a change in an enclosure device, other than a drive status.					
System (0x0)	Informational (0x0)	Notification (0x4)	ESM (0x7)	0x2806	Data Field Type: 0x0705

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Not Used					
				0x2807	
Enclosure ID Not Unique: **(SYMsm Description: Tray ID not unique)** **Logged when the controller determines that there are multiple sub-enclosures with the same ID value selected.**					
System (0x0)	**Critical (0x1)**	**Notification (0x4)**	**ESM (0x7)**	**0x2808**	**Device: Sub-enclosure ID in conflict**
Line Good: **(SYMsm Description: Controller tray component changed to optimal)** **Logged when a subsystem line has transitioned to the Good state.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Enclosure (0xA)**	**0x2809**	**Device: Line number that has changed state**
Line Missing: **(SYMsm Description: Controller tray component missing)** **Logged when an expected subsystem line is missing.**					
System (0x0)	**Critical (0x1)**	**Notification (0x4)**	**Enclosure (0xA)**	**0x280A**	**Device: Line number that is missing**
Line Failed: **(SYMsm Description: Controller tray component failed)** **Logged when a subsystem line has transitioned to the Failed state.**					
System (0x0)	**Critical (0x1)**	**Notification (0x4)**	**Unknown (0x0)**	**0x280B**	**Device: Line number that has changed state**
Enclosure Good: **(SYMsm Description: Drive tray component changed to optimal)** **Logged when an enclosure has transitioned to the Good state.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**ESM (0x7)**	**0x280C**	**Device: Enclosure ID** **Origin: FRU Info**
Enclosure Fail: **(SYMsm Description: Drive tray component failed)** **Logged when an enclosure has transitioned to the Failed state.**					
System (0x0)	**Critical (0x1)**	**Notification (0x4)**	**ESM (0x7)**	**0x280D**	**Device: Enclosure ID** **Origin: FRU Info**
Battery Low: **(SYMsm Description: Standby power source not fully charged)** **Logged when the battery charge is low.**					
System (0x0)	Critical (0x1)	Notification (0x4)	Battery (0x9)	0x280E	

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Redundancy Loss: **(SYMsm Description: Environmental card - loss of communication)** **Logged when a redundant path is not available to devices.**					
System (0x0)	**Critical (0x1)**	**Notification (0x4)**	**ESM (0x7)**	**0x280F**	**Device: Enclosure ID** **Origin: FRU Group Qualifier for Sub-enclosure group (Byte 27) or drive slot**
Redundancy Restored: **(SYMsm Description: Environmental card - communication restored)** **Logged when a redundant path to devices is restored.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**ESM (0x7)**	**0x2810**	**Device: Enclosure ID** **Origin: FRU Group Qualifier for Sub-enclosure group (Byte 27) or drive slot**
Not Used					
				0x2811	
Minihub Normal: **(SYMsm Description: Mini-hub canister changed to optimal)** **Logged when Mini-hub canister is changed to optimal.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Minihub (0x4)**	**0x2812**	**ID = Type/Channel** **Type = 1: Host Side** **Type = 2: Drive Side**
Minihub Failed: **(SYMsm Description: Mini-hub canister failed)** **Logged when Mini-hub canister is failed.**					
System (0x0)	**Critical (0x1)**	**Notification (0x4)**	**Minihub (0x4)**	**0x2813**	**ID = Type/Channel** **Type = 1: Host Side** **Type = 2: Drive Side**
GBIC Optimal: **(SYMsm Description: GBIC changed to optimal)** **Logged when GBIC is changed to optimal.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Minihub (0x4)**	**0x2814**	**ID = Type/Channel** **Type = 1: Host Side** **Type = 2: Drive Side**
GBIC Failed: (SYMsm Description: GBIC failed) Logged when GBIC is failed.					
System (0x0)	Critical (0x1)	Notification (0x4)	Minihub (0x4)	0x2815	ID = Type/Channel Type = 1: Host Side Type = 2: Drive Side

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Enclosure ID Conflict: **(SYMsm Description: Tray ID conflict - duplicate IDs across drive trays)** **Logged when the controller detects duplicate drive tray IDs in the subsystem.**					
System (0x0)	**Critical (0x1)**	**Notification (0x4)**	**ESM (0x7)**	**0x2816**	**None**
Enclosure ID Conflict Cleared: **(SYMsm Description: Tray ID conflict resolved)** **Logged when the controller detects that an enclosure ID conflict no longer exists.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**ESM (0x7)**	**0x2817**	**None**
Enclosure ID Mismatch: **(SYMsm Description: Tray ID mismatch – duplicate IDs in same drive tray)** **Logged when the controller detects that the two ESM boards in the same drive tray have different IDs.**					
System (0x0)	**Critical (0x1)**	**Notification (0x4)**	**ESM (0x7)**	**0x2818**	**None**
Enclosure ID Mismatch Cleared: **(SYMsm Description: Tray ID mismatch resolved)** **Logged when the controller detects that the drive tray ESM board ID mismatch has been cleared.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**ESM (0x7)**	**0x2819**	**None**
Temperature Sensor Good: **(SYMsm Description: Temperature changed to optimal)** **Logged when the controller detects that a temperature sensor has transitioned to a good status.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Temp Sensor (0x5)**	**0x281A**	**Data Field Type: 0x0800**
Temperature Sensor Warning: **(SYMsm Description: Nominal temperature exceeded)** **Logged when the controller detects that a temperature sensor has transitioned to a warning status.**					
System (0x0)	**Critical (0x1)**	**Failure (0x2)**	**Temp Sensor (0x5)**	**0x281B**	**Data Field Type: 0x0800**
Temperature Sensor Failed: **(SYMsm Description: Maximum temperature exceeded)** **Logged when the controller detects that a temperature sensor has transitioned to a failed status.**					
System (0x0)	**Critical (0x1)**	**Failure (0x2)**	**Temp Sensor (0x5)**	**0x281C**	**Data Field Type: 0x0800**
Temperature Sensor Missing: (SYMsm Description: Temperature sensor removed) Logged when the controller detects that a temperature sensor is missing.					
System (0x0)	Critical (0x1)	Failure (0x2)	Temp Sensor (0x5)	0x281 D	Data Field Type: 0x0800

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
ESM Version Mismatch: **(SYMsm Description: Environmental card firmware mismatch)** **Logged when the controller detects that two ESMs do not have the same version of firmware running**					
System (0x0)	**Critical (0x1)**	**Notification (0x4)**	**ESM (0x7)**	**0x281E**	**Data Field Type: 0x0800** **The tray number appears in the device field and as extra data.**
ESM Version Mismatch Clear: **(SYMsm: Environmental card firmware mismatch resolved)** **Logged when the controller detects that the firmware mismatch has been cleared**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**ESM (0x7)**	**0x281F**	**Data Field Type: 0x0800** **The tray number appears in the device field and as extra data.**
Controller Report Warning: **(SYMsm: Two controllers present but NVSRAM (offset 0x35, bit 6) set for NOT reporting a missing second controller)** **Logged when two controllers are present even though the NVSRAM bit for not reporting a missing second controller is set.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x2820**	**None**
Mini Hub Unsupported: **(SYMsm: Incompatible mini-hub canister)** **Logged when an incompatible mini-hub canister is detected.**					
System (0x0)	**Critical (0x1)**	**Notification (0x4)**	**MiniHub (0x4)**	**0x2821**	**None**

Command Handler events

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Format Unit: **(SYMsm Description: Format unit issued)** **Logged when the controller processes a format command. The LUN value indicates the LUN that the controller is formatting.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Volume (0xD)**	**0x3000**	**ID field: Indicates the status of the format command :** **0 - Write zeros is being done to the unit** **1 - The configuration manager is initializing the LUN and controller data structures used.** **2 - The entire format operation has successfully completed, status has been returned to the host.**
Quiesce: **(SYMsm Description: Quiescence issued)** **Logged for the quiescence command.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Controller (0x8)**	**0x3001**	**Id field: Indicates the state of the quiesce command :** **0 - Quiescence is stopped.** **1 - Quiescence was started.**
Reassign Blocks: **(SYMsm Description: Reassign blocks issued from host)** **Logged for a reassign blocks command that has been issued from the host.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Volume (0xD)**	**0x3002**	**Id: Total number of blocks to be reassigned.** **Data Field Type: 0x0208**
Reserve: **(SYMsm Description: Reserve issued)** **Logged for the reserve command.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Volume (0xD)**	**0x3003**	**LUN: LUN being reserved.** **Id: Indicates the reserving host** **Device: If non-zero, Third party reservation information. The high order byte indicates that a 3rd party reservation was done the low order byte is the third party id.**

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Release: **(SYMsm Description: Release issued)** **Logged for the release command.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Volume (0xD)**	**0x3004**	**LUN: LUN being reserved.** **Id: Indicates the reserving host** **Device: If non-zero, Third party reservation information. The high order byte indicates that a 3rd party reservation was done the low order byte is the third party id.**
Synchronize Cache: **(SYMsm Description: Synchronize controller cache issued)** **Logged when controllers begins execution of Synchronize Cache.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Controller (0x8)**	**0x3005**	**None**
Safe Pass Through: **(SYMsm Description: Safe pass-through issued)** **These log entries are made by the set pass through and save pass through command handlers respectively before the pass through command is sent to the drive. The following passed through commands are not logged: Test Unit Ready, Read Capacity, Inquiry, Mode Sense. All other commands are logged regardless of their success or failure.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Drive (0x1)**	**0x3006**	**Data Field Type: 0x0611**
Mode Select 1: **(SYMsm Description: Mode select for page 1 received)** **Logged when Mode Select for Page 0x01 is received and the Post Error bit value has changed from the value stored in NVSRAM.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Volume (0xD)**	**0x3007**	**Id: Contains new post error (PER) bit value**
Mode Select 2: **(SYMsm Description: Mode select for page 2 received)** **Logged when mode select for Page 0x02 is received..**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Volume (0xD)**	**0x3008**	**Data Field Type: 0x0608** **Data buffer length = 16** **Data: Page 0x02 Mode Select data sent to the controller in SCSI format.**
Mode Select 8: (SYMsm Description: Mode for caching page 8 received) Logged when Mode Select Page 0x08 (Caching page) is received.					
System (0x0)	Informational (0x0)	Command (0x3)	Volume (0xD)	0x3009	Data Field Type: 0x0608 Data buffer length = 12 Data: Page 0x08 Mode Select data sent to the controller in SCSI format.

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Mode Select A: **(SYMsm Description: Mode select for control mode page A received)** **Logged when Mode Select Page 0x0A (Control mode page) is received.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Controller (0x8)**	**0x300A**	**Data Field Type: 0x0608** **Data buffer length = 8** **Data: Page 0x0A Mode Select data sent to the controller in SCSI format**
Mode Select 2A: **(SYMsm Description: Mode select for array physical page 2A received)** **Logged when Mode Select Page 0x2A (Array physical page) is received.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Controller (0x8)**	**0x300B**	**Data Field Type: 0x060C**
Mode Select 2B: **(SYMsm Description: Mode select for array logical page 2B received)** **Logged when Mode Select Page 0x2B (Logical Array page) is received.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Volume (0xD)**	**0x300C**	**Data Field Type: 0x0608** **Data buffer length = 132** **Data: Page 0x2B Mode Select data sent to the controller in SCSI format.**
Mode Select 2C: **(SYMsm Description: Mode select for redundant controller page 2C received)** **Logged when Mode Select Page 0x2C (Redundant controller page) is received.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Controller (0x8)**	**0x300D**	**Data Field Type: 0x0608** **Data buffer length: = 106** **Data: Page 0x2C Mode Select data sent to the controller in SCSI format.**
Mode Select 2E: **(SYMsm Description: Mode select for vendor-unique cache page 2E received)** **Logged when Mode Select Page 0x2E - (Vendor unique cache page) is received.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Controller (0x8)**	**0x300E**	**Data Field Type: 0x0608** **Data buffer length = 30** **Data: Page 0x2E Mode Select data sent to the controller in SCSI format.**
Mode Select 2F: (SYMsm Description: Mode select for time page 2F received) Logged when Mode Select Page 0x2F (Time page) is received.					
System (0x0)	Informational (0x0)	Command (0x3)	Controller (0x8)	0x300F	Device: Contains the time passed to the controller

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Mode Select 3A: **(SYMsm Description: Mode select for hot spare page 3A received)** **Logged when Mode Select Page 0x3A (The global hot spare page) is received.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Controller (0x8)**	**0x3010**	**Id: Action code specified in the page data** **Device: Hot spare device specified in the page data**
Defect List: **(SYMsm Description: Defect list received)** **Currently Not Logged.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Controller (0x8)**	**0x3011**	
Write Buffer: **Write buffer received** **Logged when Write Buffer is received to the following buffer ids:** **0xE8 – SubSystem Identifier** **0xE9 – Subsystem Fault** **0xEA – Drive Fault** **0xED – Host Interface Parameters** **0xEE - User configuration options** **0xF0 - BootP Storage**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Controller (0x8)**	**0x3012**	**Origin: contains the buffer id.** **Data Field Type: 0x0612**
Controller Firmware Download:**(SYMsm Description: Download controller firmware issued)** **Logged when controller firmware download is started.**					
Controller (0x1)	**Informational (0x0)**	**Command (0x3)**	**Controller (0x8)**	**0x3013**	**Device:** 0 **= Download to drive started** 1 **= Download had completed** **Origin: Error value on completion of download** 0 **= Download Success** Other **= Error occurred, value of internal controller status**
Drive Firmware Download Start: (SYMsm Description: Drive firmware download started) Logged when drive firmware download has started.					
Drive (0x2)	Informational (0x0)	Command (0x3)	Drive (0x1)	0x3014	

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Pass Through: **(SYMsm Description: Drive pass-through issued)** **Currently Not Logged.**					
Drive (0x2)	**Informational (0x0)**	**Command (0x3)**	**Drive (0x1)**	**0x3015**	
Alternate Controller: **(SYMsm Description: Alternate controller transition issued)** **Currently Not Logged.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Controller (0x8)**	**0x3016**	
Set Pass Through: **(SYMsm Description: Set pass-through issued)** **Currently Not Logged** **These log entries are made by the set pass through and save pass through command handlers respectively before the pass through command is sent to the drive. The following passed through commands are not logged: Test Unit Ready, Read Capacity, Inquiry, Mode Sense. All other commands are logged regardless of their success or failure.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Drive (0x1)**	**0x3017**	
Set Pass Command: **(SYMsm Description: Set pass command issued)** **Currently Not Logged.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Drive (0x1)**	**0x3018**	
Mode Select Active/Passive Mode: **(SYMsm Description: Volume ownership changed due to failover)** **Logged when a Mode Select command to make the controller Active is received.**					
System (0x0)	**Critical (0x1)**	**Command (0x3)**	**Controller (0x8)**	**0x3019**	
Drive Firmware Download Fail: **(SYMsm Description: Drive firmware download failed)** **Logged when drive firmware download has failed.**					
Drive (0x2)	**Informational (0x0)**	**Command (0x3)**	**Drive (0x1)**	**0x301A**	
Drive Firmware Download Complete: **(SYMsm Description: Drive firmware download completed)** **Logged when drive firmware download has completed successfully.**					
Drive	**Informational**	**Command**	**Drive**	**0x301B**	
ESM Firmware Download Start: (SYMsm Description: Environmental card firmware download started) Logged when ESM firmware download has started.					
Drive (0x2)	Informational (0x0)	Command (0x3)	ESM (0x7)	0x301C	Lun: Tray ID of tray containing ESM

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
ESM Firmware Download Fail: **(SYMsm Description: Environmental card firmware download failed)** **Logged when ESM firmware download has failed.**					
Drive (0x2)	**Informational (0x0)**	**Command (0x3)**	**ESM (0x7)**	**0x301D**	**Lun: Tray ID of tray containing ESM**
ESM Firmware Download Complete: **(SYMsm Description: Environmental card firmware download completed)** **Logged when ESM firmware download has successfully completed.**					
Drive (0x2)	**Informational (0x0)**	**Command (0x3)**	**ESM (0x7)**	**0x301E**	**Lun: Tray ID of tray containing ESM**

EEL events

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
AEN Posted: **(SYMsm Description: AEN posted for recently logged event)** **Logged when the controller posts an AEN.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x3101**	**Data Field Type: 0x0100** **Data: Sense data of the AEN as defined in the Software Interface Specification.**
EEL Deferred Error: **(SYMsm Description: Deferred error (EEL))** **Currently Not Logged**					
System (0x0)	**Informational (0x0)**	**Error (0x1)**	**Controller (0x8)**	**0x3102**	
VKI Common Error: **(SYMsm Description: VKI commom error)** **Logged when VKI_CMN_ERROR is called with the error level set to ERROR. Calls made with a level of CONTINUE or NOTE will not be logged**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x3200**	**Data Field Type: 0x0700**
VKI Panic: **(SYMsm Description: VKI panic)** **Logged when VKI_CMN_ERROR is called with the error level set to PANIC. Calls made with a level of CONTINUE or NOTE will not be logged.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x3201**	**Data Field Type: 0x0700**

RDAC, Quiesence and ICON Manager events

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
SysWipe: **(SYMsm Description: Sys wipe request sent to controller)** **Logged when a sys wipe request is sent to the controller. This routine is not called by the controller SW or FW currently. If logged it means the command was entered through the shell interface. If this entry is seen a corresponding entry of MEL_EV_ICON_SYS_WIPE_ALT should also be logged by the alternate controller.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x4000**	**None**
NVSRAM Clear: **(SYMsm Description: NVSRAM clear request sent to alternate controller)** **Logged when an NVSRAM clear message is sent to the alternate controller. This is normally logged as part of a mode select command to the RDAC mode page 0x2C. The companion entry of MEL_EV_ICON_NV_CLR_ALT should also be seen in the event log along with this entry.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x4001**	**None**
SysWipe Alternate: **(SYMsm Description: Sys wipe request received by alternate controller)** **Logged when a sys wipe request is received by the alternate controller. This is an unexpected log entry that is logged when the routine iconMgrSendSysWipe is executed from the shell of the alternate controller. This routine is not called by the controller SW. The companion entry of MEL_EV_ICON_SYS_WIPE should also be logged if this entry is seen.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x4002**	**None**
NVSRAM Clear Alternate: **(SYMsm Description: NVSRAM clear request received by alternate controller)** **Logged when an NVSRAM clear message is received from the alternate controller. No additional data is logged. The companion entry of MEL_EV_ICON_NV_CLR should also be seen in the event log along with this entry.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x4003**	**None**
Quiesce Message Received: (SYMsm Description: Alternate controller quiescence message received) Logged when a quiescence manager message was received from the alternate controller.					
System (0x0)	Informational (0x0)	Notification (0x4)	Controller (0x8)	0x4004	Id: Message that was received: **0** = Start controller level quiescence and return Done when completed. **1** = Stop controller level quiescence. **2** = The alternate controller has quiesced. **3** = Release the controller from quiescence.

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Controller Quiesce Begin: **(SYMsm Description: Controller quiescence started)** **Logged when a controller level quiescence was begun on the controller.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x4005**	**Id: Value of the forceOption parameter that was passed to the routine.**
Alternate Controller Quiesce Begin: **(SYMsm Description: Alternate controller quiescence started)** **Logged when a controller level quiescence was begun on the alternate controller.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x4006**	**Id: Value of the forceOption parameter that was passed to the routine.**
Subsystem Quiesce Begin: **(SYMsm Description: Subsystem quiescence started)** **Logged when a subsystem level quiescence was begun.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x4007**	**Id: Value of the forceOption parameter that was passed to the routine.**
Controller Quiesce Abort: **(SYMsm Description: Controller quiescence halted)** **Logged when a controller level quiescence is aborted.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x4008**	**Id: Quiescence state of controller at beginning of the abort.**
Controller Quiesce Release: **(SYMsm Description: Controller quiescence released)** **Logged when a controller level quiescence is released.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x4009**	**Id: Quiescence state of controller at beginning of release.**
Alternate Controller Quiesce Release: **(SYMsm Description: Alternate controller quiescence released)** **Logged when a controller level quiescence on alternate is released.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x400A**	**Id: Quiescence state of alternate controller at beginning of release.**
Reset All Channels: **(SYMsm Description: All channel reset detected)** **Logged when the controller detects that the alternate controller has been removed or replaced.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x400B**	
Alternate Controller Reset Hold: (SYMsm Description: Controller placed offline) Logged when the controller successfully puts the alternate controller in the reset/hold state.					
System (0x0)	Informational (0x0)	Notification (0x4)	Controller (0x8)	0x400C	

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Alternate Controller Reset Release: **(SYMsm Description: Controller placed online)** **Logged when the controller successfully releases the alternate controller from the reset/failed state.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x400D**	
Auto Volume Transfer: **(SYMsm Description: Automatic volume transfer started)** **Logged when an Auto Volume Transfer is initiated.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x400E**	**Lun: Number of Volumes being transferred** **Origin: 0 = Normal AVT** **1 = Forced AVT (LUN will be zero)**
Alternate controller has been reset: **(SYMsm Description: Controller reset by its alternate)** **Logged when the alternate controller was reset. The controller number in the event reflects the controller that was held in reset.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x400F**	**None**
Controller Reset: **(SYMsm Description: Controller reset)** **Logged when the controller is going to reset itself through the controller firmware. This event is not logged when the controller is reset because of hardware errors (such as watchdog timeout conditions). The controller number reflects the controller number of the board that was reset.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x4010**	**None**

SYMbol server events

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Assign Volume Group Ownership: **(SYMsm Description: Assign volume group ownership)** **Logged on entry to assignVolumeGroupOwnership_1.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Volume Group (0xE)**	**0x5000**	**Data Field Type: 0x0603 & 0x0803**
Create Hotspare: **(SYMsm Description: Assign hot spare drive)** **Logged on entry to assignDriveAsHotSpares_1.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Unknown (0x0)**	**0x5001**	**Data Field Type: 0x0804 or 0x0805**
Create Volume: **(SYMsm Description: Create volume)** **Currently Not Logged**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Unknown (0x0)**	**0x5002**	
Delete Hotspare: **(SYMsm Description: De-assign hot spare drive)** **Logged on entry to deassignDriveAsHotSpares_1.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Unknown (0x0)**	**0x5003**	**Data Field Type: 0x0805**
Delete Volume: **(SYMsm Description: Delete volume)** **Logged on entry to deleteVolume_1.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Volume (0xD)**	**0x5004**	**LUN: Volume be deleted**
Set Controller Failed: **(SYMsm Description: Place controller offline)** **Logged on entry to setControllerToFailed_1.**					
System (0x0)	**Critical (0x1)**	**Command (0x3)**	**Controller (0x8)**	**0x5005**	**Data Field Type: 0x0813**
Set Drive Failed: **(SYMsm Description: Fail drive)** **Logged on entry to setDriveToFailed_1.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Drive (0x1)**	**0x5006**	**None**
Start Volume Format: (SYMsm Description: Initialize volume group or volume) Logged on entry to startVolumeFormat_1.					
System (0x0)	Informational (0x0)	Command (0x3)	Volume (0xD)	0x5007	None

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Initialize Drive: **(SYMsm Description: Initialize drive)** **Logged on entry to initializeDrive_1.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Drive (0x1)**	**0x5008**	**None**
Controller Firmware Start: **(SYMsm Description: Controller firmware download started)** **Logged when a controller firmware download starts.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Controller (0x8)**	**0x5009**	
Load Drive Firmware: **(SYMsm Description: Download drive firmware issued)** Logged when a Download drive firmware is issued					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Drive (0x1)**	**0x500A**	
Controller NVSRAM Start: **(SYMsm Description: Controller NVSRAM download started)** **Logged when a controller NVSRAM download starts.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Controller (0x8)**	**0x500B**	
Set Volume Group Offline: **(SYMsm Description: Place volume group offline)** **Logged on entry to setVolumeGroupToOffline_1.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Volume Group (0xE)**	**0x500C**	**Data Field Type: 0x0603**
Set Volume Group Online: **(SYMsm Description: Place volume group online)** **Logged on entry to setVolumeGroupToOnline_1.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Volume Group (0xE)**	**0x500D**	**Data Field Type: 0x0603**
Start Drive Reconstruction: **(SYMsm Description: Reconstruct drive/volume)** **Logged on entry to startDriveReconstruction_1.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Drive (0x1)**	**0x500E**	**None**
Start Volume Group Defragment: (SYMsm Description: Start volume group defragment) Logged on entry to startVolumeGroupDefrag_1.					
System (0x0)	Informational (0x0)	Command (0x3)	Volume Group (0xE)	0x500F	Data Field Type: 0x0603

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Start Volume Group Expansion: **(SYMsm Description: Add free capacity to volume group)** **Logged on entry to startVolumeGroupExpansion_1.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Volume Group (0xE)**	**0x5010**	**Data Field Type: 0x0603 & 0x0809**
Start Volume RAID Migration: **(SYMsm Description: Change RAID level of volume group)** **Logged on entry to startVolumeRAIDMigration_1.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Volume Group (0xE)**	**0x5011**	**Data Field Type: 0x0603 & 0x080A**
Start Volume Segment Sizing: **(SYMsm Description: Change segment size of volume)** **Logged on entry to startVolumeSegmentSizing_1.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Volume (0xD)**	**0x5012**	**Data Field Type: 0x0802**
Set Controller To Passive: **(SYMsm Description: Change controller to passive mode)** **Logged on entry to setControllerToPassive_1.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Controller (0x8)**	**0x5013**	**Data Field Type: 0x0813**
Set Controller To Active: **(SYMsm Description: Change controller to active mode)** **Logged on entry to setControllerToActive_1.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Controller (0x8)**	**0x5014**	**Data Field Type: 0x0813**
Set Storage Array Cache Parameters: **(SYMsm Description: Update cache parameters of Storage Array)** **Logged on entry to setSACacheParams_1. Instructs the SYMbol Server's controller to propagate a controller cache change to all controllers in the storage array.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Unknown (0x0)**	**0x5015**	**Data Field Type: 0x080B**
Set Storage Array User Label: (SYMsm Description: Change name of Storage Array) Logged on entry to setSAUserLabel_1. Instructs the controller to change the shared storage array name.					
System (0x0)	Informational (0x0)	Command (0x3)	Unknown (0x0)	0x5016	Data Field Type: 0x080C

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Set Controller Time: **(SYMsm Description: Synchronize controller clock)** **Logged on entry to setControllerTime_1.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Controller (0x8)**	**0x5017**	**Data Field Type: 0x080D**
Set Volume Cache Parameters: **(SYMsm Description: Change cache parameters of volume)** **Logged on entry to setVolumeCacheParams_1.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Volume (0xD)**	**0x5018**	**Data Field Type: 0x080E**
Set Volume Parameters: **(SYMsm Description: Change parameters of volume)** **Logged on entry to setVolumeParams_1.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Volume (0xD)**	**0x5019**	**Data Field Type: 0x080F**
Set Volume User Label: **(SYMsm Description: Change name of volume)** **Logged on entry to setVolumeUserLable_1.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Volume (0xD)**	**0x501A**	**Data Field Type: 0x0801**
Set Controller To Optimal: **(SYMsm Description: Place controller online)** **Logged on entry to setControllerToOptimal_1.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Controller (0x8)**	**0x501B**	**Data Field Type: 0x0813**
Set Drive To Optimal: **(SYMsm Description: Revive drive)** **Logged on entry to setDriveToOptimal_1.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Drive (0x1)**	**0x501C**	**None**
Force Volume To Optimal: **(SYMsm Description: Revive volume)** **Logged on entry to forceVolumeToOptimal_1.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Volume Group (0xE)**	**0x501D**	**None**
Set Storage Array Tray Positions: (SYMsm Description: Change positions of trays in physical view) Logged on entry to setSATrayPositions_1.					
System (0x0)	Informational (0x0)	Command (0x3)	Unknown (0x0)	0x501E	Data Field Type: 0x0810
Set Volume Media Scan Parameters: (SYMsm Description: Change media scan (scrub) settings of volume) Logged on entry to setVolumeMediaScanParameters_1.					
System (0x0)	Informational (0x0)	Command (0x3)	Volume (0xD)	0x501F	Data Field Type: 0x0811

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Set Storage Array Media Scan Rate: **(SYMsm Description: Change media scan (scrub) settings of Storage Array)** **Logged on entry to setSAMediaScanRate_1.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Unknown (0x0)**	**0x5020**	**Data Field Type: 0x0812**
Clear Storage Array Configuration: **(SYMsm Description: Reset configuration of Storage Array)** **Logged on entry to clearSAConfiguration_1. Clears the entire array configuration, deleting all volumes and returning to a clean initial state.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Unknown (0x0)**	**0x5021**	**None**
Auto Storage Array Configuration: **(SYMsm Description: Automatic configuration on Storage Array)** **Logged on exit from to autoSAConfiguration_1.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Unknown (0x0)**	**0x5022**	**None**
RPC Function Return Code: **(SYMsm Description: Controller return status/function call for requested operation)** **Logged on the return from RPC function returning ReturnCode.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Unknown (0x0)**	**0x5023**	**Data Field Type: 0x0814**
Write Download Checkpoint: **(SYMsm Description: Internal download checkpoint)** **Logged whenever the download checkpoint is updated.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Controller (0x8)**	**0x5024**	**Data Field Type: 0x0815**
Controller Firmware Download Fail: **(SYMsm Description: Controller firmware download failed)** **Logged when a controller firmware download fails.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Controller (0x8)**	**0x5025**	
Controller Firmware Download Complete: **(SYMsm Description: Controller firmware download completed)** **Logged when a controller firmware download successfully completes.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Controller (0x8)**	**0x5026**	
Controller NVSRAM Download Fail: (SYMsm Description: Controller NVSRAM download failed) Logged when a controller NVSRAM download fails.					
System (0x0)	Informational (0x0)	Command (0x3)	Controller (0x8)	0x5027	

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Controller NVSRAM Download Complete:**(SYMsm Description: Controller NVSRAM download completed)** **Logged when a controller NVSRAM download successfully completes.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Controller (0x8)**	**0x5028**	
Battery Update: **(SYMsm Description: Reset controller battery age)** **Logged when the battery parameters are updated.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Unknown (0x0)**	**0x5029**	**Data Field Type: 0x0816**
Assign Volume Ownership: **(SYMsm Description: Assign volume ownership)** **Logged when volume ownership is modified.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Volume (0xD)**	**0x502A**	**None**
Volume Expand: **(SYMsm Description: Increase volume capacity)** **Logged when volume capacity is increased**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Volume (0xD)**	**0x502B**	**None**
Snap Params Set: **(SYMsm Description: Change parameters of snapshot repository volume)** **Logged when the snapshot parameters are changed.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Volume (0xD)**	**0x502C**	**None**
Recreate Snap: **(SYMsm Description: Re-create snapshot volume)** **Logged when the snapshot is recreated (restarted).**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Volume (0xD)**	**0x502D**	**None**
Disable Snap: **(SYMsm Description: Disable snapshot volume)** **Logged when the snapshot has been disabled (stopped).**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Volume (0xD)**	**0x502E**	**None**
Delete Ghost: (SYMsm Description: Delete missing volume) Logged when a missing volume is deleted.					
System (0x0)	Informational (0x0)	Command (0x3)	Volume (0xD)	0x502F	None

Storage Partitions Manager events

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Create Cluster: **(SYMsm Description: Create host group)** **Logged on entry to spmCreateCluster.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Unknown (0x0)**	**0x5200**	**Data Field Type: 0x0900**
Delete Cluster: **(SYMsm Description: Delete host group)** **Logged on entry to spmDeleteCluster.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Unknown (0x0)**	**0x5201**	**Data Field Type: 0x0901**
Rename Cluster: **(SYMsm Description: Rename host group)** **Logged on entry to spmRenameCluster.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Unknown (0x0)**	**0x5202**	**Data Field Type: 0x0903**
Create Host: **(SYMsm Description: Create host)** **Logged on entry to spmCreateHost.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Unknown (0x0)**	**0x5203**	**Data Field Type: 0x0907**
Delete Host: **(SYMsm Description: Delete host)** **Logged on entry to spmDeleteHost.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Unknown (0x0)**	**0x5204**	**Data Field Type: 0x0901**
Rename Host: **(SYMsm Description: Rename host)** **Logged on entry to spmRenameHost.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Unknown (0x0)**	**0x5205**	**Data Field Type: 0x0903**
Move Host: **(SYMsm Description: Move host)** **Logged on entry to spmMoveHost.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Unknown (0x0)**	**0x5206**	**Data Field Type: 0x0902**

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Create Host Port: **(SYMsm Description: Create host port)** **Logged on entry to spmCreateHostPort.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Unknown (0x0)**	**0x5207**	**Data Field Type: 0x0904**
Delete Host Port: **(SYMsm Description: Delete host port)** **Logged on entry to spmDeleteHostPort.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Unknown (0x0)**	**0x5208**	**Data Field Type: 0x0901**
Rename Host Port: **(SYMsm Description: Rename host port)** **Logged on entry to spmRenameHostPort.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Unknown (0x0)**	**0x5209**	**Data Field Type: 0x0905**
Move Host Port: **(SYMsm Description: Move host port)** **Logged on entry to spmMoveHostPort.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Unknown (0x0)**	**0x520A**	**Data Field Type: 0x0902**
Set Host Port Type: **(SYMsm Description: Set host port type)** **Logged on entry to spmSetHostPortType.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Unknown (0x0)**	**0x520B**	**Data Field Type: 0x0906**
Create SAPort Group: **(SYMsm Description: Create Storage Array port group)** **Logged on entry to spmCreateSAPortGroup.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Unknown (0x0)**	**0x520C**	**Data Field Type: 0x0900**
Delete SAPort Group: **(SYMsm Description: Delete Storage Array port group)** **Logged on entry to spmDeleteSAPortGroup.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Unknown (0x0)**	**0x520D**	**Data Field Type: 0x0900**
Move SA Port: (SYMsm Description: Move Storage Array port) Logged on entry to spmMoveSAPort.					
System (0x0)	Informational (0x0)	Command (0x3)	Unknown (0x0)	0x520E	Data Field Type: 0x0902

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Create LUN Mapping: **(SYMsm Description: Create volume-to-LUN mapping)** **Logged on entry to spmCreateLUNMapping.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Volume (0xD)**	**0x520F**	**Data Field Type: 0x0908**
Delete LUN Mapping: **(SYMsm Description: Delete volume-to-LUN mapping)** **Logged on entry to spmDeleteLUNMapping.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Volume (0xD)**	**0x5210**	**Data Field Type: 0x0901**
Move LUN Mapping: **(SYMsm Description: Change volume-to-LUN mapping)** **Logged on entry to spmMoveLUNMapping.**					
System (0x0)	**Informational (0x0)**	**Command (0x3)**	**Volume (0xD)**	**0x5211**	**Data Field Type: 0x0909**
Write DACSTORE Error: **(SYMsm Description: Error writing configuration)** **Logged when an error occurs when attempting to update the SPM DASCSTORE region.**					
System (0x0)	**Informational (0x0)**	**Error (0x1)**	**Unknown (0x0)**	**0x5212**	**Data Field Type: 0x090A**

SAFE events

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Feature Enabled: **(SYMsm Description: Premium feature enabled)** **Logged when a feature is successfully enabled.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Unknown (0x0)**	**0x5400**	**Id: Feature Code**
Feature Disabled: **(SYMsm Description: Premium feature disabled)** **Logged when a feature is successfully disabled.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Unknown (0x0)**	**0x5401**	**Id: Feature Code**
Non-Compliance: **(SYMsm Description: Premium feature out of compliance)** **Logged when there are features enabled that have not been purchased.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Unknown (0x0)**	**0x5402**	**Id: Features not in compliance**
Tier Non-Compliance: **(SYMsm Description: Premium feature exceeds limit)** **Logged when there are features that are not in tier compliance (e.g. 6 storage partitions when 4 have been purchased).**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Unknown (0x0)**	**0x5403**	**Id: Features not in tier compliance**
ID Changed: **(SYMsm Description: Feature Enable Identifier changed)** **Logged when a new SAFE ID is successfully generated and stored.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Unknown (0x0)**	**0x5404**	

Runtime Diagnostic events

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Runtine Diagnostics OK: (SYMsm Description: Controller passed diagnostics) **Logged when controller successfully passed runtime diagnostics.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x5600**	**Id: 1 if user initiated Data Field Type : 0x0A00 Data Field Value: ID of test requested. 0 – all tests.**
Alternate controller runtime diagnostics OK: (SYMsm Description: This controller's alternate passed diagnostics.) **Logged when alternate controller successfully passed diagnostics.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x5601**	**Id: 1 if user initiated Data Field Type : 0x0A00 Data Field Value: ID of test requested. 0 – all tests.**
Runtime diagnostics timeout: (SYMsm Description: This controller's alternate failed – timeout waiting for results) **Logged when alternate controller failed due to timeout waiting for diagnostic results.**					
System (0x0)	**Critical (0x1)**	**Failure (0x2)**	**Controller (0x8)**	**0x5602**	**Id: 1 if user initiated Data Field Type : 0x0A00 Data Field Value: ID of test requested. 0 – all tests.**
Diagnostics in progress: (SYMsm Description: Diagnostics rejected - already in progress) **Logged when Runtime Diagnostics request rejected because already in progress.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x5603**	**Id: 1 if user initiated Data Field Type : 0x0A00 Data Field Value: ID of test requested. 0 – all tests.**
No alternate present for diagnostic execution: (SYMsm Description: Diagnostics rejected – this controller's alternate is absent or failed) Logged when Runtime Diagnostics request rejected because the alternate controller is either absent, failed, or in passive mode.					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x5604**	**Id: 1 if user initiated Data Field Type : 0x0A00 Data Field Value: ID of test requested. 0 – all tests.**

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
ICON error during runtime diagnostics: (SYMsm Description: Diagnostics rejected – error occurred when sending the Icon message) **Logged when Runtime Diagnostics request failed because an error occurred when sending the ICON message.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x5605**	**Id: 1 if user initiated Data Field Type : 0x0A00 Data Field Value: ID of test requested. 0 – all tests.**
Runtime diagnostic initialization error:**(SYMsm Description: Diagnostics rejected - ctlrDiag task unable to queue DIAG_INIT_MSG message)** **Logged when Runtime Diagnostics request failed because ctlrDiag task was unable to queue the DIAG_INIT_MSG message.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x5606**	**Id: 1 if user initiated Data Field Type : 0x0A00 Data Field Value: ID of test requested. 0 – all tests.**
Runtime Diagnostics error – unknown return value:**(SYMsm Description: Diagnostics returned unknown ReturnCode)** **Logged when Runtime Diagnostics status unknown because of unknown ReturnCode.**					
System (0x0)	**Informational (0x0)**	**Unknown (0x0)**	**Controller (0x8)**	**0x5607**	**Id: 1 if user initiated Data Field Type : 0x0A00 Data Field Value: ID of test requested. 0 – all tests.**
Runtime Diagnostics error – bad test ID:**(SYMsm Description: Diagnostics rejected - test ID is incorrect)** **Logged when Runtime Diagnostics request rejected because test ID is invalid.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x5608**	**Id: 1 if user initiated Data Field Type : 0x0A00 Data Field Value: ID of test requested. 0 – all tests.**
Runtime Diagnostics error – drive error:**(SYMsm Description: Diagnostics unable to select a drive for I/O)** **Logged when Runtime Diagnostics unable to select a drive to use for I/O.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x5609**	**Id: 1 if user initiated Data Field Type : 0x0A00 Data Field Value: ID of test requested. 0 – all tests.**

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Runtime Diagnostics error – UTM not enabled:**(SYMsm Description: Diagnostics rejected – access volume (UTM)is not enabled)** **Logged when Runtime Diagnostics request rejected because UTM is not enabled.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x560A**	**Id: 1 if user initiated Data Field Type : 0x0A00 Data Field Value: ID of test requested. 0 – all tests.**
Runtime Diagnostics error – lock error:**(SYMsm Description: Diagnostics rejected - CtlrDiag task cannot obtain Mode Select lock)** **Logged when Runtime Diagnostics request failed because the ctlrDiag task was unable to obtain the Mode Select lock.**					
System (0x0)	**Critical (0x1)**	**Failure (0x2)**	**Controller (0x8)**	**0x560B**	**Id: 1 if user initiated Data Field Type : 0x0A00 Data Field Value: ID of test requested. 0 – all tests.**
Runtime Diagnostics error – lock error on alternate: (SYMsm Description: Diagnostics rejected – CtlrDiag task on controller's alternate cannot obtain Mode Select lock) **Logged when Runtime Diagnostics request failed because the ctlrDiag task on the alternate controller was unable to obtain the Mode Select lock.**					
System (0x0)	**Critical (0x1)**	**Failure (0x2)**	**Controller (0x8)**	**0x560C**	**Id: 1 if user initiated Data Field Type : 0x0A00 Data Field Value: ID of test requested. 0 – all tests.**
Runtime Diagnostics error – Diagnostic read test failed:**(SYMsm Description: Diagnostics read test failed on controller)** **Logged when Runtime Diagnostics Read test failed on this controller.**					
System (0x0)	**Critical (0x1)**	**Failure (0x2)**	**Controller (0x8)**	**0x560D**	**Id: 1 if user initiated Data Field Type : 0x0A00 Data Field Value: ID of test requested. 0 – all tests.**
Runtime Diagnostics error – Diagnostic read failure on alternate controller**(SYMsm Description: This controller's alternate failed diagnostics read test)** **Logged when Runtime Diagnostics Read test failed on the alternate controller.**					
System (0x0)	**Critical (0x1)**	**Failure (0x2)**	**Controller (0x8)**	**0x560E**	**Id: 1 if user initiated Data Field Type : 0x0A00 Data Field Value: ID of test requested. 0 – all tests.**

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Runtime Diagnostics error – Diagnostic write test failed:**(SYMsm Description: Diagnostics write test failed on controller)** **Logged when Runtime Diagnostics Write test failed on this controller.**					
System (0x0)	**Critical (0x1)**	**Failure (0x2)**	**Controller (0x8)**	**0x560F**	**Id: 1 if user initiated Data Field Type : 0x0A00 Data Field Value: ID of test requested. 0 – all tests.**
Runtime Diagnostics error – Diagnostic write test failed on alternate controller**(SYMsm Description: This controller's alternate failed diagnostics write test)** **Logged when Runtime Diagnostics Write test failed on the alternate controller.**					
System (0x0)	**Critical (0x1)**	**Failure (0x2)**	**Controller (0x8)**	**0x5610**	**Id: 1 if user initiated Data Field Type : 0x0A00 Data Field Value: ID of test requested. 0 – all tests.**
Runtime Diagnostics error – loopback error:**(SYMsm Description: Controller passed diagnostics, but loopback test identified an error on loop(s))** **Logged when this controller passed diagnostics, but the loopback test identified an error on one or more of the loops.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x5611**	**Id: 1 if user initiated Data Field Type : 0x0A00 Data Field Value: ID of test requested. 0 – all tests.**
Runtime Diagnostics error – loopback error on alternate:**(SYMsm Description: This controller's alternate passed diagnostics, but loopback test identified an error on loop(s))** **Logged when the alternate controller passed diagnostics, but the loopback test identified an error on one or more of the loops.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x5612**	**Id: 1 if user initiated Data Field Type : 0x0A00 Data Field Value: ID of test requested. 0 – all tests.**
Runtime Diagnostics error – bad channel:**(SYMsm Description: Diagnostics loopback test identified bad destination channel(s))** **Logged when the specified destination channels were identified as bad during the Runtime Diagnostics Loopback Data test.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x5613**	**Id: 1 if user initiated Data Field Type : 0x0A02 Data Field Value: Number of bad channels**

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Runtime Diagnostics error – Source link down:**(SYMsm Description: A host-side port (link) has been detected as down)** **Logged when this controller passed diagnostics, but the specified source link was down.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Channel (0x6)**	**0x5614**	**Id: 1 if user initiated** **Data Field Type : 0x0A01** **Data Field Value: Channel ID**
Not Used					
				0x5615	
Runtime Diagnostics error – Configuration error:**(SYMsm Description: Diagnostics rejected – configuration error on controller)** **Logged when configuration error on this controller for running diagnostics.**					
System (0x0)	**Critical (0x1)**	**Failure (0x2)**	**Controller (0x8)**	**0x5616**	**Id: 1 if user initiated** **Data Field Type : 0x0A00** **Data Field Value: ID of test requested. 0 – all tests.**
Runtime Diagnostics error – Alternate controller configuration error:**(SYMsm Description: Diagnostics rejected - configuration error on this controller's alternate)** **Logged when configuration error of the alternate controller for running diagnostics.**					
System (0x0)	**Critical (0x1)**	**Failure (0x2)**	**Controller (0x8)**	**0x5617**	**Id: 1 if user initiated** **Data Field Type : 0x0A00** **Data Field Value: ID of test requested. 0 – all tests.**
Runtime Diagnostics error – No memory:**(SYMsm Description: Diagnostics rejected - no cache memory on controller)** **Logged when there is no cache memory on controller for running diagnostics.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x5618**	**Id: 1 if user initiated** **Data Field Type : 0x0A00** **Data Field Value: ID of test requested. 0 – all tests.**
Runtime Diagnostics error –No memory on alternate controller:**(SYMsm Description: Diagnostics rejected - no cache memory on this controller's alternate)** **Logged when there is no cache memory on the alternate controller for running diagnostics.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x5619**	**Id: 1 if user initiated** **Data Field Type : 0x0A00** **Data Field Value: ID of test requested. 0 – all tests.**

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
Runtime Diagnostics error – Controller not quiesced:**(SYMsm Description: Diagnostics rejected - data transfer on controller is not disabled (quiesced))** **Logged when Runtime Diagnostics request rejected because controller is not quiesced.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x561A**	**Id: 1 if user initiated Data Field Type : 0x0A00 Data Field Value: ID of test requested. 0 – all tests.**
Runtime Diagnostics error – Alternate Controller not quiesced:**(SYMsm Description: Diagnostics rejected – data transfer on this controller's alternate is not disabled (quiesced))** **Logged when Runtime Diagnostics request rejected because the alternate controller is not quiesced.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x561B**	**Id: 1 if user initiated Data Field Type : 0x0A00 Data Field Value: ID of test requested. 0 – all tests.**
Runtime Diagnostics Mode Error:**(SYMsm Description: Diagnostics rejected – both controllers must be in active mode)** **Logged when Runtime Diagnostics request rejected because both controllers must be in active mode.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x561C**	**Id: 1 if user initiated Data Field Type : 0x0A00 Data Field Value: ID of test requested. 0 – all tests.**
Runtime Diagnostics – Begin Initialization Controller: **(SYMsm Description: Diagnostics initiated from this controller)** **Logged when Runtime Diagnostics is initiated from this controller.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x561D**	**Id: 1 if user initiated Data Field Type : 0x0A00 Data Field Value: ID of test requested. 0 – all tests.**
Runtime Diagnostics – Begin Diagnostics Controller: **(SYMsm Description: Running diagnostics on this controller)** **Logged when Runtime Diagnostics is started on this controller.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x561E**	**Id: 1 if user initiated Data Field Type : 0x0A00 Data Field Value: ID of test requested. 0 – all tests.**
Runtime Diagnostics – Download in Progress: (SYMsm Description: Diagnostics rejected – download is in progress) Logged when Runtime Diagnostics request is rejected because download is in progress.					
System (0x0)	Informational (0x0)	Notification (0x4)	Controller (0x8)	0x561F	Id: 1 if user initiated Data Field Type : 0x0A00 Data Field Value: ID of test requested. 0 – all tests.

Stable Storage events

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
SSTOR Database Creation: **(SYMsm Description: Internal configuration database created)** **Logged when an internal configuration database is created.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x6000**	**None**
SSTOR Database Merge: **(SYMsm Description: Internal configuration database merged)** **Logged when an internal configuration database is merged.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x6001**	**None**
SSTOR Drive Mismatch: **(SYMsm Description: Internal configuration database – mismatch of drives)** **Logged when there is a drive mismatch in the internal configuration database.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x6002**	**None**
SSTOR To Few Sundry: **(SYMsm Description: Internal configuration database – not enough optimal drives available)** **Logged when there are not enough optimal drives available.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x6003**	**None**
SSTOR Re Synchronize: **(SYMsm Description: Internal configuration database is being resynchronized)** **Logged when the internal configuration database is being resynchronized.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x6004**	**None**
SSTOR SS IO Failed: **(SYMsm Description: Internal configuration database read or write operation failed)** **Logged when an internal configuration database read or write operation fails.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x6005**	**None**
SSTOR Merge Failed: **(SYMsm Description: Internal configuration database – merge failed)** **Logged when a stable storage database merge operation fails.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x6006**	**None**

Hierarchical Config DB events

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
DBM Config DB Cleared: **(SYMsm Description: Internal configuration database cleared)** **Logged when an internal configuration database is cleared.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x6100**	**None**
DBM Config DB Full: **(SYMsm Description: Internal configuration database full)** **Logged when an internal configuration database is full.**					
System (0x0)	**Critical (0x1)**	**Notification (0x4)**	**Controller (0x8)**	**0x6101**	**None**
DBM Config DB Expanded: **(SYMsm Description: Internal configuration database – mismatch of drives)** **Logged when there is a drive mismatch on an internal configuration database.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x6102**	**None**
DBM HCK ALTCTL Reset: **(SYMsm Description: This controller's alternate was reset)** **Logged when this controller's alternate is reset.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x6103**	**None**
DBM HCK ALTCTL Failed: **(SYMsm Description: This controller's alternate was failed)** **Logged when this controller's alternate is failed.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x6104**	**None**
DBM Corrupt File SYS: **(SYMsm Description: Internal configuration database – file system corrupted)** **Logged when the file system is corrupted on an internal configuration database.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x6105**	**None**
DBM Invalid File SYS Version: **(SYMsm Description: Internal configuration database – incorrect file system version)** **Logged when an incorrect file system version is found in an internal configuration database.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Controller (0x8)**	**0x6106**	**None**

Snapshot Copy events

Event: Event Description					
Log Group	Priority	Event Group	Component	Event Number	Optional Data
CCopy Repo Overwarn: **(SYMsm Description: Snapshot repository volume capacity – threshold exceeded)** **Logged when the repository usage crosses over the warning threshold. This is an indication that something needs to be done to correct the dwindling free space in the repository before the snapshot fails.**					
System (0x0)	**Critical (0x1)**	**Notification (0x4)**	**Volume (0xD)**	**0x6200**	**None**
CCopy Repo Full: **(SYMsm Description: Snapshot repository volume capacity - full)** **Logged when the repository usage drops below the warning threshold. This could result from either a deletion of a point-in-time image or the capacity of the repository volume has been expanded or the warning threshold was changed.**					
System (0x0)	**Critical (0x1)**	**Notification (0x4)**	**Volume (0xD)**	**0x6201**	**None**
CCopy Snap Failed: **(SYMsm Description: Snapshot volume failed)** **Logged when a snapshot volume fails.**					
System (0x0)	**Critical (0x1)**	**Failure (0x2)**	**Volume (0xD)**	**0x6202**	**None**
CCopy Snap Created: **(SYMsm Description: Snapshot volume created)** **Logged when a new snapshot volume is created.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume (0xD)**	**0x6203**	**None**
CCopy Snap Deleted: **(SYMsm Description: Snapshot volume deleted)** **Logged when a snapshot volume is deleted.**					
System (0x0)	**Informational (0x0)**	**Notification (0x4)**	**Volume (0xD)**	**0x6204**	**None**

Data field types

Table 90. Data field types

Name	Data Field Type	Data Description
Controller Sense Data	0x0100	Controller sense data follows
Transition (Currently not used)	0x0101	2 byte values follow: old value/state in byte 1
Channel ID (Currently not used)	0x0102	4 byte ID follows channel & ID or tray & slot
Controller Number (Currently not used)	0x0103	4 byte value follows 0 even ID 1 odd ID controller
Block Number (Currently not used)	0x0104	4 byte LBA follows
Host Number (Currently not used)	0x0105	4 byte host number follows
Software Revision Number (Currently not used)	0x0106	4 byte SW revision number follows
Error Number (Currently not used)	0x0107	4 byte error number follows - event/component specific
Parity Error (Currently not used)	0x0108	
Device Name (Currently not used)	0x0109	8 bytes - device name string
Number of Blocks (Currently not used)	0x010A	4 byte number of blocks
Unit Number	0x010B	4 byte unit or device number
Component Unique (Currently not used)	0x010C	4 bytes of component specific unique data
Drive Sense	0x010D	First 32 bytes of drive sense data
Drive Inserted (Currently not used)	0x010E	Channel/device number of inserted device
Drive Removed (Currently not used)	0x010F	Channel/device number of removed device
Chip Status	0x0110	Value from chip being logged
ECC Parity Error	0x0111	14 Bytes of parity info **Type** (1 byte): 0x01: Spectra Double Bit ECC 0x02: Spectra Single Bit ECC 0x03: Processor Double Bit ECC 0x04: Processor Single Bit ECC **Syndrome** (1 byte): **Address** (4 bytes): Address of error **Upper Word** (4 bytes): **Lower Word** (4 bytes):
FCC Destination Drive Codes	0x0112	
Chip Address	0x0201	4 bytes chip address
Register Value (Currently not used)	0x0202	4 byte register value
Tally Type (Currently not used)	0x0203	4 bytes tally type that exceeded threshold
Destination Device (Currently not used)	0x0204	
Chip Period (Currently not used)	0x0205	4 bytes - SCSI chip sync clock factor
No Memory	0x0206	4 bytes: 0 = Processor Memory 1 = RPA Memory
Bus Number (Currently not used)	0x0207	
Reassign Blocks Data	0x0208	Data: First eight device numbers and block addresses that were successfully reassigned by the controller. Data is pairs of device and block numbers each 4 bytes.
Piece Number (Currently not used)	0x0301	
Repair (Currently not used)	0x0302	

Table 90. Data field types (continued)

Name	Data Field Type	Data Description
VDD Operation (Currently not used)	0x0303	1 byte VDD operation 0: Restore 1: Recovery 2: Repair 3: Interrupted Write 4: Extra Copy 5: Log Data 6: Stripe Write 7: New Data Write 8: New Parity Write 9: Write Cache
VDD Data, Parity or Repair Operation (Currently not used)	0x0304	1 byte 0: Data operation 1: Parity operation 2: Repair operation
VDD Algorithm (Currently not used)	0x0305	1 byte VDD algorithm in use
Configuration States (Currently not used)	0x0401	
LUN States (Currently not used)	0x0402	4 bytes - LUN state transition below
Controller State (Currently not used)	0x0403	4 bytes - Controller states
Controller Active-Active Mode	0x0404	**Primary controller state** (2 bytes) **Alternate controller state** (2 bytes) 0 = Passive Mode 1 = Active Mode
Controller Active-Passive Mode	0x0405	**Primary controller state** (2 bytes) **Alternate controller state** (2 bytes) 0 = Passive Mode 1 = Active Mode
User Data Length (Currently not used)	0x0501	A maximum of 64 bytes can be sent
User Data (Currently not used)	0x0502	
Configuration Data (Currently not used)	0x0601	
Drive Fault Data (Currently not used)	0x0602	
Drive Group Data	0x0603	Drive List
Fault Data (Currently not used)	0x0604	
Post Error (Currently not used)	0x0605	
3rd Party ID (Currently not used)	0x0606	
Reconfiguration Data (Currently not used)	0x0607	
Mode Select Page Data	0x0608	Mode Select Page data in SCSI format. Length varies according to Mode Select Page
Reconstruction (Currently not used)	0x0609	
Mode Select Page 0x08 Data (Currently not used)	0x060A	
Mode Select Page 0x0A Data (Currently not used)	0x060B	
Mode Select Page 0x2A Data	0x060C	Data: Contains pairs of device and status numbers of device whose statuses were changed by the mode select command. A maximum of 40 pairs are logged using the following structure: **Device** (4 bytes) **Action** (1 byte)
Mode Select Page 0x2B Data (Currently not used)	0x060D	

Table 90. Data field types (continued)

Name	Data Field Type	Data Description
Mode Select Page 0x2C Data (Currently not used)	0x060E	
Mode Select Page 0x2E Data (Currently not used)	0x060F	
Mode Select Time Data (Currently not used)	0x0610	4 bytes - new time value
Mode Select Page 0x3A Data (Currently not used)	0x0611	
VDD Information	0x0612	**Flags** (4 bytes): Beginning flags contents unspecified. **VpState** (4 bytes): State of the virtual piece **blockNum** (4 bytes): Beginning block number for the restore operation. **Cluster** (4 bytes): Beginning cluster number **Stripe** (4 bytes): Beginning stripe number **Offset** (4 bytes): Beginning offset within the stripe **Blocks** (4 bytes): Number of blocks to restore **remBlocks** (4 bytes): Number of remaining blocks to restore **dataDev** (4 bytes): Device number of the data drive not used for recover operations **parityDev** (4 bytes): Device number of the parity drive.
VDD Status	0x0613	**Flags** (4 bytes): buf flags **Error** (4 bytes): buf error
Pass Through Data	0x0614	**Direction of data transfer** (1 byte) **Pass through CDB** (16 bytes)
Write Buffer Data	0x0615	The data buffer contains a maximum of 64 bytes of data sent to the ID
Download Destination (Currently not used)	0x0616	1 byte download device types
VDD Recovery Data	0x0617	Array of 6 byte entries (Maximum of 36 per MEL entry) indicating the LBA and Number of blocks being recovered. **LBA** (4 bytes) **Number of Blocks** (2 bytes)
Data Scrubbing End Tallies	0x0618	**Flags** (4 bytes): buf flags **Error** (4 bytes): buf error **Unrecovered** (1 byte): Number of Unrecovered errors found during scrub **Recovered** (1 byte): Number of recovered errors found during scrub **Mismatch** (1 byte): Number of data/parity mismatches found during scrub **Unfixable** (1 byte): Number of unfixable errors found during scrub
VDD Information Extended (Currently not used)	0x0650	
ASCII Text Data	0x0700	Data is variable length ASCII String
ACS Error	0x0701	4 bytes of ACS error data 1: Mirroring Error 2: Buffer Error 3: Image Error 4: CRC Error 5: Flash Error 6: ICON Error 7: Internal Error 8: Other Error
Enclosure ID (Currently not used)	0x0702	4 bytes sub enclosure ID
AC Status (Currently not used)	0x0703	
Line State Change Data	0x0704	**Byte 0:** Unused **Byte 1:** Transition Data 0 = Good to bad transition 1 = Bad to good transition **Byte 2:** Line Number **Byte 3:** User Component Code

Table 90. Data field types (continued)

Name	Data Field Type	Data Description
Enclosure Data	0x0705	**Byte 0:** Transition Data 0 = Good to bad transition 1 = Bad to good transition **Byte 1:** FRU of device defined by sense data **Byte 2:** 1st Additional FRU byte **Byte 3:** 2nd Additional FRU byte
LBA Information	0x0706	**Starting LBA** (4 bytes) **Number of Block** (4 bytes)
EEL Information	0x0707	**Recovered:** (4 bytes) 0 = Unrecovered 1 = Recovered **Detection** (4 bytes): Detection point in code where logged **LBA** (4 bytes): LBA of error Number of Blocks (4 bytes): Number of blocks involved in the request **ASC** (4 bytes): Internal controller error code **Recovery** (4 bytes): EEL defined recovery actions **Flags** (4 bytes): EEL flags
SYMbol Tray Number	0x0800	Tray location
Volume Label Update	0x0801	Volume Label Update Descriptor
SYMbol Volume Segment Update	0x0802	Volume Segment Sizing Descriptor
SYMbol Group Ownership Update Descriptor	0x0803	Volume Group Ownership information
SYMbol Hotspare Count	0x0804	Number of Hot Spares (4 bytes)
SYMbol Drive Reference List	0x0805	Drive Reference List
SYMbol Volume Creation Descriptor (Currently not used)	0x0806	
SYMbol Controller Firmware Descriptor	0x0807	Firmware Update Descriptor
SYMbol Drive Firmware Descriptor (Currently not used)	0x0808	
SYMbol Group Expansion Descriptor	0x0809	Volume Group Expansion Descriptor
SYMbol Group Migration Descriptor	0x080A	Volume RAID Migration Descriptor
SYMbol Storage Array Cache Update Descriptor	0x080B	Storage Array Parameter Update Descriptor
SYMbol Storage Array User Label Update	0x080C	Storage Array User Assigned Label
SYMbol Time	0x080D	Controller Time (8 bytes)
SYMbol Volume Cache Descriptor	0x080E	Volume Cache Parameters Update Descriptor
SYMbol Volume Parameters Descriptor	0x080F	Volume Parameters Update Descriptor
SYMbol Tray Position List	0x0810	Tray Position List
SYMbol Volume Media Scan Descriptor	0x0811	Volume Media Scan Parameters Update Descriptor
SYMbol Storage Array Media Scan Rate	0x0812	Storage Array Media Scan Rate (4 bytes)
SYMbol Controller Number	0x0813	**Controller Number** (4 bytes) 0 = This controller 1 = Alternate controller
SYMbol Return Code	0x0814	**RPC Function** (4 bytes) See RPC Function Number table **Return Code** (4 bytes) See SYMbol Return code table

Table 90. Data field types (continued)

Name	Data Field Type	Data Description
Download checkpoint data	0x0815	Checkpoint data
Battery Component Data	0x816	**Battery Reset** (4 bytes) 0 – battery reset not requested 1 – battery reset requested **Component Location** (12 bytes) – A unique ID that identifies the component to the controller firmware. Contents are not specified.
Snapshot parameters descriptor	0x0817	Snapshot Parameters Update Descriptor
Ghost WWN	0x0818	World Wide Name of the missing volume (16 bytes)
User Assigned Label	0x0900	
SYMbol Reference Data	0x0901	
SYMbol Reference Pair Data	0x0902	
SYMbol Reference Data with User Assigned Label	0x0903	
Host Port Creation Descriptor	0x0904	
Host Port Rename Descriptor	0x0905	
Host Port Type Update Descriptor	0x0906	
Host Creation Descriptor	0x0907	
LUN Mapping Creation Descriptor	0x0908	
LUN Mapping Update Descriptor	0x0909	
Error Return Code	0x090A	
Runtime Diagnostics Descriptor	0x0A00	data field Value: 0 - all tests Else - ID of test required
Runtime Diagnostics Channel ID	0x0A01	Data is a byte indicating the channel number that failed.
Runtime Diagnostics Channel List	0x0A02	Data is a length and a byte array of the failed channels.

RPC function numbers

RPC Function Number		SYMbol Function
1	0x01	**discoverControllers_1()**
		This function is used to query a SYMbol server for all controllers that it knows about. The responder will also indicate in its response structure whether it is actually a net-attached controller, or is a host-based agent that is returning information about multiple attached controllers.
2	0x02	**bindToController_1()**
		This function is used to bind a new connection to a particular controller. If the server is actually a controller itself, the controller will just ensure that its CONTROLLER REF is the same as the one passed in as an argument. If the server is an agent, it will use the CONTROLLER REF argument to determine which locally-attached controller should be used for all further interactions over the RPC connection.
3	0x03	**assignVolumeGroupOwnership_1()**
		Instructs the SYMbol Server's controller to transfer ownership of a volume group and its associated volumes to another controller.
4	0x04	**assignDrivesAsHotSpares_1()**
		Instructs the SYMbol Server's controller to create a given number of hot spare drives out of the drives currently unassigned.
5	0x05	**assignSpecificDrivesAsHotSpares_1()**
		Instructs the SYMbol Server's controller to create hot spare drives out of the given drives.
6	0x06	**getVolumeCandidates_1()**
		Instructs the SYMbol Server's controller to return a list of volume candidates for the specified type of volume creation operation.
7	0x07	**createVolume_1()**
		Instructs the SYMbol Server's controller to create new volume using the specified parameters.
8	0x08	**deassignDrivesAsHotSpares_1()**
		Instructs the SYMbol Server's controller to delete a specified hot spare drive. After the deletion has occurred the drive is marked as unassigned.
9	0x09	**deleteVolume_1()**
		Instructs the SYMbol Server's controller to delete a specified volume from a volume group.
10	0x0A	**SetControllerToFailed_1()**
		Instructs the SYMbol Server's controller to fail the specified controller. Note that a controller is not allowed to fail itself.

RPC Function Number		SYMbol Function
11	**0x0B**	**setDriveToFailed_1()**
		Instructs the SYMbol Server's controller to mark the specified drive as failed.
12	**0x0C**	**startVolumeFormat_1()**
		Instructs the SYMbol Server's controller to initiate a format of the specified volume.
13	**0x0D**	**initializeDrive_1()**
		Acquaints a newly plugged in drive to a storage array by setting up appropriate structures on the disk.
14	**0x0E**	**loadControllerFirmware_1()**
		Downloads a portion of a new firmware image to the SYMbol Server's controller.
15	**0x0F**	**loadControllerNVSRAM_1()**
		Downloads an entire NVSRAM image to the SYMbol Server's controller. **Note that the FirmwareUpdateDescriptor must contain the ENTIRE image of the NVSRAM; iterative download of multiple segments is not allowed when transferring NVSRAM.**
16	**0x10**	**resetMel_1()**
		Clear all entries from the Major Events Log.
17	**0x11**	**setVolumeGroupToOffline_1()**
		Instructs the SYMbol Server's controller to place a volume group offline. Useful for pluggable volume groups.
18	**0x12**	**setVolumeGroupToOnline_1()**
		Returns an offline volume group to online operation.
19	**0x13**	**startDriveReconstruction_1()**
		Forces a volume reconstruction using the newly plugged in drive. The parameter is a reference to the new drive.
20	**0x14**	**startVolumeGroupDefrag_1()**
		Initiates a volume group defragmentation operation.
21	**0x15**	**startVolumeGroupExpansion_1()**
		Initiates a volume group expansion (DCE) operation.
22	**0x16**	**startVolumeRAIDMigration_1()**
		Initiates a volume RAID migration (DRM) operation.
23	0x17	startVolumeSegmentSizing_1()
		Initiates a volume segment sizing (DSS) operation.

RPC Function Number		SYMbol Function
24	**0x18**	**setControllerToPassive_1()**
		Instructs the SYMbol Server's controller to place the specified controller in passive mode.
25	**0x19**	**setControllerToActive_1()**
		Instructs the SYMbol Server's controller to place the specified controller in active mode.
26	**0x1A**	**setSACacheParams_1()**
		Instructs the SYMbol Server's controller to propagate a controller cache change to all controllers in the storage array.
27	**0x1B**	**setSAUserLabel_1()**
		Instructs the SYMbol Server's controller to change the shared SA name.
28	**0x1C**	**setControllerTime_1()**
		Sets the internal clock of the SYMbol Server's controller. The time should be expressed in seconds since midnight (GMT) on 1/1/1970.
29	**0x1D**	**setVolumeCacheParams_1()**
		Sets the volume cache properties of a volume indicated in the VolumeCacheParamsUpdate structure.
30	**0x1E**	**setVolumeParams_1()**
		Sets various volume parameters. Primarily used to fine tune a volume.
31	**0x1F**	**setVolumeUserLabel_1()**
		Sets the user assigned label for the volume specified in the VolumeLabelUpdate structure.
32	**0x20**	**startSAIdentification_1()**
		Causes the storage array to physically identify itself. The identification will continue until a stop command is issued. This function does not block.
33	**0x21**	**startDriveIdentification_1()**
		Causes the drives specified to physically identify themselves until a stop command is issued. This function does not block.
34	**0x22**	**stopIdentification_1()**
		Explicitly stops the physical identification of an SA unit.
35	**0x23**	**SetHostInterfaceParams_1()**
		Change the preferred ID used for the specified I/O interface.
36	0x24	setControllerToOptimal_1()
		Instructs the SYMbol Server's controller to attempt to revive the specified controller from the failed state.

RPC Function Number		SYMbol Function
37	**0x25**	**setDriveToOptimal_1()**
		Instructs the SYMbol Server's controller to attempt to revive the given drive. Success will be reported via a definition change event on the given drive.
38	**0x26**	**forceVolumeToOptimal_1()**
		Instructs the SYMbol Server's controller to attempt to revive the given volume group.
39	**0x27**	**getControllerHostInterfaces_1()**
		Obtains the most up-to-date information about the host-side I/O interfaces of the controller that responds to the request.
40	**0x28**	**getObjectGraph_1()**
		Gets a bundle of information consisting of all possible entities that comprise a storage array. Normally used by the management app to construct a representation of the storage array.
41	**0x29**	**getVolumeActionPercentComplete_1()**
		Gets the completion percentage of a long running volume oriented operation. If no operation is running on the given volume then a -1 will be returned.
42	**0x2A**	**getRecoveryFailureList_1()**
		Gets a list of failure objects to assist in recovery. Each entry contains a recovery procedure key that can be used by the client as desired, and a SYMbol reference to the object associated with the failure.
43	**0x2B**	**getSAInfo_1()**
		Gets information pertaining to the general characteristics of the storage array. Normally used simply to check the status and management version of each storage array at start up.
44	**0x2C**	**getVolumePerformanceInfo_1()**
		Samples the performance of several volumes and reports on their performance. The Nth VolumePerformance structure in the VolumePerformanceList should correspond to the Nth reference in the VolumeRefList.
45	**0x2D**	**setSATrayPositions_1()**
		Used to store the user selectable tray ordering data on the controller.
46	**0x2E**	**setVolumeMediaScanParams_1()**
		Sets the media scan parameters for the specified volume.
47	**0x2F**	**setSAMediaScanPeriod_1()**
		Sets the media scan period (in days) for the array. Each controller will scan volumes such that a complete scan completes every N days, as specified by the argument passed to this procedure.

RPC Function Number		SYMbol Function
48	**0x30**	**getChangeInfo_1()**
		Fetches an indication of the most recent state/configuration changes that occurred on the storage array. This function is used to initiate a (potentially) "hanging" poll for change notifications. The call "hangs", in the sense that the caller gives a maximum wait time. The controller can stall up to the given interval before returning the result to the caller.
49	**0x31**	**clearSAConfiguration_1()**
		Clears the entire array configuration, deleting all volumes and returning to a clean initial state. This is a highly destructive and dangerous operation!
50	**0x32**	**autoSAConfiguration_1()**
		Tells the controller to automatically configure the Storage Array.
51	**0x33**	**getMelExtent_1()**
		Retrieves the beginning and ending sequence numbers in the Mel.
52	**0x34**	**getMelEntries_1()**
		Retrieves a list of MelEntries starting with the beginning sequence number and ending with the ending sequence number.
53	**0x35**	**getCriticalMelEntries_1()**
		Retrieves a list of MelEntries within the specified extent that have a severity level of CRITICAL.
54	**0x36**	**getControllerNVSRAM_1()**
		Reads the specified regions of NVSRAM.
55	**0x37**	**setControllerNVSRAM_1()**
		Modifies a portion of the target controller's NVSRAM.
56	**0x38**	**setSAPassword_1()**
		Sets a new password value for the array.
57	**0x39**	**pingController_1()**
		Verifies that the controller is operating properly.
58	**0x3A**	**startVolumeParityCheck_1()**
		Initiates a parity check operation for the specified volume.
59	**0x3B**	**getParityCheckProgress_1()**
		Queries for the status of an in-progress parity check operation. The return value is one of the following: An integer in the range 0-100, indicating the percent complete for an operation that is still in progress, or a negative integer indicating either a successfully complete scan or a scan that was stopped because of an error condition.

RPC Function Number		SYMbol Function
60	**0x3C**	**Not Used**
61	**0x3D**	**getLUNMappings_1()**
		Retrieves the Storage Pools Manager's LUNMappings data which apply to a particular ref.
62	**0x3E**	**createSAPortGroup_1()**
		Creates a new SAPortGroup & returns its ref. If a group by that name already exists, returns its ref.
63	**0x3F**	**deleteSAPortGroup_1()**
		Removes all SAPorts from an SAPortGroup, and deletes the group.
64	**0x40**	**moveSAPort_1()**
		Removes the SA Port 'itemRef' from any SA Port Group that it might be in, & moves it to the group 'containerRef'. If this leaves the previous SAPortGroup empty, the previous SAPortGroup is deleted.
65	**0x41**	**getSAPort_1()**
		Retrieves a storage array port.
66	**0x42**	**createHost_1()**
		Creates a new Host. If a Host already exists with 'label', returns a ref to it.
67	**0x43**	**createCluster_1()**
		Creates a new Host Group. If a Host Group already exists with 'label', returns a ref to it.
68	**0x44**	**deleteCluster_1()**
		Removes all Hosts from a Host Group, and deletes the Host Group.
69	**0x45**	**renameCluster_1()**
		Modifies a Host Group's label.
70	**0x46**	**deleteHost_1()**
		Removes all HostPorts from a Host, and deletes the Host. If this leaves the Host Group that the Host was in empty, the Host Group is deleted.
71	**0x47**	**renameHost_1()**
		Modifies a Host's label.
72	0x48	moveHost_1()
		Removes the Host 'itemRef' from any Host Group it might be in, & moves it to the Host Group 'containerRef'. If this leaves the previous Host Group empty, the previous Host Group is deleted.

RPC Function Number		SYMbol Function
73	**0x49**	**createHostPort_1()**
		Creates a new HostPort with the 'name' & 'label', & returns its ref. If a HostPort already exists with 'name' & 'label', returns its ref.
74	**0x4A**	**deleteHostPort_1()**
		Deletes a host port. If this leaves the Host that the HostPort was in empty, the Host is deleted. Then, if deleting the Host leaves the Host Group that the Host was in empty, the Host Group is deleted.
75	**0x4B**	**RenameHostPort_1()**
		Modifies a HostPort's name &/or label.
76	**0x4C**	**MoveHostPort_1()**
		Removes the HostPort 'itemRef' from any Host it might be in, & moves it to the Host 'containerRef'. If this leaves the previous Host empty, the Host is deleted. Then, if deleting the Host leaves the Host Group that the Host was in empty, the Host Group is deleted.
77	**0x4D**	**CreateLUNMapping_1()**
		Creates a LUN mapping.
78	**0x4E**	**deleteLUNMapping_1()**
		Deletes a LUN mapping.
79	**0x4F**	**getUnlabedHostPorts_1()**
		Get the volatile connections and host ports.
80	**0x50**	**setHostPortType_1()**
		Get the possible host port type labels.
81	**0x51**	**moveLUNMapping_1()**
		Move a LUN mapping.
82	**0x52**	**enableFeature_1()**
		Enable add-on(optional) features
83	**0x53**	**disableFeature_1()**
		Disable a single add-on(optional) feature
84	**0x54**	**stateCapture_1()**
		Capture diagnostic information
85	0x55	loadDriveFirmware()
		Downloads a portion of a new firmware image to a drive in the SYMbol Server.

RPC Function Number		SYMbol Function
86	**0x56**	**loadESMFirmware()**
		Downloads a portion of a new firmware image to an ESM card in the SYMbol Server.
87	**0x57**	**getHostSpecificNVSRAM()**
		Reads the Host Type Dependent regions of NVSRAM.
88	**0x58**	**setHostSpecificNVSRAM()**
		Modifies the Host Type Dependent regions of the target controller's NVSRAM.
89	**0x59**	**setBatteryParams()**
		Sets the battery properties for the given battery.
90	**0x5A**	**assignVolumeOwnership()**
		Instructs the SYMbol Server's controller to transfer ownership of a volume to another controller.
91	**0x5B**	**IssueRuntimeDiagnostics()**
		Issues Runtime Diagnostics.
92	**0x5C**	**resetController()**
		Requests a reboot of the given controller.
93	**0x5D**	**quiesceController()**
		Issues a quiesce command to the given controller.
94	**0x5E**	**unquiesceController()**
		Removes the given controller from a quiesced state.
95	**0x5F**	**startVolumeExpansion()**
		Initiates a Volume Expansion (DVE or DCE/DVE) operation.
96	**0x60**	**createSnapshot()**
		Creates a snapshot volume of a given base.
97	**0x61**	**disableSnapshot()**
		Disables (stops) a snapshot.
98	**0x62**	**recreateSnapshot()**
		Recreates (restarts) a snapshot.
99	0x63	setSnapshotParams()
		Modifies the parameters of a snapshot.
100	0x64	getRepositoryUtilization()
		Returns repository-utilization information for selected snapshots.

RPC Function Number		SYMbol Function
101	**0x65**	**calculateDVECapacity()**
		Calculates the volume's maximum capacity after a DVE operation.
102	**0x66**	**getReadLinkStatus()**
		Gets the Read Link Status information.
103	**0x67**	**setRLSBaseline()**
		Sets the Read Link Status baseline information.

SYMbol return codes

Table 91. SYMbol return codes

Return Code		Definition
1	0x01	RETCODE_OK The operation completed successfully.
2	0x02	RETCODE_ERROR The operation cannot complete because either (1) the current state of a component does not allow the operation to be completed or (2) there is a problem with the Storage Array. Please check your Storage Array and its various components for possible problems and then retry the operation.
3	0x03	RETCODE_BUSY The operation cannot complete because a controller resource is being used by another process. If there are other array management operations in progress, wait for them to complete, and then retry the operation. If this message persists, turn the power to the controller tray off and then on.
4	0x04	RETCODE_ILLEGAL_PARAM The operation cannot complete because of an incorrect parameter in the command sent to the controller. Please retry the operation. If this message persists, contact your Customer Support Representative.
5	0x05	RETCODE_NO_HEAP An out of memory error occurred on one of the controllers in the Storage Array. Contact your Customer Support Representative about the memory requirements for this Storage Array.
6	0x06	RETCODE_DRIVE_NOT_EXIST The operation cannot complete because one or more specified drives do not exist. Please specify only drives currently installed in the Storage Array and then retry the operation.
7	0x07	RETCODE_DRIVE_NOT_UNASSIGNED The operation cannot complete because one or more specified drives do not have an unassigned status. Please specify only drives with an unassigned status and then retry the operation.
8	0x08	RETCODE_NO_SPARES_ASSIGNED None of the selected drives were assigned as hot spares. Possible causes include (1) the maximum number of hot spares have already been assigned or (2) the selected drives have capacities that are smaller than all other drives in the Storage Array. If you suspect the second cause, please use the Drive>>Properties option in the Array Management Window to obtain the selected drives' capacity.

Table 91. SYMbol return codes (continued)

Return Code		Definition
9	0x09	RETCODE_SOME_SPARES_ASSIGNED Some but not all of the selected drives were assigned as hot spares. Check the Physical View in the Array Management Window to determine which drives were assigned. Possible causes include (1) the maximum number of hot spares have been assigned or (2) some of the selected drives have capacities that are smaller than all other drives in the Storage Array. If you suspect the second cause, please use the Drive>>Properties option in the Array Management Window to obtain the selected drives' capacity.
10	0x0A	RETCODE_VOLUME_NOT_EXIST The specified volume does not exist. The volume might have been deleted by a user on another management station accessing this Storage Array.
11	0x0B	RETCODE_VOLUME_RECONFIGURING The operation cannot complete because a volume is performing a modification operation. Please wait until the modification completes and then retry the operation. Use the Volume>>Properties option in the Array Management Window to check the progress.
12	0x0C	RETCODE_NOT_DUAL_ACTIVE The operation cannot complete because the controllers in the Storage Array must be Active/Active. Please use the Controller>>Change Mode option in the Array Management Window to change the controller to active.
13	0x0D	RETCODE_TRY_ALTERNATE This operation must be performed by the alternate controller.
14	0x0E	RETCODE_BACKGROUND An operation is running in the background.
15	0x0F	RETCODE_NOT_IMPLEMENTED This option is currently not implemented.
16	0x10	RETCODE_RESERVATION_CONFLICT The operation cannot complete because an application has reserved the selected volume. Please wait until the volume has been released and then retry the operation.
17	0x11	RETCODE_VOLUME_DEAD The operation cannot complete because either the volume remains failed or has transitioned to failed. Please use the Recovery Guru in the Array Management Window to resolve the problem.
18	0x12	RETCODE_INTERNAL_ERROR The operation cannot complete because of an internal target error. Please retry the operation. If this message persists, contact your Customer Support Representative.
19	0x13	RETCODE_INVALID_REQUEST The operation cannot complete because of a general configuration request error. Please retry the operation. If this message persists, contact your Customer Support Representative.
20	0x14	RETCODE_ICON_FAILURE The operation cannot complete because there is a communications failure between the controllers. Please turn the power to the controller tray off and then on and then retry the operation. If this message persists, contact your Customer Support Representative.

Table 91. SYMbol return codes (continued)

Return Code		Definition
21	0x15	RETCODE_VOLUME_FORMATTING The operation cannot complete because a volume initialization is in progress. Please wait until the initialization completes and then retry the operation. Use the Volume>>Properties option in the Array Management Window to check the progress.
22	0x16	RETCODE_ALT_REMOVED The operation cannot complete because the other controller is not present. Please insert the other controller and retry the operation.
23	0x17	RETCODE_CACHE_SYNC_FAILURE The operation cannot complete because the cache between the controllers could not be synchronized. This normally occurs if the controller's alternate pair has not completed its start-of-day routine. Please wait at least two minutes and then retry the operation. If this message persists, contact your Customer Support Representative.
24	0x18	RETCODE_INVALID_FILE The download cannot complete because a file is not valid. Replace the file and retry the operation.
25	0x19	RETCODE_RECONFIG_SMALL_DACSTORE The modification operation cannot complete because the controller configuration area (DACStore) is too small. Contact your Customer Support Representative.
26	0x1A	RETCODE_RECONFIG_FAILURE The modification operation cannot complete because there is not enough capacity on the volume group. If you have any unassigned drives, you can increase the capacity of the volume group by using the Volume Group>>Add Free Capacity option and then retry the operation.
27	0x1B	RETCODE_NVRAM_ERROR Unable to read or write NVSRAM.
28	0x1C	RETCODE_FLASH_ERROR There was a failure in transferring the firmware to flash memory during a download operation. Please retry the operation.
29	0x1D	RETCODE_AUTH_FAIL_PARAM This operation cannot complete because there was a security authentication failure on a parameter in the command sent to the controller. Please retry the operation. If this message persists, contact your Customer Support Representative.
30	0x1E	RETCODE_AUTH_FAIL_PASSWORD The operation cannot complete because you did not provide a valid password. Please re-enter the password.
31	0x1F	RETCODE_MEM_PARITY_ERROR There is a memory parity error on the controller.
32	0x20	RETCODE_INVALID_CONTROLLERREF The operation cannot complete because the controller specified in the request is not valid (unknown controller reference).

Table 91. SYMbol return codes (continued)

Return Code		Definition
33	0x21	RETCODE_INVALID_VOLUMEGROUPREF The operation cannot complete because the volume group specified in the request is not valid (unknown volume group reference). The volume group might have been deleted or modified by a user on another management station accessing this Storage Array.
34	0x22	RETCODE_INVALID_VOLUMEREF The operation cannot complete because the volume specified in the request is not valid (unknown volume reference). The volume might have been deleted or modified by a user on another management station accessing this Storage Array.
35	0x23	RETCODE_INVALID_DRIVEREF The operation cannot complete because the drive specified in the request is not valid (unknown drive reference). The drive might have been used or modified by a user on another management station accessing this Storage Array.
36	0x24	RETCODE_INVALID_FREEEXTENTREF The operation cannot complete because the free capacity specified in the request is not valid (unknown free capacity reference). The free capacity might have been used or modified by a user on another management station accessing this Storage Array.
37	0x25	RETCODE_VOLUME_OFFLINE The operation cannot complete because the volume group is offline. Please place the volume group online by using the Volume Group>>Place Online option in the Array Management Window.
38	0x26	RETCODE_VOLUME_NOT_OPTIMAL The operation cannot complete because some volumes are not optimal. Please correct the problem causing the non-optimal volumes using the Recovery Guru and then retry the operation.
39	0x27	RETCODE_MODESENSE_ERROR The operation cannot complete because state information could not be retrieved from one or more controllers in the Storage Array.
40	0x28	RETCODE_INVALID_SEGMENTSIZE The operation cannot complete because either (1) the segment size requested is not valid, or (2) the segment size you specified is not allowed because this volume has an odd number of segments. Therefore, you can only decrease the segment size for this volume to a smaller number.
41	0x29	RETCODE_INVALID_CACHEBLKSIZE The operation cannot complete because the cache block size requested is not valid.
42	0x2A	RETCODE_INVALID_FLUSH_THRESHOLD The operation cannot complete because the start cache flush value requested is not valid.
43	0x2B	RETCODE_INVALID_FLUSH_AMOUNT The operation cannot complete because the stop cache flush value requested is not valid.
44	0x2C	RETCODE_INVALID_LABEL The name you have provided cannot be used. The most likely cause is that the name is already used by another volume. Please provide another name.
45	0x2D	RETCODE_INVALID_CACHE_MODIFIER The operation cannot complete because the cache flush modifier requested is not valid.

Table 91. SYMbol return codes (continued)

Return Code		Definition
46	0x2E	RETCODE_INVALID_READAHEAD The operation cannot complete because the cache read ahead requested is not valid.
47	0x2F	RETCODE_INVALID_RECONPRIORITY The operation cannot complete because the modification priority requested is not valid.
48	0x30	RETCODE_INVALID_SCANPERIOD The operation cannot complete because the media scan duration requested is not valid.
49	0x31	RETCODE_INVALID_TRAYPOS_LENGTH The number of trays requested has exceeded the maximum value.
50	0x32	RETCODE_INVALID_REGIONID The operation cannot complete because the requested NVSRAM region is not valid.
51	0x33	RETCODE_INVALID_FIBREID The operation cannot complete because the preferred loop ID requested is not valid. Please specify an ID between 0 and 127.
52	0x34	RETCODE_INVALID_ENCRYPTION The operation cannot complete because the encryption routine requested is not valid.
53	0x35	RETCODE_INVALID_RAIDLEVEL The operation cannot complete because of the current RAID level of the volume group. Remember that some operations cannot be performed on certain RAID levels because of redundancy or drive requirements.
54	0x36	RETCODE_INVALID_EXPANSION_LIST The operation cannot complete because the number of drives selected is not valid.
55	0x37	RETCODE_NO_SPARES_DEASSIGNED No hot spare drives were deassigned. Possible causes include (1) the drives are not hot spares, (2) the hot spares are removed, (3) the hot spares are failed, or (4) the hot spares are integrated into a volume group. Check these possible causes and then retry the operation.
56	0x38	RETCODE_SOME_SPARES_DEASSIGNED Not all of the requested hot spare drives were deassigned. Possible causes include (1) the drives are not hot spares, (2) the hot spares are removed, (3) the hot spares are failed, or (4) the hot spares are integrated into a volume group. Check these possible causes and then retry the operation.
57	0x39	RETCODE_PART_DUP_ID The operation cannot complete because the identifier or name you provided already exists. Please provide another identifier or name and then retry the operation.
58	0x3A	RETCODE_PART_LABEL_INVALID The operation cannot complete because the name you provided is not valid. Please provide a non-blank name and then retry the operation.

Table 91. SYMbol return codes (continued)

Return Code		Definition
59	0x3B	RETCODE_PART_NODE_NONEXISTENT The operation cannot complete because the host group, host, or host port you have selected no longer exists. The object might have been deleted or modified by a user on another management station accessing this Storage Array. Please close and re-open the dialog box to refresh the information.
60	0x3C	RETCODE_PART_PORT_ID_INVALID The creation of the host port cannot complete because the host port identifier is not valid. Either the identifier is empty or has characters other than 0-9 and A-F. Please enter a valid host port identifier and then retry the operation.
61	0x3D	RETCODE_PART_VOLUME_NONEXISTENT The creation of a new volume-to-LUN mapping cannot complete because the volume you have selected no longer exists. The volume might have been deleted or modified by a user on another management station accessing this Storage Array. Please close and open the dialog box to refresh the information.
62	0x3E	RETCODE_PART_LUN_COLLISION The operation cannot complete because the logical unit number (LUN) is already in use. Please select another LUN.
63	0x3F	RETCODE_PART_VOL_MAPPING_EXISTS The operation cannot complete because the volume you have selected already has a volume-to-LUN mapping. The mapping might have been defined by a user on another management station accessing this Storage Array. Please close and re-open the dialog box to refresh the information.
64	0x40	RETCODE_PART_MAPPING_NONEXISTENT The operation cannot complete because the volume-to-LUN mapping you have selected no longer exists. The mapping might have been deleted by a user on another management station accessing this Storage Array. Please close and re-open the dialog box to refresh the information.
65	0x41	RETCODE_PART_NO_HOSTPORTS The operation cannot complete because the host group or host has no host ports. Please define a host port for the host group or host and then retry the operation.
66	0x42	RETCODE_IMAGE_TRANSFERRED The image was successfully transferred.
67	0x43	RETCODE_FILE_TOO_LARGE The download cannot complete because a file is not valid. Replace the file and retry the operation.
68	0x44	RETCODE_INVALID_OFFSET A problem has occurred during the download. Please retry the operation.
69	0x45	RETCODE_OVERRUN The download cannot complete because a file is not valid. Replace the file and retry the operation.
70	0x46	RETCODE_INVALID_CHUNKSIZE A problem has occurred during the download. Please retry the operation.
71	0x47	RETCODE_INVALID_TOTALSIZE The download cannot complete because a file is not valid. Replace the file and retry the operation.

Table 91. SYMbol return codes (continued)

Return Code		Definition
72	0x48	RETCODE_DOWNLOAD_NOT_PERMITTED Unable to perform the requested download because the NVSRAM option to support this download type is disabled. Contact your Customer Support Representative.
73	0x49	RETCODE_SPAWN_ERROR A resource allocation error (unable to spawn a task) occurred on one of the controllers in the Storage Array.
74	0x4A	RETCODE_VOLTRANSFER_ERROR The operation cannot complete because the controller was unable to transfer the volumes to its alternate controller. Please check the alternate controller for problems and then retry the operation.
75	0x4B	RETCODE_INVALID_DLSTATE The operation cannot complete because the controller pair is in an Active/Passive mode. Please use the Controller>>Change Mode option in the Array Management Window to change the passive controller to active and then retry the operation.
76	0x4C	RETCODE_CACHECONFIG_ERROR The operation cannot complete because of an incorrect controller configuration. Possible causes include (1) the controller pair is in an Active/Passive mode, or (2) controller cache synchronization failed. Please use the Controller>>Change Mode option in the Array Management Window to change the passive controller to active and then retry the operation. If this message persists, contact your Customer Support Representative.
77	0x4D	RETCODE_DOWNLOAD_IN_PROGRESS The operation cannot complete because a download is already in progress. Please wait for the download to complete and, if necessary, retry the operation.
78	0x4E	RETCODE_DRIVE_NOT_OPTIMAL The operation cannot complete because a drive in the volume group is not optimal. Please correct the problem causing the non-optimal drive using the Recovery Guru and then retry the operation.
79	0x4F	RETCODE_DRIVE_REMOVED The operation cannot complete because a drive in the volume group is removed. Please insert a drive and then retry the operation.
80	0x50	RETCODE_DUPLICATE_DRIVES The operation cannot complete because the selected drive is already part of the volume group. Please select another drive and retry the operation.
81	0x51	RETCODE_NUMDRIVES_ADDITIONAL The operation cannot complete because the number of drives selected exceeds the maximum additional drives allowed. Please select a smaller number of drives and then retry the operation.
82	0x52	RETCODE_NUMDRIVES_GROUP The operation cannot complete because either (1) the number of drives selected is not valid for the RAID level of the volume group or (2) the number of drives in the volume group is not valid for the proposed RAID level.
83	0x53	RETCODE_DRIVE_TOO_SMALL The operation cannot complete because at least one of the drives selected has a capacity that is not large enough to hold the existing data of the volume group. Please select another drive and retry the operation.

Table 91. SYMbol return codes (continued)

Return Code		Definition
84	0x54	RETCODE_CAPACITY_CONSTRAINED The operation cannot complete because there is no free capacity or not enough free capacity on the volume group to accommodate the new RAID level.
85	0x55	RETCODE_MAX_VOLUMES_EXCEEDED The operation cannot complete because the maximum number of volumes for this Storage Array has been reached.
86	0x56	RETCODE_PART_IS_UTM_LUN The operation cannot complete because the logical unit number (LUN) is already in use by the Access Volume. Please select another LUN.
87	0x57	RETCODE_SOME_SPARES_TOO_SMALL One or more drives were assigned as hot spares. However, some of the drives do not have a capacity large enough to cover all of the drives in the Storage Array. If a drive fails that has a capacity larger than these hot spares drive(s), it will not be covered by these drives. Check the capacity of the newly-assigned hot spare drives by using the Drive>>Properties option in the Array Management Window. You might want to deassign the smaller hot spare drives.
88	0x58	RETCODE_SPARES_SMALL_UNASSIGNED Not all of the drives that you attempted to assign as hot spares were assigned. In addition, one or more drives that were assigned as hot spares do not have a capacity large enough to cover all of the drives in the Storage Array. If a drive fails that has a capacity larger than these hot spares drive(s), it will not be covered by these drives. Check the capacity of the newly-assigned hot spare drives by using the Drive>>Properties option in the Array Management Window. You might want to deassign the smaller hot spare drives.
89	0x59	RETCODE_TOO_MANY_PARTITIONS Cannot create or change a volume-to-LUN mapping because either you have not enabled the Storage Partitioning feature or the Storage Array has reached its maximum number of allowable partitions. Storage Partitioning is a Premium Feature that must be specifically enabled through the user interface. Use the Storage Array>>Premium Features option to enable the feature. If you have not previously obtained a Feature Key File for Storage Partitioning, contact your storage supplier.
90	0x5A	RETCODE_PARITY_SCAN_IN_PROGRESS A redundancy check is already in progress. Either a redundancy check is currently being performed or it was cancelled but the time-out period (1 to 2 minutes) has not been reached. Please wait until the check has completed or timed out and then retry the operation.
91	0x5B	RETCODE_INVALID_SAFE_ID The Feature Enable Identifier contained in the Feature Key File you have selected does not match the identifier for this Storage Array. Please select another Feature Key File or obtain a Feature Key File using the correct identifier. You can determine the Feature Enable Identifier for this Storage Array by selecting the Storage Array>>Premimum Feature>>List option.
92	0x5C	RETCODE_INVALID_SAFE_KEY The Feature Key File you have selected is not valid. The security (digest) information contained in the file does not match what was expected from the controller. Please contact your Customer Support Representative.

Table 91. SYMbol return codes (continued)

Return Code		Definition
93	0x5D	RETCODE_INVALID_SAFE_CAPABILITY The Premium Feature you are attempting to enable with this Feature Key File is not supported on the current configuration of this Storage Array. Please determine the configuration (such as appropriate level of firmware and hardware) necessary to support this feature. Contact your Customer Support Representative if necessary.
94	0x5E	RETCODE_INVALID_SAFE_VERSION The Feature Key File you have selected is not valid. The version information contained in the file does not match what was expected from the controller. Please contact your Customer Support Representative.
95	0x5F	RETCODE_PARTITIONS_DISABLED Cannot create an unmapped volume, since storage partitions are disabled.
96	0x60	RETCODE_DRIVE_DOWNLOAD_FAILED A firmware download to a drive failed.
97	0x61	RETCODE_ESM_DOWNLOAD_FAILED A firmware download to an ESM card failed.
98	0x62	RETCODE_ESM_PARTIAL_UPDATE Firmware download to tray (ESMs) failed for one ESM, so versions mismatch.
99	0x63	RETCODE_UTM_CONFLICT The operation could not complete because the NVSRAM offset 0x32 is attempting to enable a logical unit number (LUN) for an access volume that conflicts with a LUN for a volume that already exists on the Storage Array. If you are downloading a new NVSRAM file, you will need to obtain a new file with the offset set to a LUN that does not conflict. If you are setting this NVSRAM offset using the Script Editor ″set controller nvsramByte″ command, you must choose a different LUN that does not conflict.
100	0x64	RETCODE_NO_VOLUMES A volume must exist to perform the operation.
101	0x65	RETCODE_AUTO_FAIL_READPASSWORD The operation cannot complete because either there is a problem communicating with any of the drives in the Storage Array or there are currently no drives connected. Please correct the problem and then retry the operation.
102	0x66	RETCODE_PART_CRTE_FAIL_TBL_FULL The operation cannot complete because the maximum number of host-groups, hosts, and host-ports have been created for this Storage Array.
103	0x67	RETCODE_ATTEMPT_TO_SET_LOCAL The operation cannot complete because you are attempting to modify host-dependent values for region ID 0xF1. You must change host-dependent values in one of the host index areas.
104	0x68	RETCODE_INVALID_HOST_TYPE_INDEX The operation cannot complete because the host index must be between 0 and {MAX_HOST_TYPES-1}.
105	0x69	RETCODE_FAIL_VOLUME_VISIBLE The operation cannot complete because there is already an access volume mapped at the host group or host.
106	0x6A	RETCODE_NO_DELETE_UTM_IN_USE The operation cannot complete because you are attempting to delete the access volume-to-LUN mapping that you are currently using to communicate with this Storage Array.
107	0x6B	RETCODE_INVALID_LUN The operation cannot complete because the logical unit number (LUN) is not valid. Please specify a number between 0 and 31.

Table 91. SYMbol return codes (continued)

Return Code		Definition
108	0x6C	RETCODE_UTM_TOO_MANY_MAPS The operation cannot complete because the logical unit number you are attempting to map to this access volume is outside the allowable range. Please select one of the logical unit numbers (LUN) that have already been mapped to one of the other access volumes.
109	0x6D	RETCODE_DIAG_READ_FAILURE Diagnostics Read test failed. The controller has been placed offline. Use the Recovery Guru to replace the faulty controller. For information on read test failures, refer to online Help.
110	0x6E	RETCODE_DIAG_SRC_LINK_DOWN The Diagnostics passed, but I/Os were performed internally because the test was unable to communicate on the host/source links. For information on host/source link communication errors, refer to online Help.
111	0x6F	RETCODE_DIAG_WRITE_FAILURE Diagnostics Write test failed. The controller has been placed offline. Use the Recovery Guru to replace the faulty controller. For information on write test failures, refer to online Help.
112	0x70	RETCODE_DIAG_LOOPBACK_ERROR The Diagnostics passed, but the loopback test identified an error on one or more of the loops. For information on loop errors, refer to online Help.
113	0x71	RETCODE_DIAG_TIMEOUT The diagnostics operation failed because the controller did not respond within the allotted time. The controller has been placed offline. Use the Recovery Guru to recover from the offline controller.
114	0x72	RETCODE_DIAG_IN_PROGRESS The diagnostics request failed because an internal controller or user initiated diagnostics is already in progress.
115	0x73	RETCODE_DIAG_NO_ALT The diagnostics request failed because the operation requires two Active/Optimal controllers.
116	0x74	RETCODE_DIAG_ICON_SEND_ERR The diagnostics failed because of an ICON communication error between controllers.
117	0x75	RETCODE_DIAG_INIT_ERR The diagnostics request failed because of an internal initialization error.
118	0x76	RETCODE_DIAG_MODE_ERR Controllers must be in active/active mode to run diagnostics.
119	0x77	RETCODE_DIAG_INVALID_TEST_ID The diagnostics request failed because the controller does not support one or more selected diagnostic tests.
120	0x78	RETCODE_DIAG_DRIVE_ERR The diagnostics request failed because the controller was unable to obtain the location (drive number) of the diagnostics data repository.
121	0x79	RETCODE_DIAG_LOCK_ERR The diagnostics request failed because the controller was unable to obtain a mode select lock.
122	0x7A	RETCODE_DIAG_CONFIG_ERR The diagnostics request failed because a diagnostic volume cannot be created.
123	0x7B	RETCODE_DIAG_NO_CACHE_MEM The diagnostics request failed because there was not enough memory available to run the operation.
124	0x7C	RETCODE_DIAG_NOT_QUIESCED The diagnostics request failed because the operation cannot disable data transfer.
125	0x7D	RETCODE_DIAG_UTM_NOT_ENABLED The diagnostics request failed because an Access Volume is not defined.
126	0x7E	RETCODE_INVALID_MODE_SWITCH The controller mode switch to passive failed because the controller has Auto-Volume Transfer mode enabled. For more information about AVT, see ″Learn about Auto-Volume Transfer and Multi-Path Drivers″ in the Learn More section of the online help.
127	0x7F	RETCODE_INVALID_PORTNAME The operation cannot complete because the I/O interface specified in the request is not valid (unknown port name).

Table 91. SYMbol return codes (continued)

Return Code		Definition
128	0x80	RETCODE_DUPLICATE_VOL_MAPPING The operation cannot complete because the volume-to-LUN mapping has already been assigned to this storage partition (host group or host). A storage partition cannot have duplicate volume-to-LUN mappings.
129	0x81	RETCODE_MAX_SNAPS_PER_BASE_EXCEEDED The operation cannot complete because the maximum number of snapshot volumes have been created for this base volume.
130	0x82	RETCODE_MAX_SNAPS_EXCEEDED The operation cannot complete because the maximum number of snapshot volumes have been created for this Storage Array.
131	0x83	RETCODE_INVALID_BASEVOL The operation cannot complete because you cannot create a snapshot volume from either a repository volume or another snapshot volume.
132	0x84	RETCODE_SNAP_NOT_AVAILABLE The operation cannot complete because the snapshot volume's associated base volume or repository volume is missing.
133	0x85	RETCODE_NOT_DISABLED The re-create operation cannot complete because the snapshot volume must be in the disabled state.
134	0x86	RETCODE_SNAPSHOT_FEATURE_DISABLED The operation cannot complete because the Snapshot Volume Premium Feature is disabled or unauthorized.
135	0x87	RETCODE_REPOSITORY_OFFLINE The operation cannot complete because the snapshot volume's associated repository volume is in an offline state.
136	0x88	RETCODE_REPOSITORY_RECONFIGURING The delete operation cannot complete because the snapshot volume's associated repository volume is currently performing a modification operation. Please wait until the modification completes and then retry the operation. Use the Volume>>Properties option in the Array Management Window to check the progress.
137	0x89	RETCODE_ROLLBACK_IN_PROGRESS The delete operation cannot complete because there is a rollback operation in progress.
138	0x8A	RETCODE_NUM_VOLUMES_GROUP The operation cannot complete because the maximum number of volumes has been created on this volume group.
139	0x8B	RETCODE_GHOST_VOLUME The operation cannot complete because the volume on which you are attempting to perform the operation is missing. The only action that can be performed on a missing volume is deletion.
140	0x8C	RETCODE_REPOSITORY_MISSING The delete operation cannot complete because the snapshot volume's associated repository volume is missing.
141	0x8D	RETCODE_INVALID_REPOSITORY_LABEL The operation cannot complete because the name you provided for the snapshot repository volume already exists. Please provide another name and then retry the operation.
142	0x8E	RETCODE_INVALID_SNAP_LABEL The operation cannot complete because the name you provided for the snapshot volume already exists. Please provide another name and then retry the operation.
143	0x8F	RETCODE_INVALID_ROLLBACK_PRIORITY The operation cannot complete because the rollback priority you specified is not between 0 and 4. Please specify a value in this range and then retry the operation.
144	0x90	RETCODE_INVALID_WARN_THRESHOLD The operation cannot complete because the warning threshold you specified is not between 0 and 100. Please specify a value in this range and then retry the operation.
145	0x91	RETCODE_CANNOT_MAP_VOLUME The operation cannot complete because the volume you specified is a snapshot repository volume. You cannot map a logical unit number (LUN) or host to a snapshot repository volume.
146	0x92	RETCODE_CANNOT_FORMAT_VOLUME The initialization operation cannot complete because the volume you specified is either a snapshot volume, a snapshot repository volume, or a standard volume that has associated snapshot volumes. You cannot initialize these types of volumes.

Table 91. SYMbol return codes (continued)

Return Code		Definition
147	0x93	RETCODE_DST_NOT_FIBRE The operation cannot complete because the drive-side interface is SCSI not fibre channel.
148	0x94	RETCODE_REPOSITORY_TOO_SMALL The operation cannot complete because the capacity you specified for the snapshot repository volume is less than the minimum size (8MB) required.
149	0x95	RETCODE_RESPOSITORY_FAILED The operation cannot complete because the snapshot repository volume is failed. Please use the Recovery Guru in the Array Management Window to resolve the problem.
150	0x96	RETCODE_BASE_VOLUME_FAILED The operation cannot complete because the base volume associated with this snapshot failed. Please use the Recovery Guru in the Array Management Window to resolve the problem.
151	0x97	RETCODE_BASE_VOLUME_OFFLINE The operation cannot complete because the base volume associated with this snapshot is offline. Please use the Recovery Guru in the Array Management Window to resolve the problem.
152	0x98	RETCODE_BASE_VOLUME_FORMATTING The create snapshot operation cannot complete because a base volume initialization is in progress. Please wait until the initialization completes and then retry the operation. Use the Volume>>Properties option in the Array Management Window to check the progress.

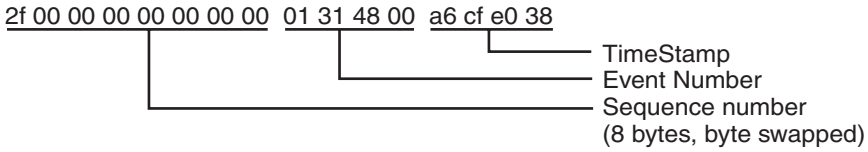
Event decoding examples

Example 1: AEN event

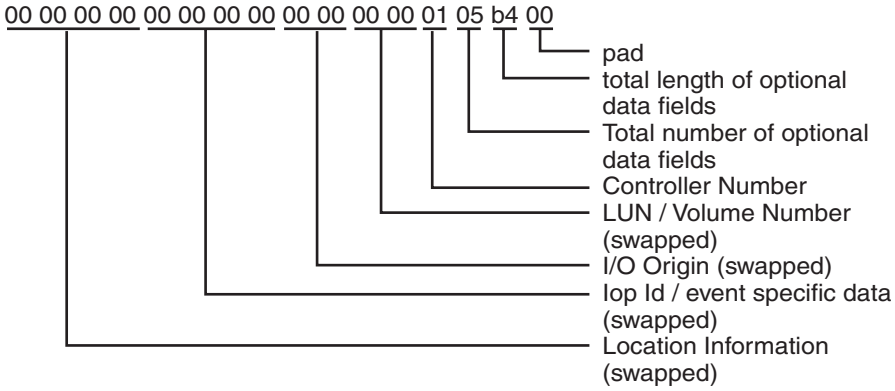
The following is an event as saved from the event viewer.

```
Sequence number: 47
Event type: 3101
Category: Internal
Priority: Informational
Description: AEN posted for recently logged event
Event specific codes: 6/95/2
Component type: Controller
Component location: Controller in slot B
Raw data:
2f 00 00 00 00 00 00 00 01 31 48 00 a6 cf e0 38
00 00 00 00 00 00 00 00 00 00 00 00 01 05 b4 00
20 00 00 01 70 00 06 00 00 00 00 98 00 00 00 00
95 02 00 00 00 00 00 00 01 00 00 00 00 00 00 00
00 00 00 00 20 00 00 81 00 00 00 00 00 08 18 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 7a 7a
7a 20 20 20 20 20 20 20 20 00 00 81 20 20 20 20
20 20 44 99 10 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 81
00 00 00 00 00 05 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
20 00 00 81 00 00 00 00 00 00 00 00 00 00 00 00
30 33 32 38 30 30 2f 31 30 32 38 35 31 00 00 00
00 00 00 00
```

The raw data contains both constant length and optional event data for each event. It can be interpreted as follows:

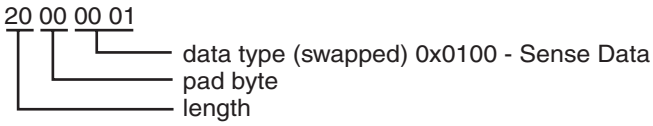


Constant Length Event Data is present for every event log entry. Its length is 32 (0x20) bytes.



This example has five optional data fields with a total length of 180 (0xb4) bytes. Each optional data field has a header and data. Headers consists of the length and the data type of the optional data field. Each optional data record contains a maximum of 32 data bytes. The data type is defined in the MEL spec. To find the next data field, add the optional data field length plus the length of the header (4) to the current position in the buffer. You have reached the end when the number of optional data fields decoded equals the total number of optional fields.

First optional data field



Data:

```
                          70 00 06 00 00 00 00 98 00 00 00 00
95 02 00 00 00 00 00 00 01 00 00 00 00 00 00 00
00 00 00 00
```

To get to the second data field add 34 (length of 32 + 4 header) to your position.

Second optional data field

```
          20 00 00 81
```

Length is 0x20 - Data type is (continued) sense data

```
                                          00 00 00 00 00 08 18 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 7a 7a
7a 20 20 20 20 20 20 20
```

The remainder of the optional data fields can be found by the same method.

Third optional data field

```
           20 00 00 81
```

Length is 0x20 - Data type is (continued) sense data

```
                                                      20 20 20 20
20 20 44 99 10 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00
```

Fourth optional data field

```
           20 00 00 81
```

Length is 0x20 - Data type is (continued) sense data

```
00 00 00 00 00 05 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Fifth optional data field

```
           20 00 00 81
```

Length is 0x20 - Data type is (continued) sense data

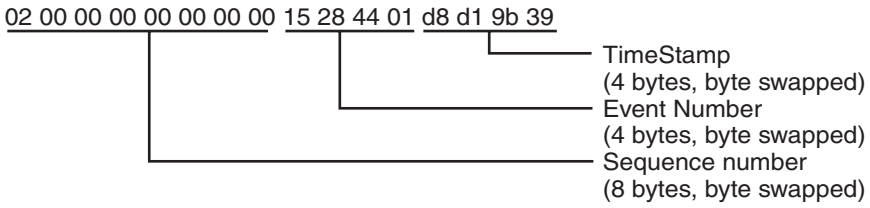
```
                    00 00 00 00 00 00 00 00 00 00 00 00
30 33 32 38 30 30 2f 31 30 32 38 35 31 00 00 00
00 00 00 00
```

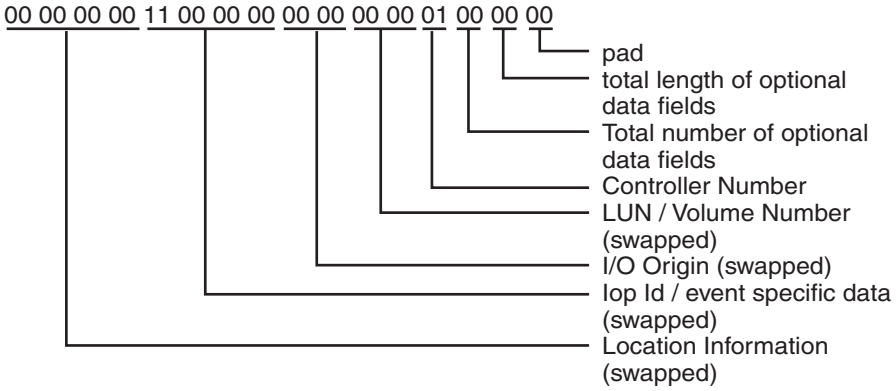
Example 2: Mini hub event

The following is an event as saved from the event viewer.

```
Date/Time: 8/17/00 6:51 AM
Sequence number: 2
Event type: 2815
Category: Internal
Priority: Critical
Description: GBIC failed
Event specific codes: 0/0/0
Component type: mini hub
Component location: None
Raw data:
02 00 00 00 00 00 00 00 15 28 44 01 d8 d1 9b 39
00 00 00 00 11 00 00 00 00 00 00 00 01 00 00 00
```

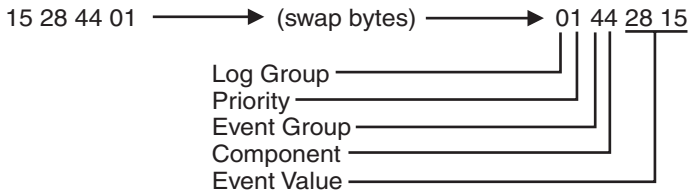
The raw data is composed of only Constant Length Event Data for this event. From the raw data, the mini hub that is reporting the error can be determined. The raw data can be interpreted as follows:





Step 1: Decode Event Number field

The first step in decoding any event with this manual is to decipher the Event Number. This requires swapping the order of the bytes in the **Event Number** field of the raw data as follows:

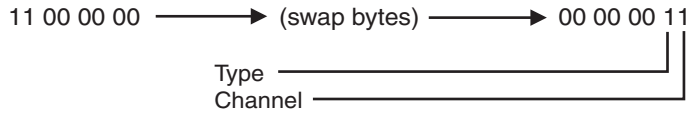


Under the Event Number title in the table given in “Event descriptions” on page 358, find the value that matches the Event Value in the raw data. The corresponding text entry preceding this Event Number in the table states: GBIC Failed, which is also the description given next to the Description title in the formatted region of the MEL entry. The text descriptions corresponding to the Log Group, Priority, Event Group, and Component can also be found on the same line in this table.

Step 2: Decode Optional Data For Event

The information under the Optional Data title for this Event Number states that the **ID** field of the raw data contains Type/Channel information for this type of event. This data is found in the Iop ID/event-specific data field of the raw data. The first

step is to swap bytes in this field.



The information in the same table shows that Type 1 refers to a host-side mini hub. Because a 4774-based controller module can have up to two host-side mini hubs per controller, it is possible that you will use the value in the **Channel** field to determine which mini hub is reporting the error. The mini hubs for controller A (top controller) are in the first and third slots from the left when looking at the back of the controller module. The mini hubs for controller B (bottom controller) are in the second and fourth slots from the left when looking at the back of the controller module. For each controller, the mini hubs on the host side are assigned the values of 0 and 1, with the leftmost mini hub for each controller being assigned the value of 0. Because the value in the **Channel** field is 1 in this example, the second mini hub from the left for the controller that is reporting the error has a failed GBIC.

Finally, the controller that is reporting the error can be found by decoding the **Controller Number** field in the raw data. A value of 0 in the **Controller Number** field corresponds to Controller A, while a value of 1 in this field corresponds to Controller B. In this example, Controller 1 reports the error, which corresponds to Controller B.

Step 3: Summary of the Problem

For this MEL entry, controller B is reporting a GBIC failure in one of its mini hubs. When looking at the back of the controller module, the failed GBIC is in the second host-side mini hub from the left for this controller. Because the mini hubs for controller B are in slots 2 and 4, the second host-side mini hub for controller B is in slot 4. Thus, the mini hub that contains the failed GBIC is the one in slot 4. It is not currently possible to tell which GBIC in the mini hub is bad, although the fault LEDs in the mini hub can be used to determine this.

Example 3: Mini hub event

Event as saved from the event viewer:

```
Date/Time: 8/17/00 7:02 AM
Sequence number: 10
Event type: 2815
Category: Internal
Priority: Critical
Description: GBIC failed
Event specific codes: 0/0/0
Component type: mini hub
Component location: None
Raw data:
0a 00 00 00 00 00 00 00 15 28 44 01 52 d4 9b 39
00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00
```

This example is very similar to the previous example; the significant differences are in the **Optional Data** field and the **Controller Number** field. The value in the **Controller Number** field is 0, which corresponds to controller A. The value in the **Optional Data** field after byte swapping is: 00 00 00 23. Referring to step 2 in the

previous example, this corresponds to a value of 2 in the Type field, and a value of 3 in the **Channel** field. We see that a value of 2 in the **Type** field denotes a drive-side mini hub. The drive-side mini hubs are assigned the values of 0 thru 3 from right to left when looking at the back of the controller module. These values are the same independent of the controller that is reporting the error. The value in the **Channel** field contains a value that corresponds to one of these mini hub values. In this example, the value in the **Channel** field is 3, which corresponds to the fourth drive-side mini hub from the right when viewing the controller module from the rear.

In summary, controller A is reporting a GBIC failure in the leftmost drive-side mini hub. The exact GBIC that is bad cannot be determined from the MEL entry, but the LEDs in the mini hub can be used to determine which GBIC has failed.

Notices

This publication was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this publication to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product, and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM
e (logo) server
IntelliStation
TotalStorage
xSeries

Intel and Pentium III are trademarks of Intel Corporation in the United States, other countries, or both.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be the trademarks or service marks of others.

Important notes

Processor speeds indicate the internal clock speed of the microprocessor; other factors also affect application performance.

CD-ROM drive speeds list the variable read rate. Actual speeds vary and are often less than the maximum possible.

When referring to processor storage, real and virtual storage, or channel volume, KB stands for approximately 1000 bytes, MB stands for approximately 1000000 bytes, and GB stands for approximately 1000000000 bytes.

When referring to hard disk drive capacity or communications volume, MB stands for 1 000 000 bytes, and GB stands for 1 000 000 000 bytes. Total user-accessible capacity may vary depending on operating environments.

Maximum internal hard disk drive capacities assume the replacement of any standard hard disk drives and population of all hard disk drive bays with the largest currently supported drives available from IBM.

Maximum memory may require replacement of the standard memory with an optional memory module.

IBM makes no representation or warranties regarding non-IBM products and services that are ServerProven®, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. These products are offered and warranted solely by third parties.

Unless otherwise stated, IBM makes no representations or warranties with respect to non-IBM products. Support (if any) for the non-IBM products is provided by the third party, not IBM.

Some software may differ from its retail version (if available), and may not include user manuals or all program functionality.

Electronic emission notices

Federal Communications Commission (FCC) statement

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio

communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits.IBM is not responsible for any radio or television interference causedby using other than recommended cables and connectors or by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Industry Canada Class A emission compliance statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Australia and New Zealand Class A statement

Attention: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

United Kingdom telecommunications safety requirement

Notice to Customers

This apparatus is approved under approval number NS/G/1234/J/100003 for indirect connection to public telecommunication systems in the United Kingdom.

European Union EMC Directive conformance statement

This product is in conformity with the protection requirements of EU Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a nonrecommended modification of the product, including the fitting of non-IBM option cards.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to CISPR 22/European Standard EN 55022. The Limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

Attention: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Taiwan electrical emission statement

警告使用者:
這是甲類的資訊產品，在
居住的環境中使用時，可
能會造成射頻干擾，在這
種情況下，使用者會被要
求採取某些適當的對策。

Japanese Voluntary Control Council for Interference (VCCI) statement

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

IBM license agreement for machine code

Regardless of how you acquire (electronically, preloaded, on media, or otherwise) BIOS, Utilities, Diagnostics, Device Drivers, firmware, or Microcode (collectively called Machine Code), you accept the terms of this Agreement by your initial use of a Machine or Machine Code. The term Machine means an IBM Machine, its features, conversions, upgrades, elements or accessories, or any combination of them. Acceptance of these license terms authorizes you to use Machine Code with the specific product for which it is provided.

International Business Machines Corporation or one of its subsidiaries (IBM), or an IBM supplier, owns copyrights in Machine Code.

IBM grants you a nonexclusive license to use Machine Code only in conjunction with a Machine. As the rightful possessor of a Machine, you may make a reasonable number of copies of Machine Code as necessary for backup, configuration, and restoration of the Machine. You must reproduce the copyright notice and any other legend of ownership on each copy of Machine Code you make.

You may transfer possession of Machine Code and its media to another party only with the transfer of the Machine on which the Machine Code is used. If you do so, you must give the other party a copy of these terms and provide all user documentation to that party. When you do so, you must destroy all your copies of Machine Code.

Your license for Machine Code terminates when you no longer rightfully possess the Machine.

No other rights under this license are granted.

You may not, for example, do any of the following:

1. Otherwise copy, display, transfer, adapt, modify, or distribute in any form, Machine Code, except as IBM may authorize in a Machine's user documentation;
2. Reverse assemble, reverse compile, or otherwise translate the Machine Code, unless expressly permitted by applicable law without the possibility of contractual waiver;
3. Sublicense or assign the license for the Machine Code; or
4. Lease the Machine Code or any copy of it.

The terms of IBM's Machine warranty, which is incorporated into this Agreement by reference, apply to Machine Code. Please refer to that warranty for any questions or claims regarding performance or liability for Machine Code.

Power cords

For your safety, IBM provides a power cord with a grounded attachment plug to use with this IBM product. To avoid electrical shock, always use the power cord and plug with a properly grounded outlet.

IBM power cords used in the United States and Canada are listed by Underwriter's Laboratories (UL) and certified by the Canadian Standards Association (CSA).

For units intended to be operated at 115 volts: Use a UL-listed and CSA-certified cord set consisting of a minimum 18 AWG, Type SVT or SJT, three-conductor cord, a maximum of 15 feet in length and a parallel blade, grounding-type attachment plug rated 15 amperes, 125 volts.

For units intended to be operated at 230 volts (U.S. use): Use a UL-listed and CSA-certified cord set consisting of a minimum 18 AWG, Type SVT or SJT, three-conductor cord, a maximum of 15 feet in length and a tandem blade, grounding-type attachment plug rated 15 amperes, 250 volts.

For units intended to be operated at 230 volts (outside the U.S.): Use a cord set with a grounding-type attachment plug. The cord set should have the appropriate safety approvals for the country in which the equipment will be installed.

IBM power cords for a specific country or region are usually available only in that country or region.

IBM power cord part number	Used in these countries and regions
13F9940	Argentina, Australia, China (PRC), New Zealand, Papua New Guinea, Paraguay, Uruguay, Western Samoa
13F9979	Afghanistan, Algeria, Andorra, Angola, Austria, Belgium, Benin, Bulgaria, Burkina Faso, Burundi, Cameroon, Central African Rep., Chad, Czech Republic, Egypt, Finland, France, French Guiana, Germany, Greece, Guinea, Hungary, Iceland, Indonesia, Iran, Ivory Coast, Jordan, Lebanon, Luxembourg, Macao S.A.R. of the PRC, Malagasy, Mali, Martinique, Mauritania, Mauritius, Monaco, Morocco, Mozambique, Netherlands, New Caledonia, Niger, Norway, Poland, Portugal, Romania, Senegal, Slovakia, Spain, Sudan, Sweden, Syria, Togo, Tunisia, Turkey, former USSR, Vietnam, former Yugoslavia, Zaire, Zimbabwe
13F9997	Denmark

IBM power cord part number	Used in these countries and regions
14F0015	Bangladesh, Burma, Pakistan, South Africa, Sri Lanka
14F0033	Antigua, Bahrain, Brunei, Channel Islands, Cyprus, Dubai, Fiji, Ghana, Hong Kong S.A.R. of the PRC, India, Iraq, Ireland, Kenya, Kuwait, Malawi, Malaysia, Malta, Nepal, Nigeria, Polynesia, Qatar, Sierra Leone, Singapore, Tanzania, Uganda, United Kingdom, Yemen, Zambia
14F0051	Liechtenstein, Switzerland
14F0069	Chile, Ethiopia, Italy, Libya, Somalia
14F0087	Israel
1838574	Thailand
6952301	Bahamas, Barbados, Bermuda, Bolivia, Brazil, Canada, Cayman Islands, Colombia, Costa Rica, Dominican Republic, Ecuador, El Salvador, Guatemala, Guyana, Haiti, Honduras, Jamaica, Japan, Korea (South), Liberia, Mexico, Netherlands Antilles, Nicaragua, Panama, Peru, Philippines, Saudi Arabia, Suriname, Taiwan, Trinidad (West Indies), United States of America, Venezuela

Glossary

This glossary provides definitions for the terminology used for the IBM TotalStorage FAStT hardware. This glossary also provides definitions for the terminology used for the IBM TotalStorage FAStT Storage Manager.

This glossary defines technical terms and abbreviations used in this document. If you do not find the term you are looking for, see the *IBM Glossary of Computing Terms* located at: www.ibm.com/networking/nsg/nsgmain.htm

This glossary also includes terms and definitions from:

- *Information Technology Vocabulary* by Subcommittee 1, Joint Technical Committee 1, of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC JTC1/SC1). Definitions are identified by the symbol (I) after the definition; definitions taken from draft international standards, committee drafts, and working papers by ISO/IEC JTC1/SC1 are identified by the symbol (T) after the definition, indicating that final agreement has not yet been reached among the participating National Bodies of SC1.
- *IBM Glossary of Computing Terms*. New York: McGraw-Hill, 1994.

The following cross-reference conventions are used in this glossary:

See Refers you to (a) a term that is the expanded form of an abbreviation or acronym, or (b) a synonym or more preferred term.

See also Refers you to a related term.

Abstract Windowing Toolkit (AWT). A Java graphical user interface (GUI).

accelerated graphics port (AGP). A bus specification that gives low-cost 3D graphics cards faster access to main memory on personal computers than the usual PCI bus. AGP reduces the overall cost of creating high-end graphics subsystems by using existing system memory.

access volume. A special logical drive that allows the host-agent to communicate with the controllers in the storage subsystem.

adapter. A printed circuit assembly that transmits user data (I/Os) between the internal bus of the host system and the external fibre channel link and vice versa. Also called an I/O adapter, host adapter, or FC adapter.

advanced technology (AT) bus architecture. A bus standard for IBM compatibles. It extends the XT bus architecture to 16 bits and also allows for bus mastering, although only the first 16 MB of main memory are available for direct access.

agent. A server program that receives virtual connections from the network manager (the client program) in an SNMP-TCP/IP network-managing environment.

AGP. See *accelerated graphics port*.

AL_PA. See *arbitrated loop physical address*.

arbitrated loop. A shared 100 MBps fibre channel transport structured as a loop and supporting up to 126 devices and one fabric attachment. A port must successfully arbitrate before a circuit can be established.

arbitrated loop physical address (AL_PA). One of three existing fibre channel topologies, in which two to 126 ports are interconnected serially in a single loop circuit. Access to the FC-AL is controlled by an arbitration scheme. The FC-AL topology supports all classes of service and guarantees in-order delivery of FC frames when the originator and responder are on the same FC-AL. The default topology for the disk array is arbitrated loop. An arbitrated loop is sometimes referred to as Stealth Mode.

auto volume transfer/auto disk transfer (AVT/ADT). A function that provides automatic failover in case of controller failure on a storage subsystem.

AVT/ADT. See *auto volume transfer/auto disk transfer*.

AWT. See *Abstract Windowing Toolkit*.

basic input/output system (BIOS). Code that controls basic hardware operations, such as interactions with diskette drives, hard disk drives, and the keyboard.

BIOS. See *basic input/output system*.

BOOTP. See *bootstrap protocol*.

bootstrap protocol (BOOTP). A Transmission Control Protocol/Internet Protocol (TCP/IP) protocol that a diskless workstation or network computer use to obtain its IP address and other network information such as server address and default gateway.

bridge. A SAN device that provides physical and transport conversion, such as fibre channel to SCSI bridge.

bridge group. A bridge and the collection of devices connected to it. Bridge Groups are discovered by the SANavigator tool and displayed with a gray background on the Physical and Data Path Maps.

broadcast. A method of sending an SNMP request for information to all the devices on a subnet that use a single special request. Because of its efficiency, the SANavigator tool sets its default method of discovery to broadcast. However, a network administrator might disable this method on the network router.

cathode ray tube (CRT). An electrical device for displaying images by exciting phosphor dots with a scanned electron beam. CRTs are found in computer VDUs and monitors, televisions, and oscilloscopes.

CDPD. See *cellular digital packet data*.

cellular digital packet data (CDPD). A wireless standard that provides two-way, 19.2 kps packet data transmission over existing cellular telephone channels.

CGA. See *color graphics adapter*.

client. A computer system or process that requests a service of another computer system or process that is typically referred to as a server. Multiple clients can share access to a common server.

color graphics adapter (CGA). An early, now obsolete, IBM video display standard for use on IBM PCs. CGA displays 80 x 25 or 40 x 25 text in 16 colors, 640 x 200 pixel graphics in two colors or 320 x 200 pixel graphics in four colors.

command. Any selection on a dialog box or elsewhere in the user interface that causes the SANavigator tool to perform a task.

community strings. The name of a community contained in each SNMP message. SNMP has no standard mechanisms for verifying that a message was sent by a member of the community, keeping the contents of a message private, or for determining if a message has been changed or replayed.

CRC. See *cyclic redundancy check*.

CRT. See *cathode ray tube*.

cyclic redundancy check (CRC). (1) 1) A redundancy check in which the check key is generated by a cyclic algorithm. (2) 2) An error detection technique performed at both the sending and receiving stations.

dac. See *disk array controller*.

dar. See *disk array router*.

DASD. See *Direct-Access Storage Device*.

device type. Identifier used to place devices in the physical map, such as the switch, hub, storage.

direct access storage device (DASD). IBM mainframe terminology for a data storage device by which information can be accessed directly, instead of by-passing sequentially through all storage areas. For example, a disk drive is a DASD, in contrast with a tape drive, which stores data as a linear sequence.

direct memory access (DMA). The transfer of data between memory and an input/output (I/O) device without processor intervention.

disk array controller (dac). A disk array controller device that represents the two controllers of an array. See also *disk array controller*.

disk array router (dar). A disk array router that represents an entire array, including current and deferred paths to all logical unit numbers (LUNs) (hdisks on AIX). See also *disk array controller*.

DMA. See *direct memory access*.

domain. The most significant byte in the N_Port Identifier for the FC device. It is not used in the FC-SCSI hardware path ID. It is required to be the same for all SCSI targets logically connected to an FC adapter.

DRAM. See *dynamic random access memory*.

dynamic random access memory (DRAM). A storage in which the cells require repetitive application of control signals to retain stored data.

E_Port. An expansion port that connects the switches for two fabrics (also used for McData ES-1000 B ports).

ECC. See *error correction coding*.

EEPROM. See *Electrically Erasable Programmable Read-Only Memory*.

EGA. See *enhanced graphics adapter*.

electrically eErasable programmable read-only memory (EEPROM). A type of non-volatile storage device that can be erased with an electrical signal. Writing to EEPROM takes much longer than reading. It also can only be reprogrammed a limited number of times before it wears out. Therefore, it is appropriate for storing small amounts of data that are changed infrequently.

electrostatic discharge (ESD). The flow of current that results when objects that have a static charge come into close enough proximity to discharge.

enhanced graphics adapter (EGA). An IBM video display standard that provides text and graphics with a

resolution of 640 x 350 pixels of 16 colors. It emulates the Color/Graphics Adapter (CGA) and the Monochrome Display Adapter (MDA) and was superseded by the Video Graphics Display (VGA).

enhanced small disk interface (ESDI). A hard disk controller standard that allows disks to communicate with computers at high speeds. ESDI drives typically transfer data at about 10 megabits per second, although they are capable of doubling that speed.

error correction coding (ECC). A method for encoding data so that transmission errors can be detected and corrected by examination of the data on the receiving end. Most ECCs are characterized by the maximum number of errors they can detect and correct.

error detection coding. A method for encoding data so that errors that occur during storage or transmission can be detected. Most error detection codes are characterized by the maximum number of errors they can detect. The simplest form of error detection is by using a single added parity bit or a cyclic redundancy check. Adding multiple parity bits can detect not only that an error has occurred, but also which bits have been inverted, thereby indicating which bits should be re-inverted to restore the original data.

ESD. See *electrostatic discharge*.

ESDI. See *enhanced small disk interface*.

eXtended graphics array (XGA). An IBM advanced standard for graphics controller and display mode design introduced in 1990. XGA, used mostly on workstation-level systems, supports a resolution of 1024 x 768 pixels with a palette of 256 colors, or 640 x 480 with high color (16 bits per pixel). XGA-2 added 1024 x 768 support for high color and higher refresh rates, improved performance, and supports 1360 x 1024 in 16 colors.

F_Port. A port that supports an N_Port on a fibre channel switch.

fabric group. A collection of interconnected SAN devices discovered by the SANavigator tool and displayed with a blue background on the Physical and Data Path Maps.

Fibre Channel. A bi-directional, full-duplex, point-to-point, serial data channel structured for high performance capability. Physically, fibre channel interconnects devices, such as host systems and servers, FC hubs and disk arrays, through ports, called N_Ports, in one of three topologies: a point-to-point link, an arbitrated loop, or a cross point switched network, which is called a fabric. FC can interconnect two devices in a point-to-point topology, from two to 126 devices in an arbitrated loop. FC is a generalized transport mechanism that can transport any existing protocol, such as SCSI, in FC frames.

Fibre Channel Protocol for SCSI (FCP). A high-level fibre channel mapping layer (FC-4) that uses lower-level Fibre Channel (FC-PH) services to transmit SCSI command, data, and status information between a SCSI initiator and a SCSI target across the FC link by using FC frame and sequence formats.

field replaceable unit (FRU). An assembly that is replaced in its entirety when any one of its components fails. In some cases, a FRU might contain other field replaceable units.

FRU. See *field replaceable unit*.

general purpose interface bus (GPIB). An 8-bit parallel bus developed for the exchange of information between computers and industrial automation equipment.

GPIB. See *general purpose interface bus.*.

graphical user interface (GUI). A type of computer interface that presents a visual metaphor of a real-world scene, often of a desktop, by combining high-resolution graphics, pointing devices, menu bars and other menus, overlapping windows, icons, and the object-action relationship.

GUI. See *graphical user interface.*

HBA. See *host bus adapter.*

hdisk. An AIX term representing a logical unit number (LUN) on an array.

host. A system that is directly attached to the storage subsystem through a fibre-channel I/O path. This system is used to serve data (typically in the form of files) from the storage subsystem. A system can be both a storage management station and a host simultaneously.

host bus adapter (HBA). An interface between the fibre channel network and a workstation or server.

host computer. See *host*.

host group. The collection of HBAs and NASs in a fabric discovered by the SANavigator tool and displayed with a yellow background on the Physical and Data Path Maps.

hub. In a network, a point at which circuits are either connected or switched. For example, in a star network, the hub is the central node; in a star/ring network, it is the location of wiring concentrators.

IC. See *integrated circuit.*

IDE. See *integrated drive electronics.*

In-band. Transmission of management protocol over the fibre channel transport.

Industry Standard Architecture (ISA). A bus standard for IBM compatibles that allows components to be added as cards plugged into standard expansion slots. ISA was originally introduced in the IBM PC/XT with an 8-bit data path. It was later expanded to permit a 16-bit data path when IBM introduced the PC/AT.

initial program load (IPL). The part of the boot sequence during which a computer system copies the operating system kernel into main memory and runs it.

integrated circuit (IC). Also known as a *chip*. A microelectronic semiconductor device that consists of many interconnected transistors and other components. ICs are constructed on a small rectangle cut from a silicon crystal or other semiconductor material. The small size of these circuits allows high speed, low power dissipation, and reduced manufacturing cost compared with board-level integration.

integrated drive electronics (IDE). Also known as an Advanced Technology Attachment Interface (ATA). A disk drive interface based on the 16-bit IBM PC ISA in which the controller electronics reside on the drive itself, eliminating the need for a separate adapter card.

integrated services digital network (ISDN). A digital end-to-end telecommunication network that supports multiple services including, but not limited to, voice and data. ISDNs are used in public and private network architectures.

interrupt request (IRQ). A type of input found on many processors that causes the processor to suspend normal instruction execution temporarily and start executing an interrupt handler routine. Some processors have several interrupt request inputs that allow different priority interrupts.

Internet Protocol address. The unique 32-bit address that specifies the location of each device or workstation on the Internet. For example, 9.67.97.103 is an IP address.

IP address. See *Internet Protocol address*.

IPL. See *initial program Load.*

IRQ. See *interrupt request.*

ISA. See *Industry Standard Architecture.*

ISDN. See *Integrated Services Digital Network.*

isolated group. A collection of isolated devices not connected to the SAN but discovered by the SANavigator tool. The Isolated Group displays with a gray background near the bottom of the Physical and Data Path Maps.

Java Runtime Environment (JRE). A subset of the Java Development Kit (JDK) for end users and developers who want to redistribute the Java Runtime Environment (JRE). The JRE consists of the Java virtual machine, the Java Core Classes, and supporting files.

JRE. See *Java Runtime Environment*.

label. A discovered or user entered property value that is displayed underneath each device in the Physical and Data Path Maps.

LAN. See *local area network*.

LBA. See *logical block addressing*.

local area network (LAN). A computer network located on a user's premises within a limited geographic area.

logical block addressing (LBA). A hard disk sector addressing scheme in which the addressing conversion is performed by the hard disk firmware. LBA is used on all SCSI hard disks and on ATA-2 conforming IDE hard disks.

logical unit number (LUN). An identifier used on a small computer systems interface (SCSI) bus to distinguish among up to eight devices (logical units) with the same SCSI ID.

loop address. The unique ID of a node in fibre channel loop topology sometimes referred to as a Loop ID.

loop group. A collection of SAN devices that are interconnected serially in a single loop circuit. Loop Groups are discovered by the SANavigator tool and displayed with a gray background on the Physical and Data Path Maps.

loop port (FL_Port). An N-Port or F-Port that supports arbitrated loop functions associated with an arbitrated loop topology.

LUN. See *logical unit number*.

man pages. In UNIX-based operating systems, online documentation for operating-system commands, subroutines, system calls, file formats, special files, stand-alone utilities, and miscellaneous facilities. Invoked by the **man** command.

management information base (MIB). The information that is on an agent. It is an abstraction of configuration and status information.

MCA. See *micro channel architecture*.

MIB. See *management information base*.

micro channel architecture (MCA). IBM's proprietary bus that is used in high-end PS/2 personal computers. Micro Channel is designed for multiprocessing and functions as either a 16-bit or 32-bit bus. It eliminates potential conflicts that arise when installing new peripheral devices.

MIDI. See *musical instrument digital interface*.

model. The model identification assigned to a device by its manufacturer.

musical instrument digital interface (MIDI). A protocol that allows a synthesizer to send signals to another synthesizer or to a computer, or a computer to a musical instrument, or a computer to another computer.

NDIS. See *network device interface specification*.

network device interface specification (NDIS). An application programming interface (API) definition that allows DOS or OS/2 systems to support one or more network adapters and protocol stacks. NDIS is a 16-bit, Ring O (for the OS/2 operating system) API that defines a specific way for writing drivers for layers 1 and 2 of the OSI model. NDIS also handles the configuration and binding of these network drivers to multiple protocol stacks.

network management station (NMS). In the Simple Network Management Protocol (SNMP), a station that executes management application programs that monitor and control network elements.

NMI. See *non-maskable interrupt*.

NMS. See *network management station*.

non-maskable interrupt (NMI). A hardware interrupt that another service request cannot overrule (mask). An NMI bypasses and takes priority over interrupt requests generated by software, the keyboard, and other such devices and is issued to the microprocessor only in disastrous circumstances, such as severe memory errors or impending power failures.

N_Port. A node port. A fibre channel defined hardware entity that performs data communications over the fibre channel link. It is identifiable by a unique Worldwide Name. It can act as an originator or a responder.

node. A physical device that allows for the transmission of data within a network.

nonvolatile storage (NVS). A storage device whose contents are not lost when power is cut off.

NVS. See *nonvolatile storage*.

NVSRAM. Nonvolatile storage random access memory. See *nonvolatile storage*.

Object Data Manager (ODM). An AIX proprietary storage mechanism for ASCII stanza files that are edited as part of configuring a drive into the kernel.

ODM. See *Object Data Manager*.

out-of-band. Transmission of management protocols outside of the fibre channel network, typically over Ethernet.

PCI local bus. See *peripheral component interconnect local bus*.

PDF. See *portable document format*.

peripheral component interconnect local bus (PCI local bus). A standard that Intel Corporation introduced for connecting peripherals. The PCI local bus allows up to 10 PCI-compliant expansion cards to be installed in a computer at a time. Technically, PCI is not a bus but a bridge or mezzanine. It runs at 20 - 33 MHz and carries 32 bits at a time over a 124-pin connector or 64 bits over a 188-pin connector. A PCI controller card must be installed in one of the PCI-compliant slots. The PCI local bus is processor independent and includes buffers to decouple the CPU from relatively slow peripherals, allowing them to operate asynchronously. It also allows for multiplexing, a technique that permits more than one electrical signal to be present on the PCI local bus at a time.

performance events. Events related to thresholds set on SAN performance.

polling delay. The time in seconds between successive discovery processes during which Discovery is inactive.

port. The hardware entity that connects a device to a fibre channel topology. A device can contain one or more ports.

portable document format (PDF). A standard specified by Adobe Systems, Incorporated, for the electronic distribution of documents. PDF files are compact; can be distributed globally by e-mail, the Web, intranets, or CD-ROM; and can be viewed with the Acrobat Reader, which is software from Adobe Systems that can be downloaded at no cost from the Adobe Systems home page.

private loop. A freestanding Arbitrated Loop with no fabric attachment.

program temporary fix (PTF). A temporary solution or bypass of a problem diagnosed by IBM in a current unaltered release of the program.

PTF. See *program temporary fix*.

RAM. See *random-access memory*.

random-access memory (RAM). A temporary storage location in which the central processing unit (CPU) stores and executes its processes.

read-only memory (ROM). Memory in which the user cannot changed stored data except under special conditions.

RDAC. See *redundant dual active controller*.

redundant dual active controller (RDAC). A controller, used with AIX and Solaris hosts, that provides a multipath driver for a storage subsystem. An RDAC is also known as redundant disk array controller.

red, green, blue (RGB). (1) Color coding in which the brightness of the additive primary colors of light, red, green, and blue are specified as three distinct values of white light. (2) Pertaining to a color display that accepts signals that represent red, green, and blue.

RGB. See *red, green, blue*.

ROM. See *read-only memory*.

router. A computer that determines the path of network traffic flow. The path selection is made from several paths based on information obtained from specific protocols, algorithms that attempt to identify the shortest or best path, and other criteria such as metrics or protocol-specific destination addresses.

SAN. See *storage area network*.

SCSI. See *small computer system interface*.

segmented loop ports (SL_Ports). SL_Ports allow you to divide a Fibre Channel Private Loop into multiple segments. Each segment can pass frames around as an independent loop and can connect through the fabric to other segments of the same loop.

serial storage architecture (SSA). An interface specification from IBM in which devices are arranged in a ring topology. SSA, which is compatible with SCSI devices, allows full-duplex packet multiplexed serial data transfers at rates of 20Mb/sec in each direction.

server. A functional hardware and software unit that delivers shared resources to workstation client units on a computer network.

server/device events. Events that occur on the server or a designated device that meet criteria that the user sets.

Simple Network Management Protocol (SNMP). In the Internet suite of protocols, a network management protocol that is used to monitor routers and attached networks. SNMP is an application layer protocol. Information on devices managed is defined and stored in the application's Management Information Base (MIB).

SL_Port. See *segmented loop ports*.

small computer system interface (SCSI). A standard hardware interface that enables a variety of peripheral devices to communicate with one another.

SNMP. See *Simple Network Management Protocol*.

SNMPv1. The original standard for SNMP is now referred to as SNMPv1, as opposed to SNMPv2, a revision of SNMP. See also *Simple Network Management Protocol*.

SNMP time-out. The maximum amount of time the SANavigator tool will wait for a device to respond to a request. The specified time applies to one retry only.

SNMP trap events. SNMP is based on a manager/agent model. SNMP includes a limited set of management commands and responses. The management system issues messages that tell an agent to retrieve various object variables. The managed agent sends a Response message to the management system. That message is an event notification, called a trap, that identifies conditions, such as thresholds, that exceed a predetermined value.

SRAM. See *static random access memory*.

SSA. See *serial storage architecture*.

static random access memory (SRAM). Random access memory based on the logic circuit known as flip-flop. It is called *static* because it retains a value as long as power is supplied, unlike dynamic random access memory (DRAM), which must be regularly refreshed. It is however, still volatile, meaning that it can lose its contents when the power is switched off.

storage area network (SAN). A network that links servers or workstations to disk arrays, tape backup subsystems, and other devices, typically over fibre channel.

storage management station. A system that is used to manage the storage subsystem. A storage management station does not need to be attached to the storage subsystem through the fibre-channel I/O path.

subnet. An interconnected but independent segment of a network that is identified by its Internet Protocol (IP) address.

super video graphics array (SVGA). A video display standard that Video Electronics Standards Association (VESA) created to provide high resolution color display on IBM PC compatible personal computers. The resolution is 800 x 600 4-bit pixels. Each pixel can therefore be one of 16 colors.

SVGA. See *super video graphics array*.

sweep method. A method of sending SNMP requests for information to all the devices on a subnet by sending the request to every device on the network. Sweeping an entire network can take a half an hour or more. If broadcast is disabled, the recommended method is to enter the individual IP addresses of the SAN devices into the SANavigator tool. This method produces good results without unnecessarily using time to wait for

responses from every IP address in the subnet, especially for IP addresses where no devices are present. There might, however, be times when a full subnet sweep will produce valuable diagnostic information about the network or a device's configuration.

switch. A fibre channel device that provides full bandwidth per port and high-speed routing of data by using link-level addressing.

switch group. A switch and the collection of devices connected to it that are not in other groups. Switch Groups are discovered by the SANavigator tool and displayed with a gray background on the Physical and Data Path Maps.

system name. Device name assigned by the vendor's third-party software.

TCP. See *Transmission Control Protocol*.

TCP/IP. See *Transmission Control Protocol/Internet Protocol*.

terminate and stay resident program (TSR program). A program that installs part of itself as an extension of DOS when it is executed.

TFT. See *thin-film transistor*.

thin-film transistor (TFT). A transistor created by using thin film methodology.

topology. The physical or logical arrangement of devices on a network. The three fibre channel topologies are fabric, arbitrated loop, and point-to-point. The default topology for the disk array is arbitrated loop.

TL_Ports. See *translated loop port*.

translated loop ports (TL_Ports). Each TL_Port connects to a private loop and allows connectivity between the private loop devices and *off loop* devices (devices not connected to that particular TL_Port).

Transmission Control Protocol (TCP). A communication protocol used in the Internet and in any network that follows the Internet Engineering Task Force (IETF) standards for internetwork protocol. TCP provides a reliable host-to-host protocol between hosts in packed-switched communication networks and in interconnected systems of such networks. It uses the Internet Protocol (IP) as the underlying protocol.

Transmission Control Protocol/Internet Protocol (TCP/IP). A set of communication protocols that provide peer-to-peer connectivity functions for both local and wide-area networks.

trap. In the Simple Network Management Protocol (SNMP), a message sent by a managed node (agent function) to a management station to report an exception condition.

trap recipient. Receiver of a forwarded SNMP trap. Specifically, a trap receiver is defined by an IP address and port to which traps are sent. Presumably, the actual recipient is a software application running at the IP address and listening to the port.

TSR program. See *terminate and stay resident program*.

user action events. Actions that the user takes, such as changes in the SAN, changed settings, and so on. Each such action is considered a User Action Event.

vendor. Property value that the SANavigator tool uses to launch third-party software. Vendor property might be discovered but will always remain editable.

VGA. See *video graphics adapter*.

video graphics adapter (VGA). A computer adapter that provides high-resolution graphics and a total of 256 colors.

video random access memory (VRAM). A special type of dynamic RAM (DRAM) used in high-speed video applications, designed for storing the image to be displayed on a computer's monitor.

VRAM. See *video random access memory*.

WORM. See *write-once read-many*.

Worldwide Name (WWN). A registered, unique 64–bit identifier assigned to nodes and ports.

write-once read-many (WORM). Any type of storage medium to which data can be written only a single time, but can be read from any number of times. After the data is recorded, it cannot be altered. Typically the storage medium is an optical disk whose surface is permanently etched by using a laser in order to record information. WORM media are high-capacity storage devices and have a significantly longer shelf life than magnetic media.

WWN. See *worldwide name*.

XGA. See *eXtended graphics array*.

zoning. A function that allows segmentation of nodes by address, name, or physical port and is provided by fabric switches or hubs.

Index

T

U

W

Readers' Comments — We'd Like to Hear from You

IBM TotalStorage FAStT
Hardware Maintenance Manual and Problem Determination Guide

Publication No. GC26-7528-00

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	☐	☐	☐	☐	☐

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	☐	☐	☐	☐	☐
Complete	☐	☐	☐	☐	☐
Easy to find	☐	☐	☐	☐	☐
Easy to understand	☐	☐	☐	☐	☐
Well organized	☐	☐	☐	☐	☐
Applicable to your tasks	☐	☐	☐	☐	☐

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? ☐ Yes ☐ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name _____ Address _____

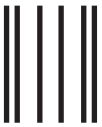
Company or Organization _____

Phone No. _____

Readers' Comments — We'd Like to Hear from You
GC26-7528-00

Cut or Fold
Along Line

Fold and Tape | **Please do not staple** | Fold and Tape



NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

International Business Machines Corporation
RCF Processing Department
Dept. M86/Bldg.050-3
5600 Cottle Road
San Jose, CA
U.S.A 95193-0001

Fold and Tape | **Please do not staple** | Fold and Tape

Cut or Fold
Along Line

Printed in U.S.A.

GC26-7528-00