IBM System Storage TS3310 Tape Library

Setup and Operator Guide

Machine Type 3576

GA32-0477-15

IBM System Storage TS3310 Tape Library

Setup and Operator Guide

Machine Type 3576

GA32-0477-15

Note!
Before using this information and the product it supports, be sure to read the information in the Safety and Environmental Notices and Notices sections.

This edition applies to the *IBM System Storage TS3310 Tape Library Setup and Operator Guide*, GA32-0477-14, and to the subsequent releases and modifications until otherwise indicated in new editions.

Contents

Figures

Tables

Read this first

This product might not be certified in your country for connection by any means whatsoever to interfaces of public telecommunications networks. Further certification might be required by law before making any such connection. Contact IBM® for information.

Accessing online technical support

For online Technical Support for your library, visithttp://www.ibm.com/support/

Sending us your comments

Your feedback is important in helping IBM provide accurate and useful information. If you have comments or suggestions for improving this publication, send your comments by:

- Emailing IBM:
  - Internet or IBMLink from US: *starpubs@us.ibm.com*
  - IBMLink from Canada: *STARPUBS at TORIBM*

  Include the following information in your email:
  - Exact publication title
  - Form number (for example, GA32–1234–02) or part number (on the back cover of the publication)
  - Page, table, or illustration numbers that you are commenting on
  - A detailed description of any information that should be changed

Registering for My Notification

My Notification registration provides email notification when new firmware levels are updated and available for download and installation. To register for My Notification:

1. Visit the web at: http://www-01.ibm.com/software/support/einfo.html.
2. Click **My Notifications**.

Note: Library firmware and tape drive firmware are verified and released together. When you are updating to the latest firmware, verify that all installed components such as tape drives and library firmware are at the latest levels noted on the Support website. Mixing different levels of library and tape drive firmware is not supported and might cause unpredictable results.

Contacting IBM technical support

In the US: Call 1-800-IBM_SERV (1-800-426-7378).

Note: Before calling, complete all the steps in “Contacting IBM technical support” on page 10-21.

All other Countries/Regions: Visit http://www.ibm.com.

To open a Service Request online: Under **Support & downloads**, click **Open a service request**.

Minimum firmware levels for common library features

Feature	Minimum firmware levels required
LTO 6 tape drive (Feature code 8342)	Library firmware must be at 630G.x or greater to support the Ultrium 6 drives. If the IBM tape device driver or ITDT (IBM Tape Diagnostic tool) is used, ensure the minimum version that is required to support Ultrium 6 tape drives are installed on the host. Ensure any host applications and software that use their own device drivers are at the minimum level that is required to support Ultrium 6 tape drives.
LTO 5 tape drive (Feature code 8242)	Library firmware must be at 587G.GS003 or greater to support the Ultrium 5 drives. If the IBM tape device driver or ITDT (IBM Tape Diagnostic tool) is used, ensure the minimum version that is required to support Ultrium 5 tape drives are installed on the host. Ensure any host applications and software that use their own device drivers are at the minimum level that is required to support Ultrium 5 tape drives.

Limits on downgrading library firmware

If your library is running firmware version 600G or later, you can only downgrade library firmware to 410G or later. If you must downgrade to a version earlier than 410G, contact IBM technical support.

Limits on restoring a saved configuration

If your library is running firmware version 600G or later, you can restore a saved configuration that was created with only firmware version 410G or later. If you must restore a configuration that is created with a firmware version earlier than 410G, contact IBM technical support.

Summary of changes for GA32-0477-15

The following list indicates the changes to the most recent edition of the document.

15th edition

Revision bars (|) display next to the information that was added or changed since the previous edition (GA32-0477-14).

Changed information

The following topics are updated:

- Changed placement for a note about library drive firmware updating functions.

Safety and environmental notices

When this product is used, observe the danger, caution, and attention notices that are contained in this guide. The notices are accompanied by symbols that represent the severity of the safety condition.

Most danger or caution notices contain a reference number (Dxxxx or Cxxxx). Use the reference number to check the translation in the *IBM Systems Safety Information* (G229-9054) publication included in your ship group.

The sections that follow define each type of safety notice and give examples.

Safety notices

Danger notice

A danger notice calls attention to a situation that is potentially lethal or extremely hazardous to people. A lightning bolt symbol always accompanies a danger notice to represent a dangerous electrical condition. A sample danger notice follows:

An electrical outlet that is not correctly wired could place hazardous voltage on metal parts of the system or the devices that attach to the system. It is the responsibility of the customer to ensure that the outlet is correctly wired and grounded to prevent an electrical shock. A lightning bolt symbol always accompanies a danger notice to represent a dangerous electrical condition.*(D004)*

Caution notice

A caution notice calls attention to a situation that is potentially hazardous to people because of some existing condition, or to a potentially dangerous situation that might develop because of some unsafe practice. A caution notice can be accompanied by one of several symbols:

If the symbol is...	It means...
	A generally hazardous condition not represented by other safety symbols.
 Class I	A hazardous condition due to the use of a laser in the product. Laser symbols are always accompanied by the classification of the laser as defined by the U. S. Department of Health and Human Services (for example, Class I, Class II, and so forth).
	A hazardous condition due to mechanical movement in or around the product.

If the symbol is...	It means...
	A hazardous condition due to the weight of the unit. Weight symbols are accompanied by an approximation of the product's weight.
	A hazardous condition due to the unit's susceptibility to electrostatic discharge.

Sample caution notices follow:

Caution

The battery is a lithium ion battery. To avoid possible explosion, do not burn. Exchange only with the IBM-approved part. Recycle or discard the battery as instructed by local regulations. In the United States, IBM has a process for the collection of this battery. For information, call 1-800-426-4333. Have the IBM part number for the battery unit available when you call. (*C007*)

Caution

The system contains circuit cards, assemblies, or both that contain lead solder. To avoid the release of lead (Pb) into the environment, do not burn. Discard the circuit card as instructed by local regulations. (*C014*)

Caution

When removing the Modular Refrigeration Unit (MRU), immediately remove any oil residue from the MRU support shelf, floor, and any other area to prevent injuries because of slips or falls. Do not use refrigerant lines or connectors to lift, move, or remove the MRU. Use handholds as instructed by service procedures. (*C016*)

Caution

Do not connect an IBM control unit directly to a public optical network. The customer must use an additional connectivity device between an IBM control unit optical adapter (that is, fibre, ESCON®, FICON®) and an external public network . Use a device such as a patch panel, a router, or a switch. You do not need an additional connectivity device for optical fibre connectivity that does not pass through a public network.

Possible safety hazards

Possible safety hazards to the operation of this product are:

Electrical

An electrically charged frame can cause serious electrical shock.

Mechanical

Hazards (for example, a safety cover missing) are potentially harmful to people.

Chemical

Do not use solvents, cleaners, or other chemicals that are not approved for use on this product.

Before the library is used, repair any of the preceding problems.

Class I laser product

Before the library is used, review the following laser safety information.

The product might contain a laser assembly that complies with the performance standards set by the US Food and Drug Administration for a Class I laser product. Class I laser products do not emit hazardous laser radiation. The product has the necessary protective housing and scanning safeguards to ensure that laser radiation is inaccessible during operation or is within Class I limits. External safety agencies reviewed the product and obtained approvals to the latest standards as they apply.

Protective devices

The library has the following protective devices:

- Monitored access to the library
- Main power switch

Monitored access to the library

The library is surrounded by an enclosure. The library can be accessed only from monitored access areas.

The enclosure around the library separates the danger area of the library from the working area. The danger area is the area in which personnel can be injured by component movements.

CAUTION:
Movements of mechanical components in the library can cause serious injury. Access to the library must be restricted to authorized personnel only.

Main power switch

To turn library power ON, press | on each power switch that is installed in the library. To turn library power OFF, press 0 on the switch. In any case of danger, immediately turn the main power switch of the library OFF.

CAUTION:
To completely remove all power, disconnect the power cord from the electrical outlet.

Attention: Except in emergencies, stop the library with the normal shutdown procedure before you switch OFF the main power switch. IBM is not responsible for damage that is caused by improper use of the main power switch. Such risk lies entirely with the user.

CAUTION:
Movements of mechanical components in the tape library can cause serious injury. Before the main power switch is turned ON and the tape library is restarted, confirm that no danger exists to personnel or property.

Rack safety

The following general safety information must be used for all rack mounted devices.

DANGER

- **Always lower the leveling pads on the rack cabinet.**
- **Always install stabilizer brackets on the rack cabinet.**
- **To avoid hazardous conditions because of uneven mechanical loading, always install the heaviest devices in the bottom of the rack cabinet. Always install servers and optional devices, starting from the bottom of the rack cabinet.**
- **Rack mounted devices are not to be used as a shelf or workspace. Do not place any object on top of rack mounted devices.**
- **Each rack cabinet might have more than one power cord. Be sure to disconnect all power cords in the rack cabinet before you service any device in the rack cabinet.**
- **Connect all devices that are installed in a rack cabinet to power devices installed in the same rack cabinet. Do not plug a power cord from a device that is installed in one rack cabinet into a power device that is installed in a different rack cabinet.**
- **An electrical outlet that is not correctly wired might place hazardous voltage on the metal parts of the system or the devices that attach to the system. It is the responsibility of the customer to ensure that the outlet is correctly wired and grounded to prevent an electrical shock.**

CAUTION:

- **Do not install a unit in a rack where the internal rack ambient temperatures might exceed the manufacturer's recommended ambient temperature for all your rack mounted devices.**
- **Do not install a unit in a rack where the air flow is compromised. Ensure that air flow is not blocked or reduced on any side, front, or back of a unit that is used for air flow through the unit.**
- **Consideration must be given to the connection of the equipment to the supply circuit so that overloading of the circuits does not compromise the supply wiring or overcurrent protection. To provide the correct power connection to a rack, refer to the rating labels on the equipment in the rack to determine the total power requirement of the supply circuit.**
- **(For sliding drawers) Do not pull out or install any drawer or feature if the rack stabilizer brackets are not attached to the rack. Do not pull out more than one drawer at a time. The rack might become unstable if you pull out more than one drawer at a time.**
- **(For fixed drawers) This drawer is a fixed drawer and must not be moved for servicing unless specified by the manufacturer. Attempting to move the drawer partially or out of the rack might cause the rack to become unstable or cause the drawer to fall out of the rack.**

(R001)

CAUTION:

Removing components from the upper positions in the rack cabinet improves rack stability during relocation. Follow these general guidelines whenever you relocate a populated rack cabinet within a room or building:

- **Reduce the weight of the rack cabinet by removing equipment, starting at the top of the rack cabinet. When possible, restore the rack cabinet to the configuration of the rack cabinet as you received it. If this configuration is not known, you must do the following:**
  - **Remove all devices in the 32U position and above.**
  - **Ensure that the heaviest devices are installed in the bottom of the rack cabinet.**
  - **Ensure that there are no empty U-levels between devices that are installed in the rack cabinet below the 32U level.**
- **If the rack cabinet you are relocating is part of a suite of rack cabinets, detach the rack cabinet from the suite.**
- **Inspect the route that you plan to take to eliminate potential hazards.**
- **Verify that the route that you choose can support the weight of the loaded rack cabinet. Refer to the documentation that comes with your rack cabinet for the weight of a loaded rack cabinet.**
- **Verify that all door openings are at least 760 x 2032 mm (30 x 80 in.).**
- **Ensure that all devices, shelves, drawers, doors, and cables are secure.**
- **Ensure that the four leveling pads are raised to their highest position.**
- **Ensure that there is no stabilizer bracket that is installed on the rack cabinet during movement.**
- **Do not use a ramp that is inclined at more than 10 degrees.**
- **When the rack cabinet is in the new location:**
  - **Lower the four leveling pads.**
  - **Install stabilizer brackets on the rack cabinet.**
  - **If you removed any devices from the rack cabinet, repopulate the rack cabinet from the lowest position to the highest position.**
- **If a long-distance relocation is required, restore the rack cabinet to the configuration of the rack cabinet as you received it. Pack the rack cabinet in the original packaging material, or equivalent. Also, lower the leveling pads to raise the casters off the pallet and bolt the rack cabinet to the pallet.**

(R002)

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 that are 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 (US 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 US) - Use a cord set with a grounding-type attachment plug. The cord set must have the appropriate safety approvals for the country in which the equipment is installed.

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

Removing a battery from a SnapHat battery holder

The battery for this product is on the Library Control Card. The yellow component that holds the battery on the Library Control Card is referred to as a "SnapHat". It snaps on the Library Control Card and is identified by its yellow color.

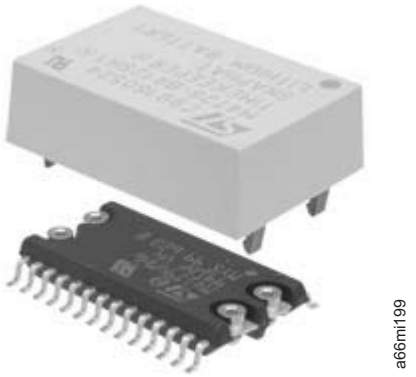


Figure 1. SnapHat battery holder

To remove the SnapHat battery holder from the Library Control Card:

1. Take the SnapHat holder by the short edges and pull it or snap it off the card.
2. When the SnapHat battery holder is free, dispose of the battery that is in the holder according to the correct battery disposal practices for your location.

Monitor recycling or disposal

Flat panel display

The fluorescent lamp or lamps in the liquid crystal display contain mercury. Dispose of it as required by local ordinances and regulations.

Monitors and Workstations

New Jersey - For information about recycling covered electronic devices in the State of New Jersey, go to the New Jersey Department of Environmental Protection website at http://www.state.nj.us/dep/dshw/recycle/Electronic_Waste/index.html

Oregon - For information about recycling covered electronic devices in the state of Oregon, go to the Oregon Department of Environmental Quality site at http://www.deq.state.or.us/lq/electronics.htm

Washington State- For information about recycling covered electronic devices in the State of Washington, go to the Department of Ecology Web site at http://www.ecy.wa.gov/programs/swfa/eproductrecycle/ or telephone the Washington Department of Ecology at 1-800Recycle.

Preface

Trained service personnel can use this maintenance information to test, diagnose, and repair the IBM System Storage® TS3310 tape library.

To ensure that you have the latest publications, visit the web at http://www.ibm.com/storage/lto.

Related publications

Refer to the following publications for information.

To obtain the latest version of these publications, visit the web at http://www.ibm.com/storage/lto.

- *IBM System Storage TS3310 Tape Library SCSI Reference* (GA32-0476) provides supported SCSI commands and protocol that governs the behavior of SCSI interface.
- *IBM System Storage TS3310 Tape Library Setup and Operator Guide* (GA32-0477) provides information for installation and operation.
- *IBM Ultrium Device Driver Installation and User 's Guide* (GA32-0430) provides instructions for attaching IBM supported hardware to open-systems operating systems. It indicates what devices and levels of operating systems are supported. It also gives requirements for adapters, and tells how to configure hosts to use the device driver. All of the above are with the Ultrium family of devices.
- *IBM Ultrium Device Driver Programming Reference* (GC35-0483) supplies information to application owners who want to integrate their open-systems applications with IBM supported Ultrium hardware. The reference contains information about the application programming interfaces (APIs) for each of the various supported operating-system environments.

Getting assistance

If this document does not help you solve the problem, contact your next level of support.

Chapter 1. Product description

The IBM System Storage™ TS3310 tape library offers high performance, capacity, and technology that is designed for reliability and the heavy demands of tape storage. The LTO Ultrium 6 cartridge has a native data capacity of 2500 GB (6250 GB at 2.5:1 compression). The Ultrium 5 cartridge has a native data capacity of 1500 GB (3000 GB at 2:1 compression). This library is highly modular with scalability that varies from the base library 5U control module with up to four extra expansion units for a total of 41U height. This automated tape library incorporates high-performance IBM LTO Ultrium Tape Drives for the midrange to enterprise open systems environment. The Ultrium 4 cartridge has a native data capacity of 800 GB (1600 GB at 2:1 compression). IBM LTO Ultrium 4 tape drives can read and write original LTO Ultrium 3 data cartridges and read LTO Ultrium 2 data cartridges. The Ultrium 3 cartridge has a native data capacity of 400 GB (800 GB at 2:1 compression). IBM LTO Ultrium 3 tape drives can read and write original LTO Ultrium 2 data cartridges and read LTO Ultrium 1 data cartridges.

The base TS3310 library contains the library control module, fixed tape cartridge storage of 30 slots, I/O station of 6 slots, a touchscreen display, cartridge handling robotics, and up to two LTO Ultrium tape drives.

You can add up to 4 optional expansion modules to a control module.

Note: Rack doors are required for any library that has more than 14 drives installed.

Each 9U expansion module can accommodate up to 4 LTO Ultrium Tape Drives and up to 92 tape cartridge slots, including 12 configurable I/O station slots.

This library supports LTO Ultrium 5 and Ultrium 6 native switched fabric Fibre Channel attachments, and LTO Ultrium 4 Tape Drives with either Serial Attached SCSI (SAS) or native switched fabric Fibre Channel attachment for connection to a wide spectrum of open system servers. This library also supports the LTO Ultrium 5 native switched fabric Fibre Channel attachment. It also supports LTO Ultrium 3 Tape Drives with either LVD Ultra160 SCSI or native switched fabric Fibre Channel attachment.

The TS3310 library supports Application Managed Encryption (AME), System Managed Encryption, (SME), and Library Managed Encryption (LME) on Ultrium 6 Fibre Channel (FC) drives with Ultrium 6 media, Ultrium 5 Fibre Channel (FC) drives with Ultrium 5 media, Ultrium 4 SAS (Serial Attached SCSI) and Fibre Channel (FC) drives with Ultrium 4 media. The AME function is standard on all libraries, while the SME and LME features require a license key.

Front panel components

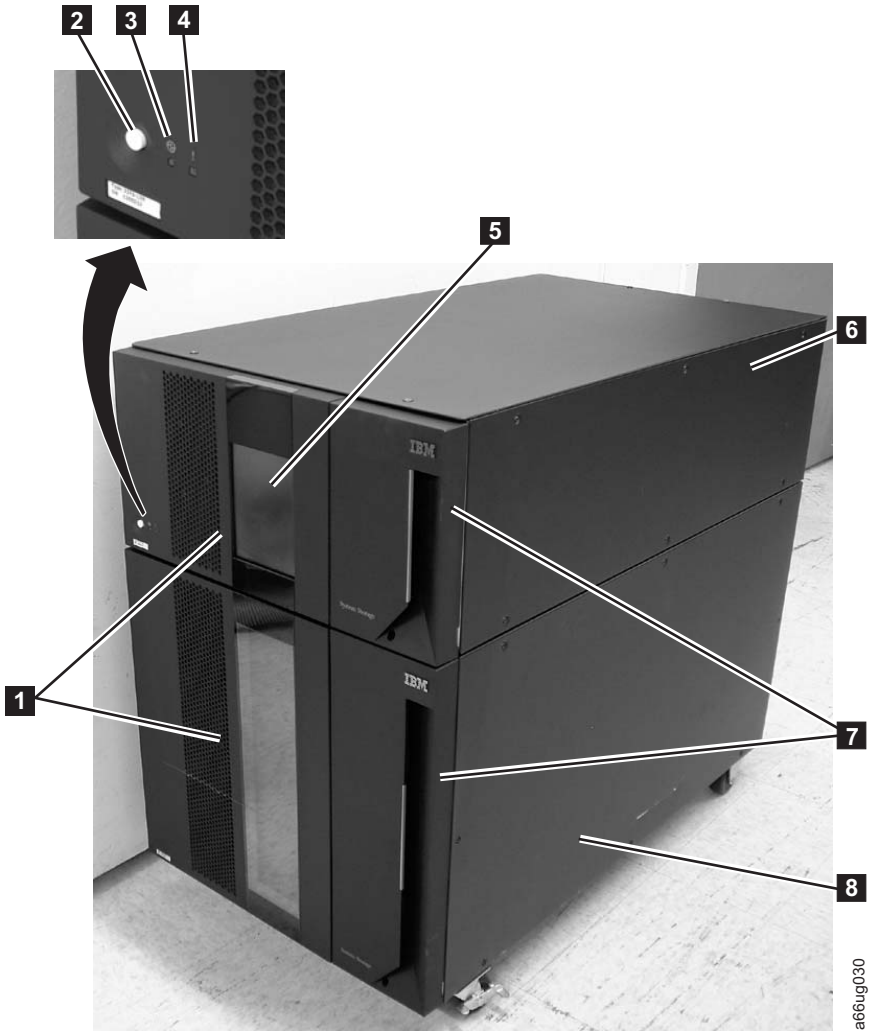


Figure 1-1. Front panel of a 14U library

1	Access doors	5	Operator Panel
2	Power button	6	5U control module
3	Green power ON LED	7	I/O stations
4	Amber Operator Intervention Alert LED	8	9U expansion module

Control module (3576 Model L5B)

All library configurations include the control module (6 in Figure 1-1 on page 1-2). The control module contains the robotics, library control blade (LCB), and touchscreen display. The control module also contains an I/O station, fixed storage slots, tape drives, and at least one power supply.

The control module can contain one or two tape drives and one or two power supplies. At least one power supply is always required.

Expansion module (3576 Model E9U)

Each 9U expansion module (8 in Figure 1-1 on page 1-2) is a supplementary module that is attached to the 5U Control Module. Like the control module, the expansion modules provide fixed storage slots, tape drive slots, and power supply slots. The I/O station in an expansion module can be configured as storage.

If an expansion module contains only cartridges (no drives). All power is derived from the control module.

I/O station

I/O stations (7 in Figure 1-1 on page 1-2) are on the front panel of the library and enable the importing and exporting of cartridges without interrupting normal library operations. A control module I/O station has a capacity of six cartridges. A 9U expansion module I/O station has a capacity of 12 cartridges.

Note:
This library reads bar code labels to identify the specific cartridges in each slot. Ensure that all cartridges placed in the library have appropriate bar code labels.

When an I/O station slot is assigned to a logical library, only that logical library can access that slot. The I/O station is shared among all logical libraries, but the I/O station slots are owned by one logical library at a time.

In a 5U library, the six I/O station slots cannot be configured as storage. In a library that has expansion modules, the I/O stations can be configured as follows:

Table 1-1. Library I/O station configurations

Number of Expansion Modules	Number of License Keys	I/O slots in expansion modules	I/O slots in control module	Total number of I/O station Slots
0	0	0	6	6
1	0	12	0	12
1	1	12	6	18
2	1	24	0	24
2	2	24	6	30
3	2	36	0	36
3	3	36	6	42
4	3	48	0	48
4	4	48	6	54

Note: I/O slots can be reassigned each time the I/O station is opened by rearranging the cartridges in the I/O station.

Access door

Each control module and expansion module has a door on the front panel that allows access to the internal components of the library.

This door is locked by the I/O station. To open the access door (**1** in Figure 1-1 on page 1-2), you must first open the I/O station.

If you want to restrict access to the library, lock the I/O station door.

From the Operator Panel: **Operations** > **Lock I/O Station** > **Lock/Unlock**

From the Web User Interface: **Manage Cartridges** > **Lock/Unlock I/O station Doors**

Attention: When any access door is opened, all in-progress motion commands stop, the picker lowers to the bottom of the library, and the library is taken offline. When this action happens, the library must be put back online manually. See "Taking a logical library offline/online" on page 8-18). When the access door is closed, the library returns any media in the picker to its original storage slot.

Operator Panel

The Operator Panel (**5** in Figure 1-1 on page 1-2) is the touchscreen display device that is located on the access door of the control module. Library operations and service functions are completed from this screen.

The Web User Interface offers some of the same functionality as the Operator Panel with a web browser that enables remote access to the library. For information about the Operator Panel and the Web User Interface, see Chapter 6, "User interfaces," on page 6-1.

Power button

Pressing **Power** (**2** in Figure 1-1 on page 1-2) on the front panel of a control module turns the picker and Operator Panel ON or OFF. However, power is still applied to the power supplies. The **Power** is used during library shutdown and to manually reboot the library.

Front panel LEDs

Two LEDs are on the front of the library to the right of the **Power** button.

- Green power ON LED (**3** in Figure 1-1 on page 1-2): When lit, this LED indicates that the library power is ON.
- Amber Operator Intervention Alert LED (**4** in Figure 1-1 on page 1-2): When lit, this LED indicates that there is a Library, Drives, or Media Operator Intervention available. To access the Operator Intervention, select **Tools** > **Operator Intervention** from the Operator Panel.

Rear panel components

The following components are located on the rear panel of the library:

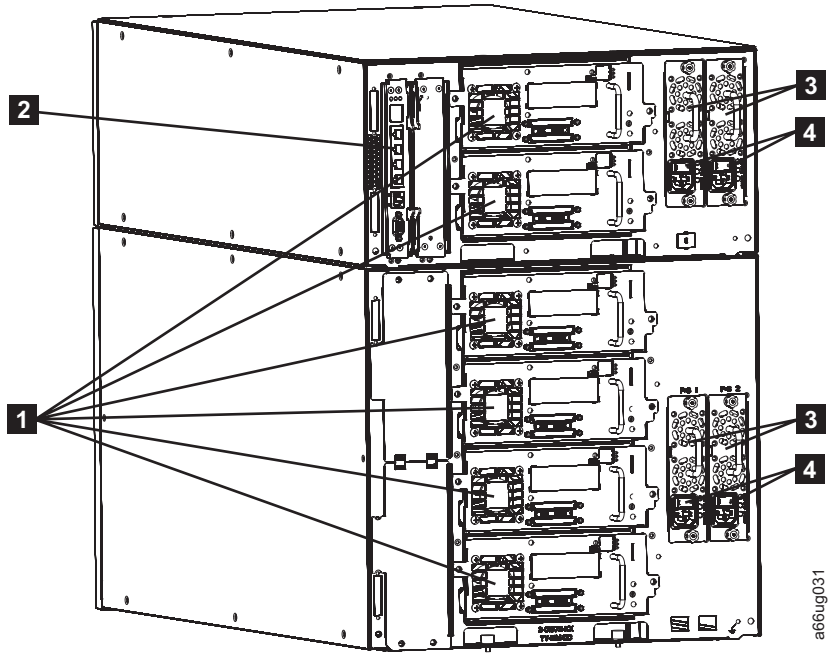


Figure 1-2. Rear panel of a 14U library

1	Tape drives (SCSI drives shown)	3	Power supplies (2 in control module; 2 in expansion module)
2	Library Control Blade	4	Power supply switches

Library Control Blade (LCB)

The Library Control Blade (2 in Figure 1-2) manages the entire library, including the Operator Panel and picker, and is responsible for running system tests to ensure that the library is functioning properly.

The LCB houses the Compact Flash Card that stores vital product data (VPD) such as library settings, serial number.

The LCB indicates status with three light-emitting diodes (LEDs). These LEDs, located near the top of the LCB, are green, amber, and blue in color.

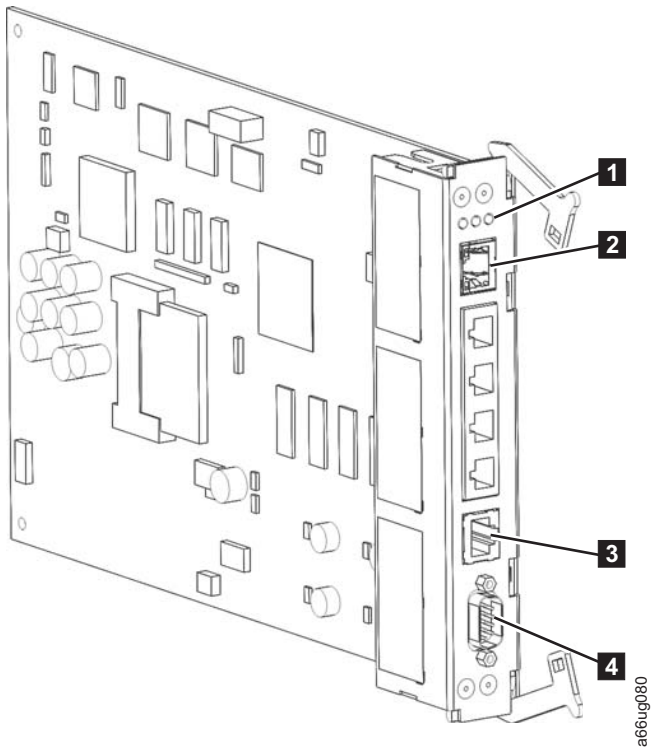


Figure 1-3. The library control blade

1. LEDs
   - Green indicates a good status.
   - Amber indicates a degraded status.
   - Blue indicates a potential fault. See "Interpreting LEDs" on page 10-8.
2. Gigabit Ethernet (external network) port
3. Service Ethernet port (10/100 Mb/s)
4. Service serial port

Tape drives

The library supports Ultrium160 SCSI, Serial Attached SCSI (SAS), and Fibre Channel tape drives.

Tape drives (**1** in Figure 1-2 on page 1-5) are hot addable (library power remains ON and operations of the installed tape drives are still active). Drives can be removed and installed without tools.

Ultrium160 SCSI tape drives are attached directly to a host. Fibre Channel tape drives are directly attached to a host or a storage area network (SAN). Each SAS link is point-to-point so a maximum of two hosts can share a dual-port SAS tape drive.

Drives that are mounted in sleds are installed into tape drive slots in the rear of the library. If a tape drive slot is empty, a metal plate covers the empty drive slot. This "metal plate" cover has a connector that plugs into the drive connector, providing electrical termination for some of the drive circuits. It also serves as a safety cover, and prevents debris from entering the library. All empty drive slots must have one of these covers that are installed for correct library operation.

Power supply

The library supports single and redundant power configurations. Each control module must have at least one power supply. A single power configuration has a power supply that is installed in the left slot of each library module as viewed from the rear. A redundant power configuration has power supplies that are installed in both slots of each library module.

The single configuration has a single AC line input and a single DC power supply. The optional redundant configuration has dual AC line input and dual DC power supplies. A power supply (**3** in Figure 1-2 on page 1-5) can be hot-swapped if the library has a redundant power supply. A redundant power supply can be hot added.

A power switch (**4** in Figure 1-2 on page 1-5) is on every power supply. This switch is used to remove all power from the library for emergency and service situations. Except in emergency situations, use the shutdown procedure before the power switch is switched OFF For more information, see "Shutting down the library" on page 8-19..

The power system of the library contains the following components:

- Power supply
- AC power cord

The power supply has three light emitting diodes (LEDs) that provide status information. These LEDs, located to the right of the power switch, are green, amber, and blue in color.

- Green indicates a good AC or DC status.
- Amber indicates a degraded status.
- Blue indicates a potential fault. See "Interpreting LEDs" on page 10-8.

Interior components

The following components are located inside the library:

- "Storage columns" on page 1-8
- "Robot assembly designs" on page 1-8

Storage columns

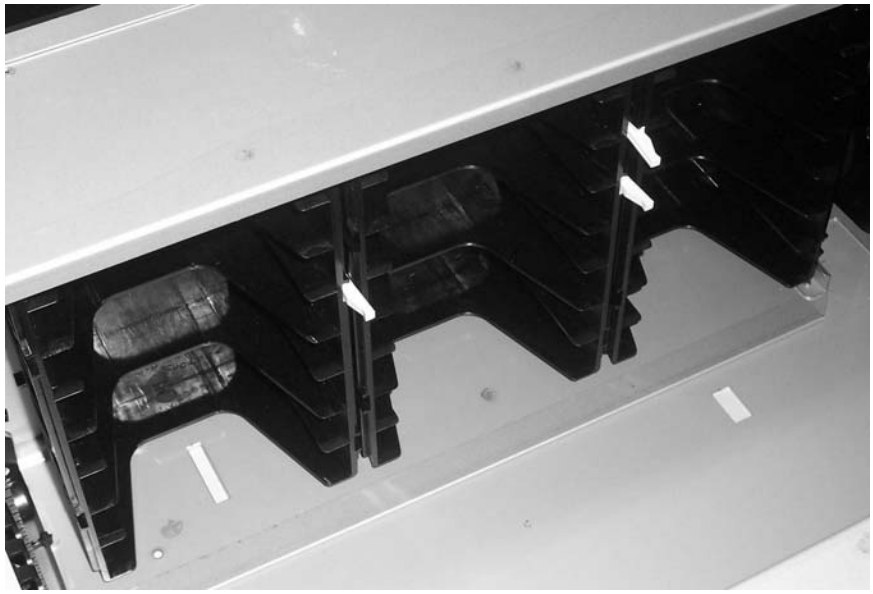


Figure 1-4. Storage columns

Storage columns within the library store cartridges while they are not being used by a drive. The library contains six storage columns. One of the six columns is the I/O station.

Robot assembly designs

The picker (robotic arm) has fingers that enable it to grab tape cartridges and move them to and from the I/O station, storage slots, and drives. A Bar Code Scanner, which is located inside the picker, reads each cartridge bar code label and the fiducial labels that identify the types of cartridge magazines and tape drives that are installed in the library.

As of November 2008, the robot assembly was changed. The two robots are identified as follows:

- Pre-November 2008 - The robot is referred to as the "Model 1 robot." The components are the "Model 1 picker" and the "Model 1 Y-carriage assembly."
- November 2008 and forward - The robot is referred to as the "Model 2 robot." The components are the "Model 2 picker," the "Model 2 Y-carriage assembly," and the "Model 2 robot controller Board."

520G is the minimum version of library firmware that supports the Model 2 robot. The Model 2 robot allows access to five extra slots in the library (the second-from-bottom row of slots are now available; the Model 1 robot cannot reach them). However, although Model 2 robot assemblies "fit" onto libraries that were built with the Model 1 robot, IBM does not support switching them out. Robot versions must not be changed in the field. If a customer has a Model 1 robot, you must replace it with a Model 1 robot or components. Similarly, if a customer has a Model 2 robot, you must replace it with a Model 2 robot or components.

Determine which robot your library contains

Physical Indicators

- Model 2 robot label. Model 2 robots have an **M2** label that is on the front of the Y-carriage assembly, visible from outside the library.
- Physical appearance. The Model 2 robot has a large PCB (called the robot controller board) on the Y-carriage assembly. It also looks different. For pictures, see “M2 robot assembly” on page 1-10).

Software Indicators

- Operator panel - **Tools** > **About Library** screen: Libraries containing a Model 2 robot have a line item called "Robot FW." Libraries containing Model 1 robots do not have this line item.
- Web client - **Service Library** > **View/Update Library Firmware Level** screen: Libraries containing a Model 2 robot show a listing for "Robot Firmware Version" in the Physical Library section of the page. Libraries containing Model 1 robots do not have this listing.
- Snapshot/log files: The “Robot Firmware” entry noted previously is contained in snapshots and logs for libraries that contain Model 2 robots. Libraries with Model 1 robots do not have the "robot firmware" entry.

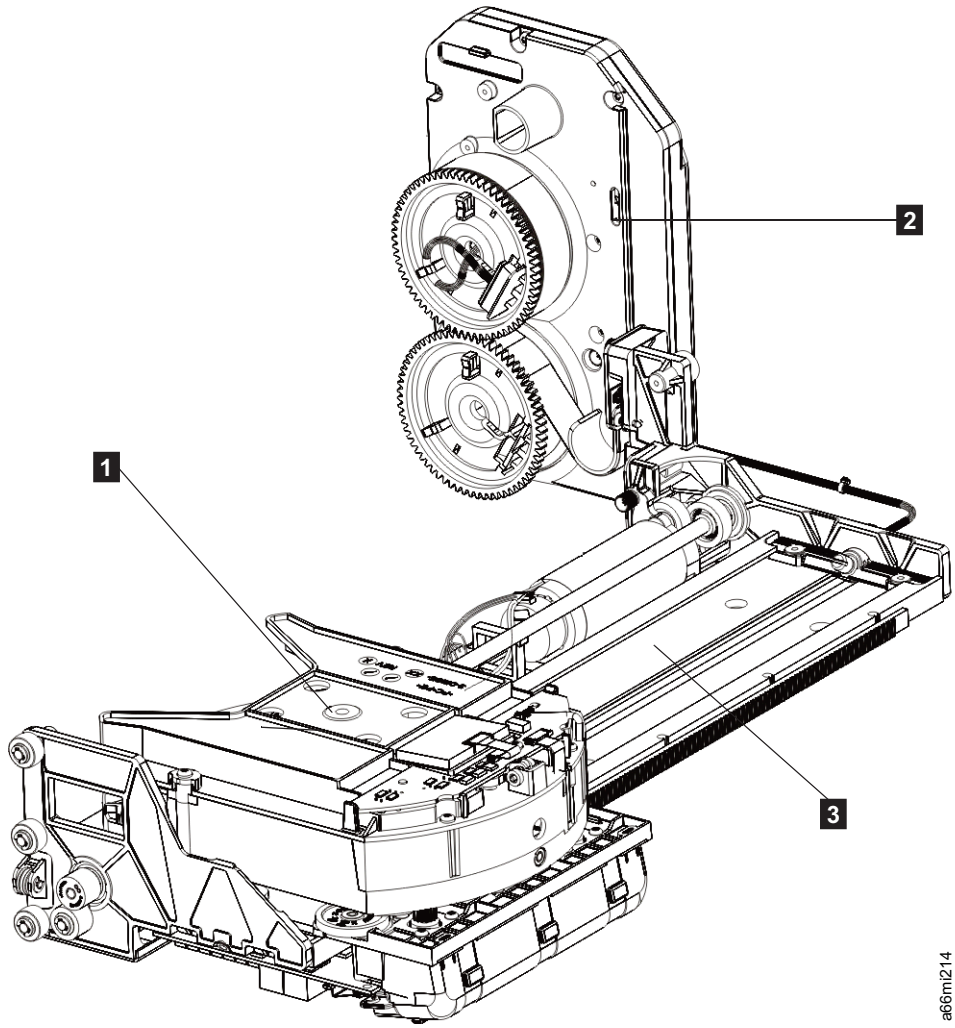


Figure 1-5. Model 1 robot assembly with original cable spool

1 Picker

3 Y-carriage assembly

2 Cable Spool

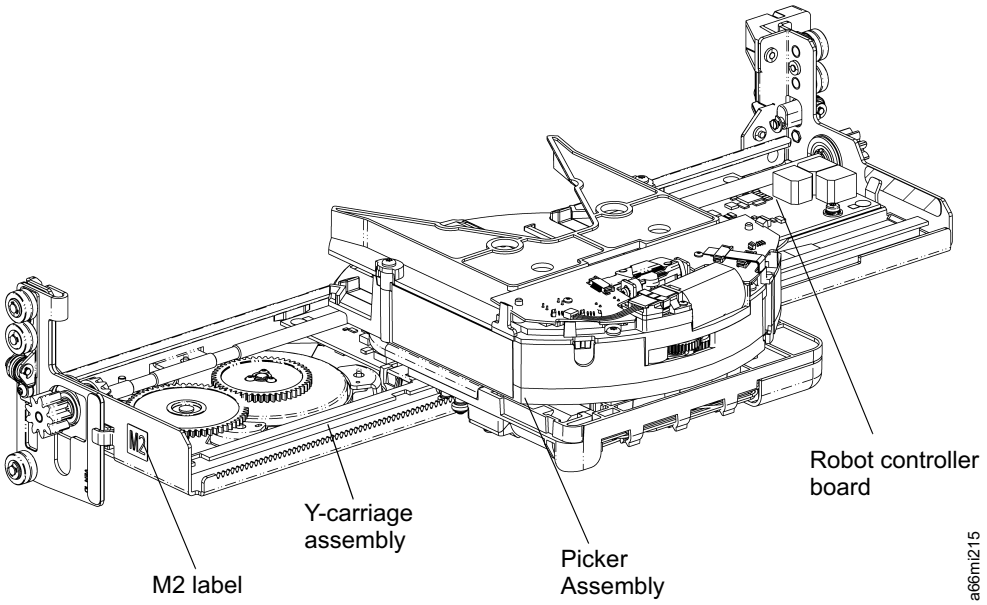


Figure 1-6. Model 2 robot assembly (picker assembly and Y-carriage assembly)

The robot assembly has two designs, referred to as **Robot Assembly** and **M2 Robot Assembly**. The differences are explained in this section.

Original robot assembly

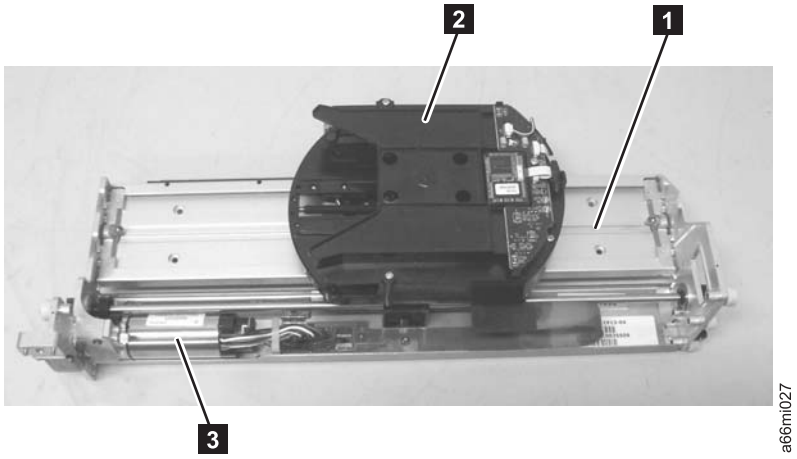


Figure 1-7. Robot assembly

The robot assembly design displays the Y-Axis assembly housing the Y Motor (3), and the picker assembly (2 that is attached to the carrier (1). The climber moves the Y-Axis/picker assembly within the library.

M2 robot assembly

While it serves the same function as the original robot assembly, the M2 robot assembly has a different design style that is depicted in the following images.

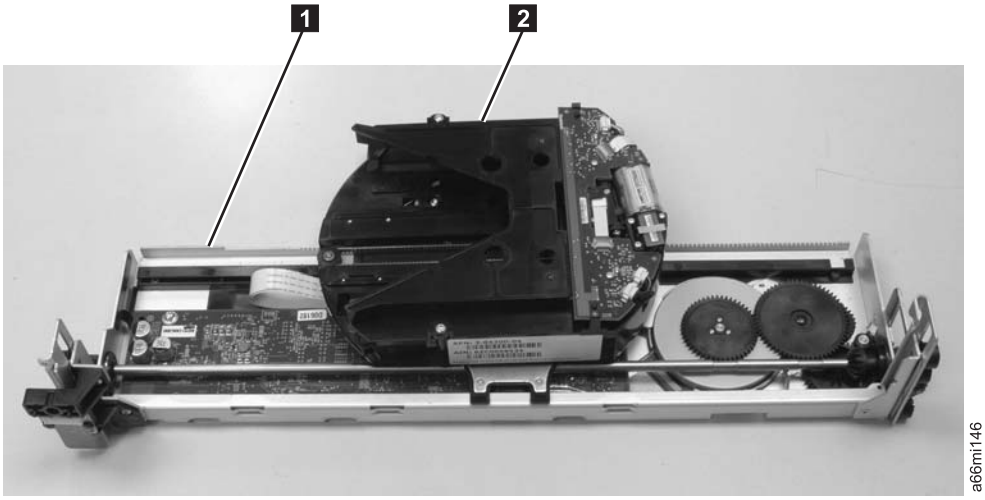


Figure 1-8. M2 robot assembly

In the M2 robot assembly, the robot assembly houses the Y-Axis controller board (**1**) and the M2 picker assembly (**2**) is attached to the carrier.

The M2 label is clearly visible on the side of the robot assembly that faces the door of the library. See Figure 1-9.

Figure 1-9. M2 label on the M2 robot assembly

Optional features

The table lists extra features that can be added to the library to enhance performance.

Table 1-2. Optional features

Type of Feature	Description	Feature Code
Ultrium 6 Tape Drive	8 Gb Fibre Channel interface	8342
Ultrium 5 Tape Drive	8 Gb Fibre Channel interface	8242
Ultrium 4 Tape Drive	3 Gb SAS interface	8139
	4 Gb Fibre Channel interface	8142
Ultrium 3 Tape Drive	Ultra160 SCSI interface	8037
	4 Gb Fibre Channel interface	8042
Power Supply	Redundant	1900
Feature Licenses	Capacity Expansion	1640
	Advanced Reporting	1650
	Path Failover	1682
	Transparent LTO encryption	5900
Library and Drive Code Update	Library and drive code update by an IBM Service Representative	0500
Rack Mount Kit	Hardware that is required to mount your library in a rack	7003
Rack PDU Line Cord	Rack PDU power cord	9848

For information on ordering additional features or replacement parts for your library, see Chapter 13, “Parts list,” on page 13-1.

Ultrium tape drives

This library supports the Ultrium 3, Ultrium 4, Ultrium 5, and Ultrium 6 tape drives. Each tape drive in the library is packaged in a container that is called a drive sled. The drive sled is a customer replaceable unit (CRU), and is designed for quick removal and replacement in the library.

The IBM Ultrium 5 and 6 tape drives support the Fibre Channel interface. The IBM Ultrium 4 tape drive supports SAS or Fibre Channel interfaces. The IBM Ultrium 3 tape drive supports LVD Ultra160 or Fibre Channel interfaces. Depending on which drive is installed, it features two HD68 SCSI connectors, two SAS SFF-8088 connectors, one LC Fibre Channel connector for Ultrium 3 and two Fibre Channel connectors for Ultrium 5 and 6.

Table 1-3. Drive and cartridge properties

Generation	Drive			Cartridge	
	Host Interface	**Sustained Native data transfer rate**	**Types**	**Physical Capacity**	**Types**

Table 1-3. Drive and cartridge properties (continued)

Generation	Drive			Cartridge	
LTO6	8 Gbps dual-port Fibre Channel	160 MB/s	• Fibre Channel	• 2500 GB Native • 6250 GB with 2.5:1 compression	• Data • Rewritable • WORM
LTO5	8 Gbps dual-port Fibre Channel	140 MB/s	• Fibre Channel	• 1500 GB Native • 3000 GB with 2:1 compression	• Data • Rewritable • WORM
LTO4	• 4 Gbps single-port Fibre Channel • 3 Gbps dual-port SAS	120 MB/s	• Fibre Channel • SAS	• 800 GB Native • 1600 GB with 2:1 compression	• Data • Rewritable • WORM
LTO3	• 4 Gbps single-port Fibre Channel • Ultrium160 SCSI	80 MB/s	• Fibre Channel • SCSI	• 400 GB Native • 800 MB with 2:1 compression	• Data • Rewritable • WORM

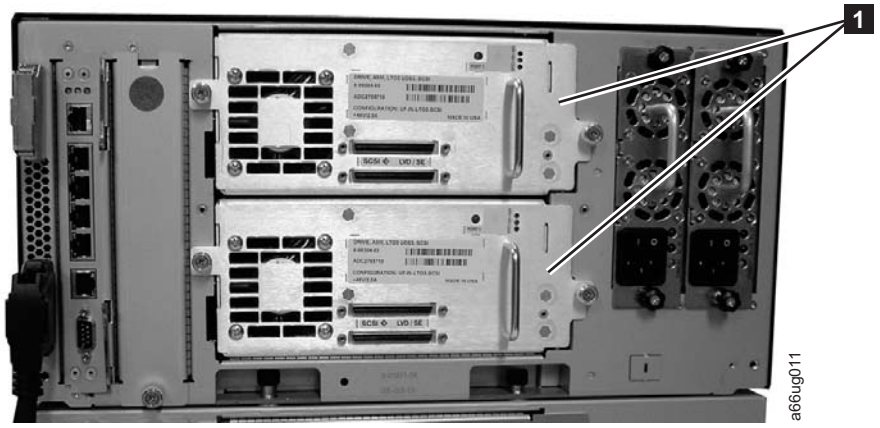


Figure 1-10. Ultra160 SCSI tape drives in the library control module

Note: Ultra160 SCSI, SAS, and Fibre Channel drives are allowed in the same physical and logical libraries. However, you must ensure that the host application supports a mix of interface drive types.

LTO-6 tape drive ports

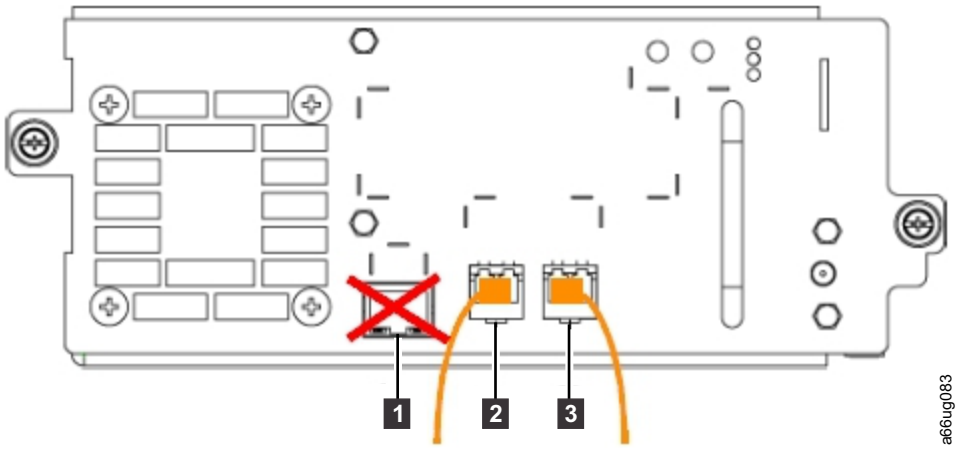


Figure 1-11. LTO-6 tape drive ports

Table 1-4. LTO-6 tape drive ports

1	Ethernet port	Update Drive Firmware code and Download Drive logs
2	Fibre Channel port 1	Default data port
3	Fibre Channel port 2	Default failover port

Speed matching

To improve system performance, this tape drive uses a technique that is called *speed matching* to dynamically adjust its native (uncompressed) data rate to the slower data rate of the attached server.

Channel calibration

The channel calibration feature of the Ultrium drives customizes each read/write data channel for optimum performance. The customization enables compensation for variations in the recording channel transfer function, media characteristics, and read/write head characteristics.

Power management

The power management function controls the drive 's electronics so that part of the electronics completely turns OFF when circuit functions are not needed for the drive 's operation.

Redundant power supply (Feature code 1900)

The optional redundant configuration power supplies can be hot-swapped without interrupting library operation. Each supply in a control module and expansion module includes its own input AC power cord. During redundant operation, each supply carries one-half the power load. If a power cord or power supply fails, the second supply sources the complete power load. Optionally, a single power supply and power cord can be installed if redundant power is not required. The second power supply slot is physically covered in this configuration. The library can be upgraded to redundant power later.

Feature licenses

A feature license controls the setting of feature-enabled flags that are based on a user input key and the library serial number that is stored in the library vital product data (VPD). A unique key exists for each library that is based on an encryption of the chassis serial number and a feature code.

After a feature is enabled, it cannot be disabled. The library 's serial number can be assigned only at the factory.

The library uses feature licenses to enable the capacity expansion, advanced reporting, path failover, and transparent LTO encryption features.

Advanced Reporting (Feature code 1650)

The Advanced Reporting feature license key enables the media analysis and drive resource functions of the TS3310 tape library. These user-configurable reporting features provide graphical displays for both diagnostic and trend analysis data that enables customers to evaluate tape drive, media performance, and drive utilization parameters.

Advanced Reporting is only available to Superuser, Administrative, and Service users through the Web User Interface (UI). Data for Advanced Reporting persists for 12 months, but it is also limited to 1 MB. The persisted data is checksum-protected and persists through a library power loss. The raw data for these reports can also be downloaded and emailed as a comma-separated values (.csv) file through the remote Web UI.

Advanced Reporting reports:

You use the Advanced Reporting function to create reports that can be configured for viewing and analysis.

Note: To use Advanced Reporting, you must have Advanced Reporting licensed on your library and your library firmware must be at version 520G or later. The Advanced Reporting license applies to your entire library, regardless of library size. Therefore, you must purchase the license only once. If you increase the size of your library, your existing license applies to your new library configuration.

Drive Utilization
Drive Utilization provides tape drive usage information that shows which tape drives are working at optimum capacity and that are under-utilized. This information can help you allocate tape drive resources properly.

Media Integrity
Media Integrity provides TapeAlert counts for various combinations of tape drives, tape cartridges, and TapeAlert flags. This information can help you determine whether a problem is because of a specific tape drive or tape cartridge.

Media Security
Media Security enables you to be notified if media is removed from the library without the administrators' knowledge or without direction from the backup application.

Details about using Advanced Reporting include

- The data for these reports is collected in log files that are located under the **Service Library** menu tree on the IBM UI. When the log files reach their maximum size, the oldest information is deleted as new information is added. This procedure can affect how much historical data you can access.
- The on-screen report contains a chart and a data table. When the log files are large, it can take a long time to load all the historical data into the data table. Therefore, the table contains data only for the previous seven days, even if you select a range longer than seven days. The graph, however, displays information for the entire range. To view all of the data, you must save or email the data file. For information on saving and emailing the data file, see "Saving and emailing Advanced Reporting reports and logs" on page 1-21.
- The reports are built according to data in the log files, not data in the current library configuration. Therefore, your library can contain tape drives or cartridges that do not show up in the report. Similarly, the report can contain tape drives and cartridges that no longer reside in the library.
- Information about a tape drive, cartridge, or operation is not recorded in the Drive Utilization log file until after a tape cartridge is mounted (loaded) and unmounted (unloaded) from the tape drive.

Drive Utilization reporting:

The Drive Utilization function records drive, read, and write history that can be used to identify drives or groups of drives that are nearing 100% utilization. It also identifies drive resources that are not being fully used. These reports provide the customer with information necessary to determine if, and when, more drives are necessary.

Data that are collected and saved for these reports include the following data:

- Drive location (module, row)
- Drive serial number
- Logical library
- Megabytes read
- Megabytes written
- Time and date of mount (in GMT)
- Time and date of dismount (in GMT)
- Media motion time (in seconds)
- Media barcode

You can access this report only from the web client. The path to open the report is **Monitor System** > **Advanced Reporting** > **Drive Utilization**.

To configure the report, select the radio button beside the appropriate settings:

- Range - Specifies the range of time that is covered in the report
  - Last seven days
  - Last four weeks (default)
  - Last three months
  - All history (as far back as there is data in the log file)
- Attribute - Specifies which values are included in the report. Select one of the following attributes:

  - Data Written/Read (default): the amount of data that is written to and read from each tape drive, which is shown separately in the chart
  - Total Read and Write: the combined total amount of data that is written to and read from each tape drive
  - Mount Count: the number of tape cartridge mounts
  - Media Mount Time: the total amount of time media that are spent in the selected drive or drives
  - Media Motion Time: the total amount of time media that are spent in motion while in the tape drive (writing, reading, rewinding, and so on)
- Chart - Indicates how the data is displayed in the chart. Select Area, Bar (default), Line, or Pie
- Type - Indicates the chart type. Select one of the following types:
  - Rollup (default) - Displays the grouping on the x-axis and the attribute amount on the y-axis
  - Trend - Shows how the attribute amount changes over time for the selected grouping
- Grouping - Specifies which one or more tape drives or partitions are included in the report. Select one of the following groupings:
  - All drives by coordinate (default): Presents the total of the selected attributes for all tape drives according to their location in the library. If more than one tape drive resides in that location during the selected range, then the attribute values for all the tape drives that reside in that location are combined in the chart
  - All drives by physical serial number
  - All partitions: Presents the total of the selected attribute for all drives according to the physical tape drive serial number
  - Selected drive by coordinate: The report chart is based on an individual tape drive location in the library. If more than one tape drive resides in that location during the selected range, then the attribute values for all the tape drives that reside in that location are combined in the chart
  - Selected drive by physical serial number: The report chart is based on an individual tape drive that is identified by its physical drive serial number
  - Selected partition: The report chart is based on an individual partition in the physical library

Media Integrity reporting:

The Media Integrity function records TapeAlert events to measure and evaluate media and drive performance in the library. The administrator can request, or configure various reports to help in managing the overall reliability and performance of the media and drives, or both.

Data that is collected and saved for these reports include

- Media barcode
- Drive serial number
- TapeAlert value
- Occurrence count of TapeAlert
- Time and date of last TapeAlert occurrence (in GMT)

You can access this report only from the web client. The path to open the report is **Monitor System** > **Advanced Reporting** > **Media Integrity**.

To configure the report, select the radio button beside the appropriate settings:

- Range - Specifies the range of time that is covered in the report
  - Last seven days
  - Last four weeks (default)
  - Last three months
  - All history (as far back as there is data in the log file)
- Attributes - Specifies which values are included in the report, and how they are combined. Select in any combination, including all (default) and none. If you select no attributes, the chart displays the TapeAlert count for the selected Grouping.
  - Cartridge Barcode - All relevant tape cartridges
  - Drive Physical Serial Number (SN) - All relevant tape drives
  - TapeAlert - The TapeAlert flags that were issued. For a description of all TapeAlert flags, see Chapter 11, “Service Action Tickets (Txxx) and Diagnostic Resolutions (DRxxx),” on page 11-1.
- Chart - Indicates how the data is displayed in the chart. Select Area, Bar (default), Line, or Pie
- Type - Indicates the chart type. Select one:
  - Rollup (default) - Displays the number of TapeAlerts for the combination of Grouping and Attributes you selected (default)
  - Trend - Shows the occurrence of TapeAlerts over time
- Grouping - Specifies which one or more drives or tape cartridges on which to base the report. Choose one:
  - All (default) - All tape drives and tape cartridges for which a TapeAlert was issued during the specified range
  - Selected Drive by Physical Serial Number - An individual tape drive. Only tape drives that issued a TapeAlert during the specified range display in the report.
  - Selected Cartridge by Barcode - An individual tape cartridge. Only tape cartridges that were associated with a TapeAlert during the specified range display in the report.
- Sorting - Specifies how the data is sorted. Choose from:
  - Alphabetical
  - Count (ascending)
  - Last Occurrence (default)

Media Security notifications:

Media Security is a feature of the library that notifies you if media is removed from the library without the administrators' knowledge or without direction from the backup application.

Note: Unexpected removal refers to tape cartridges that were removed from the library without being properly removed with the I/O station. Expected removal refers to tape cartridges that were removed properly with the I/O station.

The library detects media removal when it completes an inventory (at boot up; after an open door is closed, and so on) For example, if someone opens the front door of the library and takes a piece of media, the library can notify the administrator which tape was taken, when it was taken, and in what fashion.

You can enable the library to collect information about media removal, and then do any or all of the following; view, save, or email the log.

Note: This feature is only available if the Advanced Reporting license is installed on the library.

To configure what information gets tracked in the log, select **Monitor System** > **Advanced Reporting** > **Media Security** from the remote user interface.

You can configure the library to collect any or all of the following information. By default, the library collects nothing and the log is empty. You must select each item that you want the library to collect.

- Unexpected removal detection after power-up and reboot only
- Unexpected removal detection during library operation
- Expected removal detection from I/E slots during library operation

The log file contains the following information:

- Date and time of media removal
- Tape cartridge barcode
- Type of removal (expected or unexpected)
- Slot location coordinates (of the slot from which the tape cartridge is missing)
- Slot type (IE, storage, or cleaning)

The log lists only media that is removed from the library. It does not list media that move from one location to another within the library. When the log file reaches its maximum size, the oldest information is deleted as new information is added. This action can affect how much historical data you can access.

To view, save, or email the report, select **Service Library** > **Media Security Log** from the remote user interface. Click **Select Action**, select **Download** or **Email** options, then click **Go**.

Media usage report:

The Media usage report lists information about data that is written and read on the media and lists statistics that pertain to soft and hard read and write errors. The media usage log collects information on all media that is in the library, including media that are no longer in the library. Lifetime media usage metrics are associated with the cartridge and are kept on the embedded cartridge memory.

To view the media usage log, go to **Service Library** > **Media Usage Log**.

The log reflects what the drive reports from the embedded cartridge memory whenever the media is unloaded. If the tape cartridge was never mounted and unloaded, it does not display in the log. When the log file reaches its maximum size, old information is deleted as new information is added. This action can affect the amount of available historical data.

The log provides the following information:

- Volser - Media cartridge barcode label
- SN - Media cartridge serial number
- Mfr - Media cartridge manufacturer
- Date - Media cartridge manufacturing date (format: YYYYMMDD)

- Type - Media type
- Mounts - Cartridge mount count
- RRE - Recovered read errors
- URE - Unrecovered read errors
- RWE - Recovered write errors
- UWE - Unrecovered write errors
- LW - Cartridge lifetime MB written
- LR - Cartridge lifetime MB read
- Enc - Cartridge encryption status (U=Unknown, E=Encrypted, N=Not Encrypted

Advanced Reporting templates:

If you want to use the same configuration to create reports repeatedly, you can save the configuration as a template. You can save up to 20 templates for each type of advanced report.

To create a template:

1. From the remote UI, go to **Monitor System** > **Advanced Reporting** and select the Advanced Reporting Configuration page, either Drive Utilization or Media Integrity.
2. On the Advanced Reporting Configuration page, make the selections that you want.
3. Type a name for the template in the empty field next to the **Save** button. The name can have a maximum of 15 characters. You can use only lowercase letters, numbers, and the underscore character (_) in template names.
4. Click **Save**.

The report displays in the drop-down list in the **Report Templates** box.

To use a saved template, select the template from the drop-down list in the **Report Templates** box, and click **Load**.

To delete a template, select the template from the drop-down list in the **Report Templates** box, and click **Delete**.

Advanced Reporting configuration:

To complete Advanced Reporting Configuration from the remote UI, go to **Monitor System** > **Advanced Reporting** and select the **Advanced Reporting Configuration** page, either **Drive Utilization** or **Media Integrity**. When you first open the **Advanced Reporting Configuration** page, the system loads all the data from the library log file for that report to the Internet browser in preparation for creating your reports. If there is numerous information in the log files, this procedure can take several minutes.

The data that is loaded in the Internet browser remains unchanged until you log out of your library session or reload the data. If new data is added to the library log file during your session (for instance, a TapeAlert occurs), it does not display in the onscreen report until you either log out of the library and log on again, or reload the data.

To reload the data without logging out, click **Reload** at the bottom of the **Advanced Reporting Configuration** page. The entire data set reloads, which can take several minutes.

Look at the Report Data section of the **Advanced Reporting Configuration** page to see how many records were loaded from the log files for this report. A note states the number of records that were read.

Deleting Advanced Reporting data:

You can delete the information that is contained in the log files that are used to build the advanced reports.

Attention: After you delete the data in the log files, you cannot restore it. The **Reload** button does NOT retrieve deleted data. Save all the data for both the Drive Utilization report and the Media Integrity report before you delete the data from the library. For information about saving your data, see "Saving and emailing Advanced Reporting reports and logs."

From the remote UI, go to **Monitor System** > **Advanced Reporting** and select the Advanced Reporting Configuration page, either Drive Utilization or Media Integrity.

To delete the Advanced Reporting data, click **Delete** in the Report Data section of either Advanced Reporting Configuration page. This action deletes the data for both the Drive Utilization report and the Media Integrity report.

Saving and emailing Advanced Reporting reports and logs:

You cannot save a report as it displays on the screen, but you can save or email report data as a comma-separated values (.csv) file. You can then import the .csv data into a spreadsheet program and manipulate it to create your own reports for analysis. The .csv file contains all of the data that is in the log file that falls within the date range you specify.

Note: Administrators can configure the library email account and email notifications. Users with user or superuser privileges can receive email notifications, but they cannot configure the library email account or email notifications.

You can configure the library to automatically email Advanced Reporting logs and reports to specified recipients on a daily or weekly basis. You can create up to 20 email recipients. If you want to send the same recipient a different set of reports, you can enter the same email address more than once, with different reports selected for each. Each entry counts as a unique recipient toward the 20 total.

Note: Duplicate entries are not allowed. A duplicate entry means that the same recipient is set to receive the exact same reports in two different entries, regardless of the day or time. If you have duplicate recipients, make sure that the reports selected in each entry are not an exact match.

If you have one entry in which Recipient A receives the Drive Utilization and Media Integrity reports on Monday, you cannot create another entry to send Recipient A the Drive Utilization and Media Integrity reports on Thursday. Instead, you can create one entry for Recipient A and send the reports every day (select Daily as the day to send the report), or you can change the reports that you are

sending so that they are not the same as the first entry. You can create three entries for Recipient A as follows: 1) send out both reports on Monday; 2) send out Drive Utilization on Thursday; and 3) send out Media Integrity on Thursday (in a different entry). The recipient is the same, but the reports that are sent in each entry are different.

Before the email notifications can be sent, you must configure the library email account.

From the remote UI, select **Manage Library** > **Settings** > **Email Notifications**. Click **Select Action**, select an action, and click **Go**.

You can modify the settings of an existing email notification at any time after it is created. If an email notification is no longer needed, you can delete it.

To save or email data:

1. From the remote UI, go to **Monitor System** > **Advanced Reporting** and select either Drive Utilization or Media Integrity to generate a report.

   For information about generating a report, see "Advanced Reporting reports" on page 1-15
2. Click **Display Report** at the bottom of the page to display the report-viewing screen.
3. Scroll down to the bottom of the report-viewing screen to the **Retrieve the Report Data File** box.
4. Do one of the following actions:
   a. To save the report data as a .csv file, click **Save**.
   b. To email the report data as a .csv file, type the name of a recipient in the empty field next to the **Email** button, then click **Email**.

Each email notification includes an optional comment text box that you can use to enter information for the recipient about the library, reports, and logs. This information displays in the body of the email.

Capacity Expansion (Feature code 1640)

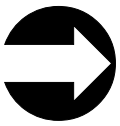
At any time, the Capacity Expansion feature (Feature code 1640) allows you to enable the unused storage slots within a library with a firmware license key.

The TS3310 tape library Model L5B control module includes license key enablement for 82 total cartridges, thus enabling all cartridge slots in the control module and approximately one half the capacity of an added expansion module. To enable the remaining cartridge storage slots, you must purchase Capacity Expansion feature #1640 for each expansion module you want to fully enable. For example, one Capacity Expansion feature #1640 is required to totally access and enable all available cartridge slots in a 14U configured library (one control module and one expansion module). Two Capacity Expansion features #1640 are required to totally access and enable all available cartridge slots in a 23U configured library (one control module and two expansion modules).

To see your library 's current configuration:

- From the Operator Panel: view the **Capacity View** home icon.
- From the Web User Interface: **Monitor System** > **System Summary**

To enter a Capacity Expansion license key:



From the Operator Panel: **Setup** > **License**

From the Web User Interface: **Manage Library** > **Settings** > **Feature Licenses**

When the license key is entered, the total number of available slots in the library increases. To verify that the number of slots did increase:

- From the Operator Panel, view the Capacity View home screen.
- From the Web User Interface: **Monitor System** > **System Summary**

Table 1-5. Licensable cartridge slots (storage and I/O) per model

Library Configuration	Number of Available I/O Station Slots*	Number of Accessible Storage Slots	Total Slots**	Capacity Expansion License Keys
5U library (control module)	6	30	36	no license key required
14U library (control module + 9U expansion module)	6/12/18	76/70/ 64	82	no license key
	6/12/18	122/116/110	128	1 license key that is required to enable the full capacity of a 14U library
23U library (control module + 2 9U expansion modules)	6/12/18/24/ 30	122/116/110/ 104/98	128	no license key
	6/12/18/24/ 30	168/162/156/ 150/144	174	each license key enables full capacity of one 9U expansion module
	6/12/18/24/ 30	212/206/200/ 194/188	218	2 license keys that are required to enable the full capacity of a 23U library

Table 1-5. Licensable cartridge slots (storage and I/O) per model (continued)

Library Configuration	Number of Available I/O Station Slots*	Number of Accessible Storage Slots	Total Slots**	Capacity Expansion License Keys
32U library (control module + 3 9U expansion modules)	6/12/18/24/30/36/42	168/162/156/150 144/138/132	174	no license key
	6/12/18/24/30/36/42	212/206/200/194 188/182/176	220	each license key enables full capacity of one 9U expansion module
	6/12/18/24/30/36/42	260/254/248/242 236/230/124	266	2 license keys enable an extra 46 slots on each of two 9U expansion modules
	6/12/18/24/30/36/42	304/298/292/286 280/274/268	310	3 license keys that are required to enable the full capacity of a 32U library
41U library (control module + 4 9U expansion modules)	6/12/18/24/30/36/42/48/54	212/206/200/194 188/182/176/170/164	220	no license key
	6/12/18/24/30/36/42/48/54	260/254/248/242 236/230/224/218/212	266	each license key enables full capacity of one 9U expansion module
	6/12/18/24/30/36/42/48/54	304/298/292/286 280/274/268/262/256	312	2 license keys enable an extra 46 slots on each of two 9U expansion modules
	6/12/18/24/30/36/42/48/54	352/346/340/334 328/322/316/310/304	358	3 license keys enable an extra 46 slots on each of three 9U expansion modules
	6/12/18/24/30/36/42/48/54	396/390/384/378 372/366/360/354/348	402	4 license keys that are required to enable the full capacity of a 41U library

*The I/O station in the 9U expansion module, contains 12 slots that can be configured as either I/O or storage slots. If the 9U expansion module I/O slots are configured as I/O, the control module slots are configured as storage slots.

**The number of available I/O and storage slots that are listed in the table are adjusted for the unusable slots in each configuration that are not accessible because of space restrictions that limit the movement of the picker. The M2 picker provides an extra 5 or 7 slots, depending upon the library configuration and the number of Capacity Expansion license keys purchased.

Path failover (Feature code 1682)

The path failover feature includes license keys for activating control path failover and data path failover. Path failover is a combination of two previous features: Control path failover (key that is entered at the library user interface) and data path failover (key that is entered at the device driver interface). A single activation key that is entered at the library user interface now activates both features, with one exception. For LTO Ultrium 3 drives with firmware level 73P5 or lower, the device driver interface data path failover key activation is still required. The path failover feature is available on select drives.

Control path failover

A control path is a logical path into the library through which a server sends standard SCSI Medium Changer commands to control the logical library. More control paths reduce the possibility that failure in one control path causes the entire library to be unavailable. Use of the control path failover feature further reduces that possibility. For information, see "Multiple control paths" on page 2-3).

Data path failover

Data path failover is designed to provide a failover mechanism in the IBM device driver, which enables you to configure multiple redundant paths in a SAN environment. In case of a path or component failure, the failover mechanism is designed to automatically provide error recovery to retry the current operation with an alternate, pre-configured path without stopping the current job. This feature allows flexibility in SAN configuration, availability, and management. For information, see "Multiple data paths for data path failover" on page 2-3.

Encryption (Feature code 5900)

The TS3310 library supports host encryption on LTO Ultrium 6 Fibre Channel drives when used with LTO Ultrium 6 or LTO Ultrium 5 data cartridges. The TS3310 library supports host encryption on LTO Ultrium 4 Fibre Channel and SAS drives when used with LTO Ultrium 4 data cartridges. The TS3310 library supports three configurations for establishing encryption policy and providing encryption keys to the drive:

- Application Managed Encryption (AME). Encryption policies and keys are established and provided by the host application. AME is a standard feature for all Ultrium 4, Ultrium 5 and Ultrium 6 drives in the TS3310 library. Since the application manages the encryption keys, volumes that are written and encrypted using the AME method can be read only by the same application that wrote them.
- System Managed Encryption (SME). SME encryption key generation and management is completed by the IBM Encryption Key Manager (EKM), a Java application that runs on a system-attached host. SME policies are established by enabling the SME capability on one or more instances of the IBM device driver, which is also used as a proxy between a key server and the drive for providing encryption keys to the drive. This encryption configuration is transparent to the host application. SME requires the Transparent LTO Encryption license key (Feature code 5900).
- Library Managed Encryption (LME). LME encryption key generation and management is completed by the IBM Encryption Key Manager (EKM), a Java application that runs on a library-attached host. LME policies are established by the library, which can also be used as a proxy between a key server and the drive for providing encryption keys to the drive. This encryption configuration

is transparent to the host application. LME requires the Transparent LTO Encryption license key (Feature code 5900).

For details on testing the configuration path for LME enabled libraries, see "Key path diagnostic tests" on page 8-20.

System-managed tape encryption and library-managed tape encryption interoperate with one another. Therefore, a tape encrypted using SME can be decrypted with LME, and vice versa, provided they both have access to the same keys and certificates.

Encryption Key Management (EKM) is a Java software program that assists encryption-enabled tape drives in generating, protecting, storing, and maintaining encryption keys that are used to encrypt information that is written to, and decrypt information that is read from, tape media. You must supply a server or servers on which to install EKM. It is recommended that you use both a primary and secondary EKM server.

For information on how to install, configure, and use the EKM, see the *IBM Encryption Key Manager component for the Java platform, Introduction, Planning, and User 's Guide GA76-0418*, and the *IBM Encryption Key Manager component for the Java platform, Quick Start Guide for LTO Ultrium 4 GA76-0420,* which are both available for download at: http://www-1.ibm.com/support/docview.wss?uid=ssg1S4000504.

For information on how to install, configure, and use the Tivoli® Key Lifecycle Manager (TKM), see the *IBM Tivoli Key Lifecycle Manager Quick Start Guide (GI11-8738)* and *IBM Tivoli Key Lifecycle Manager Installation and Configuration Guide (SC23-9977)*.

IBM Tivoli® Key Lifecycle Manager V1.0 (English) publications can be downloaded from the website: http://www.ibm.com/software/tivoli/library.

Library & drive code update (Feature code 0500)

Order feature code 0500, Library and drive code update, if you would like an IBM service representative sent to your location to update your library and drive firmware.

Location coordinates

A numbering system is used to identify components of the library. The library location coordinates contain the following digits: [Module],[Column],[Slot]. The figure illustrates how a library with a control module and an expansion module are numbered.

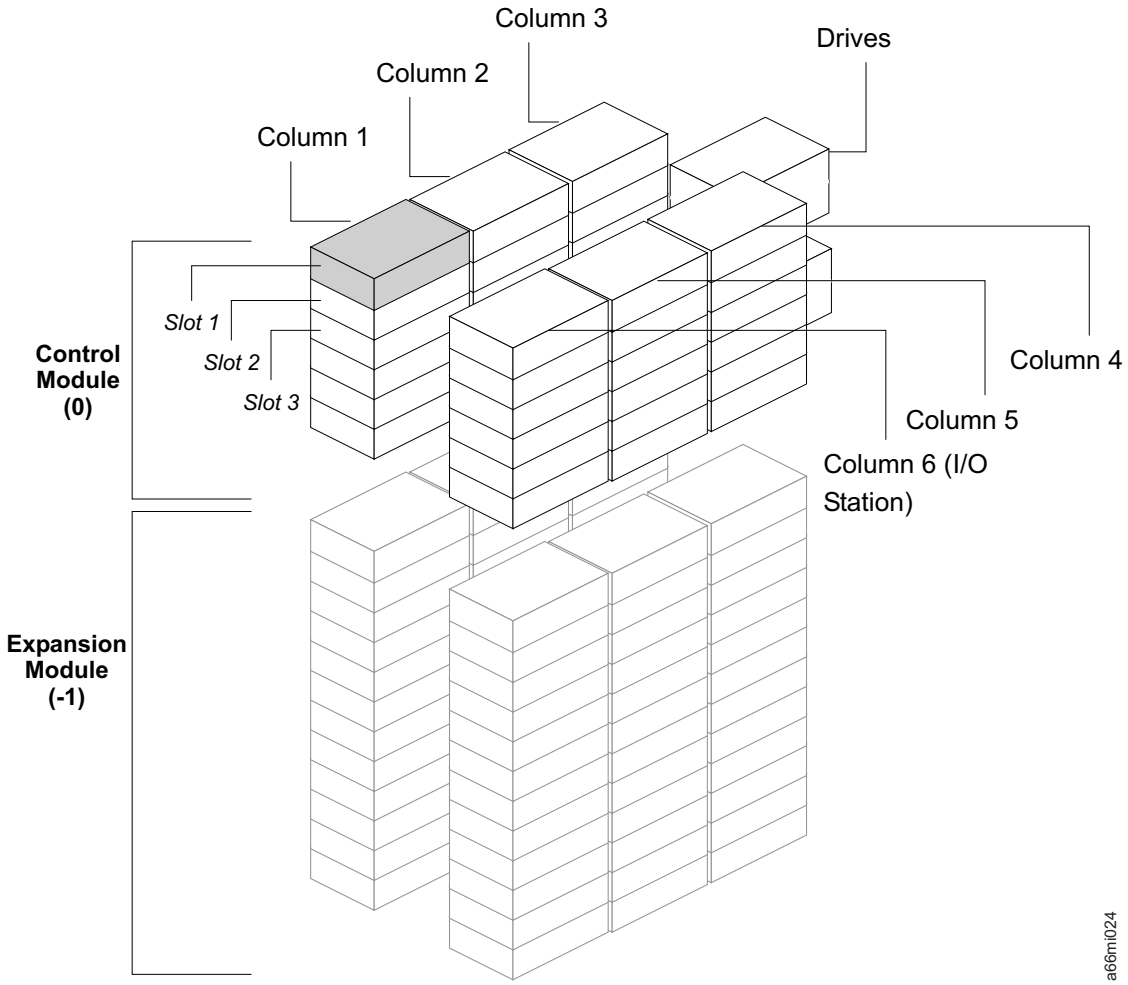


Figure 1-12. Library location coordinates

The module digit uses a zero-based numbering system. The control module is labeled as 0 (zero). The front, left-most column in the module is labeled 1. The top slot in each column is labeled 1. For information, refer to the sections that follow.

Modules

Library modules are represented by the first digit of a library coordinate. Modules are identified relative to the control module (CM). The CM is number 0. Modules that are stacked above the CM are addressed with positive integer digits, depending on their position above the CM. For example, the expansion module that is stacked directly above the CM is number 1. The expansion module that is stacked directly above module 1 is number 2, and so on.The module that is stacked below the CM is numbered with a negative integer, depending on its relative position to the CM. The expansion module directly below the CM is number -1. If an expansion module is installed above the CM, it is numbered +1.The expansion module that is stacked directly below module -1 is number -2, and so on.

Columns

A storage column is a group of slots that are arranged vertically in the library. Columns are represented by the second digit of a library coordinate. Columns are identified relative to the front left of the library. The column in the front left of the

library is number 1. The column numbering continues around the library in a clockwise direction. The I/O station column is always number 6.

Slots

Fixed storage slots are represented by the third digit of the library location coordinate. Slots are numbered from top to bottom within each column, starting with 1 at the top of the column.

Drives

Drives are addressed by module and drive bay within a module. The drive bays within a module are numbered from top to bottom. A one-based numbering system is used. The top drive bay is drive bay 1. A full address of a drive is of the form [Module, Drive Bay]. Examples: [0,1], [-1,2].

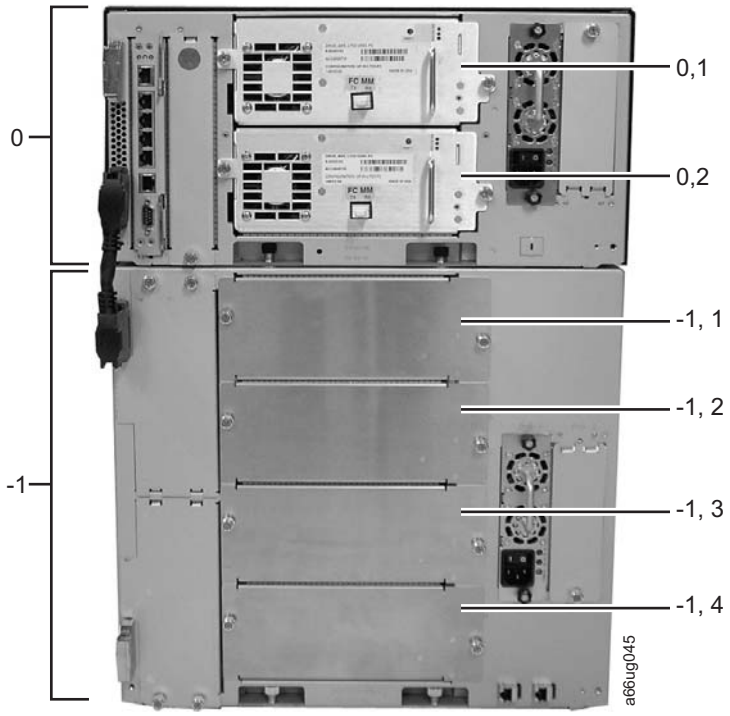


Figure 1-13. Drive location coordinates

Power supplies

Power supplies are addressed as [Module, PS#], where PS# is 1 for the left supply and 2 for the right, as viewed from the rear of the library.

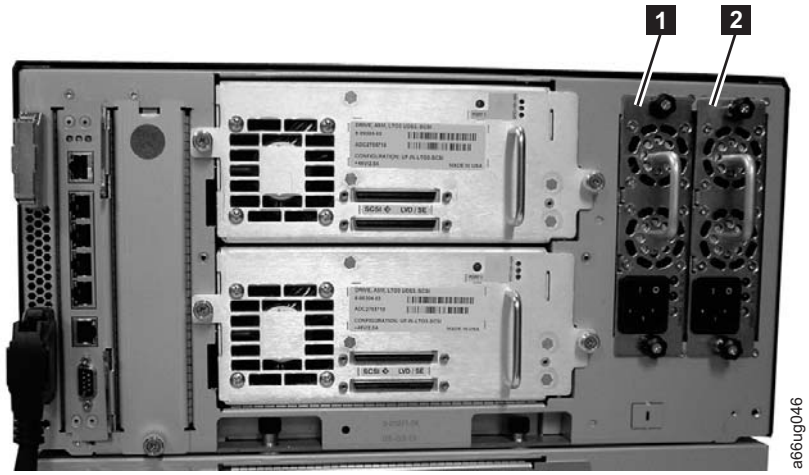


Figure 1-14. Power supply location coordinates

1	0, 1 (PS1 primary power supply in a control module)	2	0, 2 (PS2 redundant power supply in a control module)

Data cartridges

The different generations of IBM TotalStorage Ultrium data cartridges are identified by color:

- The Ultrium 6 data cartridge is black
- The Ultrium 6 WORM data cartridge is black and silver gray
- The Ultrium 5 data cartridge is burgundy
- The Ultrium 5 WORM data cartridge is burgundy and silver gray
- The Ultrium 4 data cartridge is green
- The Ultrium 4 WORM data cartridge is green and silver gray
- The Ultrium 3 data cartridge is slate blue
- The Ultrium 3 WORM data cartridge is slate blue and silver gray
- The Ultrium 2 data cartridge is purple
- The Ultrium 1 data cartridge is black

All generations contain 1/2-inch, dual-coat, metal-particle tape.

Note:

You can order tape cartridges with the bar code labels included, or you can order custom labels. To obtain tape cartridges and bar code labels, see Table 9-7 on page 9-14.

Table 1-6. Drive and cartridge properties

Generation	Drive			Cartridge	
	Host Interface	Sustained native data transfer rate	Types	Physical Capacity	Types

Table 1-6. Drive and cartridge properties (continued)

Generation	Drive			Cartridge	
LTO6	8 Gbps dual-port Fibre Channel	160 MB/s	• Fibre Channel	• 2500 GB native • 6250 GB with 2.5:1 compression	• data • Rewritable • WORM
LTO5	8 Gbps dual-port Fibre Channel	140 MB/s	• Fibre Channel	• 1500 GB native • 3000 GB with 2:1 compression	• data • Rewritable • WORM
LTO4	• 4 Gbps single-port Fibre Channel • 3 Gbps dual-port SAS	120 MB/s	• Fibre Channel • SAS	• 800 GB native • 1600 GB with 2:1 compression	• data • Rewritable • WORM
LTO3	• 4 Gbps single-port Fibre Channel • Ultrium160 SCSI	80 MB/s	• Fibre Channel • SCSI	• 400 GB native • 800 MB with 2:1 compression	• data • Rewritable • WORM

The native data capacity of Ultrium data cartridges is as follows:

- The Ultrium 6 cartridge has a native data capacity of 2500 GB (6250 GB at 2.5:1 compression)
- The Ultrium 5 cartridge has a native data capacity of 1500 GB (3000 GB at 2:1 compression)
- The Ultrium 4 cartridge has a native data capacity of 800 GB (1600 GB at 2:1 compression)
- The Ultrium 3 cartridge has a native data capacity of 400 GB (800 GB at 2:1 compression).
- The Ultrium 2 cartridge has a native data capacity of 200 GB (400 GB at 2:1 compression).
- The Ultrium 1 cartridge has a native data capacity of 100 GB (200 GB at 2:1 compression).

When tape in the cartridges is processed, Ultrium tape drives use a linear, serpentine recording format.

- The Ultrium 6 cartridge stores data on 2176 tracks, 16 tracks at a time
- The Ultrium 5 cartridge stores data on 1280 tracks, 16 tracks at a time
- The Ultrium 4 cartridge stores data on 896 tracks, 16 tracks at a time.
- The Ultrium 3 cartridge stores data on 704 tracks, 16 tracks at a time.
- The Ultrium 2 cartridge stores data on 512 tracks, 8 tracks at a time.
- The Ultrium 1 cartridge stores data on 384 tracks, 8 tracks at a time.

The first set of tracks (16 for Ultrium 6, 5, 4 and 3; eight for Ultrium 2 and 1) is written from near the beginning of the tape to near the end of the tape. The head then repositions to the next set of tracks for the return pass. This process continues until all tracks are written and the cartridge is full, or until all data is written.

Figure 1-15 shows the IBM TotalStorage LTO Ultrium 800 GB data cartridge and its components. All LTO family data cartridges are similar.

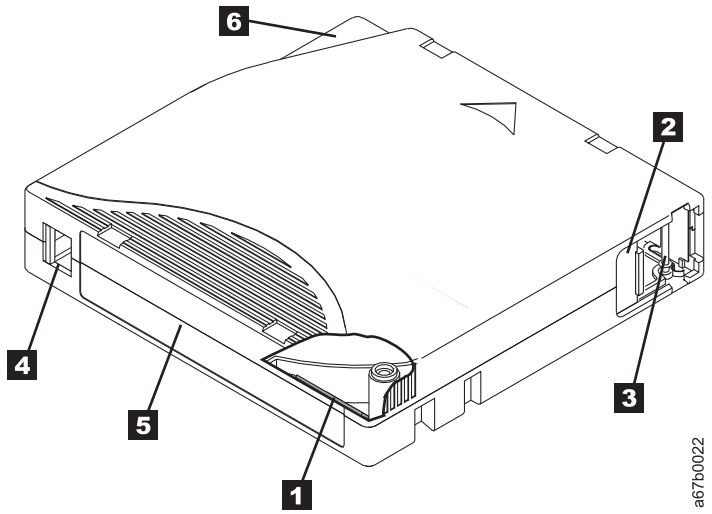


Figure 1-15. Ultrium cartridge

1	Linear Tape-Open cartridge Memory (LTO-CM) chip	4	Write-protect switch
2	cartridge door	5	Label area
3	Leader pin	6	Insertion guide

All generations of the IBM LTO Ultrium data cartridge contain a Linear Tape-Open cartridge Memory (LTO-CM) chip in the cartridge (1 in Figure 1-15). The cartridge memory chip contains information about the cartridge and the tape, such as the name of the manufacturer that created the tape, and statistical performance and usage information (such as number of loads/unloads). The CM reader uses a radio-frequency interface to read this information when the cartridge is loaded into the drive. The cartridge statistics are updated just before the cartridge is unloaded.

The cartridge door (2 in Figure 1-15) protects the tape from contamination when the cartridge is out of the drive. Behind the door, the tape is attached to a leader pin (3 in Figure 1-15). When the cartridge is inserted into the drive, a threading mechanism pulls the pin (and tape) out of the cartridge, across the drive head, and onto a non-removable take-up reel. The head can then read or write data from or to the tape.

The write-protect switch (4 in Figure 1-15) prevents data from being written to the tape cartridge. For more information, see “Write-protect switch” on page 9-3.

The label area (5 in Figure 1-15) provides a location to place a label. For information, see “Bar code labels” on page 9-6.

The insertion guide (6 in Figure 1-15 on page 1-31) is a large, notched area that prevents the cartridge from being inserted incorrectly.

Generations 3, 4, 5, and 6 of the LTO Ultrium data cartridge has a nominal cartridge life of 20,000 (20k) load and unload cycles. Generation 2 has a nominal cartridge life of 10,000 (10k) load and unload cycles. Generation 1 of the LTO Ultrium data cartridge has a nominal cartridge life of 5000 (5k) load and unload cycles.

Environmental and shipping specifications for tape cartridges

Before you use a tape cartridge, acclimate it to the operating environment for 24 hours or the time necessary to prevent condensation in the drive (the time varies, depending on the environmental extremes to which the cartridge was exposed).

The best storage container for the cartridges (until they are opened) is the original shipping container. The plastic wrapping prevents dirt from accumulating on the cartridges and partially protects them from humidity changes.

When you ship a cartridge, place it in its jewel case or in a sealed, moisture-proof bag to protect it from moisture, contaminants, and physical damage. Ship the cartridge in a shipping container that has enough packing material to cushion the cartridge and prevent it from moving within the container.

The table gives the environment for operating, storing, and shipping LTO Ultrium tape cartridges.

Table 1-7. Environment for operating, storing, and shipping the LTO Ultrium tape cartridge

	Environmental Specifications			
Environmental Factor	**Operating**	**Operational Storage**[1]	**Archival Storage**[2]	**Shipping**
Temperature	10 - 45°C (50 - 113°F)	16 - 32°C (61 - 90°F)	16 - 25°C (61 - 77°F)	-23 to 49°C (-9 to 120°F)
Relative humidity (non-condensing)	10 - 80%	20 - 80%	20 - 50%	5 - 80%
Maximum wet bulb temperature	26°C(79°F)	26°C(79°F)	26°C(79°F)	26°C(79°F)

Note:

1. The short term or operational storage environment is for storage durations of up to six months.
2. The long term or archival storage environment is for durations of six months up to 10 years.

Multi-path architecture

Storage area network (SAN)-ready multi-path architecture allows homogeneous or heterogeneous open systems applications to share the library 's robotics without middleware or a dedicated server (host) acting as a library manager. Multi-path architecture is compliant with these attachment interfaces:

- Ultra160 SCSI
- Fibre Channel
- SAS (Serial Attached SCSI)

The library is certified for SAN solutions (such as LAN-free backup). LAN-free drive sharing is not available on SAS drives.

Multi-path architecture allows more control paths and data paths to be configured for any one logical library. For information, see “Multiple control paths” on page 2-3 and “Multiple data paths for data path failover” on page 2-3.

Lightweight Directory Access Protocol (LDAP)

Local authentication control is managed on the library. An administrator sets up accounts and privileges on the library. To use local authentication, a user must enter a local user name and password. Remote authentication is managed by an LDAP server. Enabling LDAP allows existing user accounts that reside on an LDAP server to be integrated into the library 's current user account management subsystem. User account information is centralized and shared by different applications, simplifying user account management tasks.

Administrative users can configure and enable LDAP. Once LDAP is enabled, users can access the library with either LDAP or local authentication. To use LDAP authentication, a user must enter a directory service user name and password and specify an LDAP domain. To use local authentication, a user must enter only a local user name and password.

Administrative users can add, delete, and modify only local user account information. The library web client and operator panel do not allow you to create, modify, or delete user account information about an LDAP server. This procedure must be done by the directory service provider. Refer to your server documentation for information about LDAP user accounts.

LDAP server guidelines

The library supports user account information in the schema that is defined by RFC 2307. For LDAP users with user privileges, access to library logical libraries is determined by group assignment on the LDAP server. Groups must be created on the LDAP server with names that correspond to the library logical library names. Users with user privileges must be assigned to these groups on the LDAP server to have access to the corresponding logical libraries on the library. LDAP users with administrative privileges have access to all logical libraries and administrative functions and do not need to be assigned to logical library-related groups on the LDAP server. The following groups must be created on the LDAP server to enable remote login on the library:

- Library user group - Assign users to this group who need user-privilege access to the library. Enter the name of this group in the **User Group** field on the **Manage Access** > **Authentication Settings** screen on the library web client (see “Modifying authentication settings” on page 8-8).
- Partition groups - For LDAP users with user privileges, access to library partitions is determined by group assignment on the LDAP server. Groups must be created on the LDAP server with names that match the library partition names (names must match but are not case-sensitive). Users with user privileges must be assigned to these groups on the LDAP server to have access to the corresponding partitions on the library.
- Library superuser group - Assign users to this group who need superuser-privilege access to the library. LDAP users with superuser privileges have access to all partitions and superuser functions and do not need to be assigned to partition-related groups on the LDAP server. Enter the name of this group in the **Superuser Group** field on the **Manage Access** > **Authentication Settings** screen on the library web client (see “Modifying authentication settings” on page 8-8).

- Library admin group - Assign users to this group who need administrator-privilege access to the library. LDAP users with administrator privileges have access to all partitions and administrator functions and do not need to be assigned to partition-related groups on the LDAP server. Enter the name of this group in the **Administrator Group** field on the **Manage Access** > **Authentication Settings** screen on the library web client (see "Modifying authentication settings" on page 8-8).

You must have at least one user that is assigned to both the Library User Group and the Library Admin Group on the LDAP server to test the LDAP settings on the library. Since most normal users are not members of both these groups, you might need to create a special or temporary user specifically for this purpose.

Kerberos

Kerberos Authentication is a standard (RFC 1510) third-party authentication protocol that provides end-to-end security for distributed computing environments.

Note: The web client login screen gives the user a choice between using local authentication or LDAP authentication. If LDAP authentication is selected, the user is prompted for the LDAP domain.

The Operator Panel login screen gives the user the choice between using Local authentication and Remote authentication when LDAP access is enabled. If LDAP access is disabled, the Remote authentication option does not appear on the login screen.

With Local authentication the user name and password are stored on the library. With LDAP authentication the user name and password are stored on a server.

Kerberos requires LDAP information, but LDAP users are not required to use Kerberos. To configure the authentication settings, see "Modifying authentication settings" on page 8-8.

Specifications

Table 1-8. Physical specifications for the library

Physical Specification	Measurement	
	5U control module	9U expansion module
Width	44.45 cm (17.5 in.)	44.45 cm (17.5 in.)
Depth	76.83 cm (30.25 in.)	76.83 cm (30.25 in.)
Height	21.87 cm (8.61 in.)	40.0 cm (15.75 in.)

Table 1-9. Library component weight

Component	Weight
Drive	4.082 kg (9.0 lbs.)
Power supply	1.814 kg (4.0 lbs.)
Robotics	2.041 kg (4.5 lbs.)
5U control module chassis (empty)	21.55 kg (47.5 lbs.)
9U expansion module chassis (empty)	29.48 kg (65.0 lbs.)

Table 1-10. Power specifications for a 5U Control Module and 9U Expansion Module

Power Specification	Measurement			
	5U control module		9U expansion module	
Voltage	100 - 127 Vac.	200-240 Vac.	100 - 127 Vac.	200-240 Vac.
Frequency	50 - 60 Hz	50 - 60 Hz	50 - 60 Hz	50 - 60 Hz
Current	2.0 A	1.0 A	2.0 A	1.0 A
Inrush current	50 A	100 A	50 A	100 A
Power	200 W	200 W	200 W	200 W
kVA	0.2	0.2	0.2	0.2
kBtu/hr	0.68	0.68	0.68	0.68
Note: 5U control module measurements include two tape drives. 9U expansion module measurements include four tape drives. Measurements were taken while the picker/robot assembly was randomly moving and all of the drives were reading and writing.				

Table 1-11. Other specifications for the library

Specification	Measurement
Maximum altitude	2500 m (8202 ft) for operating and storage

Table 1-12. Environmental specifications for the library

Environmental Factor	Operating (see Note)	Storage	Shipping
Drive temperature	10 - 38°C (50 - 100°F)	10 - 43°C (50 to 109.4°F)	-40 to 60°C (-40 to 140°F)
Heat output	542 W (483 Cal/Hr)	Not applicable	Not applicable
Relative humidity	20 - 80%	10 - 90%	10 - 90%
Maximum wet bulb temperature	26°C (79°F) max.	27°C (80.6°F) max.	29°C (84.2°F) max.
Note: The operating environment of the library must not conflict with the media storage requirements (see the section about media storage requirements). The library is capable of operating at elevated temperatures for an extended time. However, the temperature can shorten the useful life of media that is stored in the library. If media is stored in the library for more than 10 hours, the storage temperature requirements for media must be met. It must be assumed that media stored in the library is 2 degrees above ambient temperature when the library is powered ON.			

Product environment

The library is designed to operate in a general business environment.

The library meets the acoustical requirements for general business area category 2D. Category 2D states that the library must be installed a minimum of 4 m (13 ft.) from a permanent work station.

To allow for service access, install the library a minimum of 0.9 m (3 ft.) from all obstacles.

The library is a precision computer peripheral device. To ensure maximum longevity of your library, locate the library away from dust, dirt, and airborne particulates:

- Keep the library away from high-traffic areas, especially if the floor is carpeted. Carpeting harbors dust and walking on the carpet can cause the carpet fibers and the dust to become airborne.
- Keep the library out of printer/copier rooms because of toner and paper dust. Also, do not store paper supplies next to the library.
- Keep the library away from moving air caused by doorways, open windows, fans, and air conditioners.

Ensure that the machine covers are always kept closed to minimize any contamination from airborne particles.

Supported servers, operating systems, and software

The library is supported by a wide variety of servers (hosts), operating systems, and adapters. These attachments can change throughout the lifecycle of the product.

To determine the latest supported attachments, visit the web at http://www.ibm.com/storage/lto, and look at the **Interoperability Matrix**.

Supported device drivers

IBM maintains the latest levels of device drivers and driver documentation for the library on the Internet. You can use one of the following procedures to access this material.

Note: If you do not have Internet access and you need information about device drivers, contact your sales representative.

- Open a browser, then go to one of these websites.
  - http://www.ibm.com/storage/lto
  - ftp://ftp.software.ibm.com/storage/devdrvr
- With File Transfer Protocol (FTP), enter the following specifications:
  - FTP site: `ftp.software.ibm.com`
  - IP Addr: `207.25.253.26`
  - User ID: `anonymous`
  - Password: (use your current email address)
  - Directory: `/storage/devdrvr`

IBM provides Portable Document Format (.pdf) and PostScript (.ps) versions of its device driver documentation in the `/storage/devdrvr/Doc` directory:

- `IBM_tape_IUG.pdf` contains the current version of the *IBM Tape Device Drivers Installation and User 's Guide*.
- `IBM_tape_PROGREF.pdf` contains the current version of the *IBM Tape Device Drivers Programming Reference*.

A list of device drivers for each supported server displays at `/storage/devdrvr/` in the following directories:

- AIX
- HP-UX
- Linux
- Solaris

- Windows

Note: The device driver for the AS/400® server and iSeries® server is included in the OS/400® operating system.

For information about device drivers, refer to any of the preceding directories.

Chapter 2. Installation planning

Installation planning is an important first step in the installation process. By planning the installation, all decisions about the system layout are made before actually handling the hardware. This planning simplifies the installation process.

Important: Make a copy of the Appendix E, "Library configuration form," on page E-1. With this form, make a record of your library 's configuration. Store this form in a safe location and update it any time hardware is added or settings are modified.

Determining the number of logical libraries (partitions)

You can partition the library into as many logical libraries as there are drives in the library. Ultrium 3, Ultrium 4, Ultrium 5 and Ultrium 6 drives are allowed in the same physical and logical libraries. However, you must ensure that the host application supports a mix of Ultrium 3, Ultrium 4, Ultrium 5 and Ultrium 6 drives, and a mix of interface drive types..

Basic guidelines

- Each logical library must contain at least one drive.
- A library configuration of exactly one partition equals the entire physical library.
- The library prevents requests from the server to move media across the boundaries of logical libraries.

Automatically creating partitions

When automatically creating partitions, with the Setup wizard or the automatic partition creation screens on the web client or operator panel, the default number of logical libraries that are created is the number of distinct tape drive interface/vendor combinations of the tape drives that are not currently assigned to a logical library. Previously, you created fewer partitions than the default. Now, the default is the minimum number of partitions you can create. On the Setup wizard, you can also choose to create zero partitions and instead create them later with the web client or operator panel.

Library sharing

The library 's default configuration allows a single application to operate the library through a single control path. Often, however, it is advantageous to be able to share a single library between heterogeneous (dissimilar) or homogeneous (similar) applications. Some applications (and some servers) do not allow for

sharing a library between systems. Configurations can be created that enable the library to process commands from multiple heterogeneous applications (such as an IBM eServer System p application and a Windows NT application) and multiple homogeneous applications (the same application that is run by several pSeries servers).

From the library 's Web User Interface or Operator Panel, the following actions can be completed:

- Configure the library so that it is partitioned into separate logical libraries that independently communicate with separate applications through separate control paths. This configuration requires no special capabilities from the server or application. (For information, see "Multiple logical libraries for library sharing.")
- Configure any single logical library (including the entire physical library) so that it is shared by two or more servers that are running the same application. Depending on the capabilities of the server and application, there are several ways to set up this type of configuration. Three typical ways include
  - Configuring one server (host) to communicate with the library through a single control path; all other servers send requests to that server through a network. This configuration is used by Tivoli Storage Manager (TSM).
  - Configuring all of the servers to communicate with the library through a single, common control path. This configuration is used in high-availability environments such as the IBM High Availability Clustered Microprocessing (HACMP) and the Microsoft Systems Management Server (SMS) and Clustered Server Environments. Multi-initiator configurations are supported only by certain adapters and independent software vendors (ISVs). Check with your ISV.
  - Configuring a single logical library to communicate with multiple servers through multiple control paths. This configuration requires that control paths be added (see "Multiple control paths" on page 2-3). It is used by Backup Recovery and Media Services (BRMS).

Library configuration is not limited to the examples given here. Many configurations are possible, and can be designed according to your business needs. For information, refer to your host application documentation.

Multiple logical libraries for library sharing

Multiple logical libraries are an effective way for the library to simultaneously back up and restore data from heterogeneous applications. For example, the library can be partitioned so that it processes:

- Commands from Application 1 (about Department X) in Logical Library A
- Commands from Application 2 (about Department Y) in Logical Library B
- Commands from Application 3 (about Department Z) in Logical Library C

In this configuration, the storage slots and drives in each logical library are dedicated to that library and are not shared among other libraries. Commands that are issued by the applications travel to the library through three unique control paths. Thus, the data processing for:

- Department X is confined to the storage slots and drives in Logical Library A
- Department Y is confined to the storage slots and drives in Logical Library B
- Department Z is confined to the storage slots and drives in Logical Library C

Multiple control paths

In addition to creating multiple logical libraries, any logical library can be configured to have more than one control path. When extra control paths are configured, more library-sharing configurations and availability options are made possible. Access to the logical library is on a first-come, first-served basis. Each control path for a logical library can accept commands while the library is in use by another control path. By default, a logical library can communicate with the server only through the first LUN-1-enabled drive that is installed in the partition.

Note: Microsoft Windows 2000 and Microsoft Windows 2003 Removable Storage Manager (RSM) does not support multiple control paths within a logical library. IBM recommends that RSM is disabled to use this feature.

To add or remove extra control paths, refer to "Adding a control path drive to a logical library" on page 8-29. For a particular logical library, you can enable as many control paths as there are drives in that logical library.

Multiple control paths for System i, iSeries, and AS/400 attachment

The use of control paths for the System i®, iSeries, and AS/400 servers is unique. In general, every iSeries adapter must recognize the control path that is associated with the drives to which it is connected. For the iSeries and AS/400 servers, one to six drives are supported by LVD and Fibre Channel adapters and the OS/400 5.1, OS/400 5.2, or i5/OS 5.3 operating system.

Multiple control paths for control path failover

To ensure continued processing, the library offers an optional path failover feature (Feature code 1682) that includes the control path failover function and the data path failover function.

The control path failover feature enables the host device driver to resend the command to an alternate control path for the same logical library. With control path failover installed, the alternate control path can include another HBA, SAN, or library control path drive. The device driver initiates error recovery and continues the operation on the alternate control path without interrupting the application. AIX, Linux, Solaris, HP-UX, and Windows hosts are currently supported for this feature.

The path failover license key (Feature code 1682) can be installed by the customer. For information, see "Applying a license key" on page 5-2. For ordering information, see Chapter 13, "Parts list," on page 13-1.

For information about the control path failover feature, see the *IBM Ultrium Device Drivers Installation and User 's Guide*.

Multiple data paths for data path failover

The path failover feature (Feature code 1682) includes the control path failover function and the data path failover function.

Data path failover and Load Balancing functions exclusively support native Fibre Channel tape drives in the library with the IBM device driver. Data path failover is designed to provide a failover mechanism in the IBM device driver for AIX®,

Linux, Solaris, and Windows, which enable multiple redundant paths to be configured in a SAN environment. In the event of a path or component failure, the failover mechanism is designed to automatically provide error recovery to try the current operation again with an alternate, pre-configured path without stopping the current job in progress. This feature allows flexibility in SAN configuration, availability, and management.

When a tape drive device was accessed that was configured with alternate paths across multiple host ports, the IBM device driver for AIX, Linux, and Solaris automatically selects a path through the host bus adapter (HBA) that has the fewest open tape devices and assigns that path to the application. This autonomic self-optimizing capability is called Load Balancing. The dynamic load balancing support is designed to optimize resources for devices that have physical connections to multiple HBAs in the same machine. The device driver is designed to dynamically track the usage on each HBA as applications open and close devices, and balance the number of applications with each HBA in the machine. This procedure can help optimize HBA resources and improve overall performance. Further, data path failover provides autonomic self-healing capabilities similar to control path failover, with transparent failover to an alternate data path in the event of a failure in the primary host-side path.

Data path failover is not available on HP-UX currently.

The data path failover and control path failover features are activated by the path failover license key (Feature code 1682). For information, see "Applying a license key" on page 5-2.

For information, refer to your device driver documentation.

Determining SCSI, Fibre Channel, and SAS IDs

SCSI IDs are required for Ultra160 SCSI drives. Loop IDs are required for Fibre Channel drives. SAS IDs are required for SAS drives.

SCSI drive IDs

Based on its physical position in the library, each Ultra160 SCSI tape drive is assigned a default SCSI ID (from 0 to 15). The first digit in the drive location coordinates indicates the position module, where 0 is the control module. Expansion modules that are installed physically below the control module have negative location coordinates. The modules above the control module are positive. The second digit of the drive location coordinate indicates the number of the drive within each module (1 or 2 for the control module; 1 through 4 for expansion modules). The default SCSI IDs are numbers 3 through 6, and repeat for each expansion module. The table lists an example of the default SCSI IDs for each library component in a 14U library.

Table 2-1. Default SCSI ID for each SCSI drive in a 14U library

Module	Position	Drive Location Coordinate	Default SCSI IDs
Control Module	Drive 1	0, 1	2
	Drive 2	0, 2	1

Table 2-1. Default SCSI ID for each SCSI drive in a 14U library (continued)

Module	Position	Drive Location Coordinate	Default SCSI IDs
9U Expansion Module	Drive 3	-1, 1	6
	Drive 4	-1, 2	5
	Drive 5	-1, 3	4
	Drive 6	-1, 4	3

Note: You can change a SCSI ID with the Web User Interface or the Operator Panel.

Fibre Channel drive IDs

Each Fibre Channel Ultrium tape drive in the library must have a Loop ID and corresponding Arbitrated Loop Physical Address (AL_PA) to communicate in a Fibre Channel topology. The table lists the default Loop IDs and AL_PAs for a sample 14U library configuration. Refer to table Table 2-3 to determine the Loop IDs and AL_PA values for libraries larger than 14U.

Table 2-2. Default Loop IDs and their associated AL_PAs for Fibre Channel Drives in a 14U library

Module	Drive Position	Drive Location Coordinate	Default Loop ID	Default AL_PA
Control Module	1	0, 1	0	X'EF'
	2	0, 2	1	X'E8'
9U Expansion Module	3	-1, 1	2	X'E4'
	4	-1, 2	3	X'E2'
	5	-1, 3	4	X'E1'
	6	-1, 4	5	X'E0'
Note: Loop IDs are given in decimal format and AL_PA values are given in hexadecimal format.				

You can change a Loop ID with the library 's operator panel or Web User Interface. With a method called hard addressing, the drive then automatically selects the corresponding AL_PA, which is the identifier that devices use to communicate. Valid Loop ID values range 0 - 125. The higher the number of the Loop ID (and AL_PA), the lower the priority of the device in the loop.

You can also specify Loop IDs that allow the drive to dynamically arbitrate the AL_PA with other Fibre Channel devices on the loop. This method avoids conflicts over the address and is called soft addressing. To dynamically arbitrate the AL_PA, specify a Loop ID of 126 or 127.

For a complete list of Loop IDs and their corresponding AL_PAs, see the table.

Table 2-3. Valid Loop IDs and their associated AL_PAs for Fibre Channel drives in the library

7-bit Loop ID (decimal)	8-bit AL_PA (hexadecimal)		7-bit Loop ID (decimal)	8-bit AL_PA (hexadecimal)		7-bit Loop ID (decimal)	8-bit AL_PA (hexadecimal)
0	X'EF'		43	X'A3'		86	X'4D'
1	X'E8'		44	X'9F'		87	X'4C'
2	X'E4'		45	X'9E'		88	X'4B'

Table 2-3. Valid Loop IDs and their associated AL_PAs for Fibre Channel drives in the library (continued)

7-bit Loop ID (decimal)	8-bit AL_PA (hexadecimal)	7-bit Loop ID (decimal)	8-bit AL_PA (hexadecimal)	7-bit Loop ID (decimal)	8-bit AL_PA (hexadecimal)
3	X'E2'	46	X'9D'	89	X'4A'
4	X'E1'	47	X'9B'	90	X'49'
5	X'E0'	48	X'98'	91	X'47'
6	X'DC'	49	X'97'	92	X'46'
7	X'DA'	50	X'90'	93	X'45'
8	X'D9'	51	X'8F'	94	X'43'
9	X'D6'	52	X'88'	95	X'3C'
10	X'D5'	53	X'84'	96	X'3A'
11	X'D4'	54	X'82'	97	X'39'
12	X'D3'	55	X'81'	98	X'36'
13	X'D2'	56	X'80'	99	X'35'
14	X'D1'	57	X'7C'	100	X'34'
15	X'CE'	58	X'7A'	101	X'33'
16	X'CD'	59	X'79'	102	X'32'
17	X'CC'	60	X'76'	103	X'31'
18	X'CB'	61	X'75'	104	X'2E'
19	X'CA'	62	X'74'	105	X'2D'
20	X'C9'	63	X'73'	106	X'2C'
21	X'C7'	64	X'72'	107	X'2B'
22	X'C6'	65	X'71'	108	X'2A'
23	X'C5'	66	X'6E'	109	X'29'
24	X'C3'	67	X'6D'	110	X'27'
25	X'BC'	68	X'6C'	111	X'26'
26	X'BA'	69	X'6B'	112	X'25'
27	X'B9'	70	X'6A'	113	X'23'
28	X'B6'	71	X'69'	114	X'1F'
29	X'B5'	72	X'67'	115	X'1E'
30	X'B4'	73	X'66'	116	X'1D'
31	X'B3'	74	X'65'	117	X'1B'
32	X'B2'	75	X'63'	118	X'18'
33	X'B1'	76	X'5C'	119	X'17'
34	X'AE'	77	X'5A'	120	X'10'
35	X'AD'	78	X'59'	121	X'0F'
36	X'AC'	79	X'56'	122	X'08'
37	X'AB'	80	X'55'	123	X'04'
38	X'AA'	81	X'54'	124	X'02'
39	X'A9'	82	X'53'	125	X'01'
40	X'A7'	83	X'52'	126	X'00'
41	X'A6'	84	X'51'	127	

Table 2-3. Valid Loop IDs and their associated AL_PAs for Fibre Channel drives in the library (continued)

7-bit Loop ID (decimal)	8-bit AL_PA (hexadecimal)		7-bit Loop ID (decimal)	8-bit AL_PA (hexadecimal)		7-bit Loop ID (decimal)	8-bit AL_PA (hexadecimal)
42	X'A5'		85	X'4E'			

Supported topologies

The Fibre Channel tape drive can be attached in a two-node configuration, either directly to a switch as a public device (switched fabric) or directly to a host bus adapter (HBA) as a private device. It can connect as a public device in a switched fabric topology (through an F_port) or connect with Arbitrated Loop topology (through an L_port or FL_port).

The Fibre Channel tape drive automatically configures to an L_port or an N_port when it boots. The type of port to which it configures depends on whether the drive recognizes the connection as a loop or a point-to-point connection:

- An L_Port supports a Fibre Channel Arbitrated Loop connection to an NL_port or an FL_port.
- An N_Port supports a point-to-point connection to an F_port (for example, a director-class switch) in a switched fabric topology.

Regardless of the port to which you connect the drive, it automatically configures to a public device (through an F_port or FL_port to a switch) or to a private device (through an L_port with direct attachment to a server).

Configuring Fibre Channel host port failover - The current feature implementation does not support arbitrated loop or target/initiator mode. Also, ports on the 4 Gb FC I/O blade that is used for failover must connect to the same SAN fabric.

The table lists the topologies in which the Ultrium Fibre Channel tape drive can operate, the Fibre Channel server connections that are available, and the port through which communication must occur.

Table 2-4. Choosing the port for your topology and Fibre Channel connection

Type of Topology	Type of Fibre Channel Connection to Server	
	Direct Connection(Private)	Switched Fabric(Public)
Fibre Channel Aribitrated Loop (can be Two-Node Arbitrated Loop or Two-Node Switched Fabric Loop; is limited to two nodes)	L_Port	FL_Port
Switched fabric (two nodes)	N/A	F_Port

Worldwide names

Normally, blocks of worldwide name (WWN) addresses are assigned to manufacturers by the IEEE Standards Committee, and are built into devices during manufacture. In the case of the library, however, it assigns worldwide node names and worldwide port names to the drives based on their location in the library. This technique is referred to as persistent worldwide names. Potential drive slots are each assigned a WWN that does not change when a drive is swapped or replaced.

The WWN of the drive is location-dependent and not device-dependent. That is, each time that the drive is reset or powered ON, the library reestablishes the

WWN so that a drive in Slot *x* always keeps the same WWN, even if the drive is replaced. The design of a WWN is such that if a drive needs service or replacement, host parameters do not need to be changed or reconfigured. The library 's configuration can also easily survive a reboot.

SAS drive IDs

SAS drive IDs are based on the worldwide name (WWN) assigned to the drive location in the library. This technique is the same as the Fibre Channel WWN addressing method and is referred to as persistent worldwide names. Potential drive slots are each assigned a WWN that does not change when a drive is swapped or replaced.

The WWN of the drive is location-dependent and not device-dependent. Each time the drive is reset or powered ON, the library reestablishes the WWN so that a drive in Slot *x* always keeps the same WWN, even if the drive is replaced. The design of a WWN is such that if a drive needs service or replacement, host parameters do not need to be changed or reconfigured. The library 's configuration can also easily survive a reboot.

LUN assignments for Ultrium tape drives

The logical unit number (LUN) for the Sequential Access device is always LUN 0 of the drive, and the LUN for the Medium Changer device is always LUN 1 (all other LUNs are invalid addresses). These devices are compatible with the SCSI-3 standard. For information about the SCSI commands for the tape drive and the library, see the *IBM TotalStorage LTO Ultrium Tape Drive SCSI Reference* and the *IBM System Storage TS3310 Tape Library SCSI Reference*.

Note: The Medium Changer ISCS/Loop/SAS ID is the same as the SCSI ID for the control path drive. You can enable more drives to optionally provide Medium Changer (LUN 1) addressing by configuring more than one logical library or by enabling extra control paths (see “Determining the number of logical libraries (partitions)” on page 2-1.

Server attachment

Note: Ensure that all the required or latest available host (server) operating system files and updates (.dll files, PTFs, and so on) are installed and applied.

The library can be attached to servers with

- “SCSI interface”
- “Fibre Channel interface” on page 2-10
- “SAS interface” on page 2-11

SCSI interface

Note: Although the LVD hardware in the library can operate in single-ended (SE) mode, SE operation is not recommended or supported.

The library supports SCSI LVD attachments with SCSI cables with 68-pin, D-connectors. SCSI adapters must be properly terminated.

Before the SCSI cables are installed, inspect all cables for damage. Do not install a cable if it is damaged. Report the damage immediately by contacting your place of purchase.

The maximum allowable length of your bus cabling depends on the type of SCSI bus that you use (LVD).

For a server with an LVD SCSI bus:

- Use a maximum system-to-device cable length of 10 m (33 ft) to attach to the host interface board (SCSI) and one or two daisy-chained drives.
- Use a maximum system-to-device cable length of 5 m (17 ft) to attach to the host interface board (SCSI) and three to six daisy-chained drives.

  Note: For maximum performance, it is recommended to have a maximum of one drive per SCSI bus.
- Use only the maximum system-to-device cable length of 25 m (82 ft) to attach directly to one device (a point to point interconnection).

Physical characteristics of the SCSI interface

The library operates as a set of SCSI-3 devices. The Ultrium tape drives attach to servers with an LVD Ultra160 SCSI interface. Each SCSI drive sled uses shielded, HD68-pin connectors, and can attach directly to a 2-byte-wide SCSI cable.

Any combination of up to two initiators (servers) and up to four targets (devices) is allowed on a single SCSI bus if the following conditions are met.

- The SCSI bus is terminated properly at each end
- Cable restrictions are followed according to the SCSI-3 specification

Under the SCSI-3 protocol, this type of attachment allows cable lengths of up to 25 m (81 ft) with the appropriate cable and terminator. The table gives the maximum bus length between terminators for the LVD interface.

Table 2-5. Maximum bus length between terminators

Type of Interconnection	Maximum Bus Length Between Terminators (in meters)
Point-to-point (1 server and 1 drive)	25
Multi-drop/daisy-chain (1 server and multiple drives)	12 (LVD)

For maximum performance, the quantity of tape drives that you can attach to one SCSI bus must be limited to 2, therefore multiple SCSI buses can be required (see "Multiple SCSI buses"). IBM Ultrium tape drives must be the only target devices that are active on the bus.

Multiple SCSI buses

The library has two SCSI connectors for each tape drive in the library. Each drive can be daisy-chained with a SCSI bus jumper that is included with each tape drive.

Removal of any jumpers creates a SCSI bus for each drive that is installed in your library for attachment to multiple servers or to multiple SCSI adapters on one server. Multiple SCSI buses can be required for maximum performance, depending on the application and data compression ratio. Note, however, that library (Medium Changer) control is required on at least one SCSI bus.

The Medium Changer device is required to be addressed with LUN 1 of the lowest-numbered drive position of each logical library. The Medium Changer device can be addressed with LUN 1 of other drives in any logical library.

Any bus that contains a Medium Changer device with LUN 1 of a drive is referred to as a control and data path. Any other bus is referred to as a data path. For information about control paths, see “Multiple control paths” on page 2-3.

Terminating the bus

The SCSI bus and all of the wires in the SCSI cable must be properly terminated according to the SCSI standard.

You can plug an external terminator into one of the SCSI connectors. A terminator must be installed on the last device on each end of a string of multiple devices. A terminator is included with each Ultrium tape drive.

SCSI hosts and adapters

The library is supported by a wide variety of servers (hosts), operating systems, and adapters. These attachments can change throughout the product 's lifecycle. To determine the latest supported attachments, visit the web at http://www.ibm.com/storage/lto. Or, contact your IBM sales representative.

Fibre Channel interface

Ultrium Fibre Channel tape drives use LC duplex fiber optics cables.

The maximum distances that the library supports on a Fibre Channel link is determined by the link speed, the type of fiber (50 micron or 62.5 micron), and the device to which the library is attached.

If the library attaches to an HBA, refer to the distances that are supported by the HBA. If the library attaches to a switch, the supported distances are

- For a 50-micron cable:
  - 1 Gbit link speed = up to 500 m (1640 ft)
  - 2 Gbit link speed = up to 300 m (984 ft)
  - 4 Gbit link speed = up to 150 m (492 ft)
  - 8 Gbit link speed = up to 50 m (164 ft)
- For a 62.5-micron cable:
  - 1 Gbit link speed = up to 175 m (574 ft)
  - 2 Gbit link speed = up to 150 m (492 ft)
  - 4 Gbit link speed = up to 70 m (232 ft)
  - 8 Gbit link speed = up to 21 m (68 ft)

The library uses 50-micron cables internally. Therefore, you must use a 50-micron cable to attach to the library 's port. To attach to a 62.5-micron SAN, you must attach the 50-micron cable to an active port, such as a port on a switch.

Zoning to isolate devices and enhance security

For security reasons, it is important to limit the devices that a server or servers can recognize or access. Also, some performance configurations and SAN configurations can result in a device seen multiple times from the same server. For example, if you have two HBAs from the same server that is connected to an

Ultrium tape drive in the library, the drive is detected and displays as two logical devices. That is, there are two special files for one physical device. Zoning can address these issues.

Zoning allows you to partition your SAN into logical groupings of devices so that each group is isolated from the other and can access only the devices in its own group. Two types of zoning exist: hardware zoning and software zoning. Hardware zoning is based on physical fabric port number. Software zoning is defined with WWNN or WWPN. While zoning can be reconfigured without causing an outage, some zoning configurations can become complicated. The advantage of the library 's WWNN implementation is that you can avoid the exposure of introducing zoning errors. You do not have to change the zoning configuration if a drive needs service or replacement.

Attention: It is recommended that tape storage devices are connected on a separate HBA from disk storage devices to avoid potential configuration incompatibilities.

Persistent binding to ensure SCSI ID assignment

When a server is booted, devices are discovered and assigned SCSI target and LUN IDs. It is possible for these SCSI assignments to change between boots. Some operating systems do not guarantee that devices are always allocated the same SCSI target ID after rebooting. Also, some software depends on this association, so you do not want it to change. The issue of SCSI ID assignment is addressed by persistent binding.

Persistent binding is an HBA function that allows a subset of discovered targets to be bound between a server and device. Implemented by a WWNN or WWPN, persistent binding causes a tape drive 's WWN to be bound to a specific SCSI target ID. After a configuration is set, it survives reboots and any hardware configuration changes because the information is preserved. If a drive must be replaced, the new drive assumes the WWNN of the old drive. The WWNN for the drive is location-dependent within the library. Because the WWNN does not change, persistent binding does not need to be changed which would cause an outage.

Fibre Channel hosts and adapters

The library is supported by a wide variety of servers (hosts), operating systems, and adapters. These attachments can change throughout the product 's lifecycle. To determine the latest supported attachments, visit the web at http://www.ibm.com/storage/lto.

Sharing on a storage area network

With storage area network (SAN) components, the possibilities for connecting multiple systems and multiple drives increased. Not all software and systems are designed to share drives. Before you install a drive that allows two systems to share it, check that the systems and their software support sharing. If your software does not support sharing, Fibre Channel switches have a zoning capability to form a SAN partition. For systems that do not cooperate, use zoning to prevent the systems from sharing the drive. You can remove zoned partitions as you upgrade software and system levels.

SAS interface

The Ultrium 4 SAS drives are dual port. Each SAS link is point-to-point so a maximum of two hosts can share a dual-port SAS tape drive. Sharing between two

hosts is limited to active/passive cluster failover. LAN-free drive sharing is not supported. SAS expanders are not supported.

The SAS interface uses Serial SCSI Protocol (SSP) and SCSI commands. The full-duplex signal transmission protocol supports data transfer speeds up to 3 Gbps. Actual speed is auto-negotiated by the SAS drive.

SAS cables and connectors

The Ultrium 4 SAS drive sleds have dual-port SFF-8088 mini-SAS connectors. Attachment cables are available with two SFF-8088 connectors (for connection to a host adapter with an SFF-8088 connector), or with one SFF-8088 and one SFF-8470 connector (for connection to a host adapter with an SFF-8470 connector). The cables are 1X for point-to-point connection and are available in 2.0 m or 5.5 m lengths.

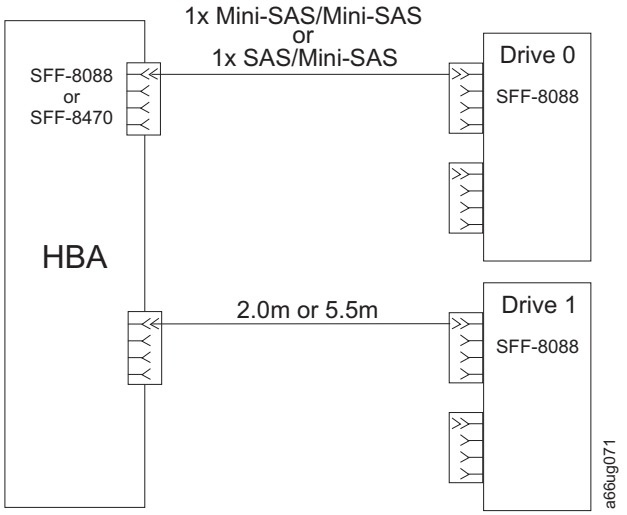


Figure 2-1. SAS drive connections with 1x point-to-point cables.

Up to 4 SAS drive sleds can be attached to one HBA 4x port with an interposer cable (FC 5400 or FC 5500) with one connection at the HBA port and 4 connections for the individual drive cables.

Important: With the 1 to 4 interposer, the individual drive cables are limited to the 2.0 m length.

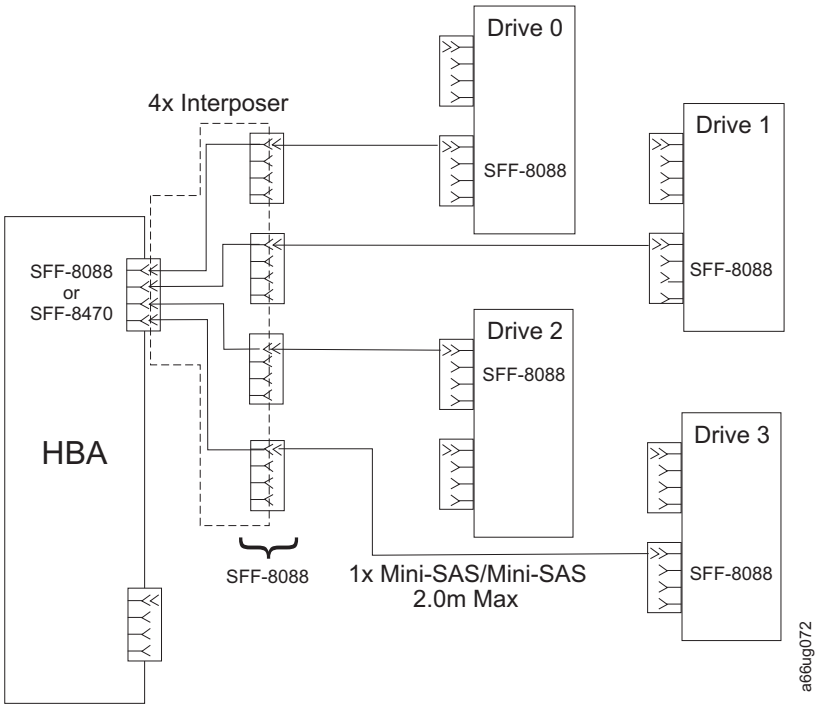


Figure 2-2. SAS drive connections with 4x interposer cable.

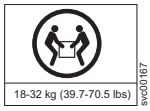
SAS hosts and adapters

The library is supported by a wide variety of servers (hosts), operating systems, and adapters. These attachments can change throughout the product 's lifecycle. To determine the latest supported attachments, visit the web at http://www.ibm.com/storage/lto or contact your IBM sales representative.

Chapter 3. Installing a new library in a rack

Follow the steps in this chapter to install a new library in a rack. For instructions on converting your rack-mounted 5U or 14U library to a desktop unit, see "Library conversions" on page 12-52. For instructions on removing or replacing a control module or expansion module in a desktop or rack-mounted library, see "Removing/replacing a control module" on page 12-3 and "Removing/replacing an expansion module" on page 12-15.

Unpacking and verifying shipment contents



Important: Because of the weight of a multi-module library, it is recommended that you install it in the lowest position in a rack. Without drive sleds and power supplies, a control module weighs approximately 50 lbs. Without drive sleds and power supplies, each 9U expansion module weighs approximately 65 lbs.

1. Open and unpack all the boxes in your shipment.
2. Remove all external packaging materials from around the library module.

   Note: Leave the library module on the lifting sling until it is ready to be installed.
3. Verify the contents of your shipment.

Table 3-1. Shipment contents

Description	Number for each control module	Number for each expansion module
Library control module 5U	1	
Expansion module E9U (maximum 4 expansion modules per rack-mounted library)		1
Module communication terminators	2	
Module-to-Module communication cable		1

Table 3-1. Shipment contents (continued)

Description	Number for each control module	Number for each expansion module
Power cord for each primary power supply (If you are installing your library in a rack, you need Feature code 9848, rack Power Distribution Unit (PDU) power cord.)	1	1
Power cord for each redundant power supply (if ordered)	1	1
Wrap plug for SCSI drives (if SCSI drives ordered)	1	
Wrap plug for Fibre Channel drives (if Fibre Channel drives ordered)	1	
Wrap plug for SAS drives (if SAS drives ordered)	1	
SCSI or fibre or SAS cable for each tape drive (if ordered)	1 per drive	1 per drive
SCSI drive-to-drive cable with each SCSI drive ordered	1 per drive	1 per drive
SCSI terminator for each SCSI tape drive	1 per drive	1 per drive
Ethernet crossover cable (for service use only)	1	
Cleaning cartridge, with label	1	
Publications prepack kit	1	
Hotline card		1
Rack Mount kit (if ordered)	1	
Additional Rack Hardware kit (rack ears)		1
Deskside kit (library feet and screws)	1	
Sling (for lifting and installing library modules)	1	1
Important: If any of these items are missing, call the appropriate number that is listed on the Hotline card included in your shipment.		

4. Remove all internal packaging materials that secure the picker assembly. The original-style picker is secured with cardboard and foam packing materials. The M2-style picker is secured to the bottom cover with two plastic shipping screws.

   Note: Failure to remove all internal packaging material before the library is powered ON results in damage to your library.

Figure 3-1. Original-style picker with internal packaging material

a. For the original-style picker, remove the fastening strap (**1** in Figure 3-1) across the top of the picker packaging material.

   Important: Be careful not to damage the picker assembly when the packing materials are removed. DO NOT USE EXCESSIVE FORCE.

b. Remove the cardboard packaging material (**2** in Figure 3-1), the foam packaging material (**3** in Figure 3-1), and the small cardboard packaging material (not shown in picture).

c. For libraries with the M2-style picker, ensure that you removed the two plastic shipping screws and the orange ribbon from the picker (Figure 3-2 on page 3-4) along with the yellow ribbon-like packing pieces from the I/O stations (Figure 3-3 on page 3-4).

Figure 3-2. M2 picker packaging screws and ribbon removed from the library

5. Remove the yellow ribbon-like packing pieces (**1** in Figure 3-3) from around the I/O Station magazines.

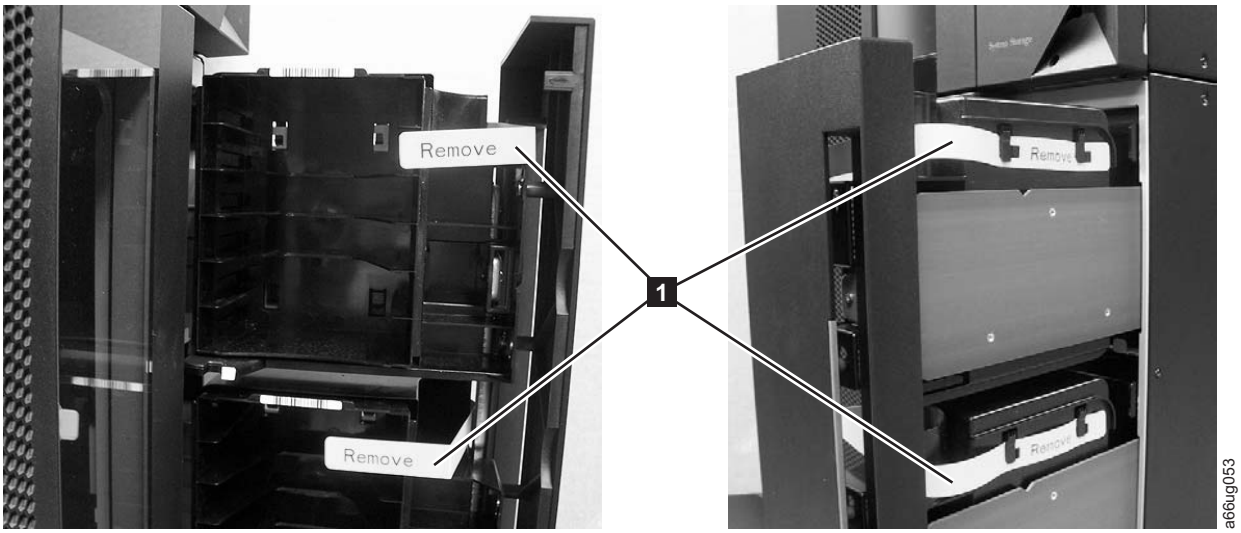


Figure 3-3. Yellow ribbon-like packing pieces

6. For libraries with the original-style picker, refer to Figure 3-4 and ensure that you removed all of the packaging material.

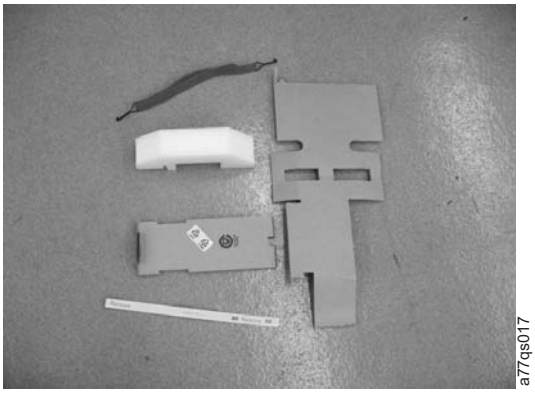


Figure 3-4. Packaging materials removed from library with the original-style picker

Reducing library weight

For weight reduction, remove the following components from each unit that must be moved for installation:

- Power supplies
- Drive sleds

Important: Because of the weight of a multi-module library, it is recommended that you install it in the lowest position in a rack. Without drive sleds and power supplies, a control module weighs approximately 50 lbs. Without drive sleds and power supplies, each expansion module weighs approximately 65 lbs.

Removing the power supply

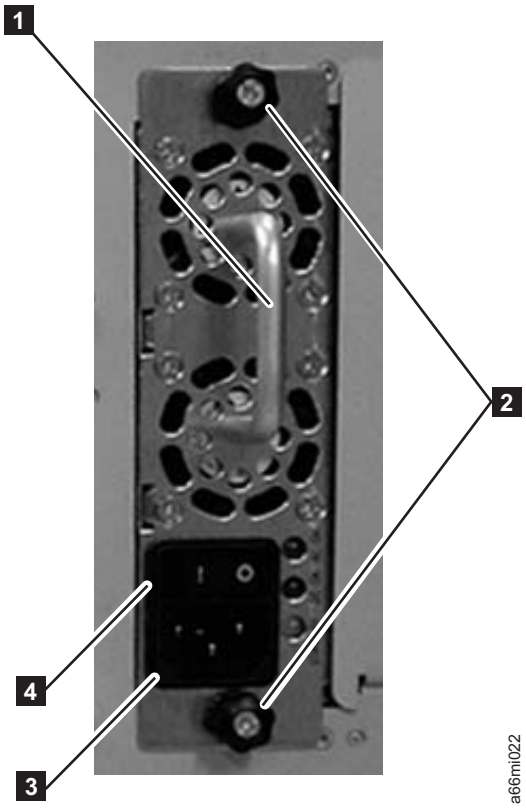


Figure 3-5. Power supply

For each installed power supply:

1. Loosen the two thumb screws (**2** in Figure 3-5) on the power supply by turning them counterclockwise.
2. To remove the power supply, grasp the handle (**1** in Figure 3-5) and slowly pull it toward you, while it is supported from underneath.

Removing a drive sled

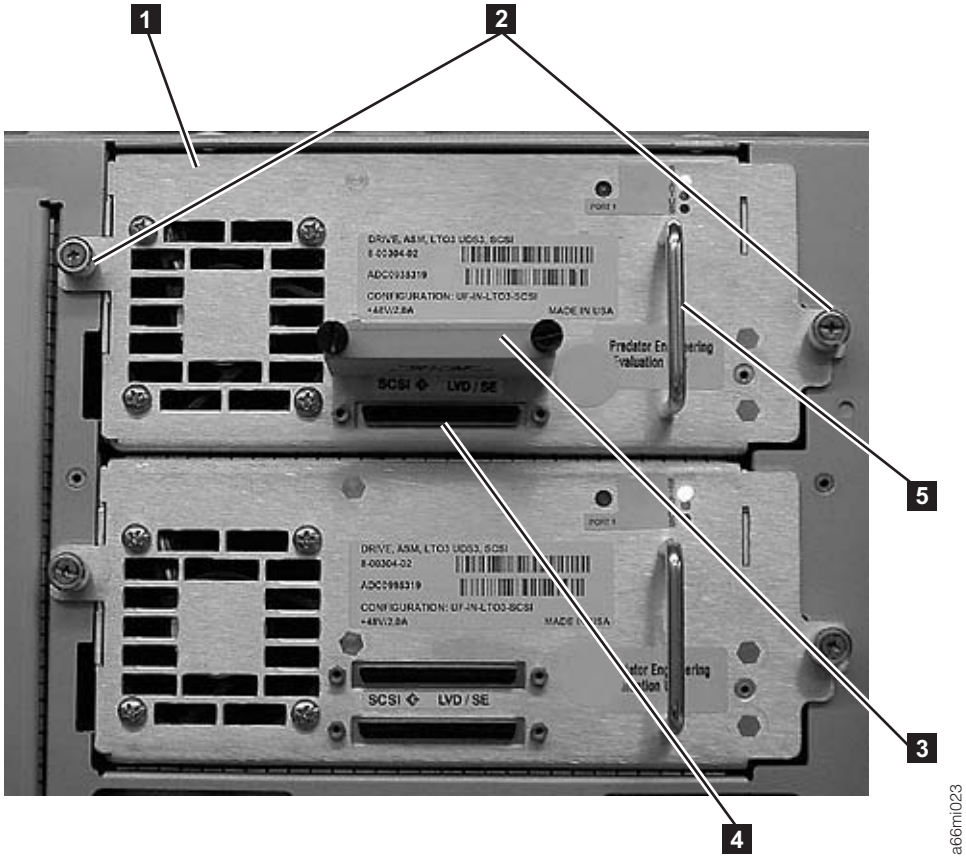


Figure 3-6. SCSI drive sled (detail)

For each installed drive:

1. Loosen the two thumb screws (**2** in Figure 3-6) that hold the drive sled in place by turning them counterclockwise.
2. To remove the drive sled, grasp the handle (**5** in Figure 3-6) and slowly pull it toward you, while the drive sled is supported from underneath.

Preparing the library module for installation

Each control module is shipped with both a top and a bottom cover. To properly install a library, you might need to move one or both covers from the control module to expansion modules. When finished, the top cover is on the top module of the library, and the bottom cover is on the bottom module of the library.

1. Ensure that the drive sleds and power supplies are removed from the modules that are installed. See "Reducing library weight" on page 3-5.
2. Refer to Figure 3-13 on page 3-13 and determine which library module is installed on the bottom.
3. If you choose a configuration that has a 9U EM on the bottom, transfer the bottom cover from the 5U control module to the 9U module that is on the bottom. Refer to "Transferring the bottom cover from the control module to an expansion module" on page 3-7. If the control module is on the bottom of your library, you do not need to move the bottom cover.
4. If you choose a configuration that has a 9U EM on the top of the library, transfer the top cover from the 5U control module to the 9U module that is on the top. Refer to "Transferring the top cover from the control module to an

expansion module" on page 3-10. If the control module is on the top of your library, you do not need to move the top cover.

Transferring the bottom cover from the control module to an expansion module

Each library comes with a bottom cover that is shipped with the control module. If you are installing an expansion module as the first or bottom module in a library, you must move the bottom cover from the control module to the bottom of the lower-most expansion module.

1. Engage the picker assembly lock mechanism (**1** in Figure 3-7). You might need to lift the picker assembly to fully engage the lock mechanism.

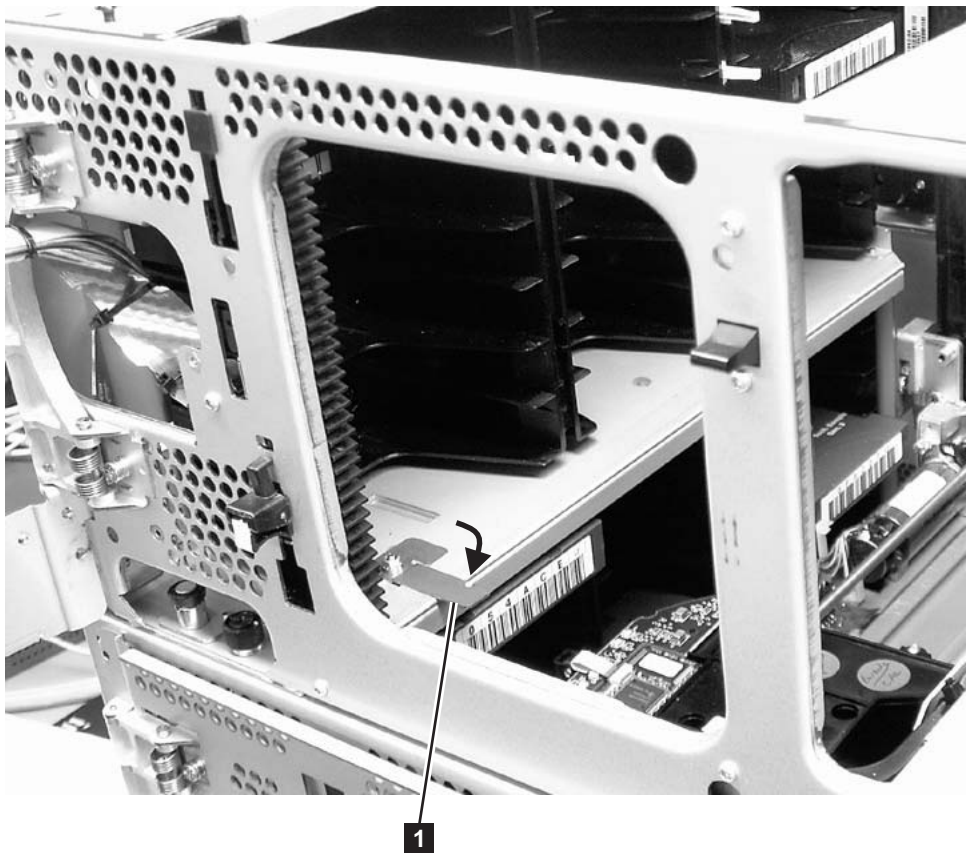


Figure 3-7. Picker locking mechanism

2. Turn the 5U control module on its side and remove the 5 - T10 Torx bottom cover screws (**1** in Figure 3-8 on page 3-8).

   Important: DO NOT loosen or remove the screw that holds the home sensor (**2** in Figure 3-8 on page 3-8). This screw has the same T10 Torx head as the cover screws, but it is longer and has a coarse thread for screwing into the plastic home sensor.

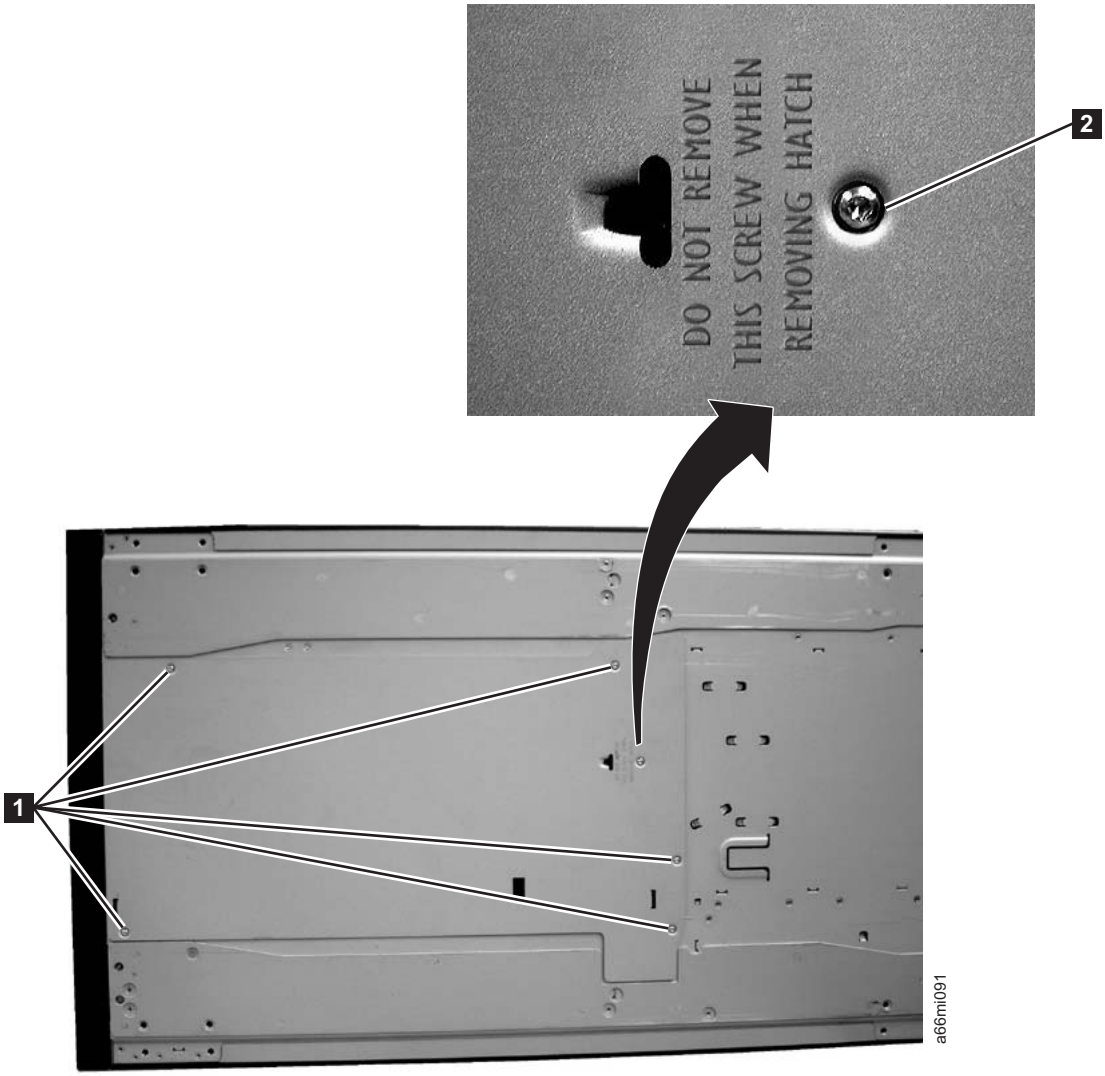


Figure 3-8. Bottom cover of the 5U control module

3. Remove the bottom cover from the 5U control module.

   Note: Ensure that the home sensor plastic piece is mounted on the inner side of the bottom cover (**1** in Figure 3-9 on page 3-9).

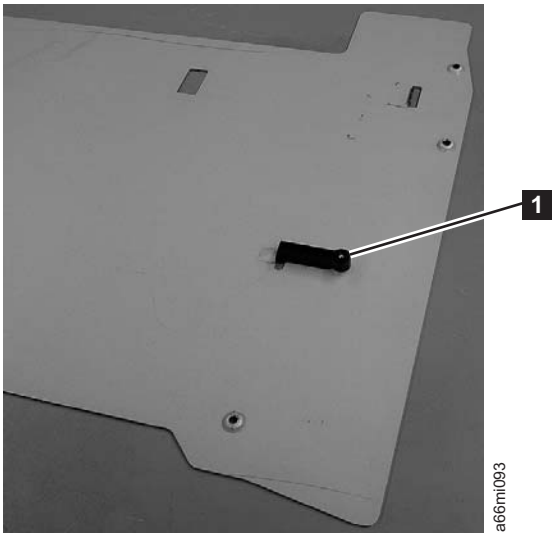


Figure 3-9. Home sensor on inner side of bottom cover

Important: Ensure that the picker lock mechanism (**1** in Figure 3-10) is engaged as shown. This procedure prevents the picker mechanism from falling out of the bottom of the 5U control module when it is returned to the upright position without a bottom cover installed.

Figure 3-10. Bottom view of picker assembly lock mechanism

4. Return the 5U control module to the upright position.
5. Ensure that the front and rear gear racks of both the control module and the expansion module are locked in the upper position (see **2** in Figure 3-20 on page 3-20).
6. Turn the expansion module on its side and install the bottom cover, with the 5 - T10 Torx screws.
7. Return the expansion module to the upright position.

Transferring the top cover from the control module to an expansion module

Each library comes with a top cover that is shipped with the control module. If you are installing the expansion module as the top module in the library, you must move the top cover from the control module to the expansion module.

1. Remove the 4 - #2 Phillips top cover screws (**1** in Figure 3-11).

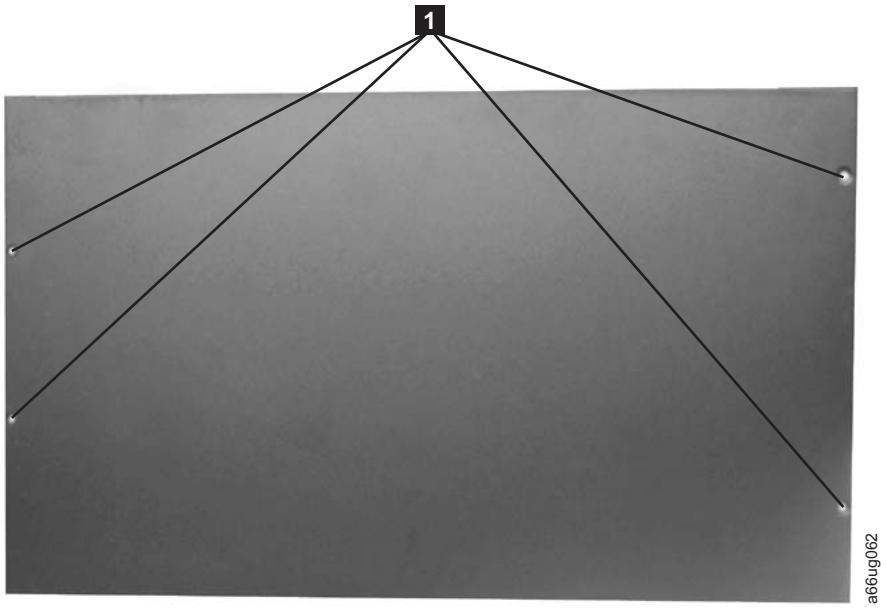


Figure 3-11. Top cover of the 5U control module

2. Remove the top cover from the 5U control module.
3. Ensure that the front and rear gear racks of both the control module and the expansion module are locked in the upper position (see **2** in Figure 4-13 on page 4-11).
4. Install the top cover, with the 4 Phillips screws (see **1** in Figure 3-11.

Verifying rack mount kit contents

The rack mount kit includes one pair of rails to install your library configuration. A single pair of rails is designed to hold the entire library configuration. (This configuration can be a control module and up to four expansion modules). If expansion modules are ordered, they are supplied with a rack mount kit that contains only items to secure each expansion module to the rack. No additional rails are required to fit the expansion modules.

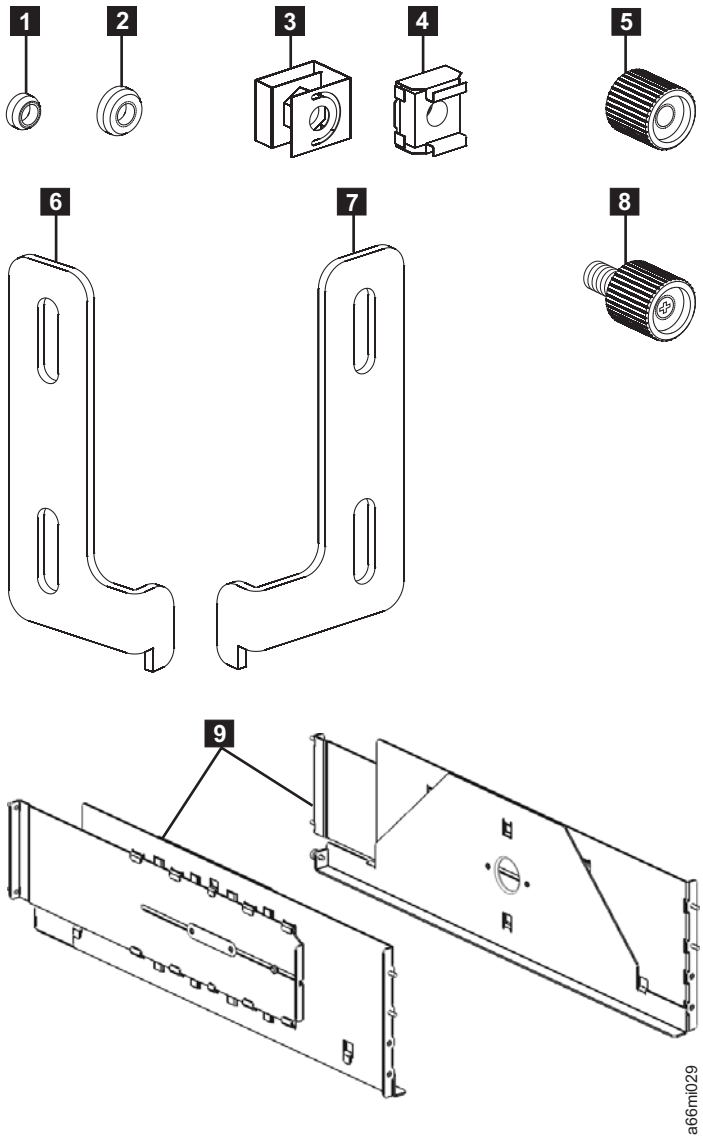


Figure 3-12. Rack mount kit hardware (parts not sized proportionately in figure)

Table 3-2. Rack mount kit contents

Quantity*	Description
16	Centering nuts: • 8 for racks with round holes (1 in Figure 3-12) • 8 for racks with square holes (2 in Figure 3-12)
8	Black thumb nuts (5 in Figure 3-12)
2	Rack ears (6 and 7 in Figure 3-12)
4	Rack ear screws (8 in Figure 3-12)
2	Rails (9 in Figure 3-12)
Important: If any of these items are missing, call the appropriate number that is listed on the Quality Hotline card included in your shipment. * Extra pieces of the small parts are included.	

Table 3-3. More rack hardware kit contents (included with each expansion module)

Quantity	Description
8	Clip/Cage nuts: • 4 clip nuts for racks with round holes (**3** in Figure 3-12 on page 3-11) • 4 cage nuts for racks with square holes (**4** in Figure 3-12 on page 3-11)
2	Rack ears (**6** and **7** in Figure 3-12 on page 3-11)
4	Rack ear screws (**8** in Figure 3-12 on page 3-11):
Important: • This additional rack hardware kit is included with all expansion modules. If you are not rack-mounting your library currently, store this kit for future use. • If any of these items are missing, call the appropriate number that is listed on the Hotline card included in your shipment.	

Identifying the location in the rack

When you are deciding on a location in your rack for the library, the Operator Panel has a touchscreen and must be positioned to allow easy access. You probably want to avoid placing the control module on the very bottom or the top of the rack. Also, the rear of the library must be free from any obstructions to allow easy access to rear panel components. If you think there is a possibility of adding another expansion module to your library in the future, you might want to allow for this possibility when you decide where to locate the library in your rack.

Note: Consider leaving a minimum clearance of 6 inches above the library for service clearance when the library is installed in a rack. Service activities might require taking the top cover off.

Refer to Figure 3-13 on page 3-13 and select one of the recommended configurations for your library installation.

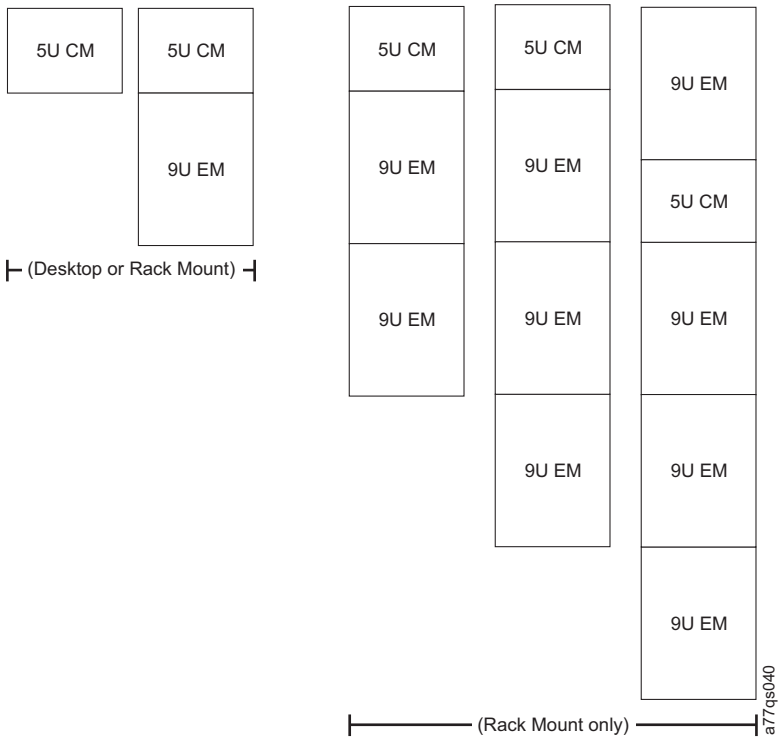
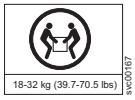


Figure 3-13. Recommended library configurations

Note: Before the rack installation of your library begins, read the information on Rack Safety in the *Safety and Environmental Notices* chapter. Also, verify that no foot pads are installed on the bottom of your library. If foot pads are installed, complete "Removing library foot pads" on page 12-54, then return here.



Important: Because of the weight of a multi-module library, it is recommended that you install it in the lowest position in a rack. Without drive sleds and power supplies, a control module weighs approximately 50 lbs. Without drive sleds and power supplies, each expansion module weighs approximately 65 lbs.

The following table gives the amount of rack space that is required for each library, which is measured in Electronics Industry Association Units (EIA units or U). One EIA is equal to 4.45 cm (1.75 inches).

An industry-standard rack has 3 mounting holes for each EIA increment (see Figure 3-14 on page 3-14.

Library	Required Rack Space in EIAs	Required Number of Rack Holes	Required Rack Space
Control Module	5 EIAs (5U)	15	22.25 cm (8.75 inches)
Expansion Module	9 EIAs (9U)	27	40 cm (15.75 inches)

The rails (**9** in Figure 3-12 on page 3-11) in the rack mount kit are used to support the bottom unit of your library, and require 5 EIAs (or 15 holes) of vertical rack space. However, there are only 4 rail studs on each rail, which is positioned in a staggered manner for increased stability. For correct installation, you must first

determine where the bottom of your library is, then identify which holes you use for the rail studs and place either cage nuts (for racks with square holes) or clip nuts (for racks with round holes) in the appropriate locations.

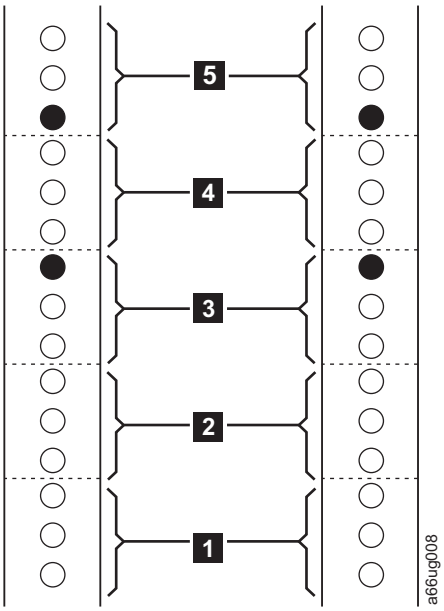


Figure 3-14. EIA identification and rail stud locations for FRONT vertical rack rails

1. With a pencil, make a mark below the first hole (**1** in Figure 3-14 and **1** in Figure 3-15 on page 3-15) in each of the five EIAs you selected for the rails in each vertical rail in your rack.
2. Locate and mark the hole that receives the rail studs as indicated by the black filled circles in Figure 3-14 and Figure 3-15 on page 3-15. The rail studs are on the front and back of each rail included in the rack mount kit.
   a. In the front vertical rack rails, rail studs are positioned as follows:
      - Top hole of the third EIA (**3** in Figure 3-14).
      - Bottom hole of the fifth EIA (**5** in Figure 3-14).
   b. In the rear vertical rack rails, rail studs are positioned as follows:
      - Bottom hole of the second EIA (**2** in Figure 3-15 on page 3-15).
      - Top hole of the fourth EIA (**4** in Figure 3-15 on page 3-15).

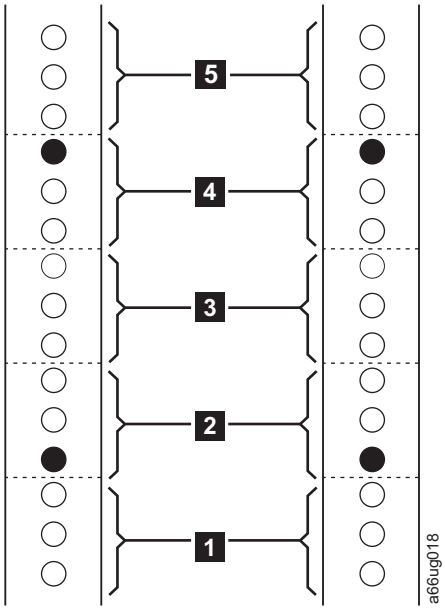


Figure 3-15. EIA identification and rail stud locations for REAR vertical rack rails

3. Install clip nuts (**3** in Figure 3-12 on page 3-11) for vertical rack rails with round holes or cage nuts (**4** in Figure 3-12 on page 3-11) for vertical rack rails with square holes in the front rack rails in the marked positions.
4. At this point, you must also install clip nuts or cage nuts into the holes that receive the rack ears that secure each additional module to the rack. These rack ears are installed only on the front vertical rails. First determine and mark the location for each of the rack ears on each of the two front vertical rails. For each module, do the following
   a. Determine where the module is placed. The control module requires 5 EIAs, and each expansion module requires 9 EIAs (27 holes). Mark the EIAs for each module.
   b. Each rack ear has two screws. These screws fit into the top hole in each of the two bottom EIAs for each module. Mark the appropriate holes for each module.

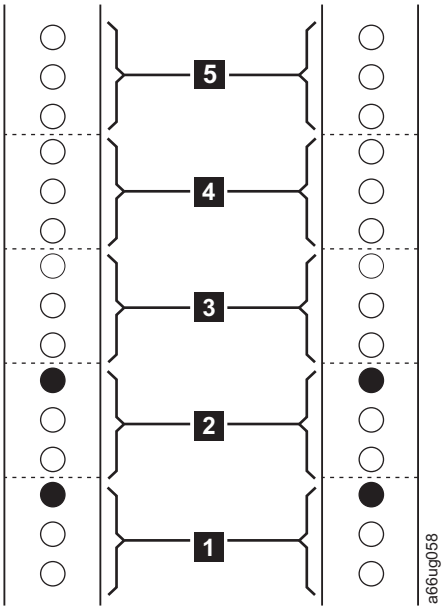
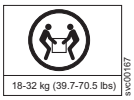


Figure 3-16. EIA identification and rail stud locations on vertical rack rails for expansion modules

5. Install clip nuts (**3** in Figure 3-12 on page 3-11) for vertical rack rails with round holes or cage nuts (**4** in Figure 3-12 on page 3-11) for vertical rack rails with square holes in the front rack rails in the marked positions.

Installing the rails

Follow these steps to install the rack mount kit rails. Only one pair of rails is required to install your library configuration.



Important: Because of the weight of a multi-module library, it is recommended that you install it in the lowest position in a rack. Without drive sleds and power supplies, a 5U control module weighs approximately 50 lbs. Without drive sleds and power supplies, each 9U expansion module weighs approximately 65 lbs.

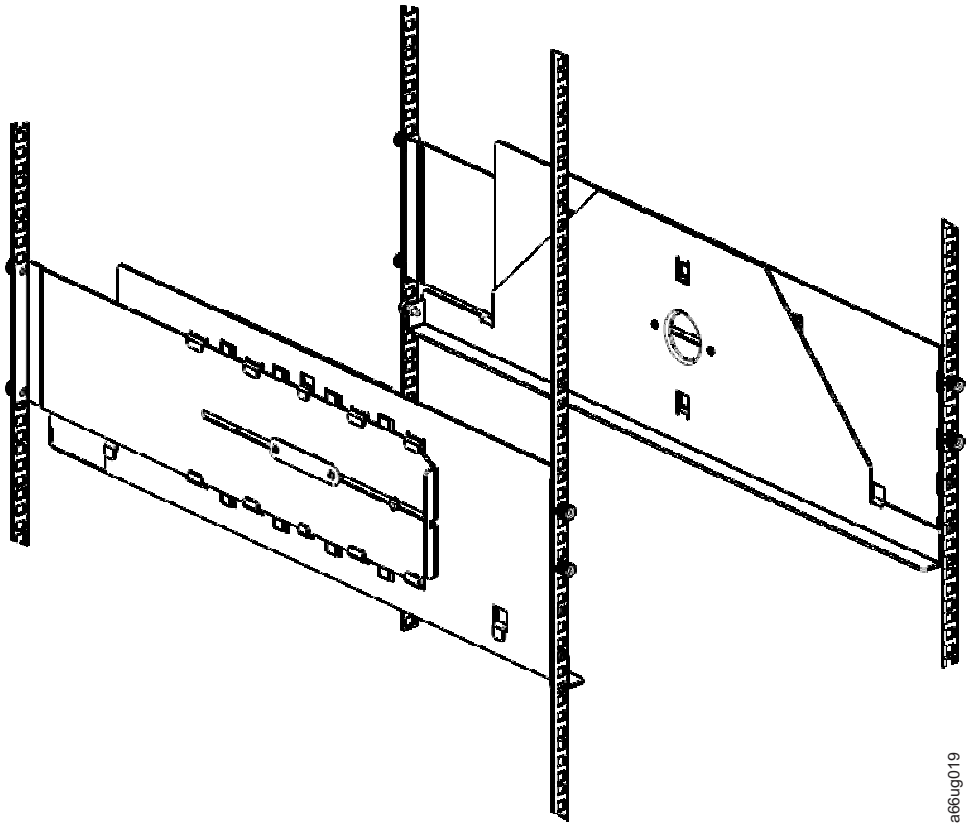


Figure 3-17. Rails that are installed in rack (front view)

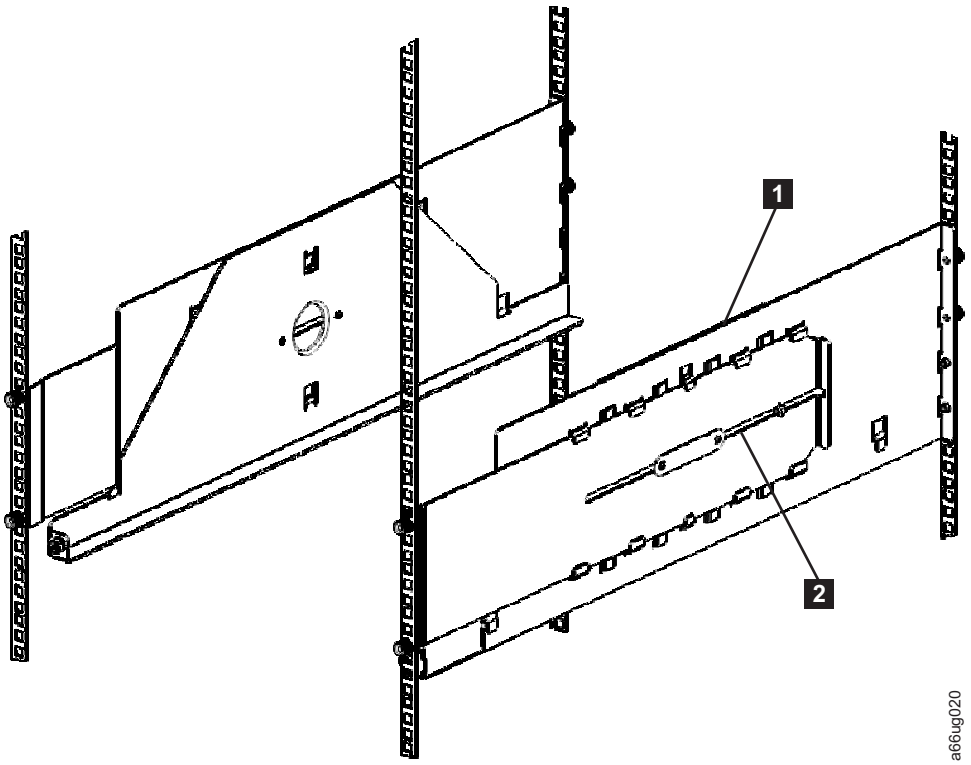


Figure 3-18. Rails that are installed in rack (rear view)

1. Collapse the rail (**1** in Figure 3-18). Loosen the nut (**2** in Figure 3-18), if necessary. The nut must be finger tight.
2. Put a centering nut on each rail stud (two studs on the front edge of each rail; two studs on the back edge of each rail) and finger-tighten. (The flat side of the centering nut must be against the flange of the rail when properly installed.)
   - Use the round hole-centering nuts (**1** in Figure 3-12 on page 3-11) for vertical rack rails with round holes.
   - Use the square hole-centering nuts (**2** in Figure 3-12 on page 3-11) for vertical rack rails with square holes.
3. From the front of the rack:
   a. Position the rail to the applicable side (right or left) and insert the rail studs through the marked holes in the vertical rack rail.

      Note: The small shelf portion of the left rail must be positioned to the right side of the rail. The small shelf portion of the right rail must be positioned to the left side of the rail. Positioning the rails in this way forms the shelf on which the library is installed.

   b. Place a thumb nut (**5** in Figure 3-12 on page 3-11) on each stud and tighten.
4. From the back of the rack:
   a. Extend the rail and insert the rail studs through the marked holes in the vertical rack rail.
   b. Place a thumb nut (**5** in Figure 3-12 on page 3-11) on each stud and tighten.
5. From the front of the rack, visually verify that the rail is aligned properly with the rack. You see thumb screw holes (for mounting the rack ears) in the following locations:

- Top hole of the first EIA (see Figure 3-14 on page 3-14)
- Top hole of the second EIA in the vertical rack rails (see Figure 3-14 on page 3-14)

6. Repeat this procedure for the other rail.

Installing the bottom library module in a rack

After you prepared the modules for installation, start with the module that is at the bottom of the library.

Important: Leave a minimum clearance of 6 inches above the library for service clearance when the library is installed in a rack. Service activities might require taking the top cover off.

Note: The bottom module in the library is the only module that must have a bottom cover installed. The top module is the only module that must have a top cover installed.

Attention: Ensure that the front and rear gear racks are locked in the upper position.

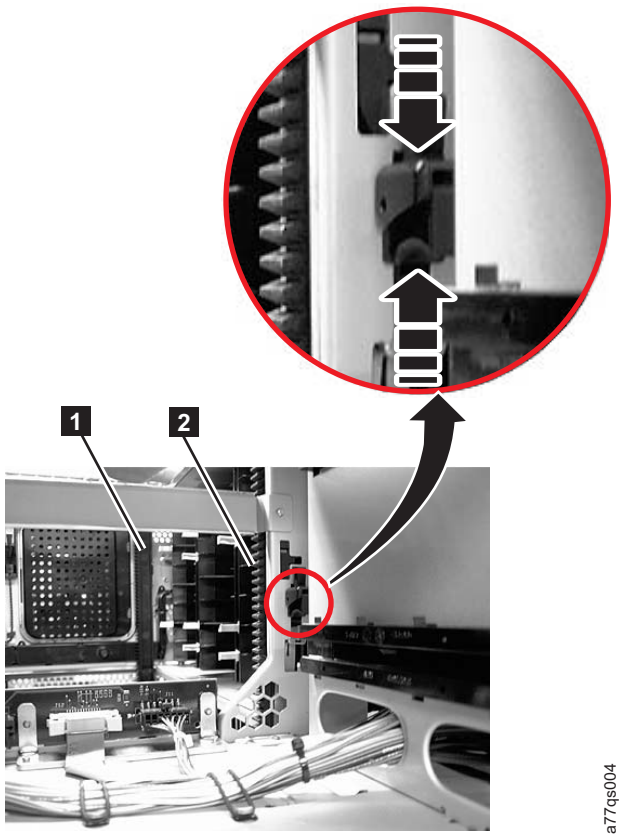


Figure 3-19. Front and back gear racks

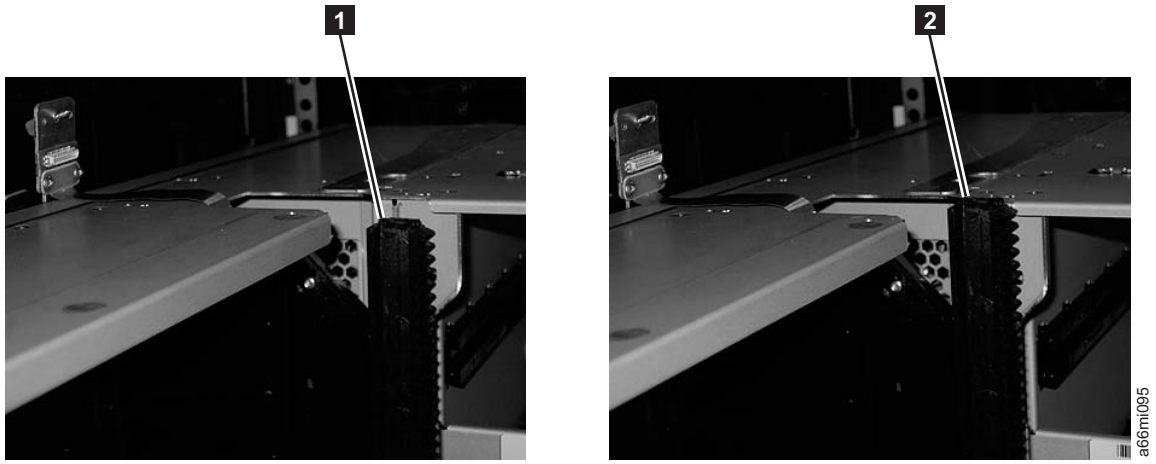


Figure 3-20. Gear racks positions (rear gear racks shown)

1	Gear rack in the down position	2	Gear rack in the up position

1. To raise the gear racks, disengage the Y-rails so the modules can be unstacked safely.

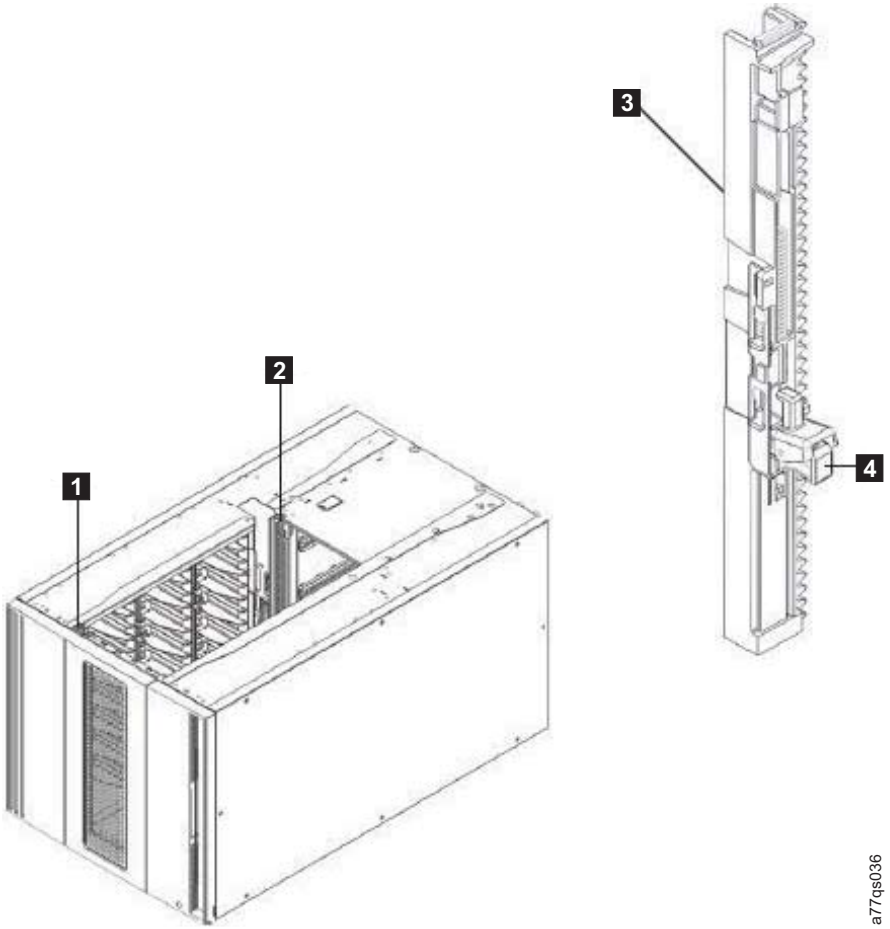


Figure 3-21. Y-Rails

1	Front Y-rail	2	Rear Y-rail
3	Y-rail (this end up)	4	Squeeze here to release

a. From the front of the library, find the Y-rail release mechanism, which is on the left side of the control module. Squeeze the handle of the Y-rail release mechanism, lift it, and release it so that it locks into place.

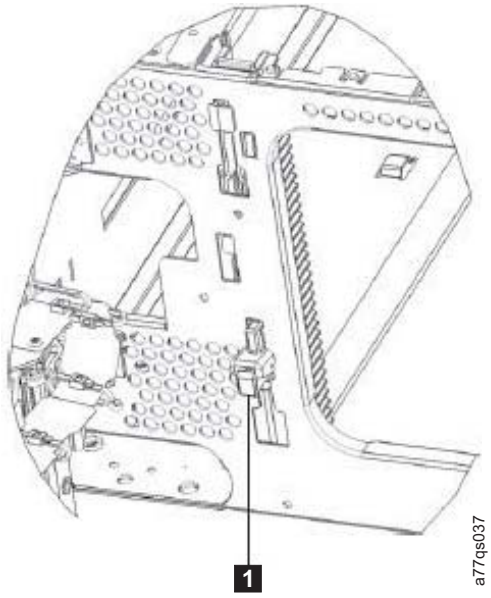


Figure 3-22. Y-rail in position

1	Y-rail in locked, non-functional position

b. From the rear of the library, find the rear Y-rail release mechanism that is in the interior of the right side of the module. Squeeze the handle of the Y-rail release mechanism, lift it, and release it so that it locks into place.

2. With a person on each side of the module, lift the module with the sling provided (see Figure 3-23 on page 3-22).

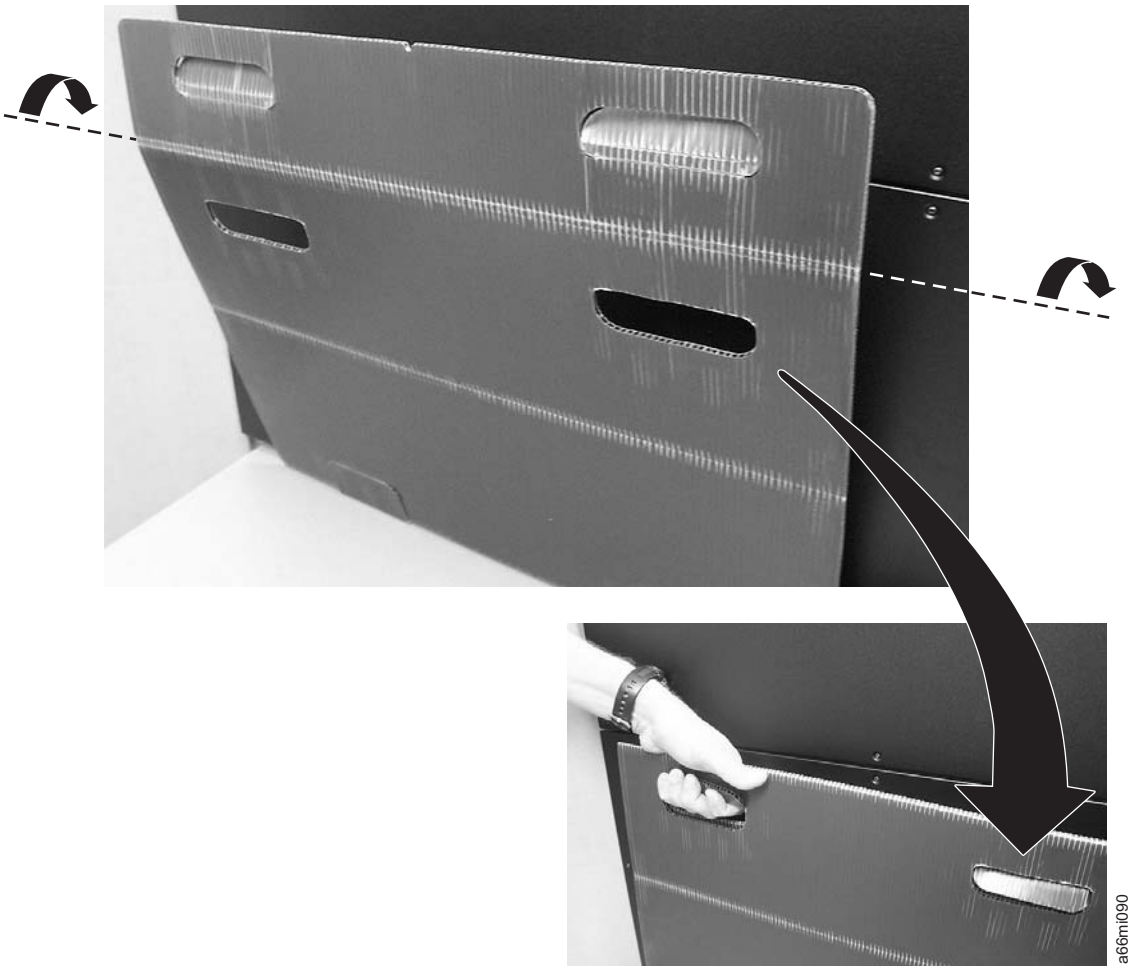


Figure 3-23. Sling handles folded properly

3. Slide the module partially onto the rail shelves in the rack.
4. Continue to support the library module from the front while you remove the sling.
5. Push the module into the rack until it contacts the flange on the rear of each rack mount rail.
6. Install and tighten the rear thumb screws (**1** in Figure 3-24 on page 3-23) on the flange on the rear of each rack mount rail.

Figure 3-24. Rear flange and thumb screw on rack rail

Installing additional modules in your library configuration

Once you have the bottom module installed, add more modules to your library.

Note: Rack doors are required for any library that has more than 14 drives installed.

1. If you are installing a 5U control module, ensure that the picker assembly lock mechanism (**1** in Figure 3-25 on page 3-24) is engaged as shown.

Figure 3-25. Picker assembly lock mechanism

2. **IMPORTANT:** Ensure that the front and rear gear racks are locked in the upper position.

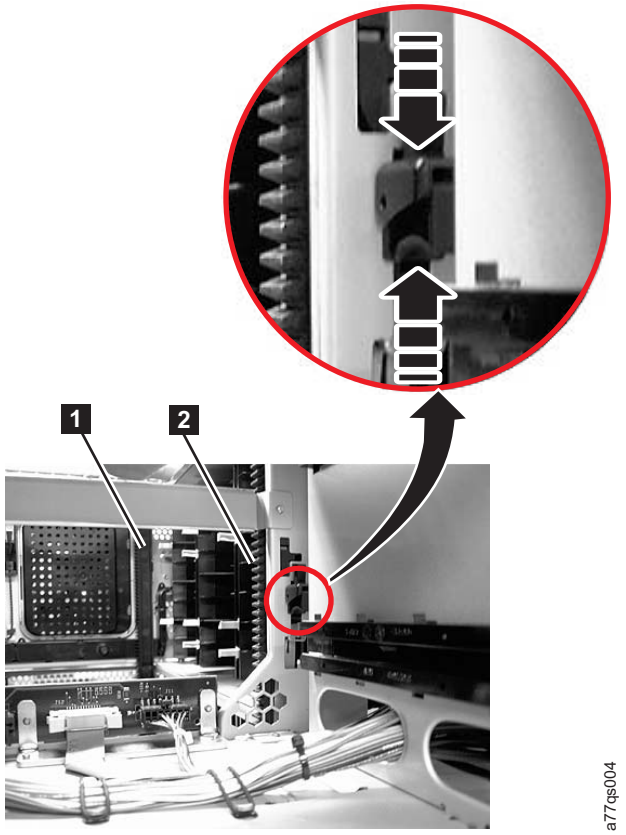


Figure 3-26. Front and back gear racks

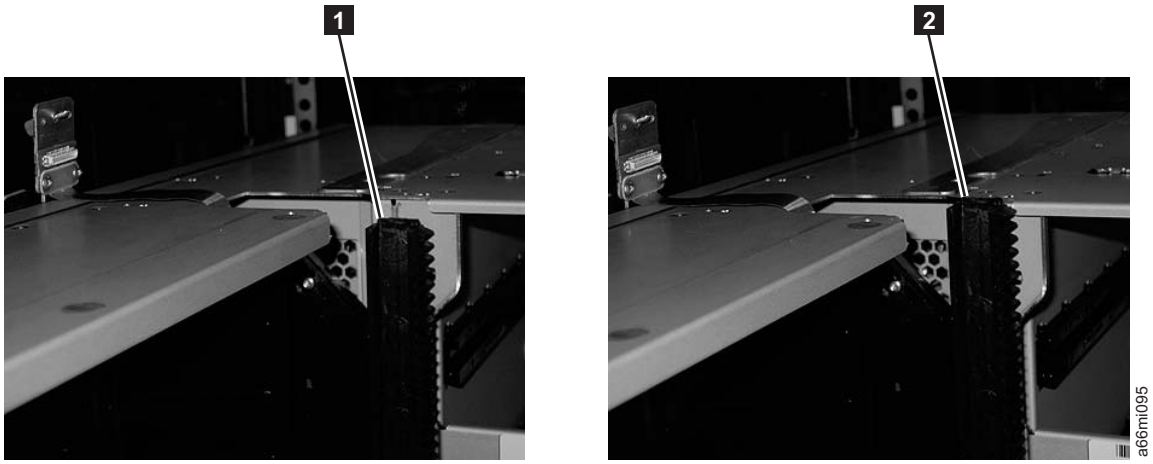


Figure 3-27. Gear racks positions (rear gear racks shown)

1	Gear rack in the down position	2	Gear rack in the up position

3. Ensure that the module-to-module alignment pin (1 in Figure 3-28 on page 3-26) is in the raised position. If necessary, raise the pin and rotate it half a turn to lock it in the raised position.

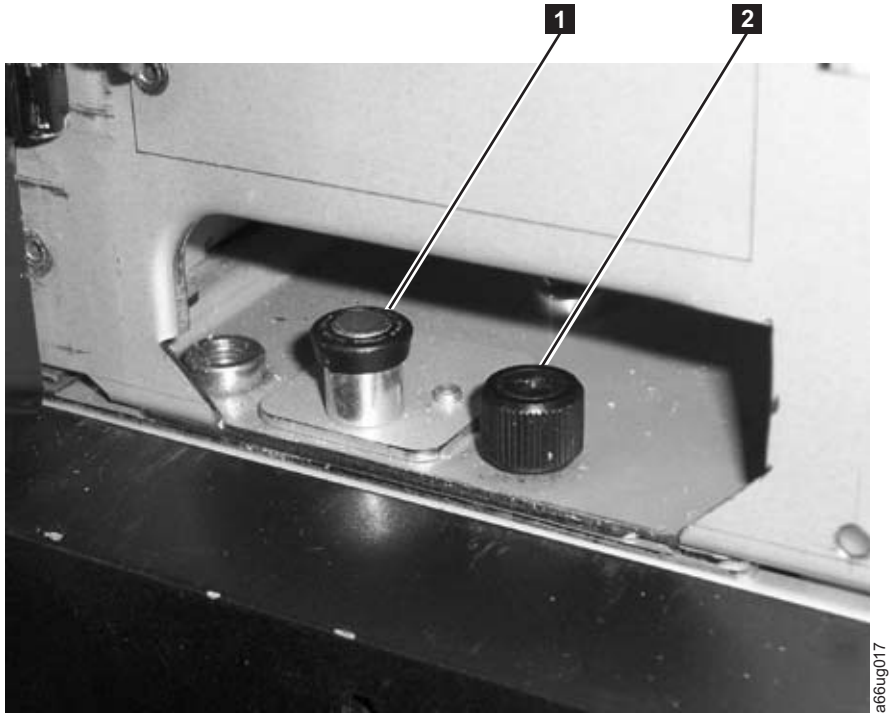


Figure 3-28. Module-to-module alignment pin and front thumb screw

4. With a person on each side of the module, lift the module with the sling provided (see Figure 3-29 on page 3-27 to see how the sling handles are folded).

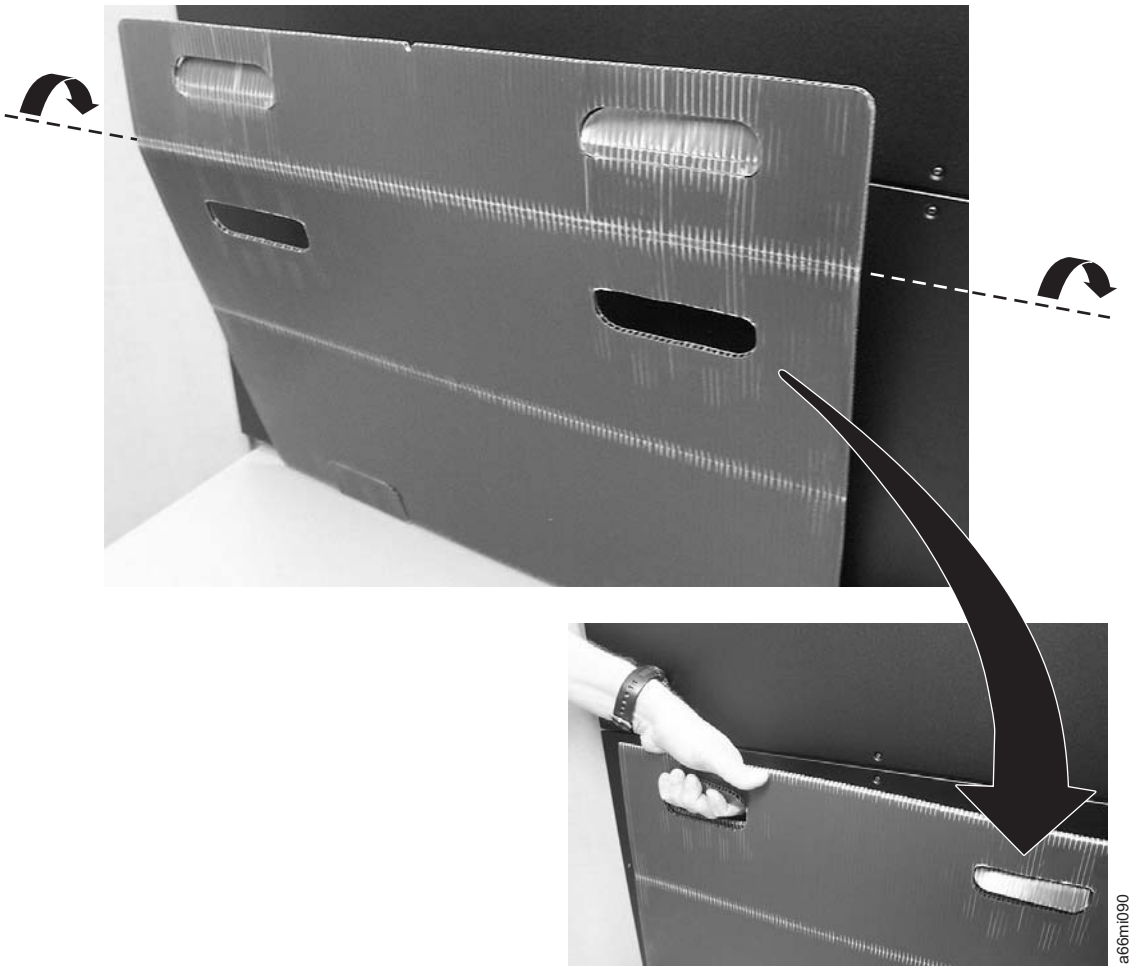


Figure 3-29. Sling

5. Slide the module partially on top of the already installed module.
6. Continue to support the library module from the front while you remove the sling.
7. Open the I/O station door, then the access door of the upper module to expose the alignment pin behind the access door.
8. Push the upper module onto the lower module.
9. Twist the upper module alignment pin (**1** in Figure 3-28 on page 3-26) to unlock it from the up position.
10. Adjust the upper module 's position on top of the lower module until the upper module alignment pin drops into the alignment pin receptacle in the lower module.
11. Tighten the front thumb screw (**2** in Figure 3-28 on page 3-26) and the thumb screw behind the I/O station door to secure the front of the upper module to the lower module.
12. Tighten the rear thumb screws (**1** in Figure 3-30 on page 3-28) that secure the upper module to the lower module.

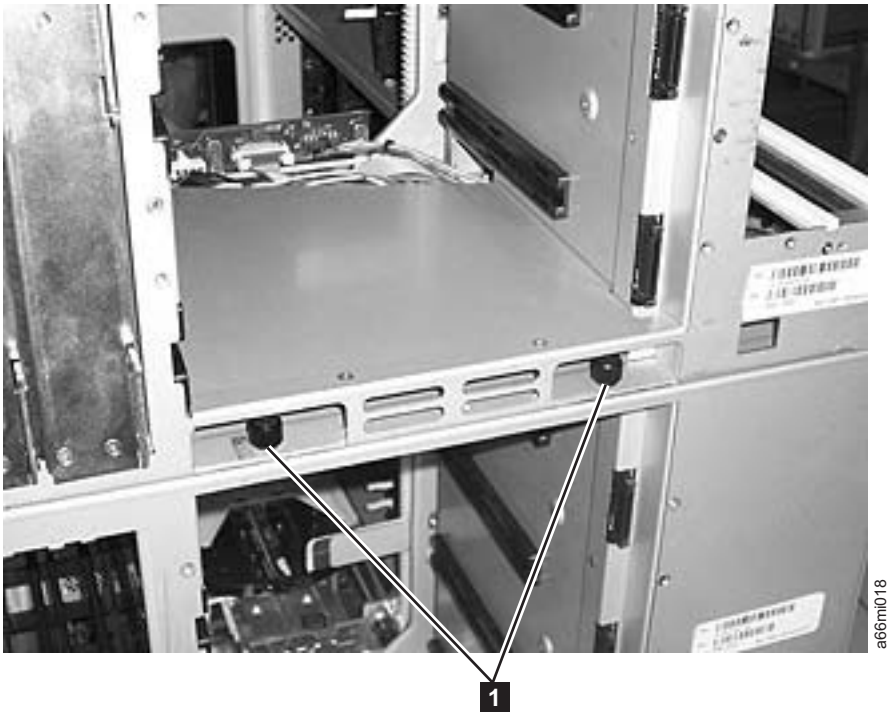


Figure 3-30. Rear thumb screws

13. Lower the gear racks into the down (operating) position by engaging the Y-rails of each module in your library configuration. Ensure that the Y-rails are properly aligned and the thumbscrews are tightened.

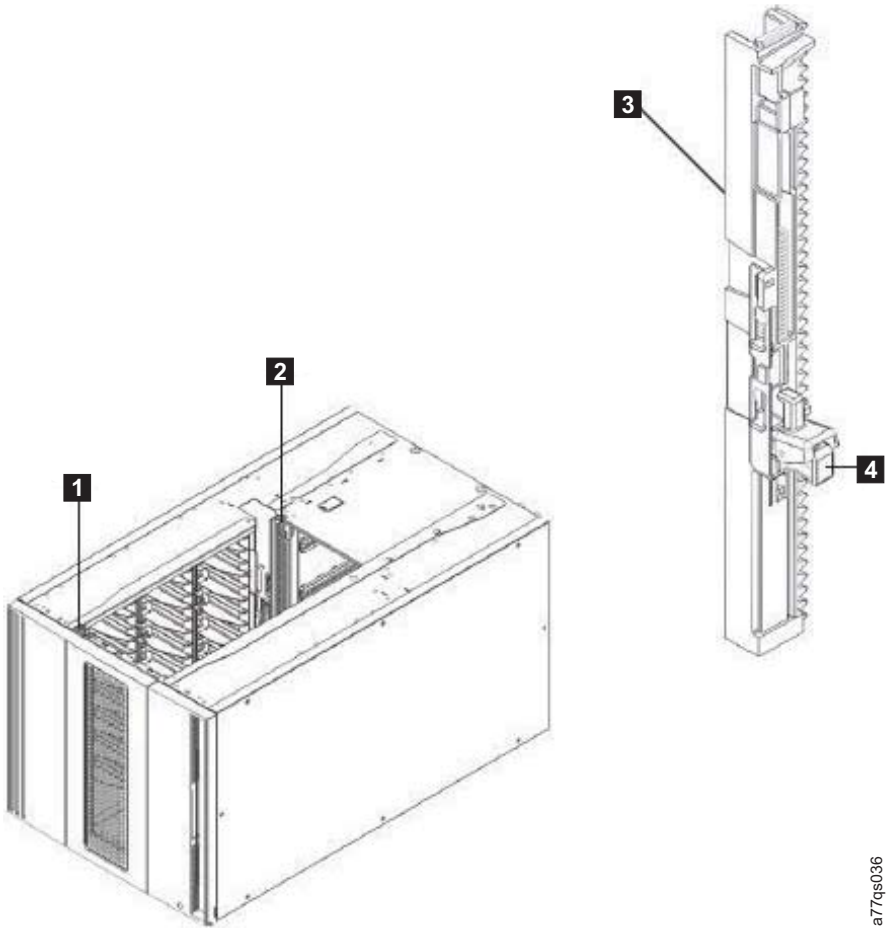


Figure 3-31. Y-Rails

1	Front Y-rail	2	Rear Y-rail
3	Y-rail (this end up)	4	Squeeze here to release

a. From the front of the library, open the I/O station and access doors of the 9U expansion module. Squeeze the handle of the Y-rail release mechanism, lift it out of its locked position, and slide it downward as far as it goes.

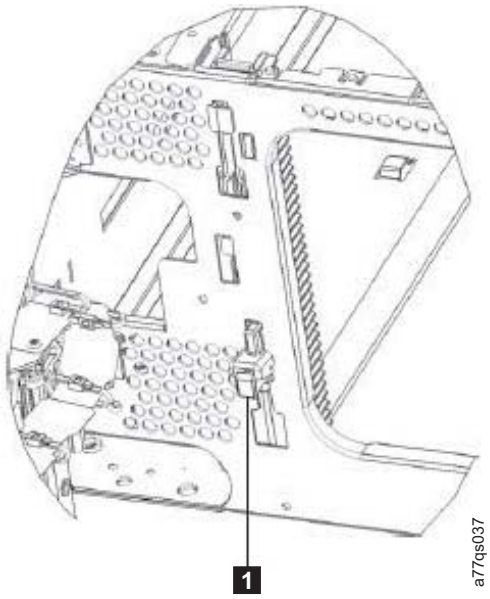


Figure 3-32. Y-rail in position

1 Y-rail in locked, non-functional position

b. From the back of the library, find the rear Y-rail release mechanism, which is in the interior of the right side of the module. Squeeze the handle of the Y-rail release mechanism, lift it out of its locked position, and slide it downward as far as it goes. Doing this procedure aligns the Y-rails with the Y-rails of the module beneath it.

Attention: Check to make sure that there is no gap between the top and bottom Y-rails on both the front and back of the library. If a gap exists, the library cannot mechanically initialize.

14. Repeat this procedure for each module in your library.
15. Store the installation-lifting sling in a secure location for possible future use.

Installing the rack ears

Install rack ears on the front of each module of a library to secure the module on the rack shelves.

1. Install the right rack ear (**2** in Figure 3-33 on page 3-31).

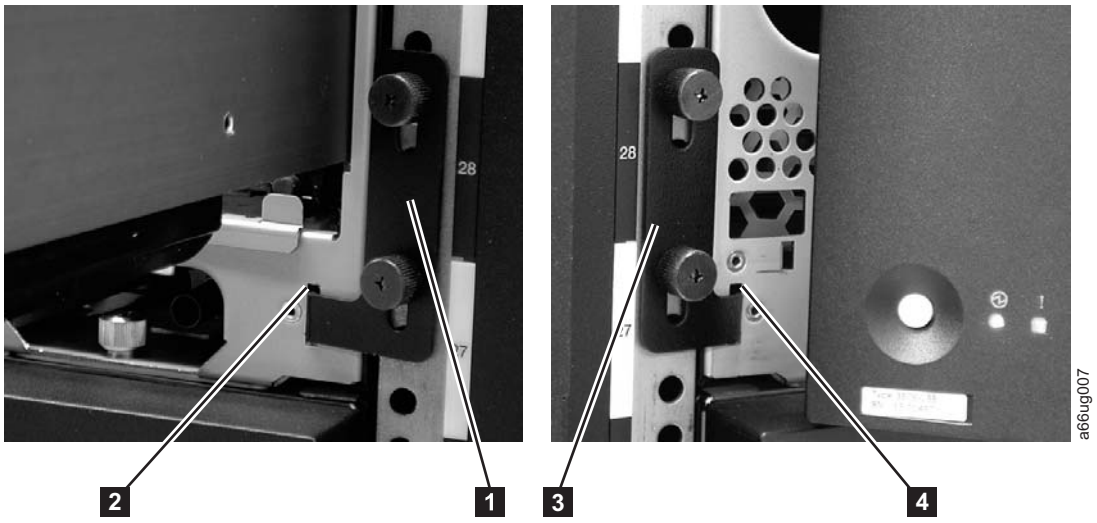


Figure 3-33. Installing the rack ears on a control module

a. At the lower right of the I/O station position on each library module, there is a slot (**2** in Figure 3-33). Insert the right rack ear (**1** in Figure 3-33 and **7** in Figure 3-12 on page 3-11) into the slot.
b. Position the right rack ear flush with the rack. The slots in the rack ear must be positioned as follows:
   - In the bottom library module, over the holes in the rack that align with the holes in the rack kit rails.
   - In the middle or top library module, over the holes in the rack that have clip/cage nuts that are installed.
c. Place the screws (**8** in Figure 3-12 on page 3-11) in the slots on the right rack ear and tighten.

2. Install the left rack ear (**3** in Figure 3-33 and **6** in Figure 3-12 on page 3-11).
   a. Open the left door of the library module slightly.
   b. Grasp the hinged side of the door and, while you are pulling on the door, push to the right to expose the slot (**4** in Figure 3-33) for the left rack ear.
   c. Insert the left rack ear (**3** in Figure 3-33) into the slot.
   d. Position the left rack ear flush with the rack. The slots in the rack ear must be positioned as follows:
      - In the bottom library module, over the holes in the rack that align with the threaded holes in the rack kit rails
      - In the middle or top library module, over the holes in the rack that have clip/cage nuts that are installed
   e. Place the screws (**8** in Figure 3-12 on page 3-11) in the slots on the left rack ear and tighten.
3. Close the I/O station and access doors.
4. Repeat this procedure for all modules in the library.

Enabling the picker assembly

Important: Picker assembly damage or library accessor errors can occur if the front or rear gear racks are not engaged properly.

1. **IMPORTANT:** Ensure that the front and rear gear racks are in the down (operating) position (see **1** in Figure 3-20 on page 3-20).
2. Feel the junction of the gear racks between each library module, front and rear. Ensure that there are no gaps between the gear racks before you release the picker assembly lock mechanism.
3. Manually raise the picker assembly while you release the lock mechanism (**1** in Figure 3-34).

Figure 3-34. Releasing the picker assembly lock mechanism

4. Release the picker assembly and observe it as it slowly drops to the bottom of the library. It must move smoothly as it travels from one module into the other.

   Note: If the picker jumps or bumps noticeably as it travels from one module into the other, an error can occur when the library is powered ON. Follow the instructions in "T083: Unlevel robot assembly not level" on page 11-39 to correct the problem.

Installing library components removed for weight reduction

At this point in the installation procedure, reinstall the drive sleds and power supplies that were removed for weight reduction.

Replacing a drive sled

Attention: NEVER install a drive sled when a cartridge is in the drive in the eject position. Remove the cartridge first.

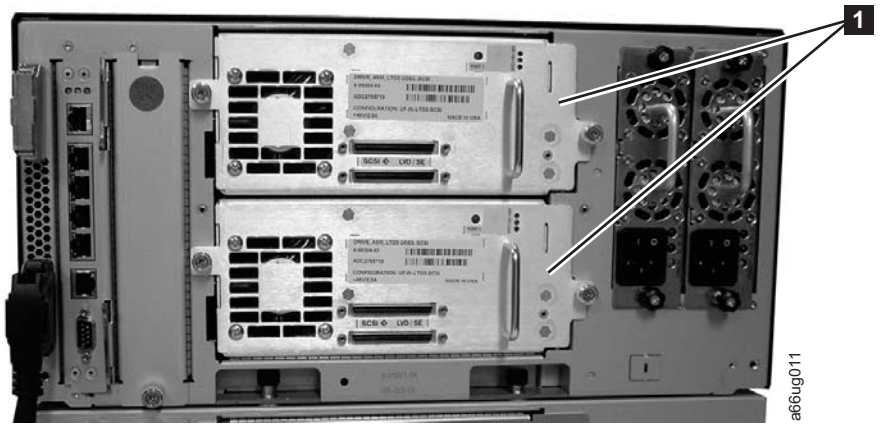


Figure 3-35. Control module drive sled

1. Align the drive sled with the guide rails and guide slots along the tracks (**3** in Figure 3-36).

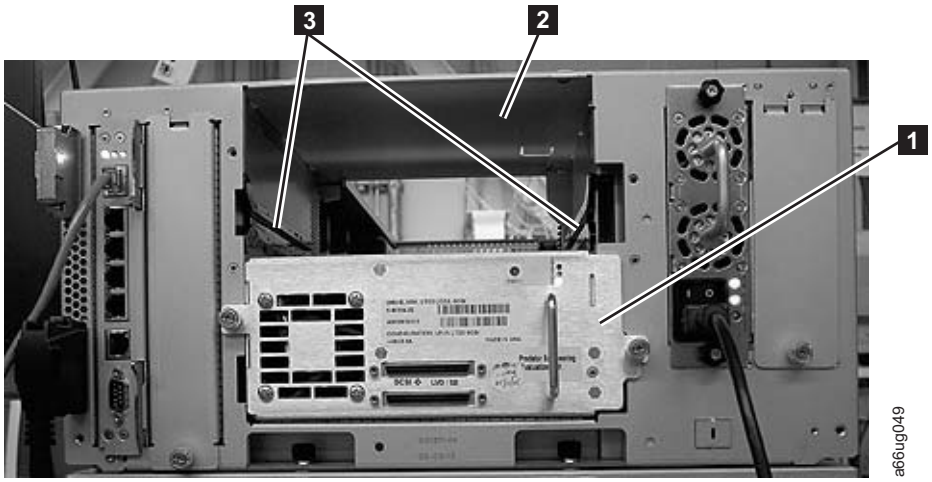


Figure 3-36. Guide rails and guide slots inside a drive slot

2. Grasp the handle (**5** in Figure 3-37 on page 3-34) and slowly slide the drive sled into the drive slot, while the drive sled is supported from underneath.

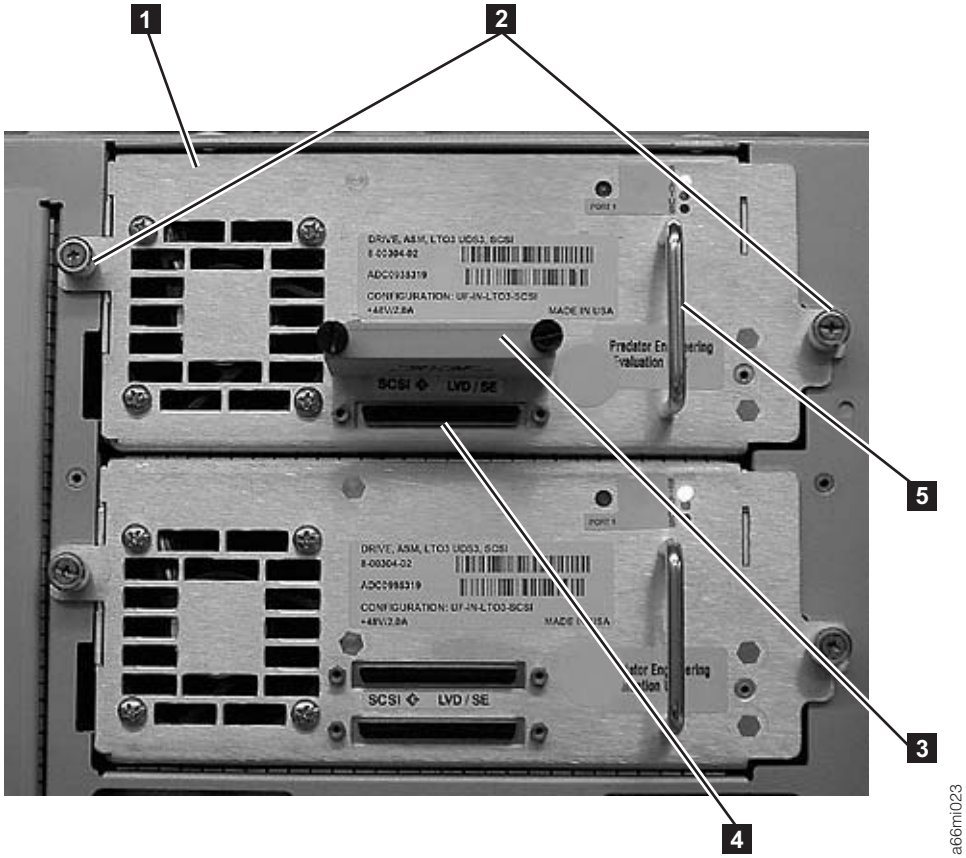


Figure 3-37. Tape drive (detail)

3. Tighten the two thumb screws (**2** in Figure 3-37) that hold the drive sled in place by turning them clockwise.
4. Repeat this procedure for all drives to be reinstalled in the library.

Installing a power supply

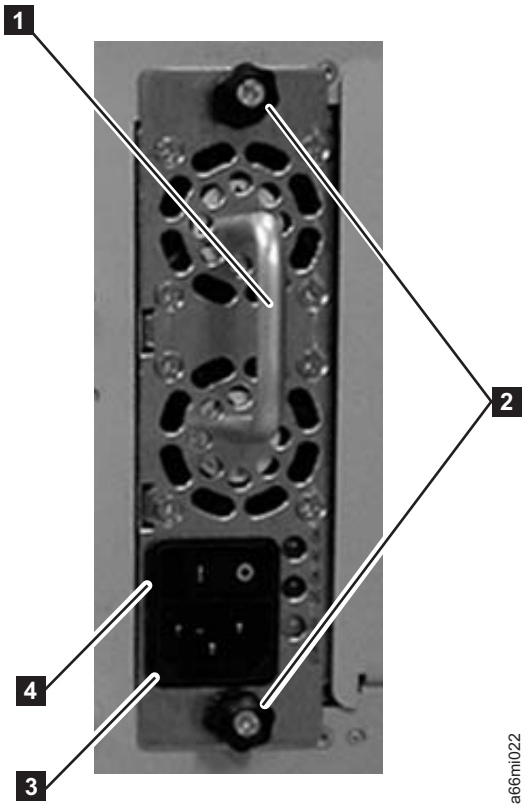


Figure 3-38. Control module power supply

1. Replace the power supply component by sliding it into the power supply slot. First, grasp the handle (**1** in Figure 3-38) while the power supply component is supported from underneath. Then, line up the power supply component with the guides in the power supply slot, and carefully push it into the library.
2. Tighten the two thumb screws (**2** in Figure 3-38) on the power supply component by turning them clockwise.
3. Repeat this procedure for each library power supply.

Cabling the library

Install the module-to-module communication cable, the module communication terminators, the customer-supplied ethernet cable, the drive sled cables, and the power supply cabling. Select and complete one of the following cabling procedures, depending upon your library configuration:

- "Cabling a 5U control module"
- "Cabling with SCSI drives" on page 3-36
- "Cabling with SAS or Fibre Channel drives" on page 3-38

Cabling a 5U control module

To cable a 5U library control module, complete the following steps:

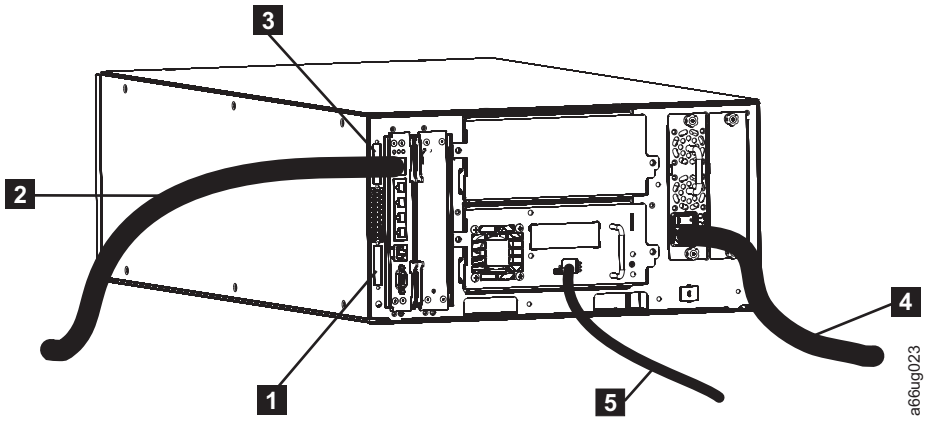


Figure 3-39. Cabling of a 5U library with Fibre Channel drives

1	Module communication terminator	4	Power cord
2	Ethernet cable (customer supplied)	5	Fibre Channel drive cable
3	Module communication terminator		

1. Install the upper module communication terminator (3 in Figure 3-39).
2. Install the lower module communication terminator (1 in Figure 3-39).
3. Connect one end of the customer-supplied ethernet cable (2 in Figure 3-39) in the Library Control Blade (LCB) ethernet port, then connect the other end of the cable to your network.
4. Connect one end of the drive-to-host cable (5 in Figure 3-39) to the library, then connect the other end of the cable to your network. Repeat this procedure for every drive in your library.

   Note: This procedure shows a Fibre Channel drive cable. SAS connections are similar. For details of SCSI cabling, see "Cabling with SCSI drives."
5. Connect one end of the power cord (4 in Figure 3-39) in the receptacle in a power supply in your library, then connect the other end of the cord to your power source. Repeat this procedure for every power supply in your library.
6. If you are adding expansion modules, continue cabling by following either "Cabling with SAS or Fibre Channel drives" on page 3-38 or "Cabling with SCSI drives."
7. When all the modules are cabled, continue with "Powering ON the library" on page 3-40.

Cabling with SCSI drives

To cable a library with SCSI cables, complete the following steps:

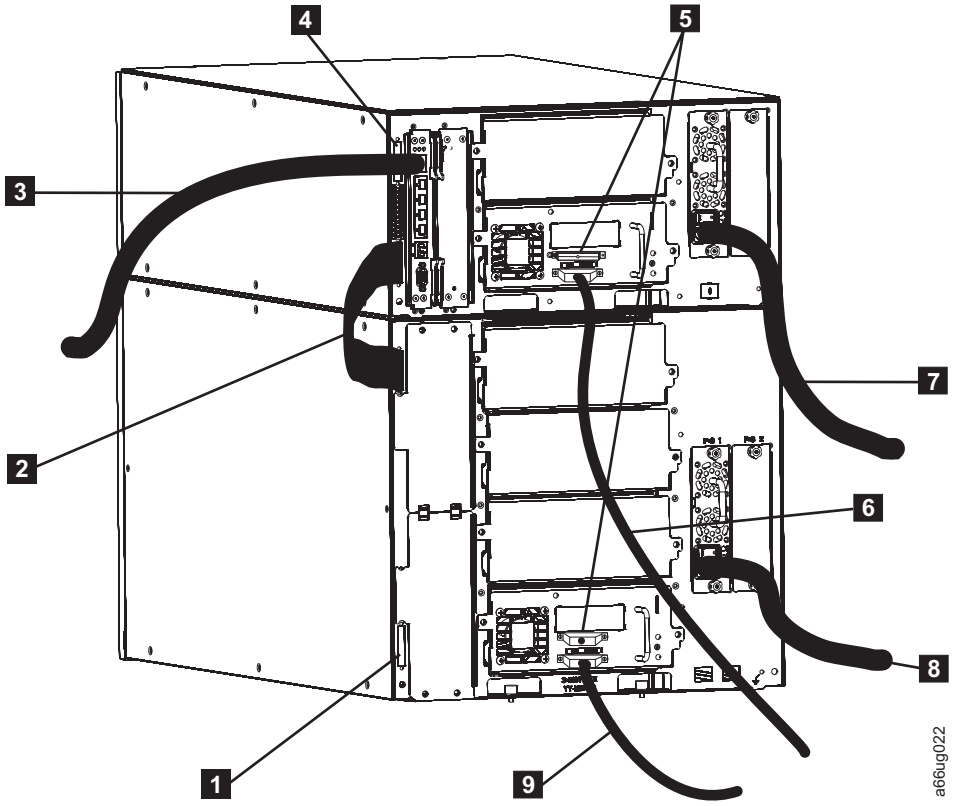


Figure 3-40. Cabling of a 14U library that contains multiple SCSI drives

1	Module communication terminator	6	SCSI drive-to-host cable
2	Module-to-module communication cable	7	Power cord (upper module)
3	Ethernet cable (customer supplied)	8	Power cord (lower module)
4	Module communication terminator	9	SCSI drive-to-host cable
5	SCSI terminators		

1. Install a module communication terminator in the upper receptacle of the upper module of your library (4 in Figure 3-40).
2. Install one end of the module-to-module communication cable (2 in Figure 3-40) in the lower receptacle of the upper module of your library. Then, install the other end in the upper receptacle of the lower module of your library.
3. Install a module communication terminator in the lower receptacle of the lower module of your library (1 in Figure 3-40).
4. Install one end of the customer-supplied ethernet cable (3 in Figure 3-40) in the Library Control Blade (LCB) ethernet port. Then, connect the other end of the cable to your network.
5. Installation of the SCSI cable and terminator depends upon how many drives are in your library. For maximum SCSI drive performance:
   - For each SCSI drive, install a SCSI terminator (5 in Figure 3-40) in the upper receptacle of each SCSI drive in your library.

- For each SCSI drive, connect one end of a SCSI cable to the lower receptacle of each SCSI drive (**6** in Figure 3-40 on page 3-37). Then, connect the other end of the cable to the host.
- If you prefer to daisy-chain your SCSI drives:
  a. Install a SCSI terminator in the upper receptacle of the top SCSI drive in the daisy-chain.
  b. Connect one end of a shorter drive-to-drive SCSI cable included in your shipment to the lower receptacle of the top SCSI drive in the daisy-chain. Then, connect the other end of the cable to the upper receptacle of the next drive in the daisy-chain. Repeat this procedure for every SCSI drive in your library.
  c. On the last drive in the daisy-chain, connect one end of the longer drive-to-host SCSI cable included in your shipment to the lower receptacle of the last drive in the daisy-chain. Then, connect the other end of the cable to the host.

  Note: Maximum performance of the SCSI drives in your library is not achieved if the drives are daisy-chained.

6. Connect one end of the power cord (**7** and **8** in Figure 3-40 on page 3-37) in the receptacle of a power supply in your library. Then, connect the other end of the cord to your power source. Repeat this procedure for every power supply in your library.
7. Continue with "Powering ON the library" on page 3-40.

Cabling with SAS or Fibre Channel drives

To cable a library with SAS or Fibre Channel drives, complete the following steps:

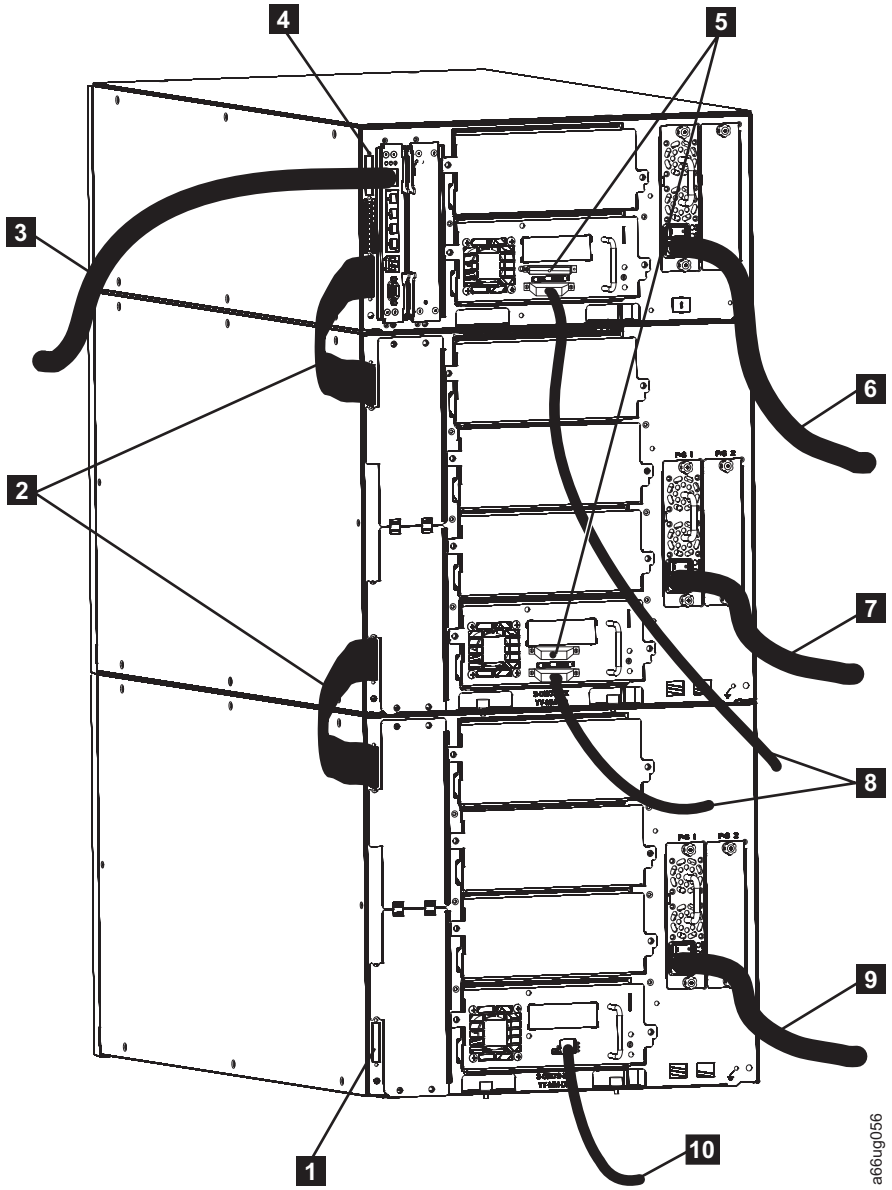


Figure 3-41. Cabling with Fibre Channel drives

1	Module communication terminator	6	Power cord (upper module)
2	Module-to-module communication cable	7	Power cord (middle module)
3	Ethernet cable (customer supplied)	8	SCSI drive-to-host cable
4	Module communication terminator	9	Power cord (lower module)
5	SCSI terminators	10	SAS or Fibre Channel drive-to-host cable

SCSI, SAS, and Fibre Channel drives can reside in the same physical or logical library. However, mixing drive interface types in the same logical library is not recommended.

1. Install a module communication terminator in the upper receptacle of the upper module of your library (4 in Figure 3-41).

2. Install one end of one of the module-to-module communication cables in the lower receptacle of the upper module of your library. Then, install the other end in the upper receptacle of the middle module of your library (**2** in Figure 3-41 on page 3-39).
3. Install one end of the other module-to-module communication cable in the lower receptacle of the middle module of your library. Then, install the other end in the upper receptacle of the bottom module of your library (**2** in Figure 3-41 on page 3-39).
4. Install a module communication terminator in the lower receptacle of the bottom module of your library (**1** in Figure 3-41 on page 3-39).
5. Install one end of the customer-supplied ethernet cable in the Library Control Blade (LCB) ethernet port. Then, connect the other end of the cable to your network (**3** in Figure 3-41 on page 3-39).
6. For each drive, install one end of the drive host SAS or fibre cable in a drive in the library. Then, connect the other end of the cable to your network (**10** in Figure 3-41 on page 3-39). Repeat this procedure for every drive in your library.

   Important: If you are cabling SAS drives to a host that uses a 4x Interposer (Feature code 5400 or 5500), the drive-to-host cables are limited to a maximum of 2.0 m length.

   The LTO-4 SAS drives use an SFF-8088 type connector. Each SAS tape drive must be connected directly to a SAS host bus adapter (HBA) with one SAS cable. The library does not currently support the use of SAS expander devices or cables.
7. Connect one end of the power cord in the receptacle of a power supply in your library. Then, connect the other end of the cord to your power source. Repeat this procedure for every power supply in your library (**6** , **7** , and **9** in Figure 3-41 on page 3-39).
8. Continue with “Powering ON the library.”

Powering ON the library

1. Turn each power supply switch (**4** in Figure 3-38 on page 3-35) to the ON (|) position.
2. Press the **Power** button on the front panel of the library. A green LED to the left of **Power** indicates that the power is ON.
3. Wait for the library to initialize. This initialization takes approximately 10 minutes.

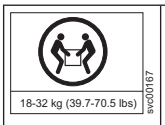
   Note: If the operator panel does not initialize, check all cable connections, ensure that all doors are tightly closed, and all power supply switches are in the ON position. Then, repeat steps 1 and 2. If the panel still does not initialize, see “Diagnosing a problem” on page 10-3.
4. When initialization is complete, configure the library. Read the information in Chapter 5, “Configuration planning,” on page 5-1 and Chapter 6, “User interfaces,” on page 6-1 before proceeding to Chapter 7, “Configuring the library,” on page 7-1.

Chapter 4. Installing a new stand-alone library on a desktop

Follow the steps in this chapter to install a new 5U or 14U library on a desktop. For instructions on converting your rack-mounted 5U or 14U library to a desktop unit or converting a 5U or 14U desktop library to a rack-mounted library, see "Library conversions" on page 12-52. For instructions on removing or replacing a control module or expansion module, see "Removing/replacing a control module" on page 12-3 and "Removing/replacing an expansion module" on page 12-15 in the *Setup and Operator 's Guide*.

Note: A desktop library can support only one expansion module. If you have two or more expansion modules, you must install the library in a rack.

Unpacking and verifying shipment contents



Important: Because of the weight of a multi-module library, it is recommended that you install it in the lowest position in a rack. Without drive sleds and power supplies, a control module weighs approximately 50 lbs. Without drive sleds and power supplies, each 9U expansion module weighs approximately 65 lbs.

1. Open and unpack all the boxes in your shipment.
2. Remove all external packaging materials from around the library module.

   Note: Leave the library module on the lifting sling until it is ready to be installed.
3. Verify the contents of your shipment.

Table 4-1. Shipment contents

Description	Number for each control module	Number for each expansion module
Library control module 5U	1	
Expansion module E9U (maximum 4 expansion modules per rack-mounted library)		1

Table 4-1. Shipment contents (continued)

Description	Number for each control module	Number for each expansion module
Module communication terminators	2	
Module-to-Module communication cable		1
Power cord for each primary power supply (If you are installing your library in a rack, you need Feature code 9848, Rack Power Distribution Unit (PDU) power cord.)	1	1
Power cord for each redundant power supply (if ordered)	1	1
Wrap plug for SCSI drives (if SCSI drives ordered)	1	
Wrap plug for Fibre Channel drives (if Fibre Channel drives ordered)	1	
Wrap plug for SAS drives (if SAS drives ordered)	1	
SCSI, Fibre Channel, or SAS cable for each tape drive (if ordered)	1 per drive	1 per drive
SCSI drive-to-drive cable with each SCSI drive ordered	1 per drive	1 per drive
SCSI terminator for each SCSI tape drive	1 per drive	1 per drive
Ethernet crossover cable (for service use only)	1	
Cleaning cartridge, with label	1	
Publications prepack kit	1	
Hotline card		1
Rack mount kit (if ordered)	1	
Extra rack hardware kit (rack ears)		1
Deskside kit (library feet and screws)	1	
Sling (for lifting and installing library modules)	1	1
Important: If any of these items are missing, call the appropriate number that is listed on the Hotline card included in your shipment.		

4. Remove all internal packaging materials that secure the picker assembly. The original-style picker is secured with cardboard and foam packing materials. The M2-style picker is secured to the bottom cover with two plastic shipping screws.

   Note: Failure to remove all internal packaging material before the library is powered ON results in damage to your library.

Figure 4-1. Original-style picker with internal packaging material

a. For the original-style picker, remove the fastening strap (**1** in Figure 4-1) across the top of the picker packaging material.

   Important: Be careful not to damage the picker assembly when the following packing materials are removed. DO NOT USE EXCESSIVE FORCE.

b. Remove the cardboard packaging material (**2** in Figure 4-1), the foam packaging material (**3** in Figure 4-1), and the small cardboard packaging material (not shown in picture).

c. For libraries with the M2-style picker, ensure that you removed the two plastic shipping screws and the orange ribbon from the picker Figure 4-2 on page 4-4 along with the yellow ribbon-like packing pieces from the I/O stations (Figure 4-3 on page 4-4).

Figure 4-2. M2 picker packaging screws and ribbon that is removed from the library

5. Remove the yellow ribbon-like packing pieces (**1** in Figure 4-3) from around the I/O station magazines.

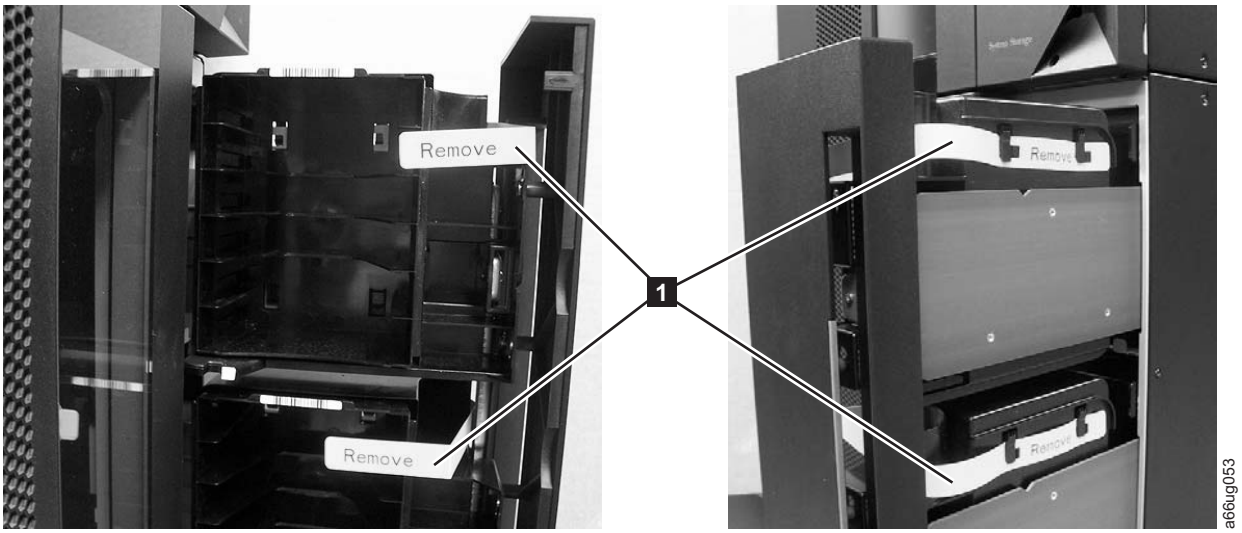


Figure 4-3. Yellow ribbon-like packing pieces

6. For libraries with the original-style picker, refer to Figure 4-4 and ensure that you removed all of the packaging material.

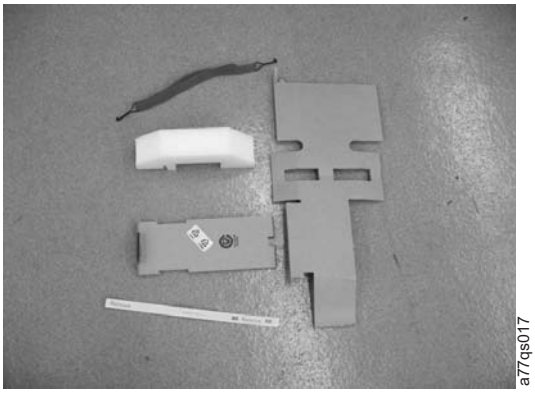


Figure 4-4. Packaging materials removed from library with the original-style picker

Reducing library weight

For weight reduction, remove the following components from each unit that must be moved for installation:

- Power supplies
- Drive sleds

Important: Because of the weight of a multi-module library, it is recommended that you install it in the lowest position in a rack. Without drive sleds and power supplies, a control module weighs approximately 50 lbs. Without drive sleds and power supplies, each expansion module weighs approximately 65 lbs.

Removing the power supply

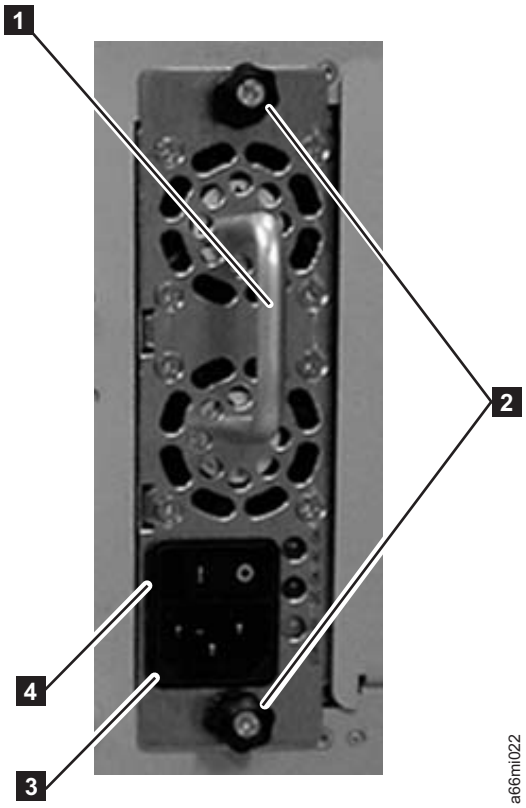


Figure 4-5. Power supply

For each installed power supply:

1. Loosen the two thumb screws (**2** in Figure 4-5) on the power supply by turning them counterclockwise.
2. To remove the power supply, grasp the handle (**1** in Figure 4-5) and slowly pull it toward you, while it is supported from underneath.

Removing a drive sled

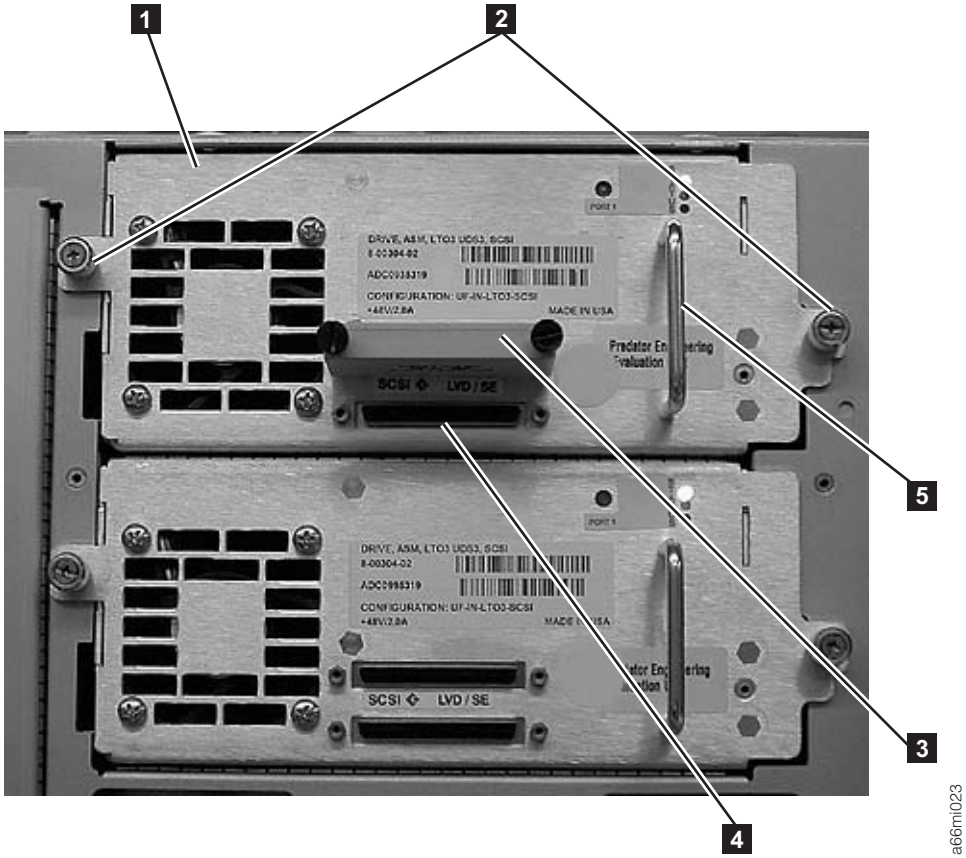


Figure 4-6. SCSI drive sled (detail)

For each installed drive:

1. Loosen the two thumb screws (**2** in Figure 4-6) that hold the drive sled in place by turning them counterclockwise.
2. To remove the drive sled, grasp the handle (**5** in Figure 4-6) and slowly pull it toward you, while the drive sled is supported from underneath.

Choosing a desktop configuration

A desktop library can have a maximum of one expansion module. The expansion module can be either the top or the bottom module in the library.

Refer to Figure 4-7 on page 4-7 and select one of the recommended configurations for your library installation.

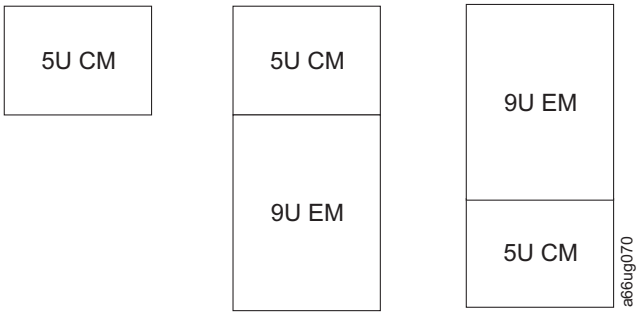


Figure 4-7. Recommended desktop library configurations

The control module is shipped with a top and a bottom cover for the library. Expansion modules do not come with covers.

- If you are building a 14U library (one control module and one expansion module), you must move one of the covers to the expansion module.
  - If the control module is on top of the expansion module, continue with "Transferring the bottom cover from the control module to an expansion module."
  - If the control module is under the expansion module, continue with "Transferring the top cover from the control module to an expansion module" on page 4-13.
- If you are building a 5U library (control module with no expansion modules), you do not need to move the covers. Continue with "Installing library foot pads" on page 4-14.

Transferring the bottom cover from the control module to an expansion module

Each library comes with a bottom cover that is shipped with the control module. If you are installing an expansion module as the first or bottom module in a library, you must move the bottom cover from the control module to the bottom of the expansion module.

1. Engage the picker assembly lock mechanism (**1** in Figure 4-8 on page 4-8). You might need to lift the picker assembly to fully engage the lock mechanism.

Figure 4-8. Picker locking mechanism

2. Turn the 5U control module on its side and remove the 5 - T10 Torx bottom cover screws (**1** in Figure 4-9 on page 4-9).

   Important: DO NOT loosen or remove the screw that holds the home sensor (**2** in Figure 4-9 on page 4-9). This screw has the same T10 Torx head as the cover screws, but it is longer and has a coarse thread for screwing into the plastic home sensor.

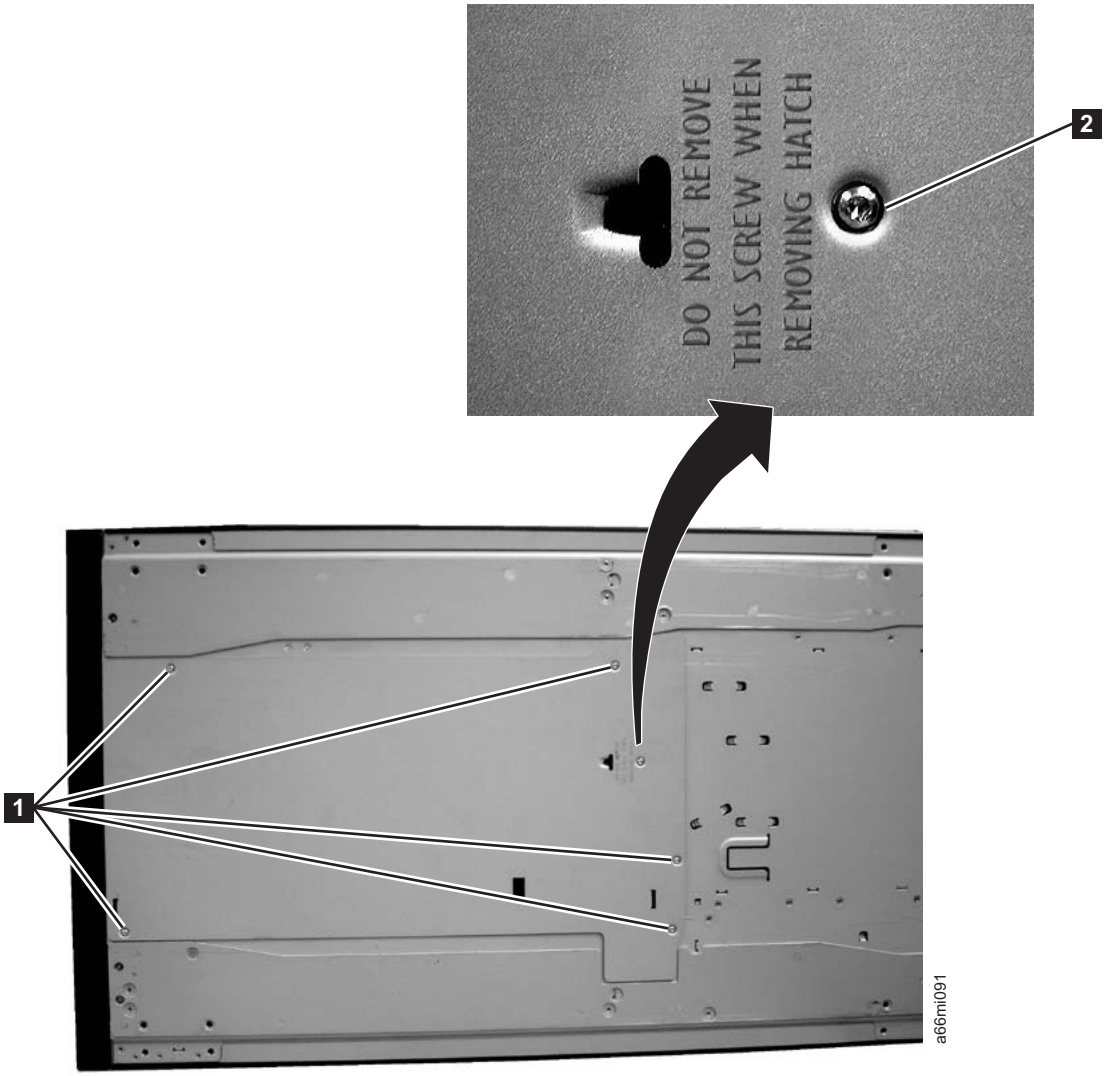


Figure 4-9. Bottom cover of the 5U control module

3. Remove the bottom cover from the 5U control module.

   Note: Ensure that the home sensor plastic piece is mounted on the inner side of the bottom cover (**1** in Figure 4-10 on page 4-10).

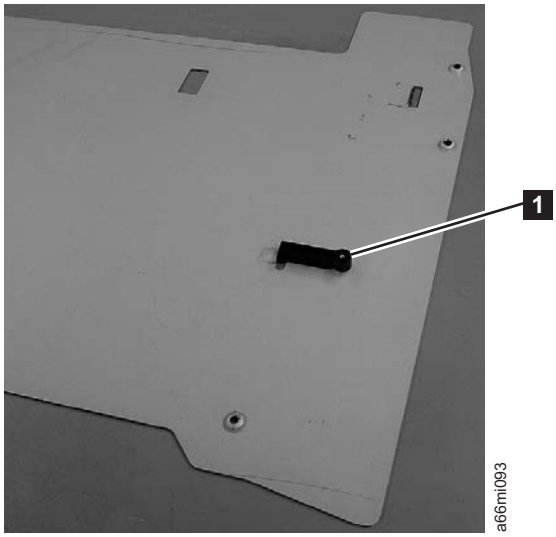


Figure 4-10. Home sensor on inner side of bottom cover

Important: Ensure that the picker lock mechanism (**1** in Figure 4-11) is engaged as shown. This procedure prevents the picker mechanism from falling out of the bottom of the 5U control module when it is returned to the upright position without a bottom cover installed.

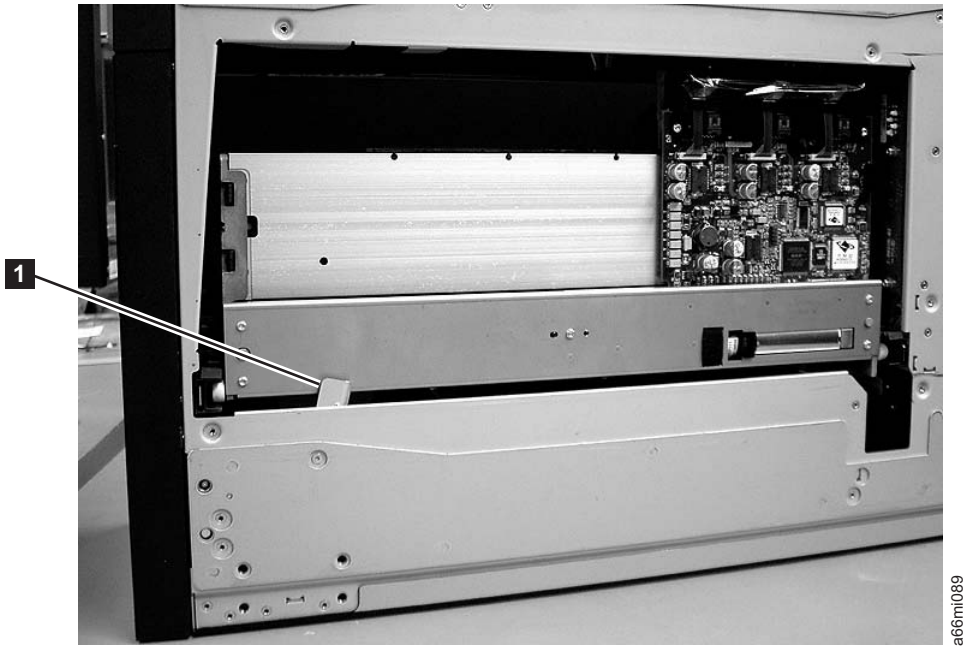


Figure 4-11. Bottom view of picker assembly lock mechanism

4. Return the 5U control module to the upright position.
5. Ensure that the front and rear gear racks of both the control module and the expansion module are locked in the upper position (see **2** in Figure 4-13 on page 4-11).

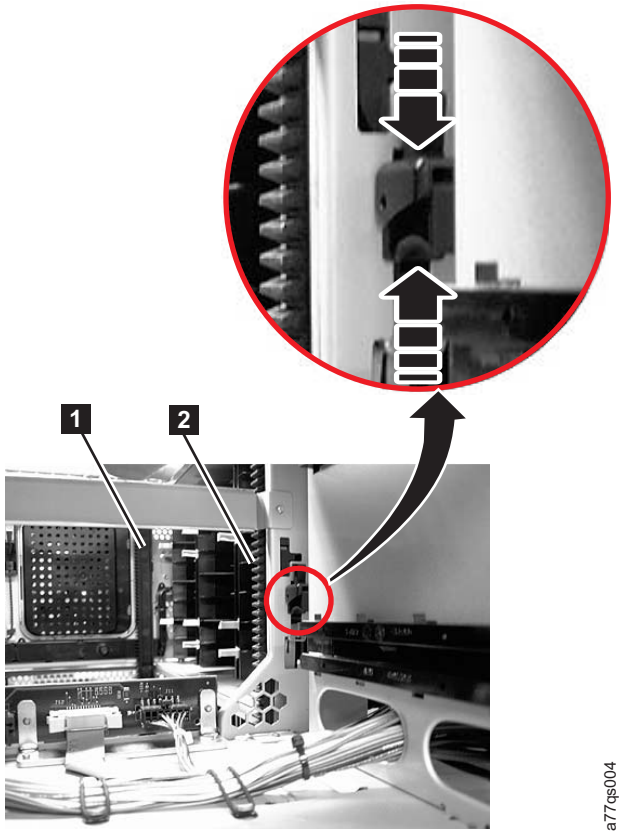


Figure 4-12. Front and back gear racks

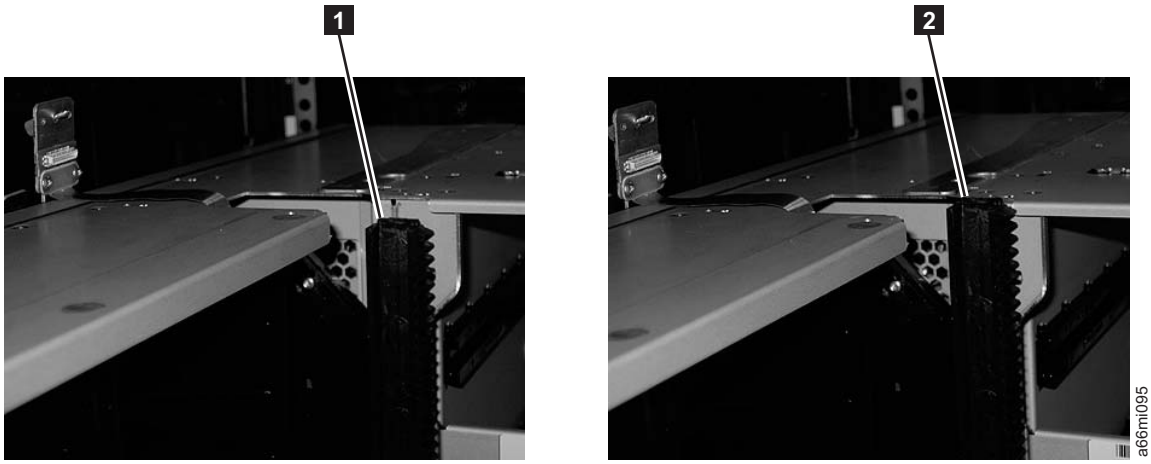


Figure 4-13. Gear racks positions (rear gear racks shown)

1	Gear rack in the down position	2	Gear rack in the up position

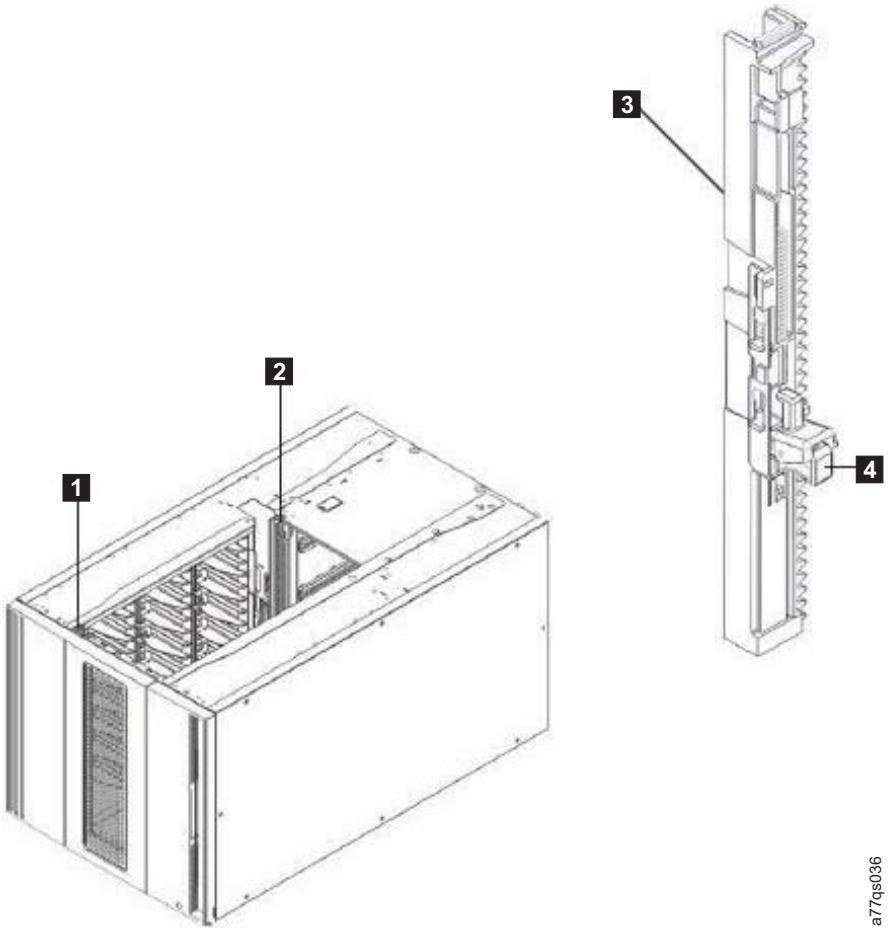


Figure 4-14. Y-Rails

1	Front Y-rail	2	Rear Y-rail
3	Y-rail (this end up)	4	Squeeze here to release

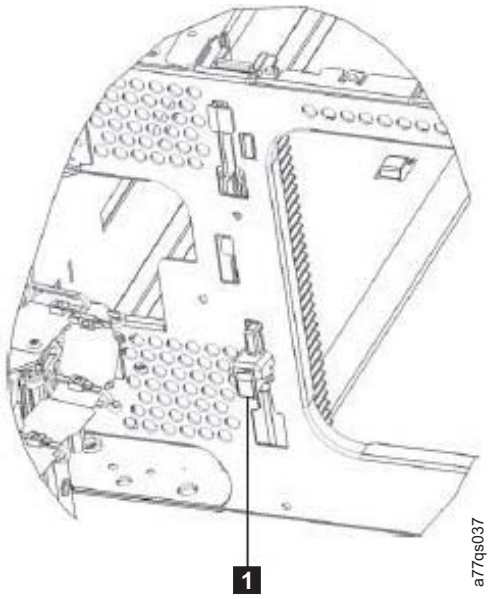


Figure 4-15. Y-rail in position

1 Y-rail in locked, non-functional position

6. Turn the expansion module on its side and install the bottom cover, with the 5 - T10 Torx screws.
7. Return the expansion module to the upright position.

Transferring the top cover from the control module to an expansion module

Each library comes with a top cover that is shipped with the control module. If you are installing the expansion module as the top module in the library, you must move the top cover from the control module to the expansion module.

1. Remove the 4 - #2 Phillips top cover screws (**1** in Figure 4-16 on page 4-14).

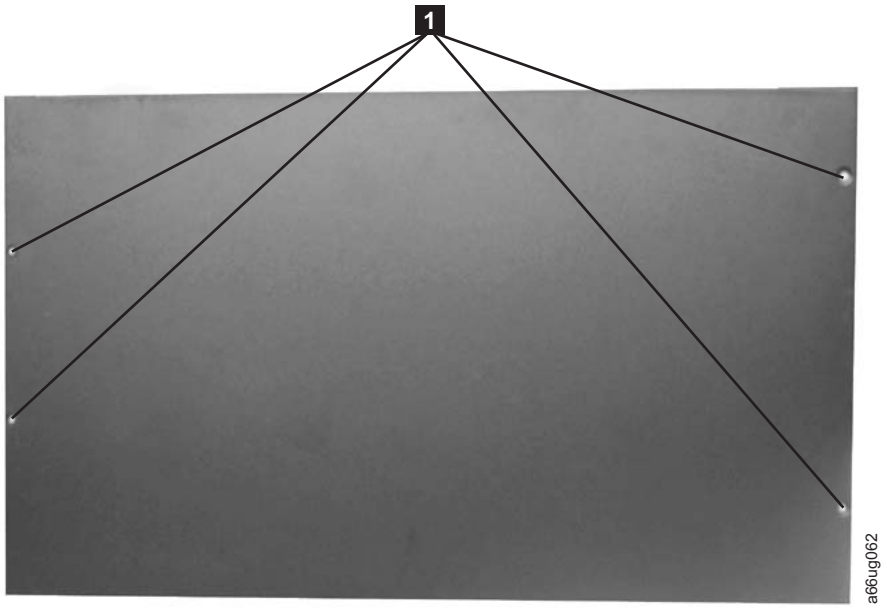


Figure 4-16. Top cover of the 5U control module

2. Remove the top cover from the 5U control module.
3. Ensure that the front and rear gear racks of both the control module and the expansion module are locked in the upper position (see **2** in Figure 4-13 on page 4-11).
4. Install the top cover on the expansion module, with the 4 - #2 Phillips screws (**1** in Figure 4-16).

Installing library foot pads

For a desktop installation, foot pads must be installed on the bottom module of your library. To install the library foot pads:

1. Carefully lay the module on its side.
2. With a #2 Phillips screwdriver, install the foot pads on the bottom of the library chassis. See Figure 4-17 on page 4-15 for foot pad locations.

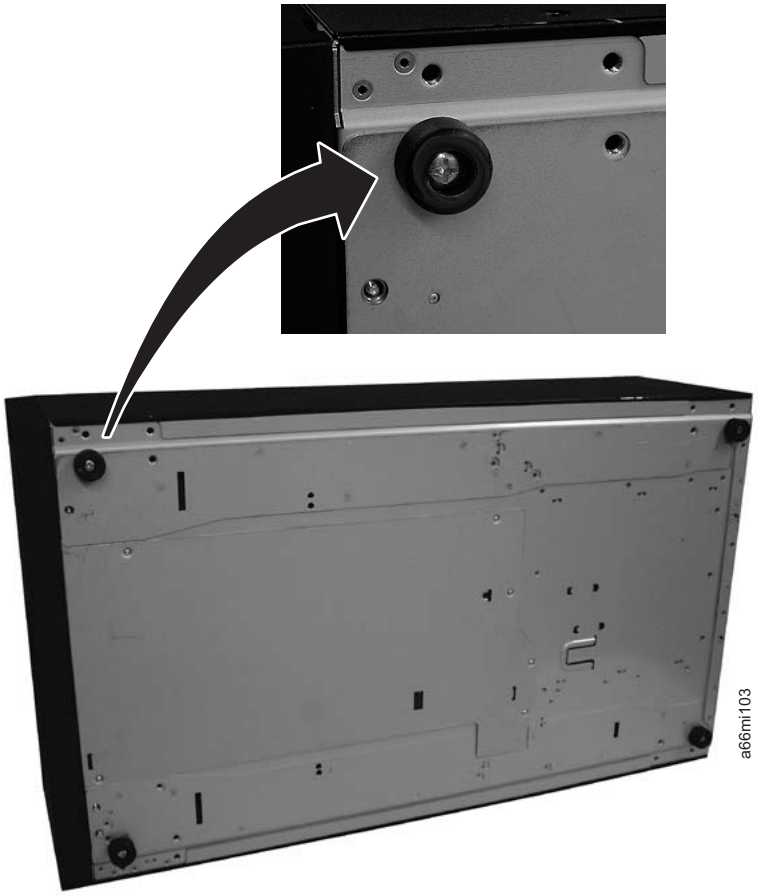


Figure 4-17. Foot pad locations

3. Carefully return the library to an upright position.
4. Use the lifting sling to place the library module in the desktop location.
5. For a 5U (control module only) library, store the installation sling in a secure location for possible future use. Then, continue the library installation with the instructions on "Enabling the picker assembly" on page 3-31.

Installing a module in the middle (or top) of your 14U library configuration

Once the bottom module is installed, you can add more modules to your library.

Attention: If you are installing the 5U control module on the top of your library, ensure that the picker assembly lock mechanism (**1** in Figure 4-18 on page 4-16) is engaged as shown in Figure 4-18 on page 4-16.

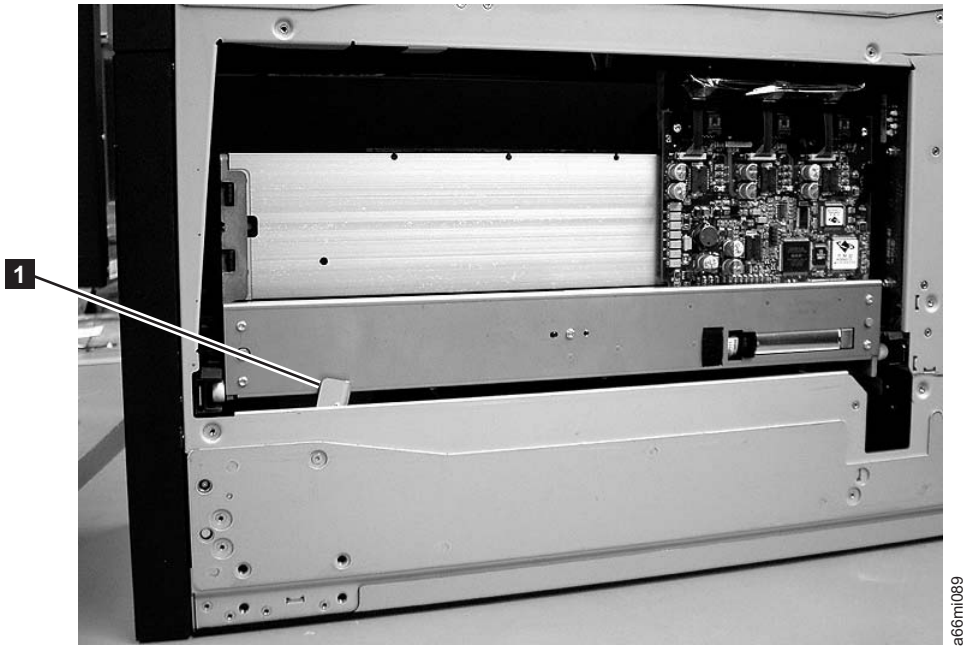


Figure 4-18. Bottom view of picker assembly lock mechanism

Also, ensure that the front and rear gear racks of the top module are locked in the upper position (see **2** in Figure 4-20 on page 4-17).

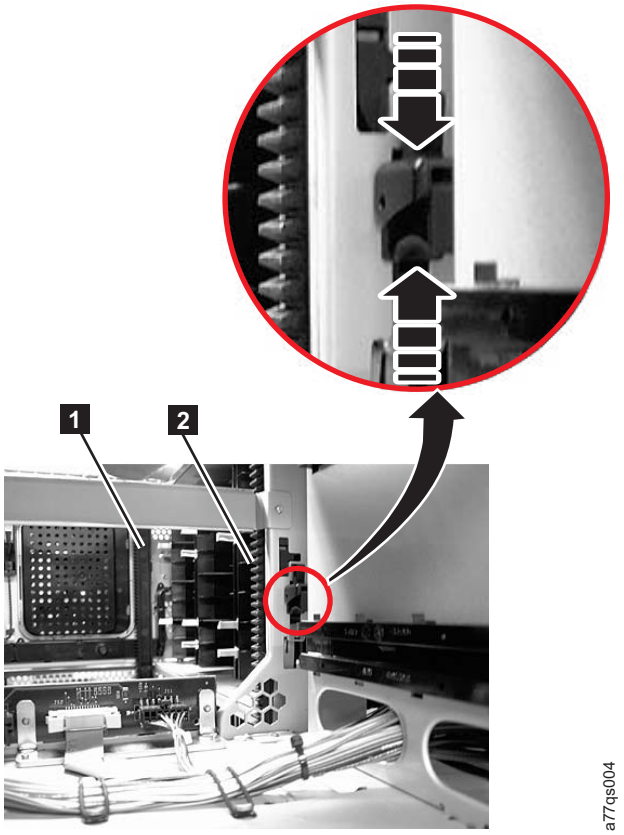


Figure 4-19. Front and back gear racks

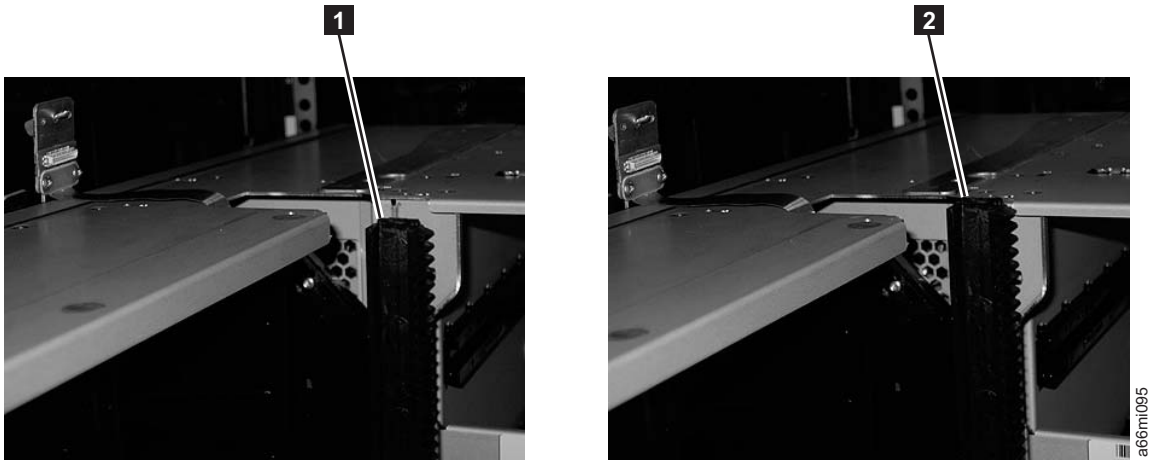


Figure 4-20. Gear racks positions (rear gear racks shown)

1	Gear rack in the down position	2	Gear rack in the up position

1. If the front and rear gear racks of the top module are NOT locked in the upper position, raise the gear racks, disengage the Y-rails so the modules can be unstacked safely.

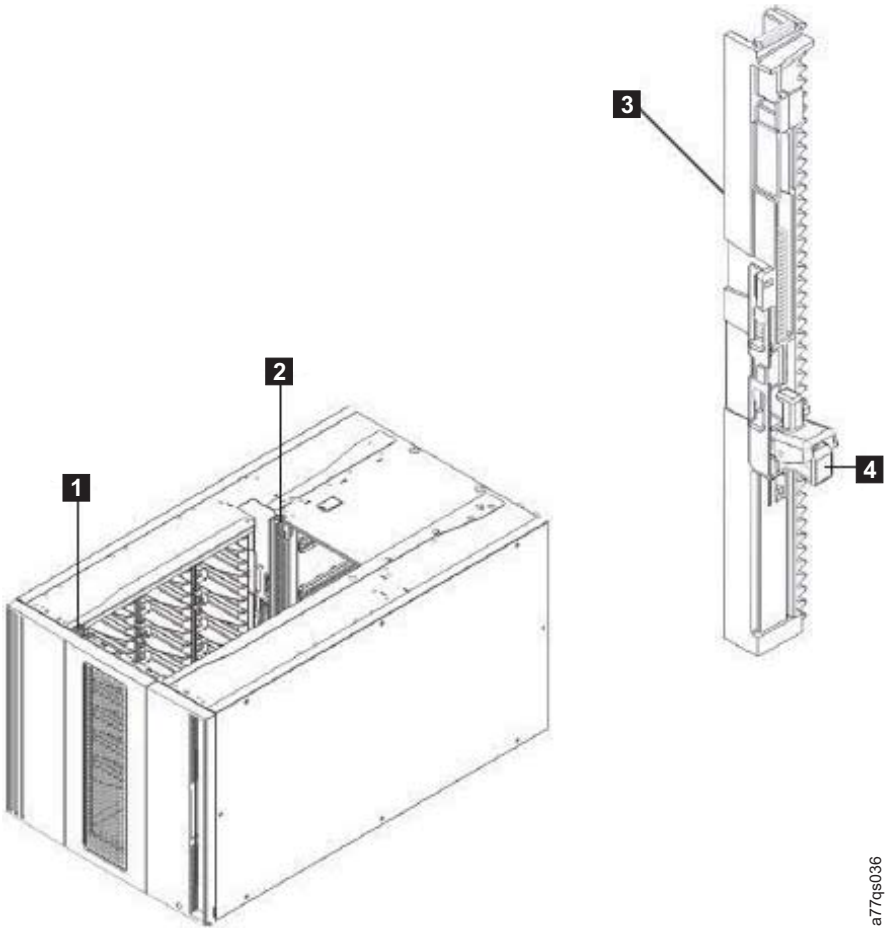


Figure 4-21. Y-Rails

1	Front Y-rail	2	Rear Y-rail
3	Y-rail (this end up)	4	Squeeze here to release

a. From the front of the library, find the Y-rail release mechanism, which is on the left side of the control module. Squeeze the handle of the Y-rail release mechanism, lift it, and release it so that it locks into place.

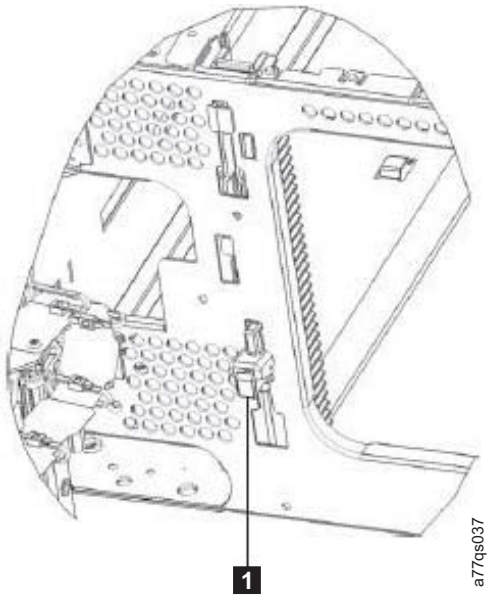


Figure 4-22. Y-rail in position

1 Y-rail in locked, non-functional position

b. From the rear of the library, find the rear Y-rail release mechanism that is in the interior of the right side of the module. Squeeze the handle of the Y-rail release mechanism, lift it, and release it so that it locks into place.

2. Ensure that the module-to-module alignment pin of the top module (**1** in Figure 4-23 on page 4-20) is in the raised position. If necessary, raise the pin and rotate it half a turn to lock it in the raised position.

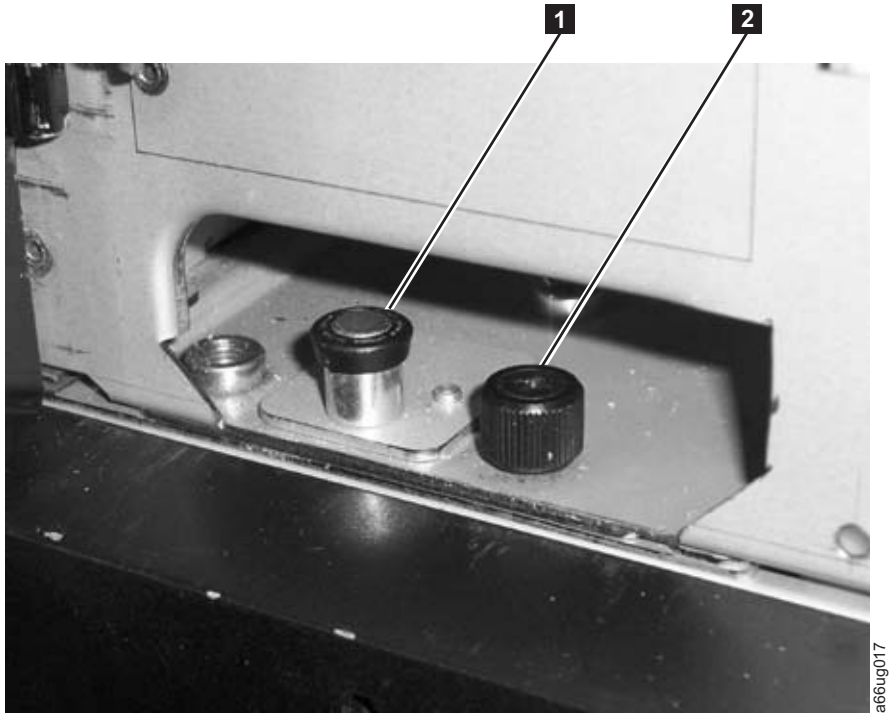


Figure 4-23. Module-to-module alignment pin and front thumb screw

3. With a person on each side of the module, lift the module with the sling provided. See Figure 4-24 on page 4-21 to see how the lifting sling handles must be folded.

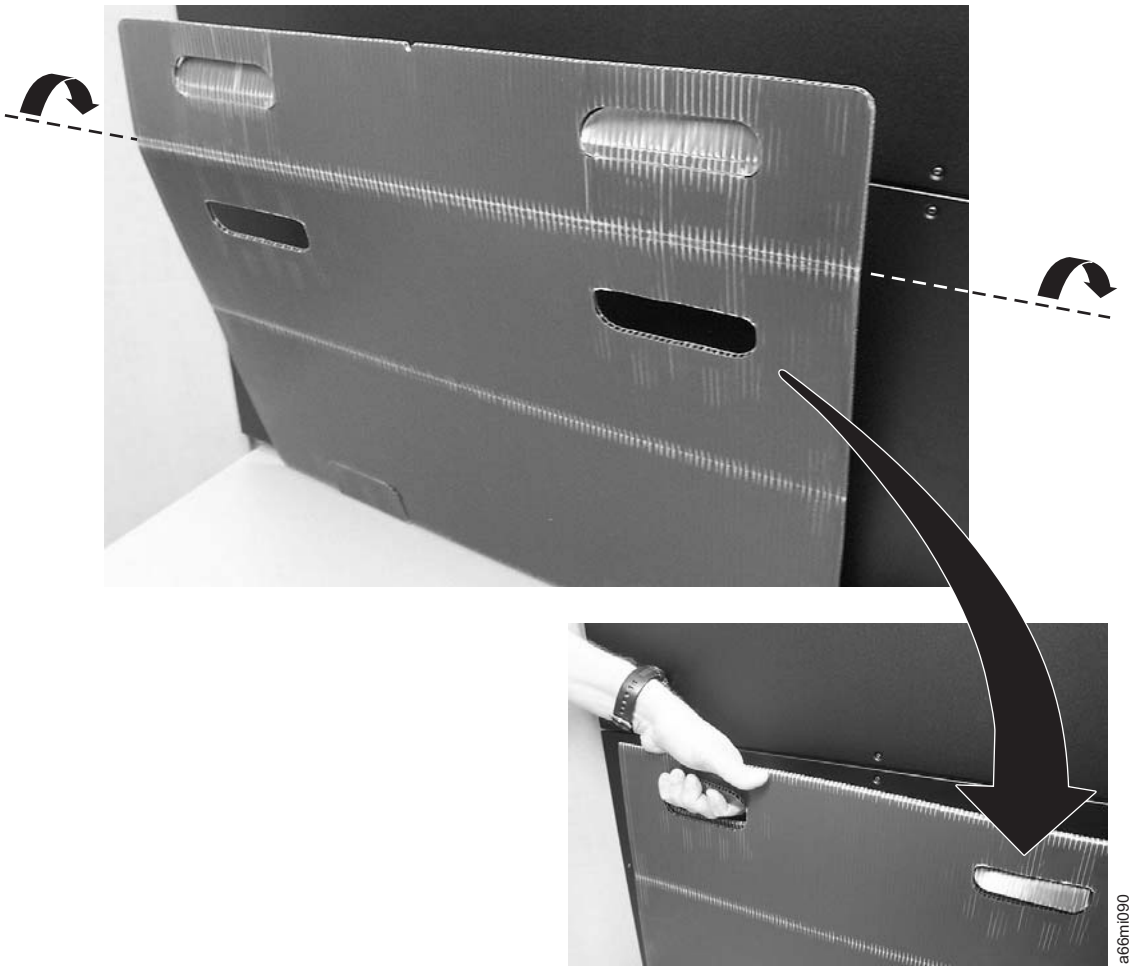


Figure 4-24. Lifting sling

4. Slide the module partially on top of the already installed module.
5. Continue to support the library module from the front while you remove the sling.
6. Open the I/O Station door then the Access Door of the upper module to expose the alignment pin behind the Access Door.
7. Push the upper module onto the lower module.
8. Twist the upper module alignment pin (**1** in Figure 4-23 on page 4-20) to unlock it from the up position.
9. Adjust the upper module 's position on top of the lower module until the upper module alignment pin drops into the alignment pin receptacle in the lower module.
10. Tighten the front thumb screw (**2** in Figure 4-23 on page 4-20) and the thumb screw behind the I/O station door to secure the front of the upper module to the lower module.
11. Tighten the rear thumb screws (**1** in Figure 4-25 on page 4-22) that secure the upper module to the lower module.

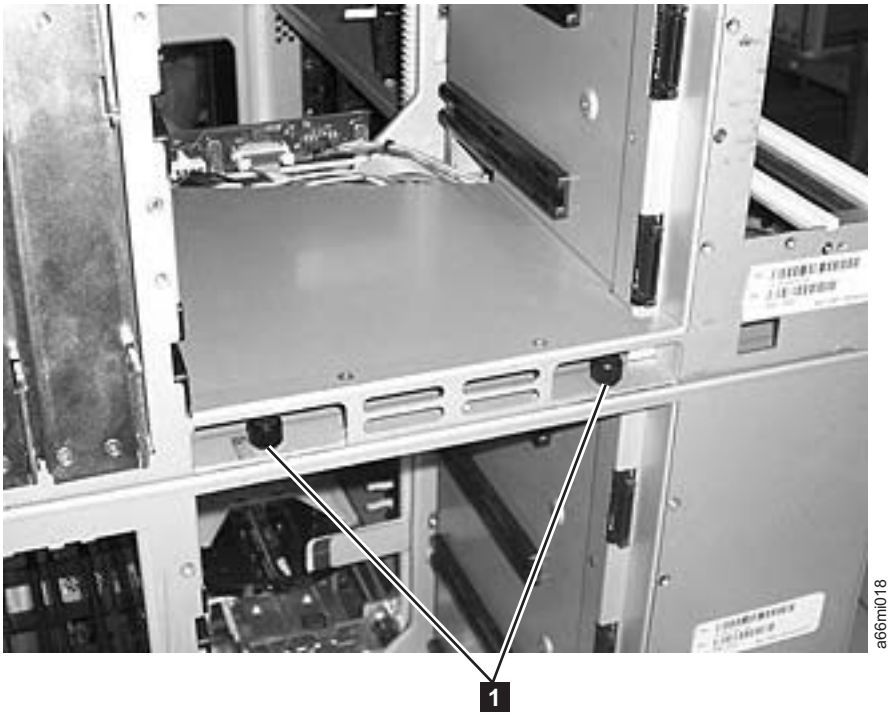


Figure 4-25. Rear thumb screws

12. Lower the gear racks into the down (operating) position by engaging the Y-rails of each module in your library configuration. Ensure that the Y-rails are properly aligned and the thumbscrews are tightened.

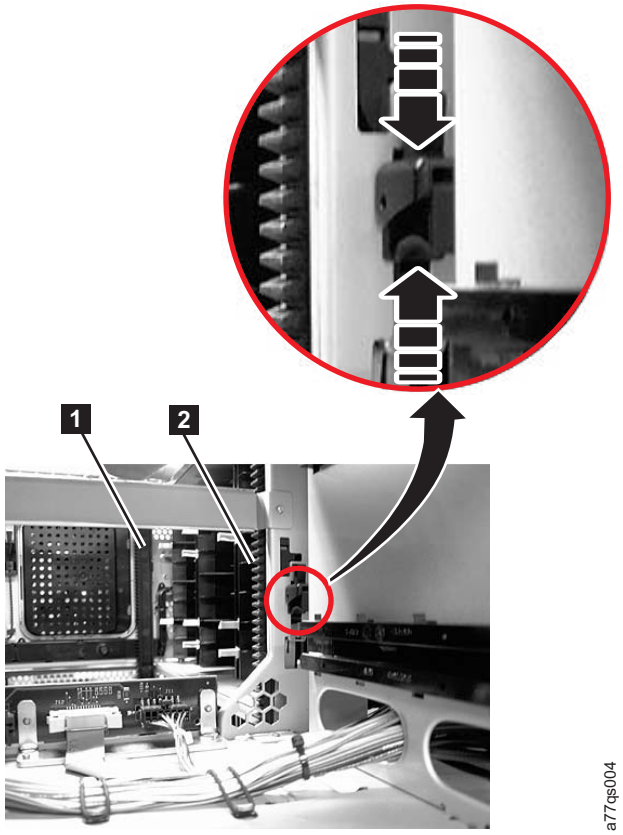


Figure 4-26. Front and back gear racks

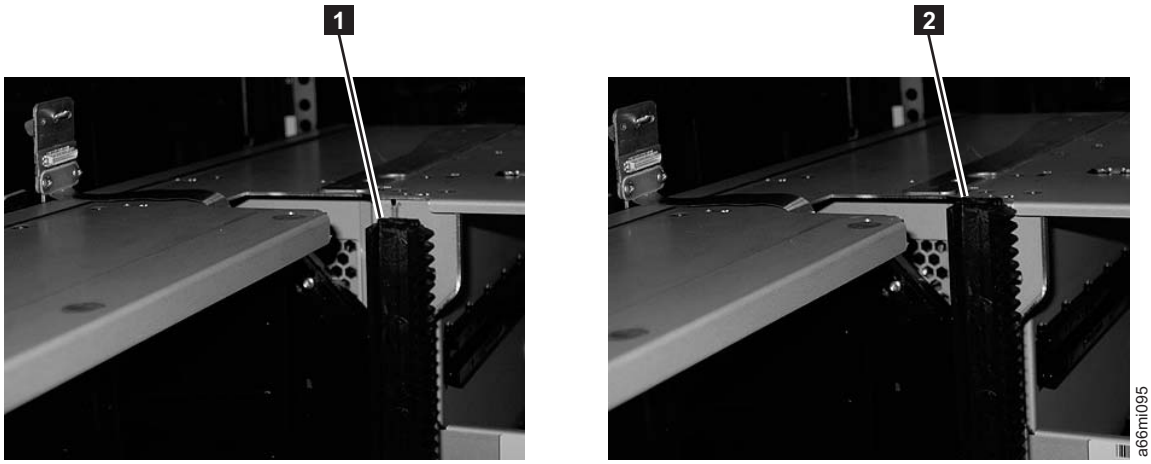


Figure 4-27. Gear racks positions (rear gear racks shown)

1	Gear rack in the down position	2	Gear rack in the up position

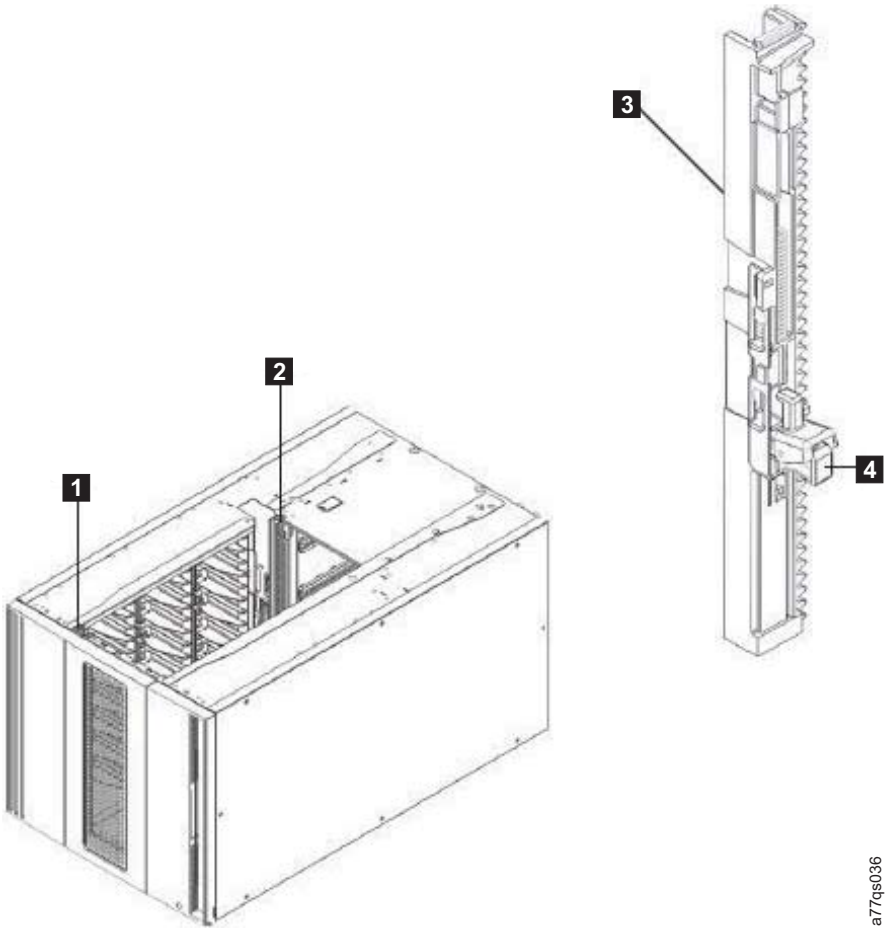


Figure 4-28. Y-Rails

1	Front Y-rail	2	Rear Y-rail
3	Y-rail (this end up)	4	Squeeze here to release

a. From the front of the library, open the I/O station and access doors of the 9U expansion module. Squeeze the handle of the Y-rail release mechanism, lift it out of its locked position, and slide it downward as far as it goes.

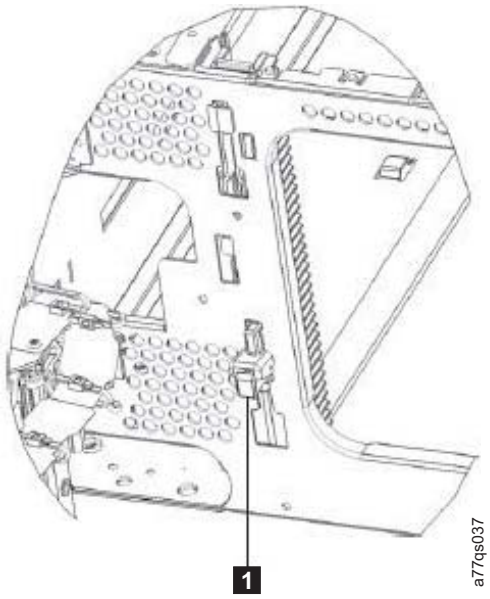


Figure 4-29. Y-rail in position

1 Y-rail in locked, non-functional position

b. From the back of the library, find the rear Y-rail release mechanism, which is in the interior of the right side of the module. Squeeze the handle of the Y-rail release mechanism, lift it out of its locked position, and slide it downward as far as it goes. Doing this procedure aligns the Y-rails with the Y-rails of the module beneath it.

   Attention: Check to make sure that there is no gap between the top and bottom Y-rails on both the front and back of the library. If a gap exists, the library cannot mechanically initialize.

13. Store the installation-lifting sling in a secure location for possible future use.

Enabling the picker assembly

Important: Picker assembly damage or library accessor errors can occur if the front or rear gear racks are not engaged properly.

1. **IMPORTANT:** Ensure that the front and rear gear racks are in the down (operating) position. See **1** in Figure 4-20 on page 4-17.
2. Feel the junction of the gear racks between each library module, front and rear. Ensure that there are no gaps between the gear racks before you release the picker assembly lock mechanism.
3. Manually raise the picker assembly while you release the lock mechanism (**1** in Figure 4-30 on page 4-26).

Figure 4-30. Releasing the picker assembly lock mechanism

4. Release the picker assembly and observe it as it slowly drops to the bottom of the library. It must move smoothly as it travels from one module into the other.

   Note: If the picker jumps or bumps noticeably as it travels from one module into the other, an error is likely to occur when the library is powered ON. Follow the instructions in "T083: Unlevel robot assembly not level" on page 11-39 the *Setup and Operator 's Guide* to correct the problem.

Installing library components removed for weight reduction

Follow these steps to install the components that were removed earlier for weight reduction.

1. Install the drive sleds in their original locations. See "Installing a drive sled." Refer to the notes you made earlier on drive position.
2. Install the power supplies beginning with the left position in each library unit that contains drives. See "Installing a power supply" on page 4-28.

Installing a drive sled

Attention: NEVER install a drive sled when a cartridge is in the drive in the eject position. Remove the cartridge first.

1. Align the drive sled with the guide rails and guide slots along the tracks (**3** in Figure 4-31 on page 4-27).

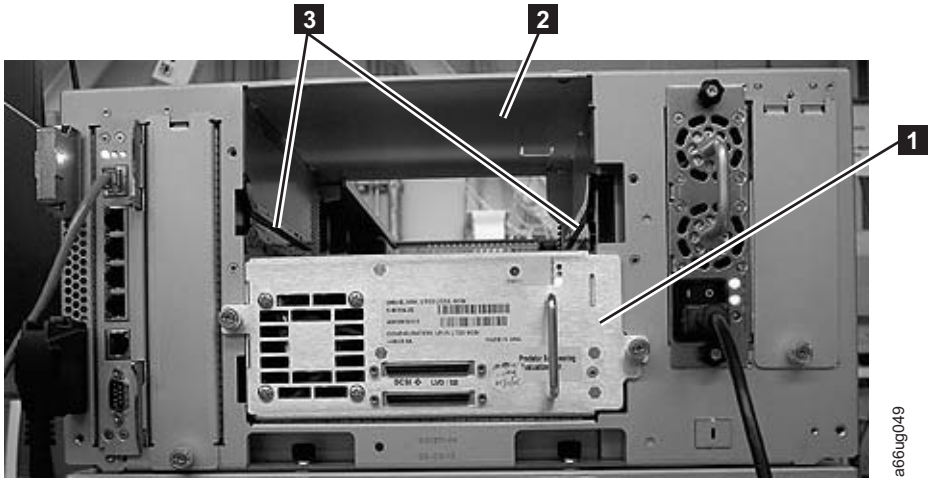


Figure 4-31. Guide rails and guide slots inside a drive slot

2. Grasp the handle (**5** in Figure 4-32) and slowly slide the drive sled into the drive slot, while the drive sled is supported from underneath.

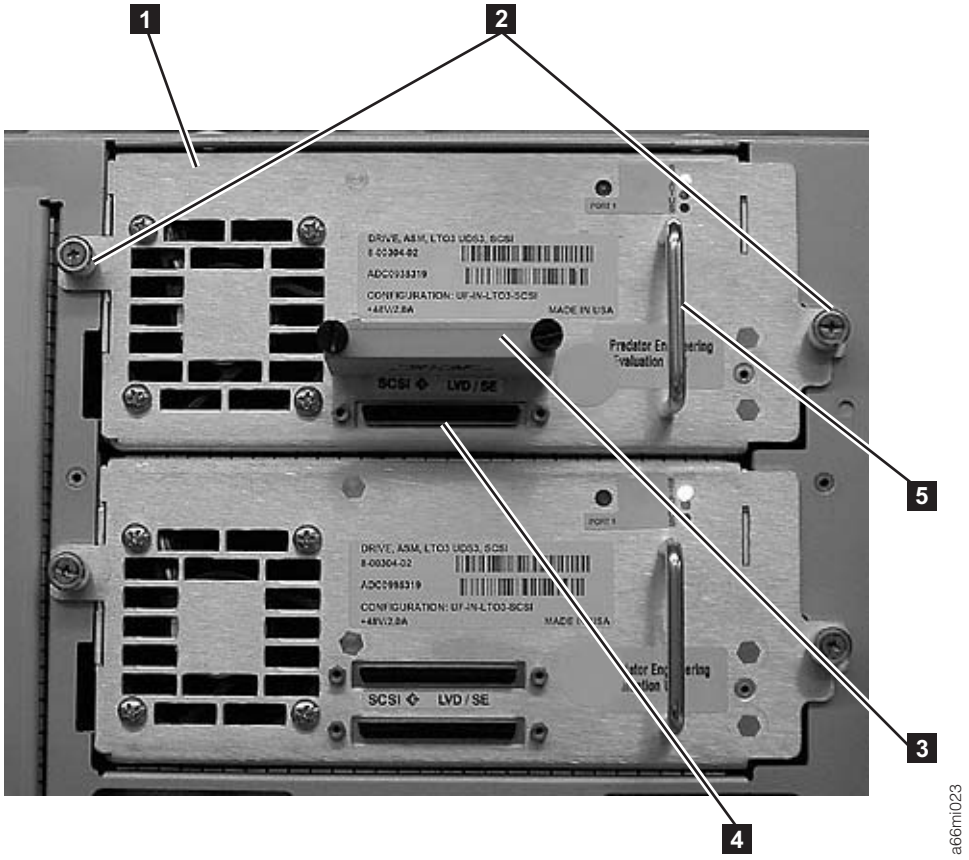


Figure 4-32. Tape drive (detail)

3. Tighten the two thumb screws (**2** in Figure 4-32) that hold the drive sled in place by turning them clockwise.
4. Repeat this procedure for all drives to be reinstalled in the library.

Installing a power supply

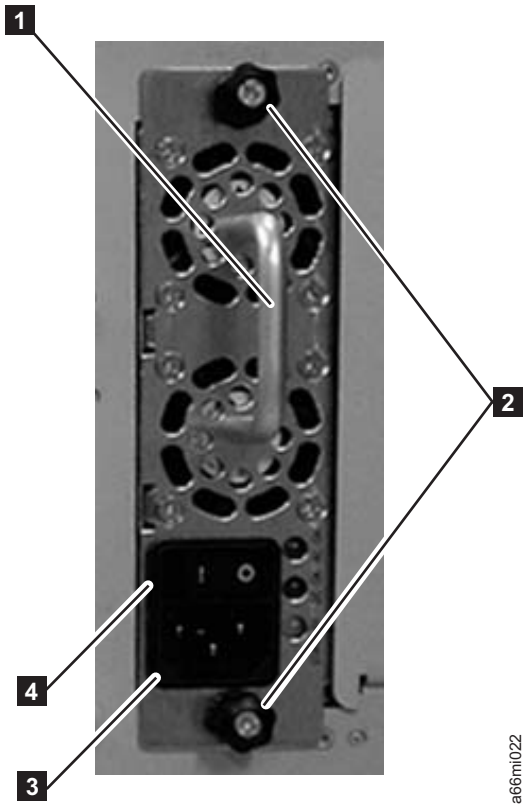


Figure 4-33. Control module power supply

1. Replace the power supply component by sliding it into the power supply slot. First, grasp the handle (**1** in Figure 4-33) while the power supply component is supported from underneath. Then, line up the power supply component with the guides in the power supply slot, and carefully push it into the library.
2. Tighten the two thumb screws (**2** in Figure 4-33) on the power supply component by turning them clockwise.
3. Repeat this procedure for each library power supply.

Cabling the library

Install the module-to-module communication cable, the module communication terminators, the customer-supplied ethernet cable, drive-to-host (SCSI, Fibre Channel, or SAS) cables, and the power supply cabling. Select and complete one of the following cabling procedures, depending upon your library configuration:

- "Cabling a 5U control module"
- "Cabling a 14U library with SCSI drives" on page 4-29

Cabling a 5U control module

To cable a 5U library control module, complete the following steps:

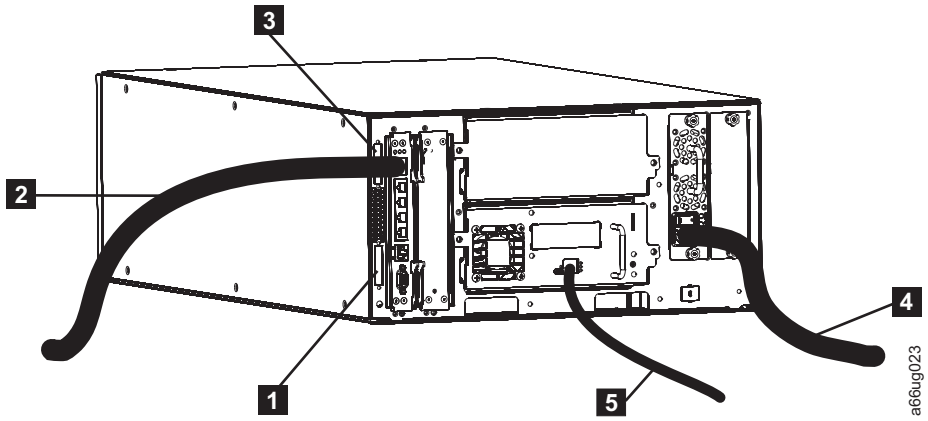


Figure 4-34. Cabling of a 5U library with Fibre Channel drives

1	Module communication terminator	4	Power cord
2	Ethernet cable (customer supplied)	5	Fibre drive-to-host cable
3	Module communication terminator		

1. Install the upper module communication terminator. 3 in Figure 4-34.
2. Install the lower module communication. 1 in Figure 4-34.
3. Connect one end of the customer-supplied ethernet cable (2 in Figure 4-34) in the Library Control Blade (LCB) ethernet port. Then, connect the other end of the cable to your network.
4. Connect one end of the drive-to-host cable (5 in Figure 4-34) to the library. Then, connect the other end of the cable to your network. Repeat this procedure for every drive in your library.

   Important: If you are cabling SAS drives to a host that is using a 4x Interposer (Feature code 5400 or 5500), the drive-to-host cables are limited to a maximum of 2.0 m length.

   Note: This procedure shows a Fibre Channel drive cable. SAS connections are similar. For details of SCSI cabling, see "Cabling a 14U library with SCSI drives."
5. Connect one end of the power cord (4 in Figure 4-34) in the receptacle in a power supply in your library. Then, connect the other end of the cord to your power source. Repeat this procedure for every power supply in your library.
6. When all the modules are cabled, continue with "Powering ON the library" on page 4-31.

Cabling a 14U library with SCSI drives

To cable a library with SCSI cables, complete the following steps:

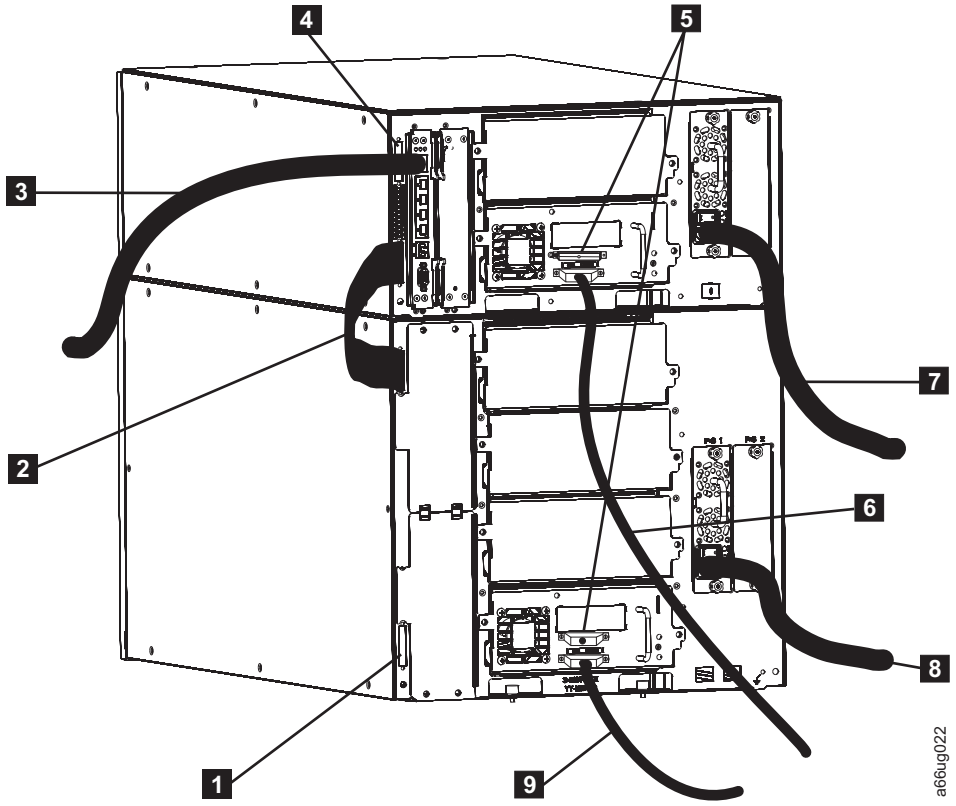


Figure 4-35. Cabling of a 14U library that contains multiple SCSI drives

1	Module communication terminator	6	SCSI drive-to-host cable
2	Module-to-module communication cable	7	Power cord (upper module)
3	Ethernet cable (customer supplied)	8	Power cord (lower module)
4	Module communication terminator	9	SCSI drive-to-host cable
5	SCSI terminators		

1. Install a module communication terminator in the upper receptacle of the upper module of your library (4 in Figure 4-35).
2. Install one end of the module-to-module communication cable (2 in Figure 4-35) in the lower receptacle of the upper module of your library. Then, install the other end in the upper receptacle of the lower module of your library.
3. Install a module communication terminator in the lower receptacle of the lower module of your library (1 in Figure 4-35).
4. Install one end of the customer-supplied Ethernet cable (3 in Figure 4-35) in the Library Control Blade (LCB) ethernet port. Then, connect the other end of the cable to your network.
5. Installation of the SCSI cable and terminator depends upon how many drives are in your library. For maximum SCSI drive performance:
   - For each SCSI drive, install a SCSI terminator (5 in Figure 4-35) in the upper receptacle of each SCSI drive in your library.

- For each SCSI drive, connect one end of a SCSI cable to the lower receptacle of each SCSI drive (**6** in Figure 4-35 on page 4-30). Then, connect the other end of the cable to the host.
- If you prefer to daisy-chain your SCSI drives:
  a. Install a SCSI terminator in the upper receptacle of the top SCSI drive in the daisy-chain.
  b. Connect one end of a shorter drive-to-drive SCSI cable included in your shipment to the lower receptacle of the top SCSI drive in the daisy-chain. Then, connect the other end of the cable to the upper receptacle of the next drive in the daisy-chain. Repeat this procedure for every SCSI drive in your library.
  c. On the last drive in the daisy-chain, connect one end of the longer drive-to-host SCSI cable included in your shipment to the lower receptacle of the last drive in the daisy-chain. Then, connect the other end of the cable to the host.

  Note: Maximum performance of the SCSI drives in your library cannot be achieved if the drives are daisy-chained.

6. Connect one end of the power cord (**7** and **8** in Figure 4-35 on page 4-30) in the receptacle of a power supply in your library, then connect the other end of the cord to your power source. Repeat this procedure for every power supply in your library.
7. Continue with "Powering ON the library."

Powering ON the library

1. Turn the switch on each power supply (**4** in Figure 4-33 on page 4-28) to the ON (|) position.
2. Push the **Power** button on the front panel of the library. A green LED to the left of **Power** indicates that the power is ON.
3. Wait for the library to initialize. This procedure takes approximately 10 minutes.

   Note: If the operator panel does not initialize, check all cable connections, and ensure that all doors are tightly closed and all power supply switches are in the ON position. Then, repeat steps 1 and 2. If the panel still does not initialize, see "Diagnosing a problem" on page 10-3 the *Setup and Operator 's Guide*.
4. When initialization is complete, configure the library. Read the information in Chapter 5, "Configuration planning," on page 5-1 and Chapter 6, "User interfaces," on page 6-1.

Chapter 5. Configuration planning

Cartridge assignments in the library

When a cleaning or data cartridge is placed in the I/O station, the library scans the I/O station. If 'Manual Cartridge Assignment' is enabled, a screen is displayed about assigning the cartridge to "System" or to a logical library. Cleaning cartridges are assigned to "System" that makes them available to all drives regardless of the logical library to which the drive is assigned. Data cartridges are assigned to a logical library, which restricts them from being accessed by another logical library. A drive Firmware (FMR) cartridge that is placed in the I/O station for drive firmware update must also be assigned as a SYSTEM cartridge when the assignment screen is presented after the I/O station door closes. Selecting CANCEL or allowing the assignment screen to time out defaults all newly discovered cartridges in the I/O station to Unassigned cartridges. These cartridges must be reassigned with the Operator (Op) Panel by reopening and closing the I/O station. If this action is not done, the cartridges remain in the I/O station as Unassigned cartridges and are not usable.

If manual Cartridge assignment is disabled from the Op Panel (**Tool** > **System Settings** > **Manual Cartridge Assignment**), the Insert Notification screen does NOT display. The inserted cartridges in the I/O station are then visible to all logical libraries, including the system logical library. The cartridges can then be manually moved with the Web UI to any logical library or used by any logical library with the host application.

When a cartridge is assigned to "System" or to a logical library, the cartridge must be physically exported from the library to the I/O station. Then, the cartridge is moved to a different slot in the I/O station before it can be reassigned to a new destination within the library. If the cartridge is left in the same I/O station slot, the library retains the same assignment, even if the I/O station door is opened and closed.

Cartridges that are placed in the I/O station before the library is powered ON do not have an initial assignment. To "force" an assignment screen for newly discovered cartridges, the I/O station must be opened and then closed. Shuffling of the cartridges to different I/O station slots is not necessary. Previously assigned cartridges before power OFF that remain in the same I/O station slots retain their original assignment.

Modifying network settings

The network settings set the connectivity of the library to the network. The connection allows the administrative user to transfer information while the library on the network is managed.

During initial installation, administrative users can modify the network settings from the Operator Panel only. After the initial configuration, administrative users can modify network settings from the Operator Panel or from the Web User Interface.

Note: Make sure that the library is connected to the network before network settings are modified.

To modify network settings, you must provide the data for the following fields:

- `Library Name` is the network name that you want to assign to the library. The library name can be up to a maximum of 12 characters long.
- **Dynamic Host Configuration Protocol** (DHCP) setting defaults to enabled. Enabling this option allows DHCP to automatically configure the library network settings. Selecting "Use DHCP" makes the **IP Address**, **Subnet Mask**, and **Default Gateway** text boxes unavailable. If "Use DHCP" is not selected, the **IP Address**, **Subnet Mask**, and **Default Gateway** text boxes are available for you to manually set the library network settings.
- **IP Address** is the IP address of the library. This text box is available only if DHCP is disabled.
- **Subnet Mask** text box is available only if DHCP is disabled.
- **Default Gateway** is the IP address of the default gateway for your portion of the ethernet network. This text box is available only if DHCP is disabled.

Note: Modifying network settings from the Web User Interface changes the network connectivity parameters and can cause your current web user session to become invalid. If this action happens, close the current session, access the web client again with the new network configuration settings, and log in again.

Applying a license key

License keys can be purchased for expanding library capacity, enabling advanced reporting, enabling control path failover and data path failover, and enabling transparent LTO encryption.

A Capacity Expansion license key (Feature code 1640) can be applied to the library during the initial configuration or at any time in the future. Capacity Expansion License keys are absolute values that can increase only a licensed feature. For example, if a license key specified a slot count of 92 slots and later a different license key was installed that specified 46 slots, the total licensed slot count is still 92 slots. It is possible to license more slots than are physically available in the library at the time. If an Expansion Module (EM) is added, the extra licensed slots become available.

An Advanced Reporting license key (Feature code 1650) enables the Media Integrity Analysis Reporting and the Drive Resource Utilization Reporting functions. Administrative or Service users can configure and view various drive and media performance reports from the web user interface. For information, see “Advanced Reporting (Feature code 1650)” on page 1-15.

A path failover license key (Feature code 1682) supplies one or both licenses for control path failover and data path failover. For information, refer to “Multiple control paths for control path failover” on page 2-3 and “Multiple data paths for data path failover” on page 2-3.

A Transparent LTO Encryption license key (Feature code 5900) enables the System Managed Encryption (SME) and Library Managed Encryption (LME). Application Managed Encryption (AME) is a standard feature of the TS3310 library and does not require a license key. For information, refer to “Encryption (Feature code 5900)” on page 1-25.

Note: The license key is made up of five alphanumeric characters.

Configuring cleaning slots

Zero to four (0 - 4) cleaning slots can be configured in your library. These slots are taken from the unassigned available storage slots. Cleaning cartridges in these slots are used by the library 's Auto Clean function when the drives request cleaning.

Host-based cleaning do not use these slots. Host-based cleaning imports cleaning cartridges (CLNxxx) as data cartridges and assigns them to a particular logical library.

Cleaning Cartridges - The preferred method of labeling a cleaning cartridge is to have **CLN** or **CLNU** as the prefix on the label. Any cartridge that is detected with a **CLN** or **CLNU** prefix is considered a universal cleaning cartridge, regardless of any media identification extension. Cartridges that contain a media identification of **C1**, **C2**, **C3**, **C4**, **C5**, and **CU** are considered cleaning cartridges and are tracked and treated as if the media label contained the prefix **CLN** or **CLNU**.

Cleaning Count - The cleaning count is the number of times a cleaning cartridge was used to clean a tape drive. Knowing this information can help you decide when to replace a cleaning cartridge. After the cleaning cartridge is inserted (imported) from the I/O station to a cleaning slot, the cleaning count (Cleans Remaining) is listed on the **Manage Cartridges** > **Cleaning Cartridges** web page. See “Inserting a cleaning cartridge” on page 8-33 for the procedure to insert a cleaning cartridge.

Host-based drive cleaning

Backup applications or archive firmware applications use different techniques to automate the process of cleaning drives. These tools specify cleaning cycles that are based on cycle counts of the drive, drive requests, or regularly scheduled intervals.

The cleaning process itself requires certain considerations:

- Cleaning cartridges must be labeled with a volume serial number. In some cases, specific labels are established as industry standard. For instance, the prefix “CLN” might be used to identify a cleaning cartridge. The library does not require a specific content to the label and accepts conventional cartridge labels.
- Insert a cleaning cartridge just as you do any other data cartridge. For example, the most common method is by using the I/O station with host application control.
- Cleaning cartridges often have limited lives that might last only 20 cycles. The controlling host application manages the number of uses of a cleaning cartridge. Errors can occur if a cartridge is inserted into a drive when the cartridge was already used the maximum number of times.

- Export a cleaning cartridge just as you would export any other data cartridge.
- The concepts of physical libraries and logical libraries must be considered when cleaning procedures and methods are set up.

Configuring I/O stations

I/O station slots are used to insert and remove cartridges into and out of the library without disrupting normal library operations. I/O stations in Expansion Modules (EMs) can be configured as either I/O station slots or storage slots.

Depending on the configuration, the library contains at least one I/O station, which can contain one or two magazines. Each magazine contains six slots.

- A 5U control module contains six I/O station slots, and one magazine.
- A 9U expansion module contains 12 I/O station slots, and two magazines. Both magazines in a 9U expansion module must be configured the same way.

Note: If the library consists of a control module only, the I/O station must be configured as I/O station slots.

Storage slots in an I/O station that is configured as storage are normally assigned across multiple logical libraries to increase or decrease the number of I/O station slots in the library. If you want to keep all the cartridges in a particular logical library together:

- Export the cartridges by logical library and keep them grouped.
- Delete all logical libraries from the I/O station.
- Import as a group back to that particular logical library after the I/O station slots are reconfigured.

Selecting drive IDs and drive types

You can change the SCSI ID for a SCSI-attached tape drive or the Loop ID for a Fibre Channel-attached tape drive. This procedure is necessary. For example, when the default ID for a tape drive that you are installing conflicts with the assigned SCSI ID of an existing tape drive. In addition, you might be using a host application that expects to communicate with a tape drive at a specific SCSI ID, but that SCSI ID might already be configured for use in another logical library.

Note: SCSI tape drives use SCSI IDs that are limited to a numerical value 0 - 15. Fibre Channel tape drives use Loop IDs that are limited to a numerical value 0 - 125. SAS drive IDs are based on the worldwide name (WWN) assigned to the drive location in the library, and cannot be changed.

For information on drive IDs, refer to “Determining SCSI, Fibre Channel, and SAS IDs” on page 2-4.

Creating and modifying logical libraries

Logical libraries are virtual sections within a library that present the appearance of multiple, separate libraries for purposes of file management, access by multiple users, or dedication to one or more host applications. By default, the library has one logical library, which includes all of the library 's resources.

Administrative users can create, modify, delete, and control access to all logical libraries. Users can be given access to only certain logical libraries and denied access to others. There are two ways to create logical libraries:

- **Automatically** - where the library divides the available resources equally among the number of logical libraries chosen.
- **Manually** - where an administrative user assigns the number of slots per logical library. (This procedure is only done through the Web User Interface.)

Note: When the logical library mode is changed from online to offline, all host application commands in progress at the start of the mode change are completed.

At a minimum, a logical library consists of one tape drive and one slot. The tape drive or slot cannot be shared with another logical library. An exception to the sharing restrictions are cleaning cartridges, which can be shared among all logical libraries. I/O station slots and cleaning slots are shared between all logical libraries.

Each logical library is specific to a tape drive interface (for example, SCSI, SAS, or Fibre Channel). Mixed media is allowed within logical libraries. For example, a logical library can contain LTO 2 and LTO 3 tape cartridges.

Automatically creating logical libraries

When the library automatically creates logical libraries, the available resources are divided equally among the number of logical libraries created. Before logical libraries are created, first designate the wanted number of cleaning slots and I/O slots (if an expansion module is present). This designation is necessary because the Automatic Create Logical Library function divides all available storage slots among the chosen number of logical libraries.

From the Operator Panel, all remaining available resources are divided among the number of automatically created logical libraries. Use the Web User Interface (UI) to manually create logical libraries.

Note: On the Web User Interface, all logical libraries must be deleted for the **Automatic** button to display. If the **Automatic** button does not display, delete all existing logical libraries.

Manually creating logical libraries

Every logical library must have at least one drive and one storage slot that is assigned to it. For example, if the library has 2 tape drives and 12 slots available, the maximum number of logical libraries that can be created is two. Up to 12 slots can be allocated between the two logical libraries in any configuration.

If the library has only one logical library with all resources assigned to it, that logical library must be deleted before resources are reallocated to a new logical library.

You might need to provide information for the following fields:

- `Logical Library Name` can be up to a maximum of 12 alphanumeric characters.

  Note: Some character combinations that are allowed in long logical library names can cause the logical library name to exceed the display space

available on the Operator Control Panel. This act does not cause a functional problem, but the last character might not be fully displayed.

- **Media Barcode Format** Choose Standard Six, Plus Six, Extended (default), Media ID Last, Media ID First, or Standard.
- **Emulation Type** Choose between TS3310 (default) and ADIC Scalar i500.
- **Automatic Drive Cleaning** is enabled by default and requires at least one cleaning cartridge and a communication interface to the tape drive with the ability of the tape drive to indicate that cleaning is needed.
- **Number of Slots** is the number of tape cartridge slots that are to be allocated to the new logical library.

Modifying the encryption method

If a logical library has encryption-supporting drives, you can select the encryption method to use.

Select**None** (default), **Application Managed Encryption**, **System Managed Encryption**, or **Library Managed Encryption**.

Note: SME and LME require the transparent LTO Encryption license key (Feature code 5900).

See “Configuring encryption settings” on page 8-6.

Modifying the logical library

You can modify an existing logical library only from the Web UI (**Manage Library** > **Logical Libraries**).

Select **Library**, select **Modify** from the `Select Action` list, and then choose **General Properties**, **Configuration Storage Slots**, or **Select Drives to Assign to Logical Library**.

Deleting logical libraries

A logical library can be deleted when it is no longer needed. After a logical library is deleted, its resources become unassigned and can be used to create more logical libraries or added to existing logical libraries.

Changing logical library access

An administrative user can control what logical libraries a specified user can access. This procedure is done by modifying a user 's account.

To change logical library access, you must provide the following information:

- **Password** - a unique string of alphanumeric characters that is viewed and modified by the Administrator.
- **Privilege level** - the library functions that a user is assigned access to. Refer to “User privileges” on page 6-9 for information on user privilege levels.

Changing logical library modes

By default, the library has one logical library enabled. The logical library mode must be changed to modify the logical library or library. There are two logical library modes: online and offline.

- **Online** - the normal operating condition for a logical library. In this mode, the robotics are enabled and all host application commands are processed.

- **Offline** - the logical library does not process any host application commands. If a logical library is taken offline, the physical library and other logical libraries are not affected.

You can take the physical library or any of its logical libraries online or offline. Some operations require that the logical library is offline. Superuser and Administrative users can take a logical library offline rather than the entire library to minimize disruption of library operations. Superuser and Administrative users must manually change the logical library mode to online or offline from the Operator Panel or the Web User Interface (UI).

Details on changing logical library modes include

- The default logical library mode is online.
- When you access these screens, only logical libraries accessible by the user display.

When you are changing logical library mode, be aware of the following information:

- **Online/Offline** toggles between states.
- If a logical library is in use, **Online/Office** is disabled.
- Set the button to read **Online** to take either the physical library or a logical library, depending on the current view, to an online state, which is the normal operating condition. In this mode, the robotics are enabled and all host commands are processed.
- Set the button to read **Offline** to take either the physical library or a logical library, depending on the current view, to an offline state. If only the physical library is taken offline, logical libraries do not process robotics commands, even though they are online. If only a logical library is taken offline, the physical library and the other logical libraries are not affected.

Types of user accounts

There are three types of user accounts: user, superuser, and administrative user.

- **Superuser** - has more privileges and can complete more functions than Users, but less than Administrators
- **User** - has access to one or more assigned logical libraries and can complete functions within a logical library, such as completing media and drive functions. A user cannot complete actions that affect the physical library, such as creating, modifying, or deleting a logical library.
- **Administrative user** - has access to the entire physical library and all of its logical libraries.

One administrative user account, Admin, is configured by default and can be modified at any time, but not deleted. An administrative user can complete all user account functions. A user cannot complete any administrative account functions. Refer to “User privileges” on page 6-9 for information on library permission levels.

Creating user accounts

Administrative users can create user accounts any time after the initial configuration. Users cannot create user accounts. A maximum of 300 user accounts can be created in the physical library.

Note: If your library is running firmware version 600G or later, the length for library user and administrator passwords are limited to 6-16 alphanumeric characters. If your library is running firmware version below 600G, the length for library user and administrator passwords are limited to 6-12 alphanumeric characters.

To create user accounts, you must provide information for the following fields:

- **User Name** is the login name of the user account you are creating.
- **Password** is a unique string of alphanumeric characters for the user account you are creating.
- **Privilege** level is set to `User`, `Superuser`, or `Admin`. Refer to "User privileges" on page 6-9 for information about user privilege levels.

Modifying user accounts

After a user account is created, the account settings, such as the password, privilege level, and logical library access, can be modified at any time by an administrative user.

Note: If your library is running firmware version 600G or later, the length for library user and administrator passwords are limited to 6-16 alphanumeric characters. If your library is running firmware version below 600G, the length for library user and administrator passwords are limited to 6-12 alphanumeric characters.

To modify user accounts, you must provide information for the following fields:

- **User Name** is the login name of the user account you are creating.
- **Password** is a unique string of alphanumeric characters for the user account you are creating.
- **Privilege** level is set to `User`, `Superuser`, or `Admin`. Refer to "User privileges" on page 6-9 for information about user privilege levels.

Deleting user accounts

When a user account is no longer needed, it can be deleted at any time.

Modifying LDAP and Kerberos settings

Administrators can enable and configure Lightweight Directory Access Protocol (LDAP). LDAP is the industry standard Internet Protocol that provides centralized user account management.

Administrators can add, delete, and modify only local user account information. The library web client does not allow you to create, modify, or delete user account information about an LDAP server. This procedure must be done by the directory service provider.

The library supports all LDAP servers. You can also use Kerberos for added security. For specific instructions on configuring Kerberos, see "Configuring Kerberos" on page 5-11.

If your library is running firmware version 600G or later, you can optionally configure Secure LDAP with one of two methods: LDAP over SSL (**LDAPS**), or LDAP over TLS (**StartTLS**). Do not use both.

The Op Panel login screen displays remote authentication login options only when LDAP is enabled.

LDAP server guidelines

The following groups must be created on the LDAP server to enable remote login on the library:

- User group - Assign users to this group who need user-privilege access to the library. Enter the name of this group in the **User Group** field on the **Manage Access** > **Authentication Settings** screen on the library web client (see "Modifying authentication settings" on page 8-8).
- Partition groups - For LDAP users with user privileges, access to library partitions is determined by group assignment on the LDAP server. Groups must be created on the LDAP server with names that match the library partition names (names must match but are not case-sensitive). Users with user privileges must be assigned to these groups on the LDAP server to have access to the corresponding partitions on the library.
- Superuser group - Assign users to this group who need superuser-privilege access to the library. LDAP users with superuser privileges have access to all partitions and superuser functions and do not need to be assigned to partition-related groups on the LDAP server. Enter the name of this group in the **Superuser Group** field on the **Manage Access** > **Authentication Settings** screen on the library web client (see "Modifying authentication settings" on page 8-8).
- Admin group - Assign users to this group who need administrator-privilege access to the library. LDAP users with administrator privileges have access to all partitions and administrator functions and do not need to be assigned to partition-related groups on the LDAP server. Enter the name of this group in the **Administrator Group** field on the **Manage Access** > **Authentication Settings** screen on the library web client (see "Modifying authentication settings" on page 8-8).

You must have at least one user that is assigned to both the Library User Group and the Library Admin Group on the LDAP server to test the LDAP settings on the library. Since most normal users are not members of both these groups, you might need to create a special or temporary user specifically for this purpose.

Configuring LDAP on the library

Before LDAP is configured, obtain the following LDAP parameters from your network administrator. You must enter these parameters in the **Manage Access** > **Authentication Settings** screen on the web client:

- Repository URI - The Uniform Resource Identifier (URI) of the LDAP server where user account information is stored. The URI includes the LDAP server host name and can include the LDAP server network port. Port 389 is the default.

  Examples: `ldap://hostname:389`

  Note: If your library is running firmware version 600G or later, you can optionally configure Secure LDAP with one of two methods (do not use both).

  – LDAPS - You can enable LDAP over SSL (LDAPS) by entering a URI in the form of `ldaps://hostname` in the **Repository URI** field. This action uses SSL to send secure communication with port 636. If the LDAP server does not support LDAPS or does not have LDAPS enabled, login operations fail.

LDAPS was deprecated in favor of StartTLS (see option). Do not use LDAPS if you are using StartTLS. When you apply LDAPS, StartTLS is not available.

- LDAP StartTLS - Select this check box to configure secure LDAP communication with TLS. StartTLS uses the same port as regular LDAP (389). If TLS mode is not supported on your LDAP server, then login operations fail. You cannot use StartTLS if you want to use LDAPS.

  Optionally, if you are using one of these methods, you can install a TLS certificate.

  – LDAP TLS Certificate - Provides more verification of the LDAP server. If the certificate is installed, the library verifies that the LDAP server is not compromised. The certificate must be the same certificate that is installed on your LDAP server and must be in .pem format. The maximum size of the file is 4 KB. The library completes only the verification if you configured Secure LDAP (either LDAPS or StartTLS). Place a copy of the certificate file in an accessible location on your computer and use **Browse** to locate and install it. When a certificate is installed, you can remove it by selecting the **Remove Certificate** check box. The library reboots after you install or remove a TLS certificate.

- Principal - An LDAP user login ID with permissions to search the LDAP directory. The library accesses LDAP with this ID.

  Example: `administrator@mycompany`

- Credential - The password for the principal authorization login ID.
- User DN - The Fully Qualified Distinguished Name that contains the users.

  Example: `cn=users,ou=system,dc=mycompany,dc=com`

- User Group - The name of the group on the LDAP server that is associated with library users who have user-level privileges. This group must exist on your LDAP server.
- Admin Group - The name of the group on the LDAP server that is associated with library users who have administrator-level privileges. This group must exist on your LDAP server.

Testing LDAP settings

The **Test LDAP Connection** button tests communication between the library and the LDAP server, and tests the currently applied LDAP settings. If there are any problems, an error message identifies the problem area.

If you change the LDAP settings, click **Submit Changes** before this button is used.

To test the settings, you must enter a user name and password, then click the button. **The user you use for the test must be a member of both the Library User Group and the Library Admin Group on the LDAP server.** Since most normal users are not members of both these groups, you might need to create a special or temporary user specifically for this purpose. After LDAP settings are configured, save the library configuration.

You can view, enable, and configure LDAP settings from the library web client. You cannot use the operator panel to configure LDAP settings.

The path to open the appropriate screen is

- From the web client, select **Manage Access** > **Authentication Settings**

Configuring Kerberos

Use Kerberos if you want extra security with remote authentication.

Ensure that both the library and the Kerberos/Active Directory® server are set to the same time (within 5 minutes). Otherwise, the authentication fails. It is recommended that you use Network Time Protocol (NTP) to synchronize the time between the library and the Kerberos server. See **Manage Library** > **Settings** > **Date & Time**. Complete these Kerberos fields in addition to the LDAP fields:

- Realm - The Kerberos realm name, which is typed in all uppercase letters. Usually the realm name is the DNS domain name.

  Example: MYCOMPANY.COM
- KDC (AD Server) - The key distribution center (in other words, the server on which Kerberos/Active Directory is installed).

  Example: mycompany.com:88
- Domain Mapping - The domain portion of the library's fully qualified domain name.

  Example: mycompany.com
- Service Keytab - Click the **Browse** button to select the service keytab file. The service keytab file is a file that you generate on your Kerberos/Active Directory server. See "Generating the Service Keytab file."

  You can view, enable, and configure Kerberos settings from the web client. You cannot use the operator panel to configure Kerberos settings. The path to open the appropriate screen is

  – From the web client, select **Manage Library** > **Settings** > **Date & Time**.

Generating the Service Keytab file

These instructions are for generating the service keytab file for use with Microsoft® Active Directory®. If you do not use Active Directory, refer to your Kerberos vendor for instructions on generating this file.

1. Set up an Active Directory domain on the Windows server.
2. If Active Directory is not already configured, run **dcpromo**.
3. **Windows 2003 servers only:** Install Windows Support Tools on the Windows 2003 server:
   a. Go to http://www.microsoft.com and search for **windows server 2003 support tools sp2** or click the following link: http://www.microsoft.com/downloads/details.aspx?FamilyID=96a35011-fd83-419d-939b-9a772ea2df90&DisplayLang=en
   b. Download both **support.cab** and **suptools.msi**.
   c. Run **suptools.msi** to begin installation.
4. Create a computer account in Active Directory.
   - Do not select any of the check boxes during creation.
   - The account name is used for the <computer account> fields that are shown in the following steps.
5. At the command prompt, map SPN to the computer account. Use the following format.

   ```
   setspn -A library/<fqdn of library><computer account>
   ```

   For example:

   ```
   setspn -A library/delos.dvt.mycompany.com kerbtest
   ```

6. At the command prompt, create the keytab file for the SPN. Use one of the following formats.
   - For Windows 2003:

     ```
     ktpass -out library.keytab -princ
     library/<fqdn of library@<realm>
     +rndPass -ptype KRB5_NT_SRV_HST -crypto RC4-HMAC-NT -
     mapUser <realm>/computers/<computer account>
     ```

     – For example:

       ```
       ktpass -out library.keytab -princ
       library/delos.dvt.mycompany.com@OURREALM.LOCAL
       +rndPass -ptype KRB5_NT_SRV_HST -crypto RC4-HMAC-NT -
       mapUser ourrealm.local/computers/kerbtest
       ```

   - For Windows 2008:

     ```
     ktpass -out library.keytab -princ library/
     <fqdn of library@<realm>
     +rndPass -ptype KRB5_NT_SRV_HST -crypto AES256-SHA1
     -mapUser <realm>/computers/<computer account>
     ```

     – For example:

       ```
       ktpass -out library.keytab -princ
       library/delos.dvt.mycompany.com@OURREALM.LOCAL
       +rndPass -ptype KRB5_NT_SRV_HST -crypto AES256-SHA1
       -mapUser ourrealm.local/computers/kerbtest
       ```

Chapter 6. User interfaces

The library has a local interface, the Operator Panel, and a remote Web User Interface (UI).

The Operator Panel is on the front door of the control module (CM) and allows users to work locally on the library with the user interface. The Web UI allows users to view and complete some library functions from remote sites and is best viewed with Internet Explorer 5.0 or higher, or Firefox 1.0 or higher.

Operator Panel

The Operator Panel is physically attached to the front door of the control module (CM). The user interface appears on the touchscreen LCD display of the Operator Panel for executing basic library management functions. Audible feedback, such as "key click" sounds, are generated when a user touches a button on the touchscreen.

Operator Panel Login screen

Figure 6-1. Operator Panel Login screen for firmware versions 585G and later

For firmware versions of 585G and later, the **Login** screen displays the **Remote Authentication** login option only when LDAP is enabled.

For initial login, the administrator uses

- User name: **admin**
- Password: **secure**

To complete the **User name**, lightly touch the blank field to display the alphabetic and numeric touch pads then, use the touch keys to spell out the user ID and touch **OK**. Similarly, enter the password and touch **OK**.

After initial login change the Administrator password. To change the password, complete the following steps:

- For firmware versions before 585G, the LDAP authentication choice is presented on the Operator Panel as **Remote authentication**. From the Operator Panel, select **Setup** > **User Mgmt** > **Modify User**.
- For firmware versions 585G and later, change the Administrator password. From the Operator Panel, select **Setup** > **User Mgmt** > **Modify User**.

Common Operator Panel elements

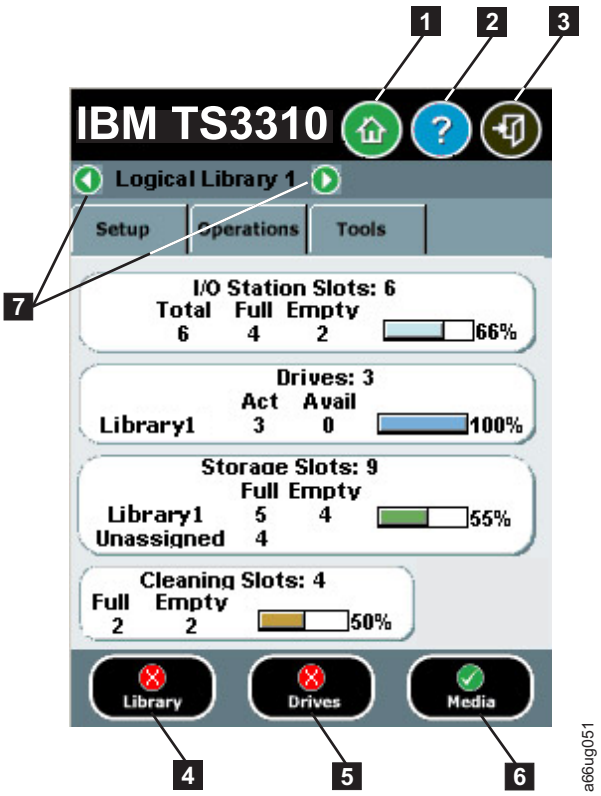


Figure 6-2. Operator Panel common header elements and subsystem status buttons

Common Header elements

All Operator Panel screens (except for the Login screen) contain the following common elements in the header:

- **Home** (1 in Figure 6-2) - displays the default **Capacity View** screen.
- **Help** (2 in Figure 6-2) - context-sensitive help for the associated page

- **Logout** (3 in Figure 6-2 on page 6-2) - ability to log out
- **Logical Library Name** - Displays the designation for the current logical library. You can click the arrows on either side of the library designation to scroll through other available logical libraries.

Note: When the library is busy performing certain tasks, a "Not Ready' message displays alternately with the 'IBM TS3310' notation at the top of the screen.

System summary and subsystem status

The health of the library can be gauged by three subsystem status buttons that are at the bottom of the home page. These buttons provide easy access to the health of the library for faster recovery if problems occur. You can select the buttons to view detailed information about the library and gain access to library subsystems. The three subsystems are

- **Library** (4 in Figure 6-2 on page 6-2)- opens the operator interventions for the library.
- **Drives** (5 in Figure 6-2 on page 6-2)- opens the operator intervention screen for drives.
- **Media** (6 in Figure 6-2 on page 6-2)- opens the operator intervention screen for media.

Each button has three states that are indicated by color. The three states are

- Good - green
- Degraded - yellow (An operator intervention is created.)
- Investigate - red (An operator intervention is created; however, the library can still be operational.)

Keyboards

When a user touches a text box that requires data entry, a keyboard screen displays. Either the alphabetic, numeric, or special characters keyboard displays, depending on the type of input field. All alphabetic character entries can display as upper or lowercase. The text box displays at the top of the screen and the number or characters display as they are entered. The **123** button opens the numeric keyboard from the alphabetic keyboard. The **abc** button opens the alphabetic keyboard from the numeric keyboard, The **!@#** button opens the special characters keyboard from the alphabetic keyboard. The back arrow erases one character at a time.

Attention: To use the touchscreen effectively, tap lightly to make your selections.

Home page

The home page screen provides tabular data on the capacity of the various areas of the library. Use this screen to see a quick summary of the capacity of the selected logical library that is based on a user login.

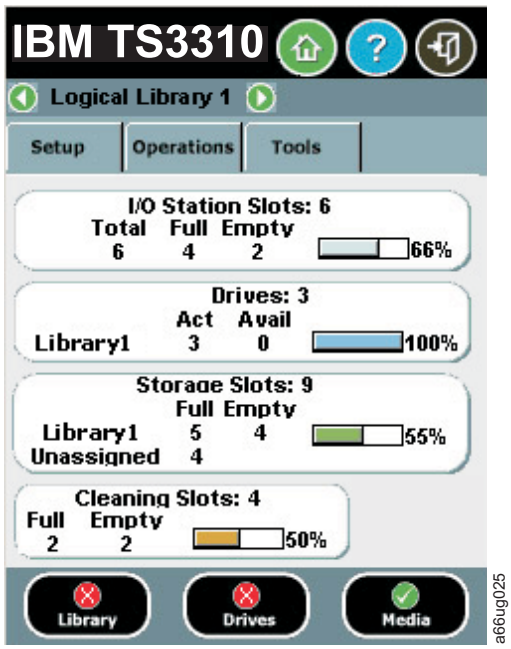


Figure 6-3. Home screen capacity view

If users have access to more than one logical library, they can navigate to other logical libraries with arrows next to the logical library name at the top of the screen.

If an administrative user is logged in, a view of the physical library displays.

If a user is logged in, the first logical library that they have access to, in alphabetical order, is displayed.

Menus available from the Operator Panel

The following three menus organize commands into logical groups:

Note: The menus available to users with the**Admin** role are **Setup**, **Operations**, and **Tools**. The menus available to users with the**User** role are **Operations** and **Tools**. The menus available to the **Service** login are **Setup**, **Operations**, **Tools**, and **Service**.

- The **Setup** menu consists of commands that you can use to set up and configure various aspects of the library, including logical libraries, user management, drive settings, licenses, date and time, network management, and control path.

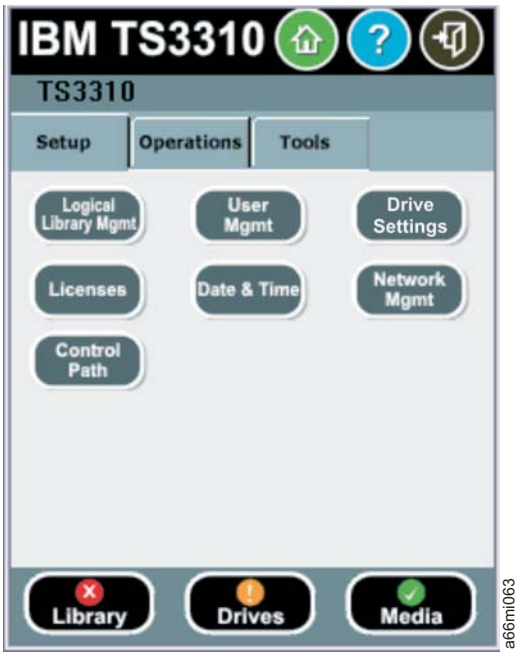


Figure 6-4. Setup menu screen

- The **Operations** menu consists of commands that enable you to change the library 's mode of operations, insert and remove cartridges, load and unload drives, move media, and shutdown/restart the library.

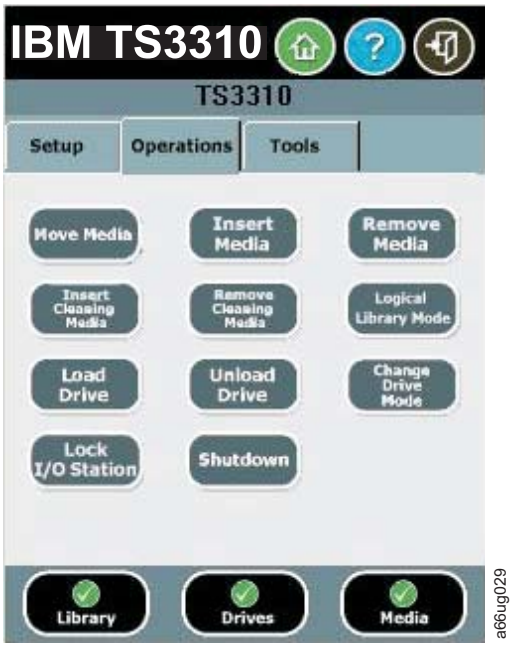


Figure 6-5. Operations menu screen

- The **Tools** menu consists of commands that you can use to maintain your library such as viewing operator interventions, capturing the library snapshot (available to Service logon only), identifying ports, and updating firmware with an FMR (Firmware) cartridge.

Figure 6-6. Tools menu screen

The menu tree shows all functions available from the **Operator Panel** interface.

Table 6-1. Tape library Operator Panel menu tree

Setup	Operations	Tools
–Logical Library Mgmt	–Move Media	–Operator Interventions
–User Mgmt	–Insert Media	–Drive Mgmt
–Drive Settings	–Remove Media	–Drive Info
–Licenses	–Insert Cleaning Media	–About Library
–Date & Time	–Remove Cleaning Media	–Service
–Network Mgmt	–Logical Library Mode	–Internal Network
–Control Path	–Load Drive	–System Settings
	–Unload Drive	–Security
	–Change Drive Mode	–Display Settings
	–Lock I/O Station	–Factory Defaults (Service logon only)
	–Shutdown	–Library Tests (Service logon only)*

*Library Tests will include Installation and Verification Test (IVT) for libraries that are built after July 1, 2008 with serial numbers with last 4 digits 8609 and above.

Web User Interface (UI)

The System Storage TS3310 web user interface supports only two browsers, either Mozilla Firefox™ version 1.0.6 and above or Microsoft® Internet Explorer™ version 6.0 and above.

To manage the library with the Web UI, you must set up the initial network configuration of the library from the Operator Panel touchscreen. For information,

see “Modifying network settings” on page 5-2 and “Step 4: Setting up the library network configuration” on page 7-3 in the .

Logging in to the Web User Interface

Initial login information is

- User: **admin**
- Password: **secure**

For information about user privileges, see “User privileges” on page 6-9.

Note: When LDAP or Kerberos is enabled, the Login screen displays a **Remote Authentication** check box. Select the **Remote Authentication** check box to log in with a directory service user name and password. Clear the **Remote Authentication** check box to log in with a local user name and password.

Common Header elements

All Web UI screens (except for the Login screen) contain the following common elements in the header:

- **Help** - context-sensitive help for the associated page
- **Logout** - ability to log out
- **About** - information about product version and library firmware

Menus available from the Web User Interface

The table lists those menus that are available from the Web UI.

Table 6-2. Menus available from the Web User Interface

Welcome Page

– Monitor System

System Summary

Library Map

Logged in Users

Network Settings

Key Path Diagnostic Status

– Advanced Reporting

-- Drive Utilization

-- Media Integrity

Media Security

– Manage Cartridges

Data Cartridges

Cleaning Cartridges

I/O Station

Lock/Unlock I/O Station Doors

– Manage Drives

Drive Summary

Control Paths

Drive IDs

Table 6-2. Menus available from the Web User Interface (continued)

Welcome Page

- Fibre Channel Ports
- -- Modify Port Properties

– Manage Library

- Perform Inventory
- Setup Wizard
- Logical Libraries
- Cleaning Slots
- I/O Station Slots

– Settings

- Feature Licenses
- Date & Time
- Email Notifications
- SMTP (Mail) Configuration
- Contact Information
- Network
- SNMP Configuration
- SNMP Destinations
- -- Add
- -- Remove
- Ethernet Speed/Duplex
- Media Detection
- Save/Restore Configuration

– Manage Access

- Users
- Authentication Settings
- Set Session Timeout

– Service Library

- Operator Interventions
- Capture Library Log
- Capture Drive Log
- Media Security Log
- Media Usage Log
- Capture IVT Log*
- View/Update Library Firmware Level
- View/Update Drive Firmware Level
- Service Drives
- Shutdown/Restart Library
- Key Path Diagnostics
- Ethernet Expansion Blade Control†

Table 6-2. Menus available from the Web User Interface (continued)

Welcome Page

* Available only to Service login. Available only on libraries built after July 1, 2008 with serial numbers with last four digits 8609 and above.

† This option is shown only when an EEB is inserted into the library.

User privileges

User privilege levels are manually assigned to user accounts created within the library. Controlling access to screens and operations within the library preserves the integrity of the library and the data that is stored within the library.

There are three types of user privileges in the library.

- **Administrative users** are allowed access to the entire physical library and all of its logical libraries. Only one administrative user must be assigned the login name **admin**.
- **Superusers** have all the privileges of Users with additional privileges associated with monitoring, operating, and servicing the library. Superusers have access to all library partitions but cannot perform the following tasks:
  - Library setup and settings
  - Changes to library configuration
  - Changes to library or drive firmware
  - Library security setup and changes
- **Users** are allowed to operate one or more assigned logical libraries, but are not allowed to perform actions that affect the physical library. See Table 6-3 on page 6-10 for access details to the available library functions.

User privileges include:

- A screen saver is started after 10 minutes of inactivity on the Operator Panel. The Web User Interface (UI) does not use a screen saver.
- Up to 18 Users and/or Administrative users can be logged in at one time on the Web UI. Only one user can be logged in at one time on the Operator Panel.
- For information on User Session timeout, see “Setting User Session Timeout” on page 8-10.
- When a Service user logs in, all other Users and Administrative users are logged out and notified that they cannot perform actions on the library. A message is posted that Service is logged in and no other users can access the library until after Service has logged out.

The following table describes how to access the library functions from both the control panel and the Web UI. For each interface, column "A" indicates Administrative privileges; "S" indicates Superuser privileges; column "U" indicates User privileges. In each column, an "X" indicates that access is allowed and the settings can be modified, an "O" indicates that access is allowed but the settings can only be observed, and a "–" indicates that access is not allowed.

Table 6-3. System functions, commands, and access

Function	Control Panel Menu Command and Access				Web UI Command and Access			
		A	S	U		A	S	U
Libraries								
Setup Wizard	N/A				**Manage Library** > **Setup Wizard**	X	—	—
Create Logical Libraries	**Setup** > **Logical Library Mgmt** > **Create Logical Library**	X	—	—	**Manage Library** > **Logical Libraries**	X	—	—
Delete Logical Libraries	**Setup** > **Logical Library Mgmt** > **Delete Logical Library**	X	—	—	**Manage Library** > **Logical Libraries**	X	—	—
Delete ALL Logical Libraries	**Setup** > **Logical Library Mgmt** > **Delete All Logical Libraries**	X	—	—	**Manage Library** > **Logical Libraries**	X	—	—
Change Logical Library Mode	**Operations** > **Logical Library Mode**	X	X	X	**Manage Library** > **Logical Libraries**	X	X*	X
Configure Encryption Settings	N/A				**Manage Library** > **Logical Libraries**	X	—	—
Perform Inventory	N/A				**Manage Library** > **Perform Inventory**	X	X	X
Display Library Information	**Tools** > **About Library**	X	X	X	**Monitor System** > **Library Map**	X	X	X
Capture Library Log	N/A				**Service Library** > **Capture Library Log**	X	X	—
Cleaning Slots	**Setup** > **Logical Library Mgmt** > **Configure Cleaning Slots**	X	—	—	**Manage Library** > **Cleaning Slots**	X	X	—
I/O Station Slots	**Setup** > **Logical Library Mgmt** > **Configure I/O Slots**	X	—	—	**Manage Library** > **I/O Station Slots**	X	—	—
I/O Station Lock/Unlock	**Operations** > **Lock I/O Station** > **Lock/Unlock**	X	X	—	**Manage Cartridges** > **Lock/Unlock I/O Station Doors**	X	X	—
Update Library Firmware	N/A				**Service Library** > **View/Update Library Firmware Level**	X	O	—
Display Advanced Reporting Reports	N/A				**Monitor System** > **Advanced Reporting**	X	X	X

Table 6-3. System functions, commands, and access (continued)

Function	Control Panel Menu Command and Access				Web UI Command and Access			
		A	**S**	**U**		**A**	**S**	**U**
Shutdown/ Restart Library	**Operations** > **Shutdown**	X	X	—	**Service Library** > **Shutdown/Restart Library**	X	X	—
* Superusers can access the **Logical Libraries** web page via the **Manage Library** menu but they can only execute the **Bring Online** and **Bring Offline** functions.								
Users/System Access								
Create New Users	**Setup** > **User Mgmt** > **Create User**	X	—	—	**Manage Access** > **Users**	X	—	—
Modify Users	**Setup** > **User Mgmt** > **Modify User**	X	—	—	**Manage Access** > **Users**	X	—	—
Enter License Key	**Setup** > **Licenses**	X	—	—	**Manage Library** > **Settings** > **Feature Licenses**	X	O	—
Display Logged in Users	N/A				**Monitor System** > **Logged in Users**	X	X	—
LDAP Configuration	N/A				**Manage Access** > **Authentication Settings**	X	O	—
User Session Timeout	**Tools** > **System Settings** > **User Session Timeout (Minutes)**	X	—	—	**Manage Access** > **Set Session Timeout**	X	—	—
Disable Remote Service User	**Tools** > **System Settings** > **Disable Remote Service Users**	X	—	—	N/A			
Drives		**A**		**U**		**A**		**U**
Set Drive Settings	**Setup** > **Drive Settings**	X	—	—	**Manage Drives** > **Drive IDs**	X	O	—
Load Drive	**Operations** > **Load Drive**	X	X	X	**Manage Drives** > **Drive Summary** > **Load**	X	X	X
Unload Drive	**Operations** > **Unload Drive**	X	X	X	**Manage Drives** > **Drive Summary** > **Unload**	X	X	X
Change Drive Mode	**Operations** > **Change Drive Mode**	X	X	X	**Service Library** > **Service Drives** > **Bring Online, Bring Offline, Reset**	X	X	—
Clean Drive	**Tools** > **Drive Mgmt** > **Clean drive**	X	—	—	**Manage Drives** > **Drive Summary** > **Clean**	X	X	—
Display Drive Information	**Tools** > **Drive Info**	X	X	X	**Service Library** > **View/Update Drive Firmware Levels**	X	O	—

Table 6-3. System functions, commands, and access (continued)

Function	Control Panel Menu Command and Access	A	S	U	Web UI Command and Access	A	S	U
Capture Drive Log	N/A				**Service Library** > **Capture Drive Log**	X	X	—
Fibre Channel Ports	**Setup** > **Drive Settings**	X	—	—	**Manage Drives** > **Fibre Channel Ports**	X	O	—
Reset Drive	N/A		X		**Service Library** > **Service Drives** > **Reset Drive**	X	X	—
Create FMR Tape	**Tools** > **Drive Mgmt** > **Create an FMR tape**	X	—	—	N/A			
Update Drive Firmware	**Tools** > **Drive Mgmt** > **Update drive firmware using FMR**	X	—	—	**Service Library** > **View/Update Drive Firmware Levels**	X	O	—
Erase FMR Tape	**Tools** > **Drive Mgmt** > **Erase an FMR tape**	X	—	—	N/A			
Media/Cartridges								
Move Data Cartridges	**Operations** > **Move Media**	X	—	X	**Manage Cartridges** > **Data Cartridges**	X	X	X
Insert Data Cartridges	**Operations** > **Insert Media**	X	X	X	**Manage Cartridges** > **I/O Station**	X	X	X
Remove Data Cartridges	**Operations** > **Remove Media**	X	X	X	**Manage Cartridges** > **Data Cartridges**	X	X	X
Cleaning Cartridges	**Operations** > **Insert Cleaning Media** and **Operations** > **Remove Cleaning Media**	X	X	X	**Manage Cartridges** > **Cleaning Cartridges**	X	X	X
Manage Cartridges in I/O Station	N/A				**Manage Cartridges** > **I/O Station**	X	X	X
Manual Cartridge Assignment	**Tools** > **System Settings** > **Manual Cartridge Assignment**	X	—	—	N/A			
System/Network Settings								
Network Configuration	**Setup** > **Network Mgmt** > **Network Configuration**	X	—	—	**Manage Library** > **Settings** > **Network**	X	O	—
Save/Restore Configuration	N/A				**Manage Library** > **Settings** > **Save/Restore Configuration**	X	—	—

Table 6-3. System functions, commands, and access (continued)

Function	Control Panel Menu Command and Access				Web UI Command and Access			
		A	S	U		A	S	U
Enable Internet Protocol ver. 6 (IPv6)	**Tools** > **System Settings** > **Enable IPv6** OR **Setup Wizard** (first time only)	X	—	—	**Manage Library** > **Settings** > **Network**	X	—	—
Date and Time	**Setup** > **Date & Time**	X	—	—	**Manage Library** > **Settings** > **Date & Time**	X	O	—
Network Time Protocol (NTP)	N/A				**Manage Library** > **Settings** > **Date & Time**	X	O	—
Trap and SNMP	N/A				**Manage Library** > **Settings** > **SNMP** and **Manage Library** > **Settings** > **SNMP Traps**	X	O	—
Control Path	**Setup** > **Control Path**	X	—	—	**Manage Drives** > **Control Paths**	X		—
Operator Intervention	**Tools** > **Operator Intervention**	X	X	—	**Service Library** > **Operator Interventions**	X	X	—
DNS Configuration	N/A				**Manage Library** > **Settings** > **Network**	X	O	—
Enter Contact Information	N/A				**Manage Library** > **Settings** > **Contact Information**	X	O	—
Set Email Notifications	N/A				**Manage Library** > **Settings** > **Email Notifications**	X	O	—
Diagnose/Test LME Key Paths	N/A				**Service Library** > **Key Path Diagnostics**	X	X	—
Internal Network Configuration	**Tools** > **Internal Network**	X	—	—	N/A			
Touch Screen Audio	**Tools** > **System Settings** > **Touch Screen Audio**	X	X	X	N/A			
Adjust Display	**Tools** > **Display Settings**	X	X	X	N/A			
Display System Summary	N/A				**Monitor System** > **System Summary**	X	X	X
Display Network Settings	N/A				**Monitor System** > **Network Settings**	X	X	X

Table 6-3. System functions, commands, and access (continued)

Function	Control Panel Menu Command and Access	A	S	U	Web UI Command and Access	A	S	U
Outgoing Server (Mail) Configuration	N/A				**Manage Library** > **Settings** > **SMTP (Mail) Configuration**	X	O	—
Ethernet Speed/Duplex Settings	N/A				**Manage Library** > **Settings** > **Ethernet Speed/ Duplex Settings**	X	O	—
Display License Key Status	N/A				**Manage Library** > **Settings** > **Feature Licenses**	X	X	—
Service								
Enter Service Menu	**Tools** > **Service**	X	—	—	N/A			
Service Drives	**Tools** > **Service** > **Drives**	X	X	—	N/A			
Service System	**Tools** > **Service** > **System**	X	X	—	N/A			
Security Settings	**Tools** > **Security**	X	—	—	N/A			

Chapter 7. Configuring the library

Initial configuration customizes the library for your specific needs and environment. The first time a new machine is powered ON, a Setup wizard program automatically displays each of the configuration components necessary to set up the library. The Setup wizard does not show on subsequent logins, but all of the configuration items can be accessed through the Setup Menu tab whenever you are logged in to the Operator Panel.

Details about the Setup wizard include

- After a timeout period of 1 hour, the Setup wizard closes, and you are logged out of the library. Use the default Admin account to log in on the Operator Panel.
- If the Setup wizard times out or you do not complete all the Setup wizard screens, the library applies the default configuration settings plus whatever modifications (if any) you made. The default settings are
  - I/O station slots: 6 (in the control module)
  - Cleaning cartridge slots: 1
  - Logical libraries: 1
- You can configure network settings from the Operator Panel or the Web interface, but you cannot log in to the library from the Web interface until you configured network settings for the first time from the Operator Panel.
- You can configure IPv4 network settings and you can enable IPv6 addressing from the Setup wizard, but you cannot configure the IPv6 network settings from the wizard. The IPv6 network settings must be configured from the Setup tab of the Operator Panel (**Setup** > **Network Mgmt**), or from the Web User Interface (**Manage Library** > **Settings** > **Network**).
- You cannot return to the Setup wizard after the initial library power ON cycle, however you can access the Setup menu configuration items whenever you are logged in to the Operator Panel.

Important: If at any point you touch **Cancel** while in the Setup wizard, the Cancel screen displays. The screen is dynamically updated to indicate what the current configuration of the library is, including any settings that were applied thus far in the wizard. From the Cancel screen, touch **Cancel** to navigate back to the last accessed screen in the Setup wizard, or touch **OK** to apply the current settings and return to the home page screen.

Important: **Use the Appendix E, "Library configuration form," on page E-1 to record all library settings. You can also electronically save and restore library settings from the Web User Interface.**

Step 1: Configuring the library with the Setup wizard

You can configure your library in two ways. If it is the first time that the library is powered ON, the **Setup Wizard: Welcome** screen automatically displays and you can skip to Step 2. If the Setup wizard does not display automatically, you can access all of the Setup configuration items by logging in to the Operator Pane, then selecting the `Setup Menu` tab.

If necessary, log in to the Operator Panel.

On the Operator Panel Log in screen:

Figure 7-1. Operator Panel Log in screen

1. Press the **User name** field to access the alphanumeric keyboards.
2. Use the alphabetic keyboard to enter **admin**, then press **OK**.
3. Press the **Password** field to access the alphanumeric keyboards.
4. Use the alphabetic keyboard to enter **secure**, then press **OK**.
5. Press **OK** again to access the **Home Page** screen that displays the default configuration of the library.

6. Delete the library 's default logical library setting.
   a. Select **Setup** > **Logical Library Mgmt** > **Delete All Logical Libraries**. and follow the on-screen prompts.

Now you are ready to configure your library.

Step 2: Ensuring that all hardware is installed

1. Read the **Hardware Installation** screen of the Setup wizard, if it is displayed.
2. Ensure that all tape drives and the customer-supplied ethernet cable are installed.
3. If the drives and ethernet cable are installed, press **Next** to continue.

Step 3: Setting the date and time

1. Enter the current date and time by touching each square and entering the current value. The library clock is on a 24-hour cycle. For example, 4:00 pm is entered as 16 (HH) and 00 (MM).
2. Press **OK** to save the date and time settings and to continue.
3. Press **Apply** when you are done setting the date and time.

Step 4: Setting up the library network configuration

Read “Modifying network settings” on page 5-2 before this step is started.

Important: You cannot access the library remotely until the network settings are applied. Numerous system functions and commands are completed only with the remote Web User Interface.

Press **No** if you do not know your network settings and want to continue to configure your library.

To set up the network configuration:

1. Press **Yes** to begin configuring the library network.
2. Check **Enable IPv6** if applicable.

   Note: IPv6 addressing can be enabled from the Setup wizard, but IPv6 network settings cannot be configured from the Setup wizard. They can be configured only from the Web User Interface or with the **Setup** > **Network Mgmt** screen from the Operator Panel after the Setup wizard is closed.
3. Choose a name for your library.
   a. Press the **Library Name** text box to access the alphanumeric keyboards.
   b. With the alphanumeric keyboards, enter the name into the **Library Name** field.

   Note: The library name can be a maximum of 12 alphanumeric characters. Any letters that are used in the library name must be lowercase.
4. If you are using IPv4 (and did not select IPv6 in Step 2), select **Dynamic Host Configuration Protocol (DHCP)** to have the library network setting automatically configured. Or, to configure your network manually, enter the following network settings:
   - **IP Address** - the Internet Protocol (IP) address of the library

- **Subnet Mask** - the IP address of the Subnet Mask
- **Default Gateway** - the IP address of the default gateway for your portion of the Ethernet network

  Note: Each IP address consists of four sets of numbers ("octets") separated by periods. Do not use "0" in the last octet of the default Gateway address because it resets the Gateway to the original address set at the factory.

5. Determine your network settings (IP address, Default Gateway, and Subnet Mask) and record this information on the Appendix E, “Library configuration form,” on page E-1.
6. Press **Apply** to save the network settings.
7. After a successful save, press **Close**.

Step 5: Entering license keys

Read “Applying a license key” on page 5-2 before this step is started.

If you purchased a Path failover license key (Feature code 1682 that includes Control path failover and Data path failover), Capacity Expansion license key (Feature code 1640), or a Transparent LTO Encryption license (Feature code 5900) with your library, enter those license keys now.

Note: A Data path failover license key (Feature code 1682) is entered at the host. Refer to the device driver documentation shipped with your library and the installation instructions that are shipped with your license keys for information.

Press **No** if you want to configure your library without entering a license key.

To enter a license key

1. Locate the license key labels.
2. Press **Yes**.
3. Press the **license key** field to access the alphanumeric keyboards.
4. Use the alphanumeric keyboards to enter the key.
5. Press **Apply**.
6. Press **Close** to continue.
7. Verify that your library has the correct number of licensed slots by selecting the **Home** icon (**1** in Figure 6-2 on page 6-2) to view the **Home Page** screen.
8. Place a license key label on the cover plate on the rear of the library to the right of the Library Control Blade.
9. Place another license key label on the Appendix E, “Library configuration form,” on page E-1 for safe keeping.
10. Repeat this procedure for each license key.

Step 6: Assigning cleaning cartridge slots

Read “Configuring cleaning slots” on page 5-3 before this step is started.

One cleaning cartridge slot is assigned as a default in the library. A maximum of four cleaning cartridge slots are allowed in the library. If you do not want to assign extra cleaning cartridge slots, press **No** to continue configuring your library.

To assign extra cleaning cartridge slots:

1. Press **Yes**.
2. With the up and down arrows, choose the number of cleaning slots that you would like to assign in your library.
3. Press **Next** to continue.

Step 7: Assigning I/O station slots

Read "Configuring I/O stations" on page 5-4 before this step is started.

The library has six I/O station slots that are assigned as a default. If you purchased a E9U expansion module and a Capacity Expansion license key (Feature code 1640), you can assign extra I/O station slots. Up to 12 I/O station slots can be assigned in each E9U expansion module. If you do not want to assign extra I/O station slots, press **No** to continue configuring your library.

To assign extra I/O station slots:

1. Press **Yes**.
2. With the up and down arrows, choose the number of I/O station slots you would like to assign in your library.
3. Press **Next** to continue.

Step 8: Assigning logical libraries

Read "Creating and modifying logical libraries" on page 5-4 before this step is started.

The library has one logical library that is configured as a default. The maximum number of logical libraries that can be configured is equal to the number of drives that are installed in the library.

If you do not want to create more libraries, press **No** to continue configuring your library.

To create more logical libraries:

1. Press **Yes** to change the number of logical libraries in your library.
2. With the up and down arrows, choose the number of logical libraries you want to set up in your library.
3. Press **Next** to continue.
4. Modify the library names that display by pressing the text box, and with the alphanumeric keyboards, type in a name.
5. Press **Next** to continue.
6. Verify that the number of cleaning slots, I/O station slots, and logical libraries that are created is correct.
7. Press **Apply** to save the settings and exit the Setup wizard.

Step 9: Inserting cleaning cartridges

Read "Cartridge assignments in the library" on page 5-1 before this step is started. If necessary, log in to the Operator Panel (see "Step 1: Configuring the library with the Setup wizard" on page 7-2).

1. Place a cleaning cartridge in the I/O station.

2. Press **System** to assign the cleaning cartridge to the entire library system and not to a specific logical library.
3. Select **Operations** > **Inserting Cleaning Media**.
4. Select the designed destination slot for the cleaning cartridge.
5. Press **OK**.
6. Repeat this procedure for each cleaning cartridge.

Step 10: Populating your library with data cartridges

Read "Cartridge assignments in the library" on page 5-1 before this step is started.

Note: This library reads bar code labels to identify the specific cartridges in each slot. Ensure that all cartridges placed in the library have appropriate bar code labels.

Two methods are available for populating your library with data cartridges:

- Bulk loading
- Importing with the I/O station

Bulk Loading

Bulk loading is another way to load media into the library. After the bulk load is complete, the library completes an inventory.

Before bulk loading, print the Library Map from the web client to see how the physical slots of the library are configured. The report shows what slots are unavailable or configured as cleaning slots or as I/O station slots. For information on accessing, see the Library Map on the Web User Interface (**Monitor System** > **Library Map**).

CAUTION:
Place cartridges in their appropriately configured slot location. For example, cleaning cartridges must not be placed in slots that are configured for storage.

When I/O station slots are configured as I/O slots, the I/O station door is unlocked, and you can open the main access door to the library. When all I/O station slots are configured as storage, the I/O station door is always locked. You are not able to open the main access door to bulk load tape cartridges into the library without first unlocking the I/O station door. If possible, bulk load the library before the I/O station slots are configured as storage. Otherwise, unlock the I/O station door. For information on locking and unlocking the I/O stations, see "Locking/unlocking the I/O station" on page 8-23. For information on configuring I/O station slots, see "Configuring I/O stations" on page 5-4.

To complete an initial bulk load, open the access door and manually insert directly into storage slots as many cartridges as you plan to use. The cartridges do not go in all the way if they are inserted incorrectly.

Note: When you open the main access door to load tape cartridges into the library, the library automatically generates a Service Action Ticket, alerting you to the fact that the door was opened. For information on resolving a Service Action Ticket, see "Service Action Tickets" on page 11-1.

Each library configuration contains a limited number of slots that are not accessible to the robot. The slot counts in this user's guide do not include these unusable slots.

To determine which Robot your library contains, see "Robot assembly designs" on page 1-8.

1. For the M2-style picker, do not load bulk cartridges into the bottom row of the library. These storage slots are not accessible by the robot because of mechanical limitations.
2. For the original-style picker, do not bulk load cartridges into the bottom two rows of the library. Also, if your library is 23U or larger, do not bulk load cartridges into the top slot of column 4 or column 5. These storage slots are not accessible by the robot because of mechanical limitations.

Storage slots are not assigned consecutively in a logical library. To ensure that your cartridges get placed in the correct logical library, insert your data cartridges with the I/O station, following this procedure.

1. Determine the number of available storage slots in each logical library by referring to the Library Map on the Web User Interface (**Monitor System** > **Library Map**).
2. Scroll between logical libraries and make note of the number of storage slots that are assigned to each logical library.
3. Load the I/O station with data cartridges.
4. Choose the logical library to which these cartridges are to be assigned.
5. Select **Operations** > **Insert Media**.
6. Repeat this procedure until all data cartridges are inserted into the library.

Step 11: Recording and saving a copy of the current system configuration

Record the system configuration data on Appendix E, "Library configuration form," on page E-1. See "Saving/restoring system configuration" on page 8-15 to save a copy of the current system configuration.

Step 12: Registering for Support Notification

Support Notification registration provides email notification when new firmware levels are updated and are available for download and installation. To register for Support Notification, visit the web at http://www-01.ibm.com/software/support/einfo.html

Note: You are responsible for the download and installation of new firmware levels. Visit the web at http://www.ibm.com/storage/support/

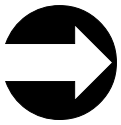
Now you are ready to use your library.

Chapter 8. Operating procedures

Library and logical libraries

The following sections provide information on operating procedures related to the library or logical libraries within your library.

Automatic RAS ticket closure



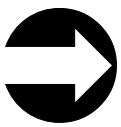
From the Operator Panel: **Tools** > **System Settings**

Automatic ticket closure is available if the library is running firmware version 600G or later. Automatic ticket closure is enabled by default. This feature can be enabled or disabled from the Operator Panel. Select **Tools** > **System Settings** and then select or clear the **Auto-Ticket Closure** check box.

When enabled, this feature closes all currently open RAS tickets when the library is rebooted. If any errors occur during the reboot, the library issues new tickets. In order for automatic ticket closure to occur, a user must intentionally initiate a reboot, by restarting the library, shutting down the library, or upgrading library firmware. Automatic ticket closure does not occur if the library shuts down unexpectedly or if the power cord is unplugged.

Closed tickets can be viewed on the library web user interface by selecting **Service Library** > **Operator Interventions** and selecting either **All Tickets**, **Unopened/Open**, **Closed**, or **Canceled**. Tickets that were auto-closed are designated as **Canceled**.

Enabling Storage Management Industry Specification (SMI-S)



From the Operator Panel: **Tools** > **System Settings**

This feature can be enabled or disabled from the Operator Panel. Select **Tools** > **System Settings** and then select or clear the **Enable SMI-S** check box.

This feature is disabled by default. Use this feature to enable or disable SMI-S on the library. See "Configuring library Security settings" on page 8-12 to enable or disable the SMI-S port for SMI-S traffic to the library (port 5988).

Viewing system information

From the Web User Interface: **Monitor System** > **System Summary**

This menu item gives information on the current assignment of I/O slots, drives, cleaning cartridge slots, storage slots, and licensed resources.

Viewing Library Map

From the Web User Interface: **Monitor System** > **Library Map**

This menu item displays a visual representation of the library, showing cleaning slots, I/O slots, storage slots, and unused slots in different colors.

Place the cursor over an item that is displayed on the Library Map, and left-click to see more information.

Accessing the Setup wizard

From the Web User Interface: **Manage Library** > **Setup Wizard**

When a new library is powered ON for the first time, the Setup wizard is available on the operator panel. This wizard allows the user to set the following configuration parameters:

- Date and Time
- Network Configuration, including choice of IPv4 or IPv6, Library Name, Static IP addresses, or DHCP
- Feature Licenses
- Cleaning Slot configuration
- I/O Station Slot configuration
- Logical Library Partitioning

After the initial power ON cycle, these configuration parameters are available separately from the Operator Panel `Setup Menu` tab.

Another version of the Setup wizard is always available from the Web User Interface (**Manage Library** > **Setup Wizard**). The Web UI Setup wizard allows the user to:

- Add feature licenses
- Set library date and time
- Select cleaning slot configuration

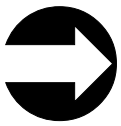
- Select I/O station slot configuration
- Allow automatic partitioning of logical libraries.

Library Verify diagnostic tests

From the Operator Panel: **Tools** > **Service** > **System**

1. Follow the menu path that is shown. Press **Yes** to take all logical libraries offline.
2. Choose one of the following diagnostic tests and follow the on-screen instructions:
   - Robotics - tests the library robotics (see "DR005: Resolving motion failure" on page 11-64)
   - I/O - tests the open/close and lock/unlock sensors of the I/O station doors (see "DR011: Resolving I/O station lock/unlock failure" on page 11-66)
   - Bar code - tests the ability of the bar code scanner to read an internal library bar code
   - Door - tests the open/close sensors of the access doors. Each access door in your library must be tested individually. During the test setup, the diagnostic test locks all of the I/O doors except the I/O door on the module that is tested. This act provides the diagnostic routine a method of testing all of the module access doors in sequence, even though the door access switches are all connected in series. After the access door tested is closed, wait until the library inventory is complete before the next test is run or normal library operations are resumed.
   - Sensors - tests and displays the sensor status of the main (access) doors, safety loop (module-to-module connectors), I/O stations, and the I/O station safety flaps. The test also displays the status of the I/O station locks. Press **Update** to retest the sensors after each change of sensor status.
3. Press **Back** or **Exit** to return to the `Library Verify` screen.
4. Press **Back** to return to the `Service` screen.
5. Press **Exit** to return to the `Library Offline` screen.
6. Press **Exit** to exit the `Library Offline` screen and return to the `Tools` menu screen.
7. Press the **Operations** tab, then press **Logical Library Mode** to bring your logical libraries online.

Creating logical libraries



From the Operator Panel: **Setup** > **Logical Library Mgmt** > **Create Logical Library**

From the Web User Interface: **Manage Library** > **Logical Libraries**

Use this menu to create logical libraries within your library. The maximum number of logical libraries allowed in the library is equal to the number of drives installed in the library. For information, see "Determining the number of logical libraries (partitions)" on page 2-1 and "Creating and modifying logical libraries" on page 5-4.

Deleting/modifying a logical library

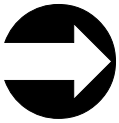
From the Operator Panel: **Setup** > **Logical Library Mgmt** > **Delete Logical Library -or- Delete All Logical Libraries**

From the Web User Interface: **Manage Library** > **Logical Libraries**

Use this menu to delete or modify logical libraries within your library. The modify function is available only from the Web User Interface. When all library resources are assigned to logical libraries, at least one logical library must be deleted to make library resources available before a new logical library can be created or an existing logical library can be modified.

The maximum number of logical libraries that are allowed in the library is equal to the number of drives that are installed in the library. For information, see "Creating and modifying logical libraries" on page 5-4.

Enabling drive logical serial number addressing



From the Operator Panel: **Tools** > **System Settings** > **Logical SN Addressing**

Administrative users can enable or disable tape driver logical serial number addressing from the Operator Panel only. The default setting is Disabled.

Logical serial number addressing allows the library to assign logical serial numbers to all tape drives in the library. Specifically, the library assigns a logical serial number to a tape drive in a specific location, not the serial number of the particular tape drive. If a tape drive is replaced by another tape drive in the same library location, the logical serial number remains the same. From the host application 's perspective, the replacement tape drive is the same as the original. By default, logical serial number addressing is disabled.

This feature can be enabled and disabled from the operator panel by navigating to the **System Settings** screen from the **Tools** tab. If you change the logical serial number addressing setting, you must shut down the library and press the library **Power** button (power cycle the library) or remove power from each tape drive for the change to take effect.

Important: Use caution with this feature, as it can be accessed by both Admin and Service login users. Enabling this feature in an existing installation changes the presentation of the drive serial numbers to the host computer and host applications. Some host operating systems, and some applications software, no longer see a drive if the serial number changes (by use of this feature) from a previously set host configuration.

It is necessary to reconfigure the host-addressing application to recognize the new tape drive serial numbers.

Assigning cleaning slots

From the Operator Panel: **Setup** > **Logical Library Mgmt** > **Configure Cleaning Slots**

From the Web User Interface: **Manage Library** > **Cleaning Slots**

Use this menu item to designate slots for cleaning cartridges in your library and automatically enable the Auto Clean function. All cleaning cartridges must have "CLN*xxx*" as part of its bar code in order for the library 's bar code scanner to recognize it as a cleaning cartridge.

Note: IBM recommends enabling the Auto Clean function on the library. With the Auto Clean function enabled, drive cleaning occurs automatically. The only time Auto Cleaning must be disabled is when your Backup Application requires that it has control.

For information, see “Configuring cleaning slots” on page 5-3.

Assigning I/O station slots

From the Operator Panel: **Setup** > **Logical Library Mgmt** > **Configure I/O Station Slots**

From the Web User Interface: **Manage Library** > **I/O Station Slots**

A 5U library has six I/O station slots. A 14U library can have 6 (in the control module), 12 (in the expansion module), or all 18 (six in the control module plus 12 in the expansion module) I/O station slots. For information, see “Configuring I/O stations” on page 5-4.

Entering license keys

From the Operator Panel: **Setup** > **Licenses**

From the Web User Interface: **Manage Library** > **Settings** > **Feature Licenses**

License keys can be purchased for Capacity Expansion (Feature code 1640), Advanced Reporting (Feature code 1650), path failover (Feature code 1682), and Transparent LTO Encryption (Feature code 5900). The Capacity Expansion license key expands the capacity of your library in increments of 46 slots. The Advanced Reporting license key enables the "Media Integrity Analysis Reporting" and the "Drive Resource Utilization Reporting" functions. The Path failover feature supplies one license key that incorporates control path and data path failover. The Transparent LTO Encryption license key enables the System Managed Encryption (SME) and Library Managed Encryption (LME) functions. For information, see “Feature licenses” on page 1-15.

After a license key is entered, run “Saving/restoring system configuration” on page 8-15 and place one of the extra license key labels on the Appendix E, “Library configuration form,” on page E-1.

Configuring encryption settings

From the Web User Interface: **Manage Library** > **Logical Libraries**

Note: The drive that is associated with the logical library must support encryption. To use Library Managed Encryption (LME), or System Managed Encryption (SME), the Encryption feature license key (Feature code 5900) must be installed.

Encryption settings are entered at a logical library level.

1. From the `Logical Library` screen, select **Modify Encryption Method** from the **Select Action** menu.
2. Select the logical library that is desired, then click **Go**.
3. The logical library that is selected must have drives that support encryption.
4. From the `Encryption Settings` screen, select the wanted encryption method.
   - None (default)
   - Application Managed Encryption (AME)
   - System Managed Encryption (SME)
   - Library Managed Encryption (LME)
5. Select the wanted encryption policy.
6. If LME is selected, enter an IPv4 or IPv6 address for the primary EKM server (or host name if DNS is enabled).
7. Enter the port number for your primary EKM server (the default port number is 3801) or enable SSL for encryption if necessary. The default SSL port number for encryption is 443.
8. Enter the IP address and port number of the secondary EKM server, if necessary.
9. Click **OK.**

Configuring and viewing Advanced Reporting reports

From the Web User Interface: **Monitor System** > **Advanced Reporting**

The Advanced Reporting license key enables Media Integrity Reporting and Drive Utilization Reporting. Administrative or Service users can configure and view various drive and media performance reports from the Web User Interface. For information, see “Advanced Reporting (Feature code 1650)” on page 1-15.

Creating user accounts

From the Operator Panel: **Setup** > **User Mgmt** > **Create User**

From the Web User Interface: **Manage Access** > **Users**

An administrator can create extra administrator and user accounts. User accounts can be restricted to specific areas of the library. For information, see “User privileges” on page 6-9.

Enter all user IDs and passwords on the Appendix E, “Library configuration form,” on page E-1.

Modifying/deleting user accounts

From the Operator Panel: **Setup** > **User Mgmt** > **Modify User**

From the Web User Interface: **Manage Access** > **Users**

An administrative user can use this menu item to modify or delete any user account.

Resetting the Admin password

The default customer Admin password is **secure**, but the customer can change it. If they forget what they changed it to, they must call Service for a reset.

You can change the password the same way a customer can, only with the **Service** menu.

1. Log in as a Service user with the default Service login and password.
2. Go to the user management screen as follows:
   - From the Operator Panel, select **Setup** > **User Mgmt** > **Modify User**.
   - From the Web client, select **Manage Access** > **Users**.
3. Follow the screens to modify a user, choosing **Admin** as the user to modify.
4. Enter the new password twice, in the **Enter Password** and **Confirm Password** text boxes.
5. With the Operator Panel, in the **Current Password** text box, enter the service password that you used to log in, then click **Apply**.
6. With the Web client, click **OK**.

Changing the Service password

Follow these instructions to change the Service password.

1. Log in as a Service user with the default Service login and password.
2. Go the `User Management` screen.
3. From the Web client, select **Manage Access** > **Users**.
4. Follow the screens to modify a user, selecting **Service** as the user to modify.
5. Enter the new password twice, in the **Enter Password** and **Confirm Password** text boxes.
6. Click **OK**.

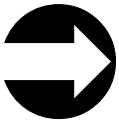
Resetting the Service password

Follow these instructions to reset the Service password.

Note: Resetting the Service password also resets the Admin password to its default setting.

1. Log in as a "reset" user with the default Service password from the Operator Panel.
2. On the Tool tab, click **Reset Password**.

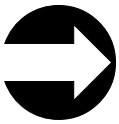
Disabling Remote Service User



From the Operator Panel: **Tools** > **System Settings** > **Disable Remote Service User**

An administrative user can disable a remote service user by checking the box on this feature.

Modifying authentication settings



From the Web User Interface: **Manage Access** > **Authentication Settings**

1. Choose **Local** for Local authentication control. Local authentication control is managed on the library. An administrator sets up accounts and privileges on the library. To use local authentication, a user must enter a local user name and password.
2. Choose LDAP to allow users to access the library with their accounts on the LDAP (Lightweight Directory Access Protocol) server. Choose **Local** to require all users to log in with a local user account. Choose **Kerberos** to authenticate users on a Kerberos server.
3. If Kerberos is enabled, specify the following information and also the LDAP information: See “Configuring Kerberos” on page 5-11 for information about configuring Kerberos.
   - Realm: The Kerberos realm name, which is typed in all uppercase letters. Usually the realm name is the DNS domain name.
   - KDC (AD Server): The server on which Kerberos is installed.
   - Domain Mapping: The domain portion of the library 's fully qualified domain name.
   - Service Keytab: Click **Browse...** to select the service keytab file. The service keytab file is a file that you generate on your Kerberos (AD) server.
4. If LDAP is enabled, specify the following general information: See “Modifying LDAP and Kerberos settings” on page 5-8 for information about configuring LDAP.
   - Repository URI is the address of the LDAP server. You can enable LDAP over SSL (LDAPS) by entering a URI in the form of `ldaps://hostname` in the **Repository URI** field. This URI uses SSL to send secure communication with port 636. If the LDAP server does not support LDAPS or does not have LDAPS enabled, login operations fail. LDAPS is deprecated in favor of StartTLS (see option). Do not use LDAPS if you use StartTLS. Once you apply LDAPS, StartTLS is not available.

Note: If your library is running firmware version 600G or later, you can optionally configure Secure LDAP with one of two methods (do not use both).

- LDAP StartTLS - Select this check box to configure secure LDAP communication with TLS. StartTLS uses the same port as regular LDAP (389). If TLS mode is not supported on your LDAP server, login operations fail. You cannot use StartTLS if you want to use LDAPS.

  Optionally, if you are using one of the methods, you can install a TLS certificate.

  – LDAP TLS Certificate - Provides extra verification of the LDAP server. If the certificate is installed, the library verifies that the LDAP server is not compromised. The certificate must be the same certificate that is installed on your LDAP server and must be in .pem format. The maximum size of the file is 4 KB. The library completes only the verification if you configured Secure LDAP (either LDAPS or StartTLS). Place a copy of the certificate file in an accessible location on your computer and use **Browse** to locate and install it. Once a certificate is installed, you can remove it by selecting the **Remove Certificate** check box. The library reboots after you install or remove a TLS certificate.

- Group DN is the URI of the location of the group information about the LDAP server (such as `ldap://ldap.server.com:389`)
- User DN is the URI of the location of the user information about the LDAP server (such as `ldap://ldap.server.com:389`)
- Default Domain is the URI of the server that displays on the login screen.

5. If LDAP is enabled, specify the following authentication and group information:
   - Principle authentication is the login ID that allows the library to access the LDAP server.
   - Credential authentication is the password for the login ID that allows the library to access the LDAP server. You must enter the same password twice.
   - User Group is the name of the group that is associated with the library.
   - Administrator Group is the name of the group that is associated with the library administrator.
6. To test the LDAP settings, click **Test LDAP Connection**. If the settings are valid, a Success message displays. If there is a problem with your LDAP settings, a failure message displays.

   Testing LDAP Settings

   Test LDAP Connection tests communication between the library and the LDAP server, and tests the currently applied LDAP settings. If there are any problems, an error message identifies the problem area. If you change the LDAP settings, click **Submit Changes** before this button is used.

   To test the settings, you must enter a user name and password, then click the button. **The user you use for the test must be a member of both the Library User Group and the Library Admin Group on the LDAP server.** Since most normal users are not members of both these groups, you might need to create a special or temporary user specifically for this purpose
7. Click **Submit Changes** to save your settings.

Note:
When Kerberos or LDAP (Lightweight Directory Access Protocol) is enabled, the login screen gives the user a choice between local authentication (the login and password are stored on the library) or LDAP authentication (the login and

password are stored on a server, and the user must specify the LDAP domain name). Kerberos requires LDAP information, but LDAP users are not required to use Kerberos.

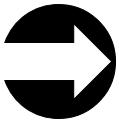
Setting User Session Timeout

From the Operator Panel: **Tools** > **System Settings** > **User Session Timeout (Minutes)**

From the Web User Interface: **Manage Access** > **Set Session Timeout**

An administrative user can set the session timeout interval to one of the discrete values of 15, 30, 60, 480, or 'Never' from the Web User Interface. From the Operator Panel, it can be set in 1-minute intervals, within the range of 15 to 480 minutes.

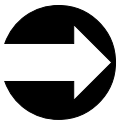
Enabling Touch Screen Audio



From the Operator Panel: **Tools** > **System Settings** > **Touch Screen Audio**

Users can enable or disable the touchscreen audio response feature.

Display settings



From the Operator Panel: **Tools** > **Display Settings**

Users can control the brightness and contrast of the local operator panel display. The default settings are Brightness = 15; Contrast = 52.

Setting DNS parameters

From the Web User Interface: **Manage Library** > **Settings** > **Network**

Domain Name System (DNS) is a keyword-based redirection service that translates text-based location names (such as www.ibm.com) to numeric IP addresses (such as 123.456.78.99). Before you can use DNS names within the library, you must specify the numeric IP address of the server that completes this translation. Once the server is defined, you can enter text addresses anywhere in the library configuration.

1. Enter the IP address of the primary DNS server.
2. (optional) Enter the IP address of a backup or alternative DNS server.

Setting the date and time

From the Operator Panel: **Setup** > **Date and Time**

From the Web User Interface: **Manage Library** > **Settings** > **Date and Time** or **Manage Library** > **Setup Wizard**

The date and time on your library must be changed at the initial installation of your library, after a power outage, and when daylight saving time comes and goes.

- From the Operator Panel, enter the current date and time by touching each square and entering the current value. The library clock is on a 24 hour cycle. For example, 4:30 would be entered as 16 (HH) and 30 (MM).
- From the Web User Interface, choose **Set the Date and Time Manually** or **Obtain the Date and Times Automatically (Network Time Protocol - NTP)**.
  - If you choose **Set the Date and Time Manually**, set the date and time as indicated. The Web UI clock is on a 12 hour cycle so it is necessary to select AM or PM. You must also select the appropriate time zone from the menu.
  - If you select **Obtain the Date and Times Automatically (Network Time Protocol - NTP)** you can enter the IP addresses (IPv4 or IPv6) of the NTP servers that you want to control the library clock.

Setting up email notifications

From the Web User Interface: Configuring the email account: **Manage Library** > **Settings** > **Email Notifications**

From the Web User Interface: Creating/modifying/deleting email notifications: **Manage Library** > **Settings** > **SMTP (Mail) Configuration**

From the Web User Interface: Setting the customer contact information: **Manage Library** > **Settings** > **Contact Information**

When enabled, this feature automatically sends an email that contains a library log (snapshot) or drive memory dump, along with the library serial number, the RAS ticket number, and the DR code to an email address that you specify whenever an Operator Intervention occurs.

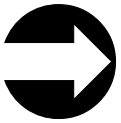
1. Follow the menu path shown.
2. From the **Select Action** menu, select **Enable, Disable, Add, Modify, Remove, or Test**.
3. Click **Go**.
4. Type the email address to which the library sends notifications.
5. Select the Alert level of the notification filter.
   - Accounts that are set to the Low filter receive email notification of all notices that are produced by the library, whether the library is in danger of failing.
   - Accounts that are set to the Medium filter receive email notification of notices of conditions that, though not yet causing immediate failure, can lead to a failure in the future, and also high-level notifications.
   - Accounts that are set to the High filter receive only those notifications that indicate the library has failed or is in immediate danger of failing.

It is recommended that you select "Low" if you must be notified of all RAS Operator 's Interventions.

6. Click **OK**.
7. Ensure that the email address you provided is enabled for notification.
8. Select **Manage Library** > **Settings** > **SMTP (Mail) Configuration**.
9. Key in the SMTP Mail Server IP address.
10. Create a name to distinguish between libraries in the sender address box. This name must be in the form of an email address. (Example: 41U@xyzcompany.com)
11. Check the box if you want to include a library log with the email notification.
12. If you select **Use Authentication**, you are prompted for a user name and password.
13. Select **Submit Change**.

Note: If the library is capturing an automatic snapshot, you are not able to manually capture a snapshot with the Web client until the automatic snapshot is complete. If this action happens, an error message displays. Wait about 10 minutes and try again.

Resetting the Library Control Blade IP address



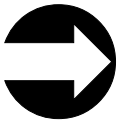
From the Operator Panel: **Tools** > **Internal Network**

The architecture of the library has two ethernet networks in it. The Library Control Blade (LCB) can be connected to your network for remote management with the web interface. There is also an “internal network” that the LCB communicates on. The internal network includes the Service Ethernet Port (which happens to be physically on the outside of the LCB).

The LCB has two networks with associated IP addresses. You cannot have two devices with the same IP trying to communicate with the LCB. The internal network is set by default to a 10.10.10.X set of IP’s.

To prevent conflict with the other devices on the network that can have the same IP, the library internal network can be reconfigured to addresses that range from 10.10.20.x to 10.10.90.x.

Configuring library Security settings



From the Operator Panel: **Tools** > **Security**

Administrative users can use the operator panel `Security Settings` screen to change the following security features:

- **Network Interface** - enables or disables all external access to the library. This setting is enabled by default to allow external access.

- **SSH** - (iLink Services) enable or disable iLink services, such as Secure Shell (SSH) (port 22), from accessing the library. This setting is enabled by default.
- **ICMP** - enables or disables external attempts to discover the library by pinging it (by using the Internet Control Message Protocol [ICMP] Echo packets). This setting is enabled by default.
- **Remote UI** - enables or disables web client user interface access (port 80) to the library. This setting is enabled by default.
- **SNMP** - enables or disables SNMP traffic (port 161) across the ethernet port. This setting is enabled by default.
- **SMI-S** - enables or disables the Storage Management Initiative Specification (SMI-S) port for SMI-S traffic to the library (port 5988). See "Enabling Storage Management Industry Specification (SMI-S)" on page 8-1 to enable or disable SMI-S on the library.. This setting is disabled by default.

You cannot configure the security settings from the web client.

Enabling SSL

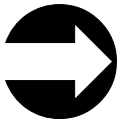
From the Operator Panel: **Tools** > **System Settings** > **Enable SSL**

Administrative users can enable or disable SSL settings from the Operator Panel. You cannot enable the SSL settings from the Web UI. The default SSL setting is Disabled.

Secure Socket Layer (SSL) is a protocol that is used for transmitting data securely over the Internet. If SSL is enabled, browsers, such as Netscape and MS Internet Explorer, use a private key that encrypts the data before it is transferred. The recipient of this secured data can then use that key to decode the information. Enabling SSL also enables an SSL-based secure authentication method for SMI-S (Storage Management Initiative Specification).

Note: Note: Before SSL settings are enabled, make sure that you enter a name for the library in the **Library Name** text box on the **Network Configuration** Operator Panel screen. After SSL settings are enabled, use that library name to access the library. If you do not use that name, you receive a security alert. In addition, make sure to complete all the text boxes that are listed on the web client **Contact Information** screen (**Manage Library** > **Settings** > **Contact Information**) before SSL settings are enabled. This information is used to identify company information in the SSL certificate.

Enabling SNMP version and SNMP traps



From the Operator Panel: **Tools** > **System Settings** > **Enable SNMP v1/v2**

From the Web User Interface: **Manage Library** > **Settings** > **SNMP** and **Manage Library** > **Settings** > **SNMP Traps**

SNMP

Messaging Simple Network Management Protocol (SNMP) is a set of protocols for remote management and monitoring of the library. Occasionally, the library can encounter a situation that you want to know about, such as an open access door that causes the library to stop. Because many servers can attach to the tape library by differing attachment methods, the library provides a standard TCP/IP protocol called Simple Network Management Protocol (SNMP) to send alerts about conditions (such as an open access door) over a TCP/IP LAN network to an SNMP monitoring server. These alerts are called SNMP traps. With the information supplied in each SNMP trap, the monitoring server (together with customer-supplied software) can alert operations staff of problems or operator interventions that occur.

The library supports SNMP v1, v2c, and v3. SNMP v3 is the default and is always enabled. SNMP v1 and v2 can be enabled/disabled. The timeout for all SNMP requests to the library must be at 10 seconds or greater (command-line parameter-t).

SNMP Community String

An SNMP community string is a text string that acts as a password to authenticate messages that are sent between the SNMP remote management application and the library (the SNMP agent). The community string is included in every SNMPv1 and SNMPv2 packet that is transmitted between the SNMP manager and the SNMP agent. This string is case-sensitive, cannot be empty, and cannot exceed 32 characters. The default community string for the TS3310 tape library is: **publicCmtyStr**

SNMP traps

Registration traps are alerts or status messages that can be collected, monitored, and used to proactively manage attached libraries with SNMP protocol with the host servers. The IBM TotalStorage TS3310 tape library supports SNMP Trap reporting.

Using SNMP, a remote station can be alerted to numerous library events such as

- **Library Identification** - model, firmware version, logical library names
- **Library Status and Health** - drive online/offline status, library online/offline status, robotics readiness, library access door status, I/O station door status, logical library status, and overall library health
- **Reliability, Availability and Serviceability (RAS) system status** - where error data is reported for monitored components within the library subsystem.

See Appendix D, “SNMP status MIB variables and traps,” on page D-1 for a listing of valid SNMP traps for the TS3310 tape library.

Administrative users can use the **SNMP Trap Destinations** screen on the Web UI to manually register the IP addresses and port numbers of external applications to enable them to receive SNMP traps from the library. After the IP addresses are registered, you can run a test to verify that the library sends the SNMP traps to the external application. Click the **Send Test Trap** option on the `SNMP Settings` screen to run the test. This test verifies only that the library sent SNMP traps to all registered IP addresses. Check the external applications to verify that the traps were received.

To enable SNMP traps:

From the Web User Interface: **Manage Library** > **Settings** > **SNMP**

To add or remove trap destination address:

From the Web User Interface: **Manage Library** > **Settings** > **SNMP Traps**

The default port number for the destination IP address is ‘162'.

SNMP MIBs

The library 's Management Information Base (MIB) contains units of information that specifically describe an aspect of the system, such as the system name, hardware number, or communications configuration. Status and error data is also gathered by MIBs and sent to one or more IP addresses that are defined during the SNMP configuration operation. See Appendix D, “SNMP status MIB variables and traps,” on page D-1 for a listing of valid SNMP traps for the TS3310 tape library.

To download the SNMP MIB file

From the Web User Interface: **Manage Library** > **Settings** > **SNMP**

SNMP Version

Note: Ensure your browser pop-up blocker is disabled when the SNMP MIB file is downloaded. Pop-up blockers prevent the `File Download` dialog box from opening.

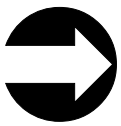
The IBM TotalStorage TS3310 tape library offers three versions of the SNMP protocol; v1, v2, and v3. Since v3 is the most secure of the three versions, it is preferred and is always enabled. You can add v1 and v2 if you want by selecting them from the Operator Panel or the Web User Interface.

To enable SNMP v1/v2:

From the Operator Panel: **Tools** > **System Settings** > **Enable SNMP v1/v2**

From the Web User Interface: **Manage Library** > **Settings** > **SNMP**

Saving/restoring system configuration



The Save/Restore Configuration operation is available only on the web client. The path to open the appropriate screen is from the Web User Interface: **Manage Library** > **Settings** > **Save/Restore Configuration**

Note: Ensure your browser software to block pop-up ad windows is disabled when the system configuration is saved. Software to block pop-up ad windows prevent the **File Download** dialog box from opening.

Administrative users can save a copy of the current configuration to an external file, or restore a saved configuration file from the external file. The system configuration must be saved before and after any procedures that might affect the configuration of the library, such as updating library or drive firmware or installing any new hardware or firmware features.

The save and restore operation is used to restore the library's configurable items to a previous state when the library is in a known working state. Do not do the save operation if the library is experiencing a problem.

Note: You cannot restore a saved configuration after you remove or replace a control module or expansion module. After you remove or replace the module, save the library configuration for future use.

Note: The saving and restoring operation must not be completed concurrently by multiple administrators that are logged in from different locations. You can access the screens, but you cannot apply changes while another administrator is completing the same operation.

The file that is saved contains the entire system configuration, plus a copy of the current version of library firmware.

Following is a partial list of the configuration items that are saved:

- Current library firmware
- Network settings:
  - IP address
  - Subnet Mask & Gateway addresses
- Feature Code licenses keys
- Logical library configuration
- Cartridge slot assignments
- Cleaning slot configuration
- I/O Station configuration
- Drive IDs:
  - SCSI ID
  - Fibre Loop ID
  - SAS ID
- Encryption method selections
- Administrator and user account information

Limits on Restoring a Saved Configuration

If your library is running firmware version 600G or later, you can restore a saved configuration that was created with firmware version 410G or later. If you need to restore a configuration created with a firmware version earlier than 410G, contact IBM Technical Support.

Enabling Internet Protocol version 6 (IPv6)

From the Operator Panel: **Tools** > **System Settings** > **Enable IPv6**

or

Setup wizard (first time only)

An administrative user can enable or disable IPv6 only from the Operator Panel. This procedure is done from the Setup wizard the first time the library is powered

ON, or at any time from the **Tools** > **System Settings** menu item. For details on setting network configuration parameters, see “Configuring the library for remote access.”

Configuring the library for remote access

From the Operator Panel: **Setup** > **Network Mgmt**

From the Web User Interface: **Manage Library** > **Settings** > **Network**

Note: Modifying network settings from the Web User Interface changes the network connectivity parameters and can cause your current web user session to become invalid. If this action happens, close the current session, access the web client again with the new network configuration settings, and log in again.

During initial installation, administrative users can modify the network settings from the Operator Panel only. After the initial configuration, administrative users can modify network settings from the Operator Panel or from the Web User Interface.

You must configure your library 's network before you can use the remote Web User Interface. For information, see “Modifying network settings” on page 5-2 and “Step 4: Setting up the library network configuration” on page 7-3.

From the Operator Panel, the network management configuration parameters can be entered in IPv4 or IPv6 format.

Note: The **Enable IPv6** box must be checked on the **Tools** > **System Settings** menu before the IPv6 format is available on the `Network Mgmt` menu.

If IPv4 is selected, the user can configure the following network settings:

- Library name
- IP address; subnet mask; default gateway
- OR Use DHCP to obtain an IP address automatically.

If IPv6 is selected, the user must select one of the following to configure the network:

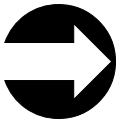
- Stateless configuration - Enable or disable automatic IP address selection with Stateless Auto Configuration.
- Static configuration - Enable or disable the static selection of an IP address by entering it manually.
- DHCP configuration - Enable or disable the selection of an IP address from a DHCP server.
- Host name configuration - Select a library name that is used to connect to the library remotely.

From the Web UI, the administrative user can enter the following network settings:

- Host name
- IP address of the primary and secondary (optional) Domain Name System (DNS) servers
- Enable Secure Socket Layer (SSL) for the Web UI

- Obtain an IPv4 and/or IPv6 address for the library
  - If "Use IPv4" is checked, the IPv4 address is obtained automatically from a DHCP server or a static IPv4 address can be entered manually.
  - If "Use IPv6" is checked, the IPv6 address is obtained automatically from a DHCP server or by Stateless Auto Configuration. A Static IPv6 address can also be entered manually.

Taking a logical library offline/online



From the Operator Panel: **Operations** > **Logical Library Mode**

From the Web User Interface: **Manage Library** > **Logical Libraries**

It is sometimes necessary to take a logical library offline before certain parts in the library are added or replaced. After the parts are added or replaced, it is necessary to bring the logical library back online. These menu items allow you to take logical libraries offline and online.

Shutting down and restarting the library

From the Operator Panel: **Operations** > **Shutdown**

From the Web User Interface: **Service Library** > **Shut down/Restart Library**

When the library is powered down under normal circumstances (the library is in an idle state - no movement, backup operations, accessing of log files), it is acceptable to power down the library with the power switch. However, when there is an operation in process, the library must be shut down with this menu item.

Shutdown shuts down the library 's operating system and firmware. This procedure prepares the library to physically turn OFF power. When a shutdown is initiated, the library finishes all active commands that are received from the host application and does not process any new commands. It also shuts down all logical libraries. Always complete a shutdown from the Operator Panel before power is removed from the library.

To completely remove power from the library, including the power supplies, press the front power switch once. To turn the library back ON, press the front power switch again and then follow the Login procedure.

Important: If you do not complete library shutdown before you power OFF the library, loss of data can occur.

Restart shuts down and restarts the library 's operating system and firmware. When a restart is initiated, the library finishes all active commands that are received from the host application and does not process any new commands. The library shuts down all logical libraries and restarts them during the reboot. In addition, the library completes an inventory of cartridges, tape drives, and slots during a reboot.

Shutting down the library

Servicing some components requires only that you take the library offline, while other componentst hat are serviced require that you power OFF the entire library. For details, see “Required library state” on page 12-1. When library power is switched OFF, the picker assembly slowly falls to rest at the bottom of the library.

Shutting down a library shuts down the library 's operating system and firmware. When a shutdown is initiated, the library finishes all active commands that are received from the host application and does not process any new commands. It takes all logical libraries offline and lowers the robot to the “shipping” position on the floor of the library. Always complete a shutdown before power is removed from the library.

Important: To completely remove all power before servicing or in an emergency, push Power, toggle each power supply switch to the OFF (O) position, and disconnect all power cords from their electrical source.

1. With the library 's Operator Panel, ensure that no applications are accessing the library. If a `Progress Screen` is open, wait until the operation completes.
2. Take the entire library (including all drives and logical libraries) offline.
   - To take each logical library offline with the Operator Panel, select **Operations** > **Logical Library Mode**.
   - To take each drive offline with the Operator Panel, select **Operations** > **Change Drive Mode**.
3. Shut down the library from the Operator Panel by selecting **Operations** > **Shutdown**. The `System Shutdown` window displays.
4. In the `System Shutdown` window, select **Shutdown** and click **Apply**.
5. In the `System Shutdown Confirmation` window, click **Yes**.
6. Press **Power** on the front of the control module.
7. Toggle each power supply switch to the OFF (O) position.
8. Disconnect the library 's power cords from their electrical source.

Restarting the library

1. With the library 's Operator Panel, ensure that no applications are accessing the library. If a `Progress Screen` is open, wait until it closes before attempting to restart the library.
2. Take the entire library (including all drives and logical libraries) offline.
   - To take each logical library offline with the Operator Panel, select **Operations** > **Logical Library Mode**.
   - To take each drive offline with the Operator Panel, select **Operations** > **Change Drive Mode**.
3. From the **Operations** menu, click **Shutdown**. The `System Shutdown` window displays.
4. In the `System Shutdown` window, select **Restart** and click **Apply**.
5. In the `System Restart Confirmation` window, click **Yes**.
6. Bring the entire library (including all drives and logical libraries) online.
   - Bring the wanted logical libraries online with the Operator Panel by selecting **Operations** > **Logical Library Mode**.
   - Rebooting the library brings any offline tape drives back online.

Key path diagnostic tests

From the Web User Interface: **Service Library** > **Key Path Diagnostics**

An Encryption key path diagnostic function is provided to assist the Administrative user in the setup, configuration, or troubleshooting of Library Managed Encryption (LME) enabled libraries. This diagnostic test consists of four tests:

1. Drive test - A drive communication test to ensure that the Library-Drive Interface (LDI) is functioning properly.
2. Ethernet test - A key server 'ping' test of all IP addresses associated with LME configured drives.
3. Key path diagnostic test - A communication test that is used to establish a link to a key manager and ensure that the communication paths between each drive and the EKM are correctly installed and set up.
4. EKM Config test - A final test to establish a link to a key manager and request a default key. This test ensures that the drive was correctly configured in the EKM to service key requests.

To run key path diagnostic tests, from the web UI, go to **Service Library** > **Key Path Diagnostics** and click **Start Tests**.

These tests are run sequentially on each IP address of each drive that is enabled for LME. If a particular test fails, the subsequent tests for that same IP address are not run, and the results show N/A. The one exception to this is that subsequent tests are still run when an Ethernet test failed.

Note: The diagnostics tests can take several minutes to complete. To run any of the tests, the tape drive that is used for the test must be unloaded, ready, and online.

If any of the tests fail, try the following resolutions and run the test again to make sure that it passes:

- Ping Test Failure - Verify that the key server host is running and accessible from the network the library is on.
- Drive Test Failure - Look for any tape drive RAS tickets and follow the resolution instructions in the ticket.
- Path Test Failure - Verify that the key server is actually running and that the port/SSL settings match the library configuration settings.
- Config Test Failure - Verify that the key server is set up to accept the tape drive you are testing.

There are two ways to run key path diagnostic tests:

- "Completing key path diagnostic tests" on page 8-21
- "Periodic key path diagnostic tests" on page 8-21

The following list describes some important factors about key path diagnostic tests:

- The key path diagnostic tests take affected partitions offline.
- The Periodic key path diagnostic tests do not take partitions offline, but it can delay moves to tape drives while they are being tested.

- The Periodic key path diagnostic test tests every connected EKM server in turn, and the library selects the tape drive to use for each test. If the selected tape drive is not available (it must be unloaded, ready, and online), then the library tries another tape drive that is connected to the key server until it finds one that is available. If no tape drives that are connected to a particular key server are available, then that server is skipped and the tests are not run. If a server is skipped for "X" number of consecutive test intervals (where "X" is configurable on the Web client), the library generates a RAS ticket. If a tape drive remains loaded for a long time, it is possible that it can never be tested. If you want to test a specific tape drive, or if you replace a tape drive, run the key path diagnostic tests manually.
- To view the status of the key path diagnostic tests, from the web user interface, select **Monitor System** > **Key Path Diagnostics**.

Completing key path diagnostic tests

Note: Tape drives must be unloaded, ready, and online in order for the test to run.

To use Key Path Diagnostic tests:

1. From the web UI, select **Service Library** > **Key Path Diagnostics**. Entering `Key Path Diagnostics` logs off all other users of the same or lower privileges and take your partitions offline. When you exit `Key Path Diagnostics`, the partitions automatically come back online. A list of all the tape drives enabled for library-managed encryption is displayed and also the partition in which each tape drive resides.
2. Select the tape drive on which you want to run diagnostic tests and click **Start Tests**. Key path diagnostic tests are completed on all applicable drives listed.
3. Click **OK** to start the diagnostic tests.
4. The library completes the tests and displays Pass or Fail results on each of the tests in the `Progress` window.

   Note: The diagnostics tests can take several minutes to complete.

Periodic key path diagnostic tests

You can enable the library to automatically complete key path diagnostic tests at selected intervals. During each interval, the library tests every configured key server. The default test interval is 4 hours. The library generates a RAS ticket if there are problems.

Periodic key path diagnostic tests are disabled by default. It is recommended that you leave `Periodic Key Path Diagnostics` disabled, unless network interruptions are a common cause of encryption failures at your site.

Attention: Running `Periodic Key Path Diagnostics` can cause an increase in RAS tickets if tests are skipped because of tape drives that are unavailable for a configurable number of consecutive test intervals. To reduce the occurrences of RAS tickets, you can specify the number of consecutive test intervals that are required to generate a RAS ticket to a higher number. Or, you can set the library to never generate a RAS ticket for missed test intervals.

To enable `Periodic Key Path Diagnostics`

1. From the Web User Interface, select **Service Library** > **Key Path Diagnostics**.
2. Select **Enable Periodic Key Path Diagnostics**.
3. Select a test interval from the **Test Interval** list.

4. Check **Enable Test Delay Reporting** if you want the library to generate a RAS ticket to inform you that the test cannot be completed within the specified number of test intervals.
   - If you check **Enable Test Delay Reporting**, from the **Test Delay Reporting Threshold** list, select the number of consecutive, missed test intervals that are required before the library generates a RAS ticket. You can select any value from 1 to 24. The default threshold is 3.
   - If you do not check **Enable Test Delay Reporting**, the library never generates a RAS ticket, no matter how many tests are missed.

Viewing error messages

From the Operator Panel: **Tools** > **Operator Interventions**

From the Web User Interface:**Service Library** > **Operator Interventions**

This menu item provides a method for managing any logged service action tickets.

If no logged service action tickets are on file, the following message is displayed: "No operator interventions were found."

Capturing a library log

From the Web User Interface: **Service Library** > **Capture Library Log**

Note: Ensure your browser pop-up blocker is disabled when the library log file is downloaded. Pop-up blockers prevent the `File Download` dialog box from opening.

This menu item allows the capturing of a library log. Wait for the `Save` window to display, then click **Save**. The log can be saved to the host or emailed to a remote site for diagnosis.

If the library is capturing an automatic snapshot, you cannot manually capture a library log until the automatic snapshot is complete. If this process happens, an error message displays. Wait about 10 minutes and try again.

Viewing library information

From the Operator Panel: **Tools** > **About Library**

From the Web User Interface: **Monitor System** > **Library Map**

The following procedures are from the Operator Panel: **Tools** > **About Library**. The **About Library** command gives status information about the library, including the

- Library name
- State

- Serial number
- Firmware level
- Machine type
- Current date and time
- Date and time of current firmware update.

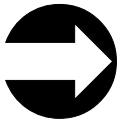
Press **Logical Library Info** to display the information about each logical library, including the

- Control path
- Serial number
- Status
- Slots
- Media
- Drives

Press **View Drive Info** to display the information that is described in "Viewing drive information" on page 8-28.

Note: If the library is 'Not Ready' because of another operation in progress, a 'Becoming Ready' message displays.

Locking/unlocking the I/O station



From the Operator Panel: **Operations** > **Lock I/O Station**

From the Web User Interface: **Manage Cartridges** > **Lock/Unlock I/O Station Doors**

This menu item enables you to set the I/O station door to either a locked or an unlocked state. This command applies to the I/O station slots in all modules of the library.

Firmware upgrades

The following sections provide information on upgrading library and drive firmware.

Note: You are responsible for the download and installation of new firmware levels. Visit the web at http://www.ibm.com/storage/support/.

Consider these IBM recommendations to provide maximum performance and reliability:

- The latest version of microcode must be installed on your IBM tape libraries and devices.
- The library code must be updated first, unless noted otherwise. This action supports any changes that are introduced in the library code for that drive, or any changes that are made to the drive for that release.
- These firmware updates are intended to increase overall reliability, improve tape handling, reduce the possibility of data errors, and enhance diagnostic capabilities.

Any time that you upgrade library or drive firmware, record the firmware level on the Appendix E, “Library configuration form,” on page E-1.

Important: Before firmware is updated,

- Resolve and close all open Operator Interventions.
- Save the current system configuration. See “Saving/restoring system configuration” on page 8-15.

Important: When firmware is updated:

- Ensure that all host applications are varied offline.
- Do not power-off the drive until the update is complete, or the firmware can be lost.

Updating library firmware

From the Web User Interface: **Service Library** > **View/Update Library Firmware Level**

Note: Ensure your browser pop-up blocker is disabled when the library firmware is updated. Pop-up blockers prevent the `Browse` dialog box from opening.

Administrative users can use the **Update Library Firmware Level** command to download firmware to the library. Updating library firmware is completed only from the Web User Interface.

Important: Before firmware is updated,

- Resolve and close all open Operator Interventions.
- Save the current system configuration. See “Saving/restoring system configuration” on page 8-15.

To update library firmware -

1. Download the latest level of library firmware to your host computer by visiting http://www.ibm.com/storage/support/.
2. From the Web User Interface, select **Service Library** > **View/Update Library Firmware Level**.
3. Browse to the file on your computer, select the ".tgz" file that was downloaded from the IBM website, then click **Update Firmware**. The Web User Interface indicates that the operation completed. The firmware file was successfully moved from the host computer to the library.
4. Wait for the library to reboot before normal library operations are resumed. It can be several minutes before the library reboots.
5. Save the current system configuration. See “Saving/restoring system configuration” on page 8-15

Important: After the update process starts, you must wait until the library reboots. Do not attempt to interrupt the process in any way, or the upgrade is not successful.

Updating drive firmware

Drive firmware is best updated with the drive 's application interface, SCSI, or Fibre Channel.

Important: Before firmware is updated,

- Resolve and close all open Operator Interventions.
- Save the current system configuration. See "Saving/restoring system configuration" on page 8-15.

Important: Before you update drive firmware with the web UI, ITDT, or FMR, make sure that tapes are not mounted in any of the drives and all cartridges are moved into the Library storage slots.

You can update drive firmware through the library 's Web User Interface. For details, see "Updating drive firmware with the Web User Interface"

Alternatively, you can update drive firmware with any of the readily available tools. For example, ITDT is available for multiple platforms and requires no special device drivers. You can download ITDT from the IBM website (refer to "The ITDT SCSI firmware update, memory dump retrieval, and drive test tool" on page 8-26). Other tools, such as NTUTIL and TapeUTIL can also be used for drive firmware updates.

The library also supports drive firmware update by creating and with an FMR cartridge. However, to create an FMR cartridge with the latest drive firmware, one of the methods that are described here must be used to download the firmware to one of the drives. An FMR cartridge can then be created and used to update the remaining drives for that drive type, SCSI, or Fibre Channel. For information on FMR cartridges, refer to "Updating drive firmware with a firmware (FMR) cartridge" on page 8-26.

Updating drive firmware with the Web User Interface

From the Web User Interface: **Service Library** > **View/Update Drive Firmware Levels**

Note: Ensure your browser pop-up blocker is disabled when drive firmware is updated. Pop-up blockers prevent the `Browse` dialog box from opening.

Administrative users can use the **View/Update Drive Firmware Levels** command to download firmware to the drive.

To update drive firmware:

1. Download the latest level of drive firmware to your host computer by visiting http://www-1.ibm.com/servers/storage/tape/lto/.
2. From the Web User Interface, select **Service Library** > **View/Update Drive Firmware Levels**.
3. Select a drive media and interface type.
4. Select the drives to be updated.
5. Click the **Select Action** menu and select **Update Firmware**. Then, select **Go**.

6. Browse to the file on your computer, select the ".ro" file that was downloaded from the IBM website, then click **Yes** to begin.
7. Save the current system configuration. See “Saving/restoring system configuration” on page 8-15

The ITDT SCSI firmware update, memory dump retrieval, and drive test tool

A newly designed tool, ITDT, is a tool with multiple functional capability and is a quick, convenient, and efficient method for drive firmware updates. As a note, drive memory dump retrievals are also run by the tool.

Some of the capabilities of this tool:

- Firmware update capability with SCSI to all IBM LTO tape drive products.
- The tool does not require any special device drivers.
- The tool is available for most major platforms (Windows, AIX, SUN, Linux, NetWare).
- The tool can upload drive memory dump files.
- The tool 's primary function is thoroughly testing a drive. However, if the library is online to the server/host where the tool resides, ITDT communicates with the drive through the library to load and unload a test cartridge, exercising some library functions.
- The tool scans the SCSI bus and finds and displays for selection all IBM LTO devices. The tool does not display and allow for selection of any non-IBM device.
- Each function has a "Help" selection that explains the required syntax and a brief explanation of the particular function.
- A Readme text file is posted with the .exe for a thorough explanation of initial tool download information from the web and an explanation of tool capabilities.
- The tool is a "command line" tool with a simple entry by keying in the executable name, **itdt**, from the directory where the tool is located.

To download the ITDT tool and instructions for using the tool, visit http://www.ibm.com/storage/support/.

Updating drive firmware with a firmware (FMR) cartridge

A firmware (FMR) cartridge is a blank tape cartridge that is used to transfer updated drive firmware code to the library. The drive code image is copied onto the FMR cartridge, which can then be used to update the drive firmware on all of the specified drives within the library. See “Creating a drive firmware (FMR) cartridge” for information.

Note: An FMR tape for updating an LTO-4 drive must be created on another LTO-4 drive with the same host interface type (for example, SAS or Fibre Channel), and likewise, an FMR for updating an LTO-3 drive must be created on another LTO-3 drive with the same host interface type (for example, SCSI or Fibre Channel). Each generation of LTO and each attachment type of drive have different firmware images.

Creating a drive firmware (FMR) cartridge:
You must create an FMR cartridge, if you do not already have one, to update drive firmware with this method. FMR cartridges are created with a blank (scratch) data cartridge. To create an FMR cartridge of a drive firmware version already in use in your library, follow the steps:

1. From the Operator Panel, select **Tools** > **Drive Mgmt** > **Create Firmware Cartridge**.
2. Select the drive type and drive from which you want to create the FMR cartridge.
3. When the Operator Panel displays the request, place a blank, scratch cartridge into the top slot of the empty I/O station. f other cartridges reside in the I/O station, remove them before the FMR cartridge is inserted.

   After the I/O station door is closed, select **System** on the `I/O Assignment` screen. The library moves the media from the I/O station to the source drive. Then, the drive instructs the source drive to create an FMR cartridge from its current code version.

Updating drive firmware with a firmware (FMR) cartridge:

1. Load the FMR cartridge in the I/O station.

   Important: Do not open the I/O station until the update process finishes.
2. Select **Tools > Drive Mgmt > Update Drive Firmware Using FMR**, then select the drive type and drives you want to update.
   - The library then successively moves this FMR cartridge into each of the specified drives to be updated.
   - The library automatically logs off all users so that they cannot complete library options while the drive firmware update operation is in progress.
   - The library updates the firmware on each targeted drive. After the update finishes, the FMR cartridge is returned to the I/O station. A message notifies you when the update operation is complete.
3. Save the current system configuration. See "Saving/restoring system configuration" on page 8-15

Other methods for updating drive firmware through the SCSI or Fibre Channel interface

Attention: Each drive connection type and each generation of drive (LTO3, LTO4, LTO5, LTO6) requires a unique firmware image.

When drive firmware is updated with the SCSI or Fibre Channel interface, the procedure varies, depending on whether your server uses an IBM tape device driver or a non-IBM tape device driver (such as a driver from Sun, Hewlett-Packard, or Microsoft).

For instructions about updating firmware from a server that uses an IBM tape device driver, refer to the *IBM Ultrium Device Drivers Installation and User 's Guide*.

To update firmware from a server that uses a non-IBM tape device driver, refer to the documentation for that device.

Drives

The following sections contain information on operating the drives installed in your library.

Viewing drive information

From the Operator Panel: **Tools** > **Drive Info**

From the Web User Interface: **Monitor System** > **Library Map** Position cursor over drive. Left-click to see drive information

This menu item provides the following information for each drive:

- Drive location
- Control path (Yes or No)
- Vendor ID
- Model number
- Type
- Serial number
- Drive firmware level
- Sled boot version
- Sled app version
- Status
- Loaded (yes or no)
- SCSI ID/WWNN/SAS address

Loading a drive

From the Operator Panel: **Operations** > **Load Drive**

From the Web User Interface: **Manage Drives** > **Load**

This menu item takes a cartridge from a cleaning slot or storage slot and loads it into the selected drive.

Unloading a drive

From the Operator Panel: **Operations** > **Unload Drive**

From the Web User Interface: **Manage Drives** > **Unload**

With this menu item, you can choose the drive to unload from a list of loaded drives. The cartridge that is unloaded from the drive is returned to its designated storage slot.

Taking a drive offline and online

From the Operator Panel: **Operations** > **Change Drive Mode**

From the Web User Interface: **Service Library** > **Service Drives**

Before a drive is replaced in the library, the installed drive that is to be replaced must be taken offline. After the new drive is installed, it must be taken online. Use these menu items to take drives offline and online.

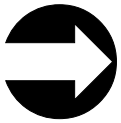
Cleaning a drive

From the Web User Interface: **Operations** > **Clean Drive**

The **Clean Drive** command provides a manual method to select a drive to be cleaned. This menu item is used when no cleaning slots are designated in the library; therefore, the Auto Clean function is disabled.

For information about designating cleaning slots in your library and enabling the Auto Clean function, see "Assigning cleaning slots" on page 8-5.

Adding a control path drive to a logical library



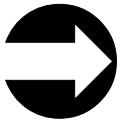
From the Operator Panel: **Setup** > **Control Path**

From the Web User Interface: **Manage Drives** > **Control Paths**

The lowest drive physically in a logical library is automatically set as the control path drive for that logical library. Each drive in a logical library can be a control path drive. Use this menu item to assign an extra control path drive in a logical library.

For information, see "Multiple control paths" on page 2-3.

Assigning drive IDs



From the Operator Panel: **Setup** > **Drive Settings**

From the Web User Interface: **Manage Drives** > **Drive IDs**

The library automatically sets SCSI, SAS, and Fibre Channel drive IDs. Use this menu item if your host system requires different IDs than the IDs chosen by the library.

For information, see "Determining SCSI, Fibre Channel, and SAS IDs" on page 2-4 and "Selecting drive IDs and drive types" on page 5-4.

Record all drive IDs on the Appendix E, "Library configuration form," on page E-1.

Modifying a Fibre Channel drive port setting

From the Operator Panel: **Setup** > **Drive IDs**

From the Web User Interface: **Manage Drives** > **Fibre Channel Ports**

Use this menu item to modify the port setting of Fibre Channel drives that are installed in your library. For information, see "Supported topologies" on page 2-7.

Note: Direct attachment of the LTO Fibre Channel drive to an AS/400 requires that the LTO Fibre Channel drive 's channel port setting is set to L-Port.

Resetting a drive

From the Web User Interface: **Service Library** > **Reset Drives** > **Reset**

From the Operator Panel: **Tools** > **Service** > **Drives** > **Drive Tests** > **Reset** > **Select Module(s)** > **Select Drive(s)**

Some hardware or firmware failures can require a drive to be reset for recovery from the failure.

Drives can be reset individually, by enclosure (module), by logical library (Web User Interface only), or by entire library.

Capturing a drive log

From the Web User Interface: **Service Library** > **Capture Drive Log**

Administrative users can use the web client to capture information about the status of the appropriate drive at the time of an error.

`Download Drive Log` information can be used to help troubleshoot library and tape drive issues.

`Download Drive Sled Log` information can be used to help troubleshoot library, tape drive sled, and tape drive issues. Drive sled logs are for Engineering use only and must be captured only when Engineering requests it.

Note: Since the log retrieval process can take up to 45 minutes, the tape drive and associated partition are automatically taken offline during the operation and brought back online when the operation completes.

Note: Ensure your browser pop-up blocker is disabled when the drive log file is downloaded. Pop-up blockers prevent the `File Download` dialog box from opening.

To capture a drive log, use the Web User Interface or ITDT. For information about ITDT, see "The ITDT SCSI firmware update, memory dump retrieval, and drive test tool" on page 8-26.

Viewing ethernet connectivity

Two places on the library Web client record whether tape drives are connected with ethernet (either with an Ethernet Expansion Blade (EEB) or connected directly to the library control blade).

Service Library > **Capture Drive Log**

Service Library > **View/Update Drive Firmware**

The table in each of these screens has a column that is called **Ethernet Connected**. If the tape drive is connected with ethernet, the tape drive IP address is listed in the column. If the tape drive is ethernet capable but not connected, the column displays "No". If the tape drive is not ethernet capable, the column displays "N/A".

Cartridges

The following sections contain information on working with cartridges.

Note: This library reads bar code labels to identify the specific cartridges in each slot. Ensure that all cartridges placed in the library have appropriate bar code labels.

Disabling/enabling manual cartridge assignment

From the Operator Panel: **Tools** > **System Settings** > **Manual Cartridge Assignment**

Administrative users can disable or enable manual cartridge assignment. When manual cartridge assignment is enabled (the default setting), the `Assign I/O` screen automatically displays on the operator panel when cartridges are placed into the I/O station. The `Assign I/O` screen prompts the user to use the Operator Panel to assign the cartridges to a specific logical library or to the system logical library. The cartridges can then be used only by the assigned logical library.

When manual cartridge assignment is disabled, the `Assign I/O` screen does not display on the Operator Panel, and the cartridges in the I/O station are visible to all logical libraries, and system logical libraries. The cartridges can also be used by any logical library.

You can disable manual cartridge assignment by clearing the **Manual Cartridge Assignment** check box on the Operator Panel `System Settings` screen. To re-enable the feature, select the **Manual Cartridge Assignment** check box. For information about cartridge assignment, see “Cartridge assignments in the library” on page 5-1.

Inserting data cartridges

From the Operator Panel: **Operations** > **Insert Media**

From the Web User Interface: **Manage Cartridges** > **I/O Station**

After a data cartridge is loaded in the I/O station, assign the data cartridge to a logical library. For information about cartridge assignment, see “Cartridge assignments in the library” on page 5-1.)

After the cartridge is assigned to a logical library, choose where in the logical library that the cartridge resides.

Note: Cartridges can be damaged during shipping or from being mishandled. Before a cartridge is inserted in your library, check that the leader pin is properly seated by sliding open the cartridge door and visually inspecting the leader pin. For information, see “Repositioning a leader pin” on page 9-17.

Removing a data cartridge

From the Operator Panel: **Operations** > **Remove Media**

From the Web User Interface: **Manage Cartridges** > **Data Cartridges**

A data cartridge is removed from a storage slot to the I/O station. Before the same data cartridge is inserted into another logical library, it must be moved from one I/O station slot to another and then assigned to a different logical library.

For information about inserting a data cartridge, see “Inserting data cartridges” on page 8-31.

Moving data cartridges

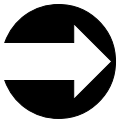
From the Operator Panel: **Operations** > **Move Media**

From the Web User Interface: **Manage Cartridges** > **Data Cartridges**

This menu item is used to move data cartridges between the I/O station, storage slots, and drives. You can view information about a specific cartridge if its volume serial number is known. Otherwise, if the volume serial number is unknown, you can filter media by one of the following locations:

- Logical library
- Enclosure

Viewing data cartridge information



From the Web User Interface: **Manage Cartridges** > **Data Cartridges**

This menu item is used to view information about a specific cartridge: its Volume Serial Number, assigned Logical Library, Media Type, Slot Type, Element Address, and Encryption.

- **Volume Serial Number** - Human-readable label (VOLSER).
- **Logical Library** - Cartridge that is assigned to logical library.
- **Media Type** - Media Type Identifier, LTO Ultrium 1 - 6.
- **Slot Type** - Storage, I/O station, or drive.
- **Element Address** - Tape cartridge slots are assigned logical element addresses by logical library. The numbering is sequential within a logical library and starts over with each logical library.
- **Encryption** - The TS3310 library supports host encryption on LTO Ultrium 6 Fibre Channel drives when used with LTO Ultrium 6 or LTO Ultrium 5 data cartridges. The TS3310 library supports host encryption on LTO Ultrium 5 Fibre Channel drives when used with LTO Ultrium 4 or LTO Ultrium 5 data cartridges. The TS3310 library supports host encryption on LTO Ultrium 4 Fibre Channel and SAS drives when used with LTO Ultrium 4 data cartridges.
  - **Unknown** - Ultrium 4, 5 and 6 media that is not loaded in a drive and the status of the data on the tape is unknown.
  - **Not Encrypted** - Ultrium 1, 2, 3, 4, 5, and 6 media that is loaded in a drive and it is determined that there is no encrypted data on the tape.
  - **Encrypted** - Ultrium 4, 5 and 6 media that is loaded in a drive and it is determined that encrypted data is written on the tape.

Inserting a cleaning cartridge

From the Operator Panel: **Operations** > **Insert Cleaning Media**

From the Web User Interface: **Manage Cartridges** > **I/O Station**

Before a cleaning cartridge is inserted, a cleaning slot must be designated in the library for the cartridge. For information on assigning a cleaning slot, see “Assigning cleaning slots” on page 8-5.

All cleaning cartridges must have "CLN*xxx*" as part of its bar code for the library 's bar code scanner to recognize it as a cleaning cartridge.

After a cleaning cartridge is loaded in the I/O station, assign it to the 'System' logical library. Manual cartridge assignment must be enabled. See “Disabling/enabling manual cartridge assignment” on page 8-31. Complete the Operator Panel or Web User Interface steps to insert the cleaning cartridge into the library.

Note: The cleaning count (Cleans Remaining) is listed on the **Manage Cartridges** > **Cleaning Cartridges** web page after the cleaning cartridge is inserted (imported) into the library.

After a cleaning cartridge is inserted into a cleaning slot, the Cleans Remaining count is equal to the maximum number of cleaning cycles (50). The actual cleans remaining is updated after the cleaning cartridge is loaded into a drive.

Note: Cartridges can be damaged during shipping or from being mishandled. Before a cartridge is inserted in your library, check that the leader pin is properly seated by sliding open the cartridge door and visually inspecting the leader pin. For information, see “Repositioning a leader pin” on page 9-17.

Removing a cleaning cartridge

From the Operator Panel: **Operations** > **Remove Cleaning Media**

From the Web User Interface: **Manage Cartridges** > **Cleaning Cartridges**

These menu items remove a cleaning cartridge from its assigned cleaning slot to the I/O station for removal from the library. This procedure is necessary when a cleaning cartridge expires and must be replaced.

To replace an expired cleaning cartridge, refer to “Inserting a cleaning cartridge” on page 8-33.

The preferred method of labeling a cleaning cartridge is to have CLN or CLNU as the prefix on the label. Any cartridge that is detected with a CLN or CLNU prefix is considered a universal cleaning cartridge, regardless of any media identification extension. Cartridges that contain a media identification of C1, C2, C3, C4, C5, and CU are considered cleaning cartridges and are tracked and treated as if the media label contained the prefix CLN or CLNU.

Chapter 9. Ultrium media

To ensure that your IBM Ultrium tape drive conforms to IBM's specifications for reliability, use only IBM LTO Ultrium tape cartridges. You can use other LTO certified data cartridges, but they might not meet the standards of reliability that are established by IBM. The IBM LTO Ultrium data cartridge cannot be used in other IBM non-LTO Ultrium tape products.

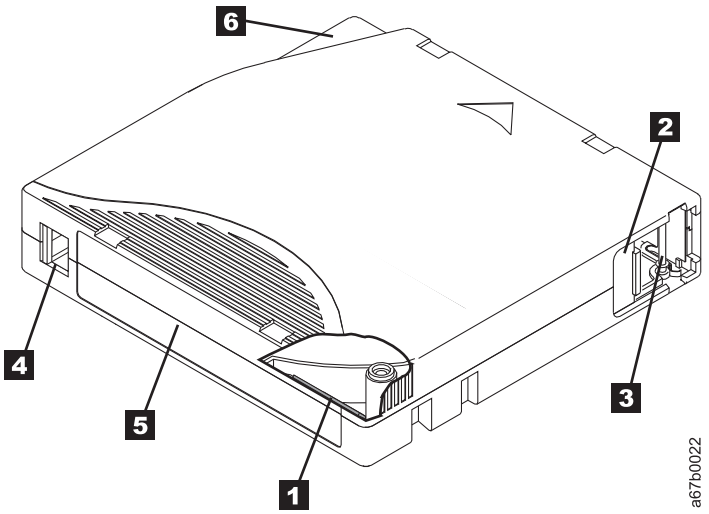


Figure 9-1. The IBM LTO Ultrium data cartridge

1	LTO cartridge memory	A chip that contains information about the cartridge and the tape, and statistical information about the cartridge 's use (For information, see “Cartridge memory chip (LTO-CM)” on page 9-3.)
2	Cartridge door	Protects the tape from contamination when the cartridge is out of the drive
3	Leader Pin	The tape is attached to a leader pin, behind the cartridge door. When the cartridge is inserted into the drive, a threading mechanism pulls the pin (and tape) out of the cartridge, across the drive head, and onto a non-removable take-up reel. The head can then read or write data from or to the tape.
4	Write-protect Switch	Prevents data from being written to the tape cartridge (For information, see “Write-protect switch” on page 9-3.)
5	Label area	Provides a location to place a label (To obtain tape cartridges and bar code labels, see “Ordering media supplies” on page 9-14).
6	Insertion guide	A large, notched area that prevents the cartridge from being inserted incorrectly

Types of cartridges

Ultrium media is available in the following types:

- "Data cartridges"
- "WORM (write once, read many) cartridges" on page 9-4
- "Cleaning cartridges" on page 9-5

Data cartridges

All generations of IBM Ultrium data cartridges contain 1/2-inch, dual-coat, metal-particle tape. When tape is processed in the cartridges, Ultrium tape drives use a linear, serpentine recording format.

Each generation of data cartridge is identified by case color, native data capacity, recording format, and nominal cartridge life.

Data Cartridge	Case Color	Native Data Capacity	Recording Format*	Nominal Cartridge Life (load/unload cycles)
Ultrium 6	Black	2500 GB (6250 GB at 2.5:1 compression)	Reads and writes data on 2176 tracks, 16 tracks at a time	20,000
Ultrium 6 WORM	Black and Silver gray			
Ultrium 5	Burgundy	1500 GB (3000 GB at 2:1 compression)	Reads and writes data on 1280 tracks, 16 tracks at a time	20,000
Ultrium 5 WORM	Burgundy and Silver gray			
Ultrium 4	Green	800 GB (1600 GB at 2:1 compression)	Reads and writes data on 896 tracks, 16 tracks at a time.	20,000
Ultrium 4 WORM	Green and Silver gray			
Ultrium 3	Slate Blue	400 GB (800 GB at 2:1 compression)	Reads and writes data on 704 tracks, 16 tracks at a time	20,000
Ultrium 3 WORM	Slate blue and Silver gray			
Ultrium 2	Purple	200 GB (400 GB at 2:1 compression)	Reads and writes data on 512 tracks, 8 tracks at a time	10,000
Ultrium 1	Black	100 GB (200 GB at 2:1 compression)	Reads and writes data on 384 tracks, 8 tracks at a time	5,000
* The first set of tracks (16 for Ultrium 6, 5, 4 and 3; eight for Ultrium 2 and 1) is written from near the beginning of the tape to near the end of the tape. The head then repositions to the next set of tracks for the return pass. This process continues until all tracks are written and the cartridge is full, or until all data is written.				

Table 9-1. Drive and cartridge properties

	Drive			Cartridge	
	Host Interface	**Sustained Native data transfer rate**	**Types**	**Physical Capacity**	**Types**
LTO6	8 Gbps dual-port Fibre Channel	160 MB/s	• Fibre Channel	• 2500 GB Native • 6250 GB with 2.5:1 compression	• Data • Rewritable • WORM
LTO5	8 Gbps dual-port Fibre Channel	140 MB/s	• Fibre Channel	• 1500 GB Native • 3000 GB with 2:1 compression	• Data • Rewritable • WORM

Table 9-1. Drive and cartridge properties (continued)

	Drive			Cartridge	
LTO4	• 4 Gbps single-port Fibre Channel • 3 Gbps dual-port SAS	120 MB/s	• Fibre Channel • SAS	• 800 GB Native • 1600 GB with 2:1 compression	• Data • Rewritable • WORM
LTO3	• 4 Gbps single-port Fibre Channel • Ultrium160 SCSI	80 MB/s	• Fibre Channel • SCSI	• 400 GB Native • 800 MB with 2:1 compression	• Data • Rewritable • WORM

Cartridge memory chip (LTO-CM)

All generations of the IBM LTO Ultrium data cartridges include a Linear Tape-Open cartridge memory (LTO-CM) chip (**1** in Figure 9-1 on page 9-1), that contains information about the cartridge and the tape (such as the name of the manufacturer that created the tape), and also statistical information about the cartridge 's use. The LTO-CM enhances the efficiency of the cartridge. For example, the LTO-CM stores the end-of-data location which, when the next time this cartridge is inserted and the WRITE command is issued, enables the drive to quickly locate the recording area and begin recording. The LTO-CM also aids in determining the reliability of the cartridge by storing data about its age, how many times it was loaded, and how many errors it accumulated. Whenever a tape cartridge is unloaded, the tape drive writes any pertinent information to the cartridge memory.

The storage capacity of the LTO Generation 6 LTO-CM is 16320 bytes. The storage capacity of the LTO Generation 4 LTO-CM is 8160 bytes. LTO Generations 1, 2, and 3 have an LTO-CM capacity of 4096 bytes.

Write-protect switch

The position of the write-protect switch on the tape cartridge (see **4** in Figure 9-1 on page 9-1) determines whether you can write to the tape. If the switch is set to:

- The locked position (solid red), data cannot be written to the tape.
- The unlocked position (black void), data can be written to the tape.

If possible, use your server 's application software to write-protect your cartridges (rather than manually setting the write-protect switch). This function allows the server 's software to identify a cartridge that no longer contains current data and is eligible to become a scratch (blank) data cartridge. Do not write-protect scratch (blank) cartridges; the tape drive is not able to write new data to them.

If you must manually set the write-protect switch, slide it left or right to the wanted position.

Capacity scaling

To control the capacity of the cartridge (for example, to obtain a faster seek time) issue the SCSI command SET CAPACITY. For information about this command, refer to the *IBM TotalStorage Ultrium Tape Drive SCSI Reference*.

WORM (write once, read many) cartridges

Certain records retention and data security applications require a Write Once, Read Many (WORM) method for storing data on tape. The LTO Ultrium generations 3, 4, 5 and 6 enable WORM support when a WORM tape cartridge is loaded into the drive.

Because standard read/write media are incompatible with the WORM feature, a specially formatted WORM tape cartridge (see Figure 9-2) is required. Each WORM cartridge has a unique, worldwide cartridge identifier (WWCID), which comprises the unique CM chip serial number and the unique tape media serial number.

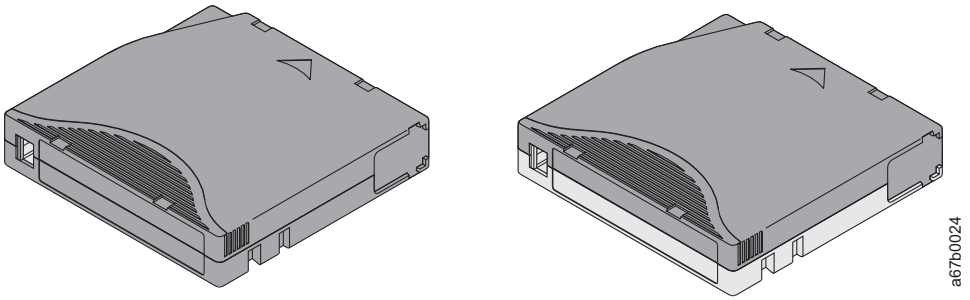


Figure 9-2. Ultrium data cartridge on the left; WORM cartridge on the right

Type of Cartridge	Case Color	Native Data Capacity	Recording Format*
Ultrium 6 WORM	Black and silver gray	2500 GB (6250 GB at 2.5:1 compression)	Reads and writes data on 2176 tracks, 16 tracks at a time
Ultrium 5 WORM	Burgundy and silver gray	1500 GB (3000 GB at 2:1 compression)	Reads and writes data on 1280 tracks, 16 tracks at a time
Ultrium 4 WORM	Green and silver gray	800 GB (1600 GB at 2:1 compression)	Reads and writes data on 896 tracks, 16 tracks at a time.
Ultrium 3 WORM	Slate blue and silver gray	400 GB (800 GB at 2:1 compression)	Reads and writes data on 704 tracks, 16 tracks at a time
* The first set of tracks (16 for Ultrium 6, 5, 4 and 3; 8 for Ultrium 2 and 1) is written from near the beginning of the tape to near the end of the tape. The head then repositions to the next set of tracks for the return pass. This process continues until all tracks are written and the cartridge is full, or until all data is written.			

Data security on WORM media

Certain built-in security measures help ensure that the data written on a WORM cartridge does not become compromised, for example:

- The format of a WORM tape cartridge is unlike that of standard read/write media. This unique format prevents a drive that lacks WORM-capable firmware from writing on a WORM tape cartridge.
- When the drive senses a WORM cartridge, the firmware prohibits the changing or altering of user data that is already written on the tape. The firmware tracks the last appendable point on the tape.

WORM media errors

The following conditions cause WORM media errors to occur:

- Information in the servo manufacturer 's word (SMW) on the tape must match information from the cartridge memory (CM) module in the cartridge. If it does not match,
  - A full-high tape drive posts a media Error Code 7 on the single-character display (SCD).
  - A library posts an error on the operator control panel
- Inserting a WORM tape cartridge into a drive that is not WORM capable causes the cartridge to be treated as an unsupported medium. The drive reports a media Error Code 7. Upgrading the drive firmware to the correct code level resolves the problem.

Requirements for WORM capability

To add WORM capability to your LTO Ultrium generation 3, 4, 5 or 6 drives, drive firmware must be at the correct code level (see “Ordering media supplies” on page 9-14).

Cleaning cartridges

With each library, a specially labeled IBM LTO Ultrium cleaning cartridge is supplied to clean the drive head. The drive itself determines when a head must be cleaned. To clean the head, insert the cleaning cartridge into the tape load compartment of the drive or the input/output (I/O) station of the library. The cleaning is completed automatically. When the cleaning is finished, the cartridge is ejected.

Note: The drive automatically ejects an expired cleaning cartridge.

IBM cleaning cartridges are valid for 50 uses. The cartridge 's LTO-CM chip tracks the number of times that the cartridge is used.

Cartridge compatibility

The table demonstrates the Ultrium cartridge compatibility with the Ultrium tape drives.

Table 9-2. Ultrium data cartridge compatibility with Ultrium tape drives

IBM Ultrium Tape Drive	IBM LTO Ultrium Data Cartridges					
	2500 GB Ultrium 6	**1500 GB Ultrium 5**	**800 GB Ultrium 4**	**400 GB Ultrium 3**	**200GB Ultrium 2**	**100GB Ultrium 1**
Ultrium 6	Read/Write	Read/Write	Read only			
Ultrium 5		Read/Write	Read/Write	Read only		
Ultrium 4			Read/Write	Read/Write	Read only	
Ultrium 3				Read/Write	Read/Write	Read only
Ultrium 2					Read/Write	Read/Write
Ultrium 1						Read/Write

Bar code labels

A bar code label contains:

- A volume serial number (VOLSER) that is human-readable
- A bar code that the library can read

Note: The tape drive does not require bar code labels, but you can choose to use labels for tape cartridge identification purposes.

Table 9-3. Bar code label requirements for Ultrium tape drives and libraries

Ultrium Tape Drive/Library	Bar Code Label Requirements
3573	Required
3576	Required
3580	Not required
3581	Required with optional Bar Code Reader
3582	Required
3583	Required
3584	Required

When read by a library 's bar code reader, the bar code identifies the cartridge 's VOLSER to the library. The bar code also tells the library whether the cartridge is a data cartridge, WORM cartridge, or cleaning cartridge. In addition, the bar code includes the two-character media-type identifier Lx, where x equals 1, 2, 3, 4, 5, 6, T, U, V, or W. Figure 9-3 on page 9-7 shows a sample bar code label for the LTO Ultrium tape cartridge.

Table 9-4. Cartridges and VOLSERs

Cartridges	VOLSER
Ultrium 6 Data Cartridge	xxxxxxL6
Ultrium 6 WORM Cartridge	xxxxxxLW
Ultrium 5 Data Cartridge	xxxxxxL5
Ultrium 5 WORM Cartridge	xxxxxxLV
Ultrium 4 Data Cartridge	xxxxxxL4
Ultrium 4 WORM Cartridge	xxxxxxLU
Ultrium 3 Data Cartridge*	xxxxxxL3
Ultrium 3 WORM Cartridge	xxxxxxLT
Ultrium 2 Data Cartridge	xxxxxxL2
Ultrium 1 Data Cartridge (READ ONLY)	xxxxxxL1
IBM LTO Ultrium Cleaning Cartridge	CLNxxxLx
*An Ultrium 3 Tape Drive must have a minimum firmware level of 54xx for it to be compatible with the WORM cartridge.	

Tape cartridges can be ordered with the labels included or with custom labels. To order tape cartridges and bar code labels, . The bar code for usage in IBM tape libraries must meet predefined specifications. They include (but are not limited to):

- Eight uppercase alphanumeric characters, where the last 2 characters must be L6, L5, L4, L3, L2, L1, LW, LV, LU, or LT

- Label and printing to be non-glossy
- Nominal narrow line or space width of 0.423 mm (0.017 in.)
- Wide to narrow ratio of 2.75:1
- Minimum bar length of 11.1 mm (0.44 in.)
- The effective tape cartridge barcode label length, including any media ID, are limited to a maximum of 12 characters. A barcode label with more than 12 characters might not be printable according to the Code 39 label specifications for the tape cartridge area to which the label is attached.

To determine the complete specifications of the bar code and the bar code label, visit the web at http://www.ibm.com/storage/lto (select **LTO Support**), or contact your IBM sales representative.

When a bar code label is attached to a tape cartridge, place the label only in the recessed label area (see **4** in Figure 9-1 on page 9-1). A label that extends outside of the recessed area can cause loading problems in the drive.

Attention: Do not place any type of mark on the white space at either end of the bar code. A mark in this area can prevent the library from reading the label.

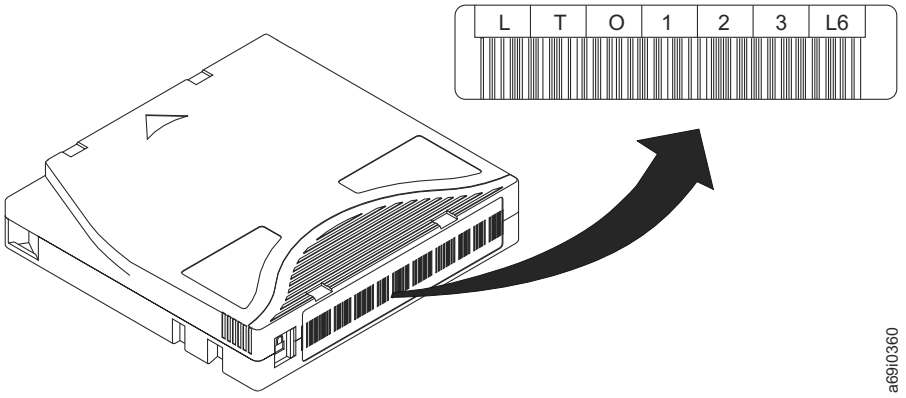


Figure 9-3. Sample bar code label on the LTO Ultrium 6 tape cartridge. The volume serial number (LTO123), cartridge type (L6), and bar code are printed on the label.

Guidelines for bar code labels

Apply these guidelines when you use bar code labels:

- Use only IBM approved bar code labels on cartridges to be used in an IBM tape library.
- Do not reuse a label or reapply a used label over an existing label.
- Before you apply a new label, remove the old label by slowly pulling it at a right angle to the cartridge case.
- Use peel-clean labels that do not leave a residue after they are removed. If there is glue residue on the cartridge, remove it by gently rubbing it with your finger. Do not use a sharp object, water, or a chemical to clean the label area.
- Examine the label before it is applied to the cartridge. Do not use the label if it has voids or smears in the printed characters or bar code. A library 's inventory operation takes much longer if the bar code label is not readable.
- Remove the label from the label sheet carefully. Do not stretch the label or cause the edges to curl.
- Position the label within the recessed label area (see **5** in Figure 9-1 on page 9-1).

- With light finger pressure, smooth the label so that no wrinkles or bubbles exist on its surface.
- Verify that the label is smooth and parallel, and has no roll-up or roll-over. The label must be flat to within 0.5 mm (0.02 in.) over the length of the label and have no folds, missing pieces, or smudges.
- Do not place other machine-readable labels on other surfaces of the cartridge. They can interfere with the ability of the drive to load the cartridge.

Unlabeled media detection

At bootup and other times the library completes an inventory of all slots and media. If a slot contains media with an unreadable barcode label (for example, the label is missing, torn, or marked up), the scanner cannot identify it, so the library reports the slot as empty.

With the **Unlabeled Media Detection** feature, you can configure the library to detect and report which slots contain media with unreadable barcodes. Cartridges with unreadable barcodes do not work for some library functions. Knowing which labels are bad allows replacement with good ones as soon as possible.

When you enable **Unlabeled Media Detection**, the calibration sensor rescans slots that are identified as empty in the inventory to see whether a cartridge is physically in the slot. If so, the library reports the cartridge as having an unreadable barcode.

Note: The library always rescans “empty” slots in the top and bottom rows of the library, even if you do not enable the **Unlabeled Media Detection** feature. This rescan is because occasionally a small or poorly placed label cannot be read by the barcode scanner in the two rows. The calibration sensor rescans the bottom row, and the picker physically checks the top row because the calibration sensor cannot reach it.

"Bottom row" here means the bottommost available row as indicated in the library configuration report.

This feature is disabled by default. When enabled, the following occurs:

- The rescan can take up to several minutes to complete.
- The library configuration report indicates media with unreadable barcodes by displaying a red triangle in the corner of the slot.
- The library user interface lists

  `No_Label`

  as the barcode for all cartridges with unreadable labels.
- The library posts a RAS ticket (T143) when an unreadable barcode label is detected. While the ticket remains open, no more T143 tickets are issued, even if more unreadable barcode labels are found.
- An unreadable barcode label is rescanned every time that the cartridge moves to a new location to check whether it is readable in the new location.

To enable the library to report unreadable barcodes:

1. Access the `System Settings` page:
   - On the Operator Panel, press **Tools** > **System Settings** > **Unlabeled Detection**.

- From the Web User Interface: **Manage Library** > **Settings** > **Media Detection**
.

2. Select one of the following from the **Unlabeled Media Detection** list:

Selection	Action
None (default) • On the Operator Panel, clear the **Unlabeled Media Detection** check box. • On the Web User Interface, clear the **Enable Unlabeled Media Detection** check box.	Completes the standard inventory only. Includes a rescan of the top and bottom rows only.
I/O • On the Operator Panel, select the **Unlabeled Media Detection** check box, then select **I/O**. • On the Web User Interface, select the **Enable Unlabeled Media Detection** check box, then select **I/O**	Rescans all slots in the I/O station that were identified as empty in the standard inventory. If media is detected, it is assumed to have an unreadable barcode.
All • On the Operator Panel, select the **Unlabeled Media Detection** check box, then select **All**. • On the Web User Interface, select the **Enable Unlabeled Media Detection** check box, then select **All**.	Rescans all slots in the library that were identified as empty in the standard inventory. If media is detected, it is assumed to have an unreadable barcode.

3. On the Operator Panel, click **Apply** or for the Web User Interface, click **Submit Changes**.

Importing unassigned media

Media is considered unassigned when it is placed into the I/O station and not assigned to a partition. When you place cartridges into the I/O station and close the door, the local Operator Panel displays a screen, asking you to assign the cartridges to a partition. If you cancel the screen and do not assign the media to any partition, the cartridges remain unassigned. Alternatively, if you disable manual cartridge assignment (Operator Panel: **Tools** > **System Settings**), the cartridge assignment screen does not display and the cartridges in the I/O station remain unassigned.

From the web client, you can import unassigned media into the library only if manual cartridge assignment is disabled. This procedure applies to both regular media and cleaning media.

Note: Whether manual cartridge assignment is enabled or disabled, if there are multiple unassigned tape cartridges in the I/O station and you select some of them to import into the library, they are ALL assigned to the first partition that you select. However, only the ones you select for import are moved into the library storage slots.

Differences in what you can see and do depending on manual cartridge assignment status:

Table 9-5. Manual cartridge assignment status

Manual Cartridge Assignment	Cartridge Assignment in I/O Station	Importing Unassigned Media	Library Configuration Report
ON (default)	You are asked to assign cartridges to a partition immediately upon placing them in the I/O station. You can "cancel" out of this window without assigning them to a partition.	From Operator Panel: **NO** From Web client: **NO**	Unassigned cartridges are not visible.
OFF	You are not asked to assign cartridges to a partition and the cartridges remain unassigned.	From Operator Panel: **YES** From Web client: **YES**	Unassigned cartridges are visible.

Handling cartridges

Attention: Do not insert a damaged tape cartridge into the drive. A damaged cartridge can interfere with the reliability of a drive and can void the warranties of the drive and the cartridge. Before a tape cartridge is inserted, inspect the cartridge case, cartridge door, and write-protect switch for breaks.

Incorrect handling or an incorrect environment can damage cartridges or their magnetic tape. To avoid damage to your tape cartridges and to ensure the continued high reliability of your IBM LTO Ultrium tape drives, use the following guidelines.

Providing training

- Post procedures that describe correct media handling in places where people gather.
- Ensure that anyone who handles tape is properly trained in handling and shipping procedures. This training includes operators, users, programmers, archival services, and shipping personnel.
- Ensure that any service or contract personnel who work on archiving are properly trained in media-handling procedures.
- Include media-handling procedures as part of any services contract.
- Define and make personnel aware of data recovery procedures.

Providing correct acclimation and environmental conditions

- Before a cartridge is used, let it acclimate to the normal operating environment for 1 hour. If condensation is visible on the cartridge, wait an extra hour.
- Ensure that all surfaces of a cartridge are dry before it is inserted.
- Do not expose the cartridge to moisture or direct sunlight.
- Do not expose recorded or blank cartridges to stray magnetic fields of greater than 100 oersteds (for example, terminals, motors, video equipment, X-ray equipment, or fields that exist near high-current cables or power supplies). Such exposure can cause the loss of recorded data or make the blank cartridge unusable.

- Maintain the conditions that are described in Table 9-6 on page 9-13.

Completing a thorough inspection

After a cartridge is purchased and before it is used, complete the following steps:

- Inspect the cartridge 's packaging to determine potential rough handling.
- When a cartridge is inspected, open only the cartridge door. Do not open any other part of the cartridge case. The upper and lower parts of the case are held together with screws; separating them destroys the usefulness of the cartridge.
- Inspect the cartridge for damage before it is used or stored.
- Inspect the rear of the cartridge (the part that loads first into the tape load compartment) and ensure that there are no gaps in the seam of the cartridge case (see **1** in Figure 9-4 and **4** in Figure 9-8 on page 9-18). If there are gaps in the seam (see Figure 9-4), the leader pin can be dislodged.

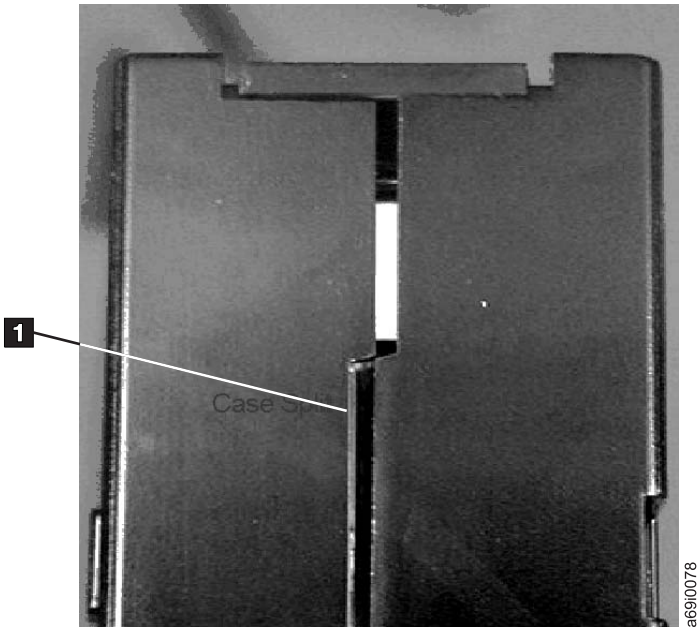


Figure 9-4. Checking for gaps in the seams of a cartridge

- Check that the leader pin is properly seated (see **2** in Figure 9-8 on page 9-18).
- If you suspect that the cartridge was mishandled but it appears usable, copy any data onto a good cartridge immediately for possible data recovery. Discard the mishandled cartridge.
- Review handling and shipping procedures.

Handling the cartridge carefully

- Do not drop the cartridge. If the cartridge drops, slide the cartridge door back and ensure that the leader pin is properly seated in the pin-retaining spring clips (see **2** in Figure 9-7 on page 9-17). If the leader pin is dislodged, go to “Repositioning a leader pin” on page 9-17.
- Do not handle tape that is outside the cartridge. Handling the tape can damage the tape 's surface or edges, which can interfere with read or write reliability. Pulling on tape that is outside the cartridge can damage the tape and the brake mechanism in the cartridge.

- If cartridges must be stacked horizontally for moving and handling, do not stack cartridges more than five high.
- Do not degauss a cartridge that you intend to reuse. Degaussing makes the tape unusable.
- For external long-term vaulted storage, store cartridges in a vertical orientation.

Ensuring correct packaging

- When a cartridge is shipped, use the original or better packaging.
- Always ship or store a cartridge in a jewel case.
- Use only a recommended shipping container that securely holds the cartridge in its jewel case during transportation. Ultrium Turtlecases (by Perm-A-Store) are tested and found to be satisfactory. They are available at http://www.turtlecase.com.

Figure 9-5. Tape cartridges in a Turtlecase

- Never ship a cartridge in a commercial shipping envelope. Always place it in a box or package.
- If you ship the cartridge in a cardboard box or a box of a sturdy material, ensure the following -
  - Place the cartridge in polyethylene plastic wrap or bags to protect it from dust, moisture, and other contaminants.
  - Pack the cartridge snugly; do not allow it to move around.
  - Double-box the cartridge (place it inside a box, then place that box inside the shipping box) and add padding between the two boxes.

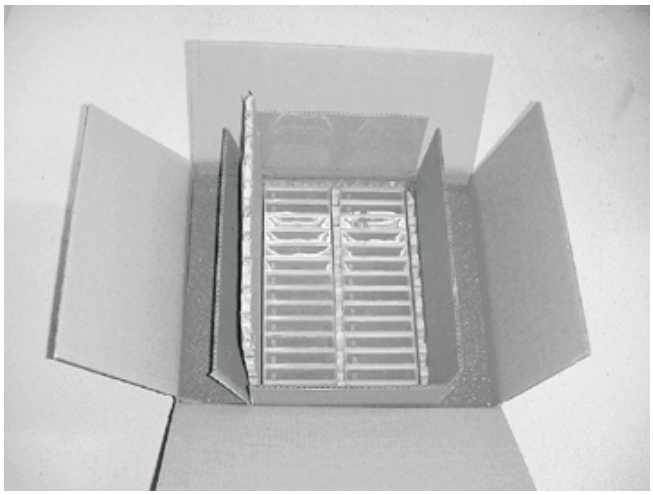


Figure 9-6. Double-boxing tape cartridges for shipping

Environmental and shipping specifications for tape cartridges

Before you use a tape cartridge, acclimate it to the operating environment to prevent condensation in the drive (the time varies, depending on the environmental extremes to which the cartridge was exposed).

The best storage container for the cartridges (until they are opened) is the original shipping container. The plastic wrapping prevents dirt from accumulating on the cartridges and partially protects them from humidity changes.

When you ship a cartridge, place it in its jewel case or in a sealed, moisture-proof bag to protect it from moisture, contaminants, and physical damage. Ship the cartridge in a shipping container that has enough packing material to cushion the cartridge and prevent it from moving within the container.

Table 9-6. Environment for operating, storing, and shipping the LTO Ultrium Tape Cartridge

	Environmental Specifications			
Environmental Factor	**Operating**	**Operational Storage**[1]	**Archival Storage**[2]	**Shipping**
Temperature	10 - 45°C (50 - 113°F)	16 - 32°C (61 - 90°F)	16 - 25°C (61 - 77°F)	-23 to 49°C(-9 to 120°F)
Relative humidity (non-condensing)	10 - 80%	20 - 80%	20 - 50%	5 - 80%
Maximum wet bulb temperature	26°C(79°F)	26°C(79°F)	26°C(79°F)	26°C(79°F)

Note:

1. The short term or operational storage environment is for storage durations of up to six months.
2. The long term or archival storage environment is for durations of six months up to 10 years.
3. Local tape temperature in excess of 52 degC can cause permanent tape damage.

Disposing of tape cartridges

Under the current rules of the US Environmental Protection Agency (EPA), regulation 40CFR261, the LTO Ultrium tape cartridge is classified as non-hazardous

waste. As such, it can be disposed of in the same way as normal office trash. These regulations are amended from time to time, and you must review them at the time of disposal.

If your local, state, country (non-US), or regional regulations are more restrictive than EPA 40CFR261, you must review them before you dispose of a cartridge. Contact your account representative for information about the materials that are in the cartridge.

If a tape cartridge must be disposed of in a secure manner, you can erase the data on the cartridge with a high-energy ac degausser. Use a minimum of 4000 oersted peak field over the entire space that the cartridge occupies. The tape must make two passes through the field at 90 degree orientation change for each pass to achieve complete erasure. Some commercial degaussers have two magnetic field regions offset 90 degrees from each other to accomplish complete erasure in one pass for higher throughput. Degaussing makes the cartridge unusable.

If you burn the cartridge and tape, ensure that the incineration complies with all applicable regulations.

Ordering media supplies

To find the closest IBM authorized distributor, visit the web at http://www.ibm.com/storage/media or call 1-888-IBM-MEDIA.

Table 9-7. Media supplies

Item Type	Description	Quantity	Order by Machine Type/Model from IBM sales representative or authorized IBM Business Partner	Order from an IBM authorized distributor
Data cartridges (with labels) (Specify the VOLSER characters that you want.)	Ultrium 6	20-PACK	Machine Type 3589 Model 550	Order from an IBM authorized distributor
	Ultrium 5	20-PACK	Machine Type 3589 Model 014	
	Ultrium 4	20-PACK	Machine Type 3589 Model 010	

Table 9-7. Media supplies (continued)

Item Type	Description	Quantity	Order by Machine Type/Model from IBM sales representative or authorized IBM Business Partner	Order from an IBM authorized distributor
Data cartridges (without labels) Order VOLSER labels separately (see "Ordering bar code labels" on page 9-16).	Ultrium 6	5-PACK	Machine Type 3589 Model 650	Order as part number 35P1902 through an IBM authorized distributor.
	Ultrium 6	20-PACK	Machine Type 3589 Model 650	Order from an IBM authorized distributor
	Ultrium 5	20-PACK	Machine Type 3589 Model 015	Order from an IBM authorized distributor
	Ultrium 5	5_PACK	Machine Type 3589 Model 015	Order as part number 46C2084 through an IBM authorized distributor.
	Ultrium 4	20-PACK	Machine Type 3589 Model 011	Order from an IBM authorized distributor
	Ultrium 4	5-PACK	Machine Type 3589 Model 011	Order as part number 95P4278 through an IBM authorized distributor.
	Ultrium 3	1	Machine Type 3589 Model 009	Order as part number 24R1922 through an IBM authorized distributor.
	Ultrium 2	1	Machine Type 3589 Model 007	Order as part number 08L9870 through an IBM authorized distributor.
	Ultrium 1	20-PACK	Machine Type 3589 Model 003	Order as part number 08L9120 through an IBM authorized distributor.
WORM cartridges (with labels) (Specify the VOLSER characters that you want.)	Ultrium 6	20-PACK	Machine Type 3589 Model 570	Order from an IBM authorized distributor
	Ultrium 5	20-PACK	Machine Type 3589 Model 034	
	Ultrium 4	20-PACK	Machine Type 3589 Model 032	
WORM cartridges (without labels) Order VOLSER labels separately (see "Ordering bar code labels" on page 9-16).	Ultrium 6	20-PACK	Machine Type 3589 Model 670	Order from an IBM authorized distributor
	Ultrium 5	20-PACK	Machine Type 3589 Model 035	
	Ultrium 4	20-PACK	Machine Type 3589 Model 033	
	Ultrium 3	20-PACK	Machine Type 3589 Model 029 Feature Code 2920 WORM cartridges that are packed in individual jewel cases with unattached blank labels.	Order as part number 96P1203 through an IBM authorized distributor.
Cleaning cartridge (with label)	Universal cleaning cartridge	5-PACK	Machine Type 3589 Model 004 Feature Code 4005	35L2086

Table 9-7. Media supplies (continued)

Item Type	Description	Quantity	Order by Machine Type/Model from IBM sales representative or authorized IBM Business Partner	Order from an IBM authorized distributor
Repair tools	Leader Pin Reattachment Kit	1	not available in this sales channel	08L9129
	Manual Rewind tool	1	not available in this sales channel	08L9130

Ordering bar code labels

The Ultrium tape drives do not require cartridge bar code labels. However, if you use your data cartridges or cleaning cartridges in an IBM tape library product, you might need cartridge bar code labels if your tape library product requires them (see "Bar code labels" on page 9-6.

You can order bar code labels with your data and cleaning cartridges, or you can order them directly from the authorized label suppliers that are listed in the table.

Table 9-8. Authorized suppliers of custom bar code labels

In America	In Europe and Asia
Tri-Optic Broomfield, CO U. S. A. Telephone: 888-438-8362 http://www.tri-optic.com	EDP Europe, Ltd. U. K. Telephone: 44 (0) 1245-322380 http://www.edpeurope.com/media-label
Dataware Houston, TX 77274 U. S. A. Telephone: 800-426-4844 http://www.datawarelabels.com/	Dataware Labels Europe Australia Telephone: (029) 496-1111 http://www.datawarelabels.com/
NetC Trumbell, CT U. S. A. Telephone: 203-372-6382 http://www.netcllc.com/	NetC Europe Ltd U. K. Telephone: 44 (0) 1823 49 1439 http://www.netclabels.co.uk
	NetC Asia Pacific Pty Ltd Australia Telephone: 61 (0) 7 5442 6263 http://www.netclabels.com.au

Repairing a cartridge

Attention: Use a repaired tape cartridge only to recover data and move it to another cartridge. Continued use of a repaired cartridge can void the warranties of the drive and the cartridge.

If the leader pin in your cartridge becomes dislodged from its pin-retaining spring clips or detaches from the tape, you must use the IBM Leader Pin Reattachment kit (part number 08L9129) to reposition or reattach it. (Do not reattach the pin if you must remove more than 7 meters (23 feet) of leader tape.) The sections that follow describe each procedure.

- "Repositioning a leader pin" on page 9-17

• "Reattaching a leader pin" on page 9-19

Repositioning a leader pin

To place the leader pin in its correct position, you need the following tools:

- Plastic or blunt-end tweezers
- Cartridge manual-rewinding tool (from Leader Pin Reattachment kit, part number 08L9129)

A leader pin that is improperly seated inside a cartridge can interfere with the operation of the drive. Figure 9-7 shows a leader pin in the incorrect **1** and correct **2** positions.

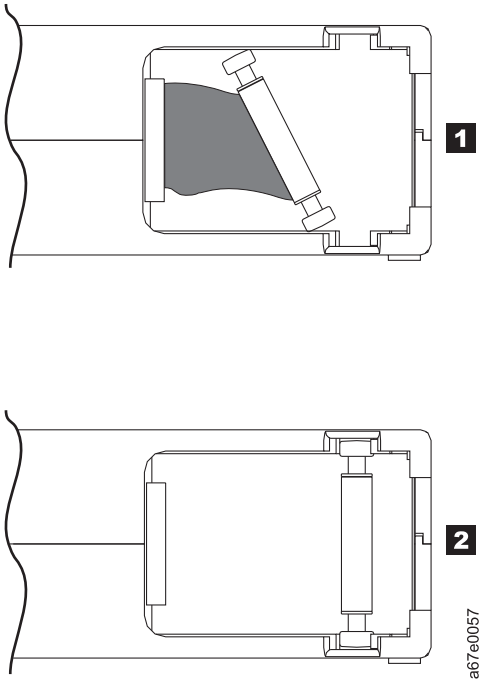


Figure 9-7. Leader pin in the incorrect and correct positions. The cartridge door is open and the leader pin is visible inside the cartridge.

To reposition the leader pin, refer to Figure 9-8 and complete the steps.

1. Slide open the cartridge door (**1**) and locate the leader pin (**2**)
   Note: If necessary, shake the cartridge gently to roll the pin toward the door.
2. With plastic or blunt-end tweezers, grasp the leader pin and position it in the pin-retaining spring clips (**3**).
3. Press the leader pin gently into the clips until it snaps into place and is firmly seated.
4. Close the cartridge door.
5. Ensure that there are no gaps in the seam of the cartridge

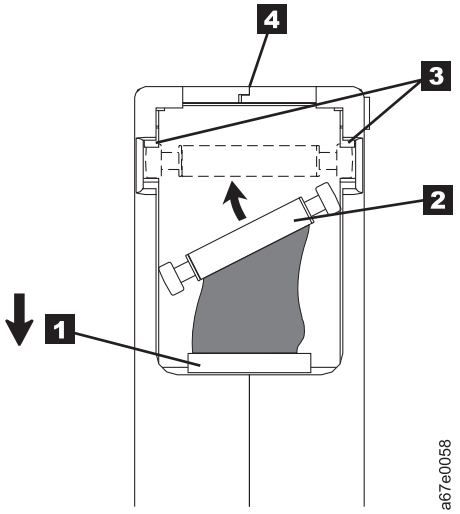


Figure 9-8. Placing the dislodged leader pin into the correct position

To rewind the tape, refer to Figure 9-9 and complete the steps.

1. Insert the cartridge manual rewind tool (**1**) into the cartridge 's hub (**2**) and turn it clockwise until the tape becomes taut.
2. Remove the rewind tool by pulling it away from the cartridge.
3. If you suspect that the cartridge was mishandled but it seems to be usable, copy any data onto a good cartridge immediately for possible data recovery. Discard the mishandled cartridge.

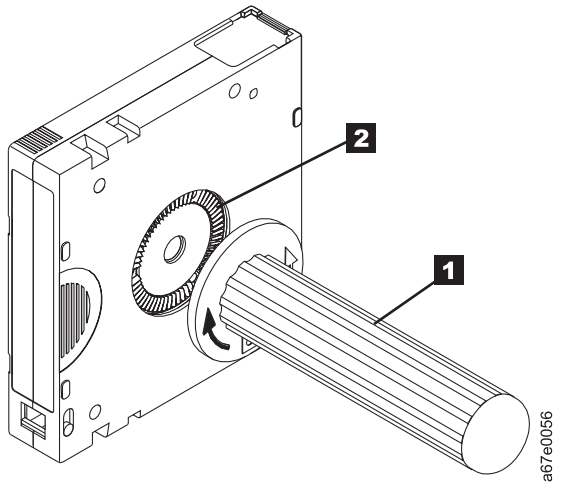


Figure 9-9. Rewinding the tape into the cartridge

Reattaching a leader pin

The first meter of tape in a cartridge is leader tape. When the leader tape is removed there is a possibility of tape breakage. After the leader pin is reattached, transfer data from the defective tape cartridge.

Important: Do not reuse the defective tape cartridge
.

The Leader Pin Reattachment kit contains three parts:

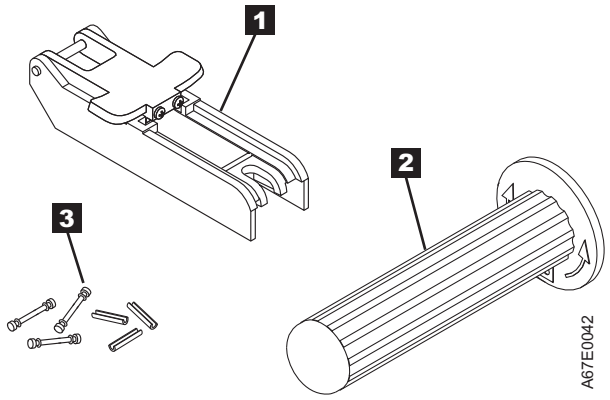


Figure 9-10. Leader Pin Reattachment kit

- **Leader pin attach tool** (1). A plastic brace that holds the cartridge door open.
- **Cartridge manual rewind tool** (2). A device that fits into the cartridge 's hub and allows the tape to wind into and out of the cartridge.
- **Pin supplies** (3). Leader pins and C-clips.

Attention:

- Use only the IBM Leader Pin Reattachment kit to reattach the leader pin to the tape. Other methods of reattaching the pin can damage the tape, the drive, or both.
- Use this procedure on your tape cartridge only when the leader pin detaches from the magnetic tape and you must copy the cartridge 's data onto another cartridge. Destroy the damaged cartridge after you copy the data. This procedure can affect the performance of the leader pin during threading and unloading operations.
- Touch only the end of the tape. Touching the tape in an area other than the end can damage the tape 's surface or edges, which can interfere with read or write reliability.

To reattach a leader pin by using the IBM Leader Pin Reattachment kit, refer to Figure 9-11 on page 9-20 and complete the steps.

1. Attach the leader pin attach tool (1) to the cartridge (2) so that the tool 's hook (3) latches into the cartridge 's door (4).
2. Pull the tool back to hold the door open, then slide the tool onto the cartridge. Open the tool 's pivot arm (5).

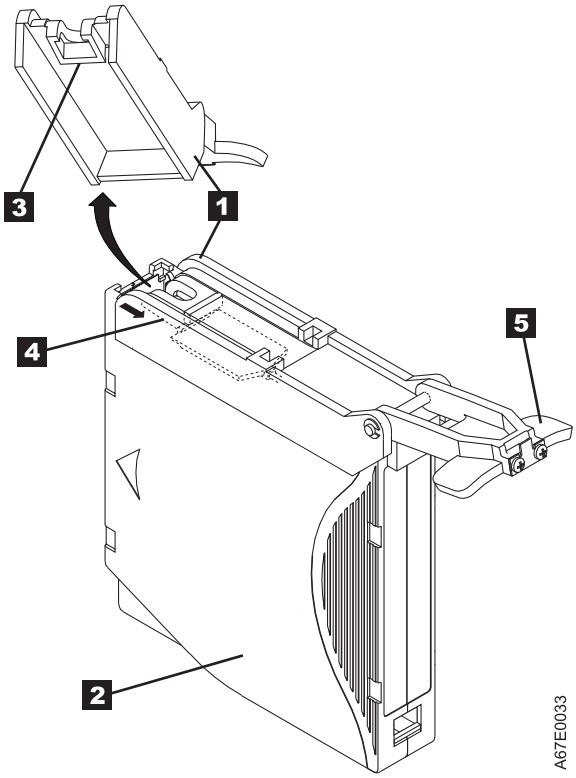


Figure 9-11. Attaching the leader pin attach tool to the cartridge. To hold the cartridge door open, hook the tool into the door and pull the tool back.

To find the end of the tape inside the cartridge, refer to Figure 9-12 on page 9-21 and complete the steps.

1. Attach the cartridge manual rewind tool (**1**) to the cartridge 's hub (**2**) by fitting the tool 's teeth between the teeth of the hub. Turn the tool clockwise until you see the end of the tape inside the cartridge. Then, slowly turn the rewind tool counterclockwise to bring the tape edge toward the cartridge door (**3**).
2. Continue to turn the rewind tool counterclockwise until approximately 13 cm (5 in.) of tape hangs from the cartridge door. If necessary, grasp the tape and pull gently to unwind it from the cartridge.
3. Remove the rewind tool by pulling it away from the cartridge. Set the tool and the cartridge aside.

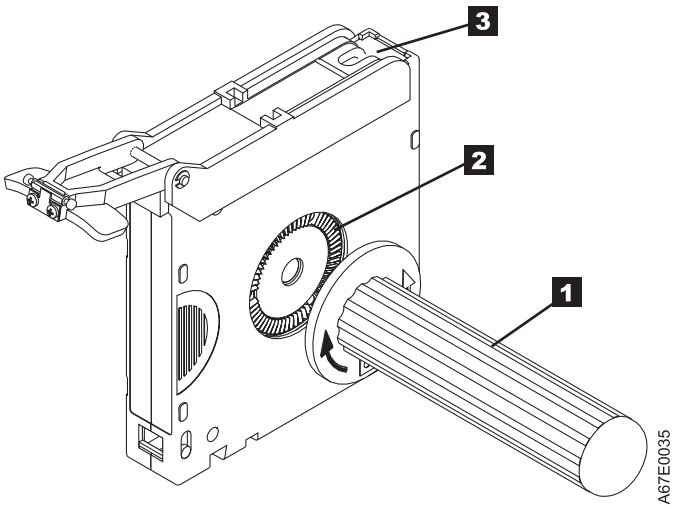


Figure 9-12. Winding the tape out of the cartridge. Turn the cartridge manual rewind tool clockwise to see the end of the tape, then turn it counterclockwise to bring the tape to the cartridge door.

To remove the C-clip from the leader pin, refer to Figure 9-13 and complete the steps.

1. On the leader pin (**1**), locate the open side of the C-clip (**2**). The C-clip is a small black part that secures the tape (**3**) to the pin.
2. Remove the C-clip from the leader pin by using your fingers to push the clip away from the pin. Set the pin aside and discard the clip.

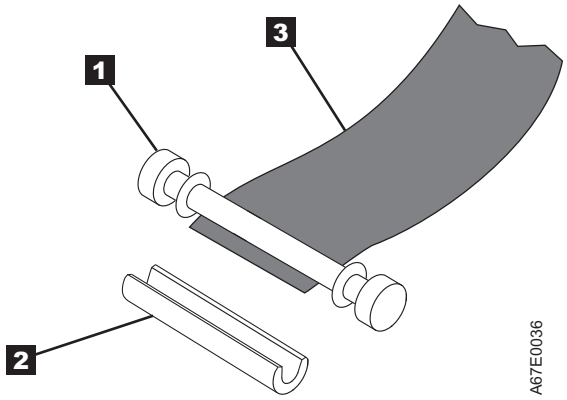


Figure 9-13. Removing the C-clip from the leader pin. Use your fingers to push the C-clip from the leader pin.

To attach the leader pin to the tape, refer to Figure 9-14 on page 9-22 and complete the steps.

1. Position the tape in the alignment groove of the leader pin attach tool (**1**).
2. Place a new C-clip into the retention groove (**2**) on the leader pin attachment tool and make sure that the clip 's open side faces up.
3. Place the leader pin that was removed earlier into the cavity (**3**) of the leader pin attach tool.

   Attention: To prevent the leader pin from rolling into the cartridge, in the following step use care when the tape is folded over the pin.
4. Fold the tape over the leader pin and hold it with your fingers.

Note: Use care to ensure that the tape is centered over the leader pin. Failure to properly center the tape on the pin causes the repaired cartridge to fail. When the tape is properly centered, a 0.25 mm (0.01 in.) gap exists on both sides of the pin.

5. Close the pivot arm (**4**) of the leader pin attach tool. Swing it over the leader pin so that the C-clip snaps onto the pin and the tape.
6. Swing the pivot arm open and trim the excess tape (**5**) so that it is flush with the reattached leader pin (**6**).
7. Use your fingers to remove the leader pin from the cavity (**3**) in the leader pin attach tool.
8. Use the cartridge manual rewind tool to wind the tape back into the cartridge (wind the tape clockwise). Ensure that the leader pin is latched by the pin-retaining spring clips on each end of the leader pin.
9. Remove the rewind tool.
10. Remove the leader pin attach tool by lifting its end away from the cartridge.

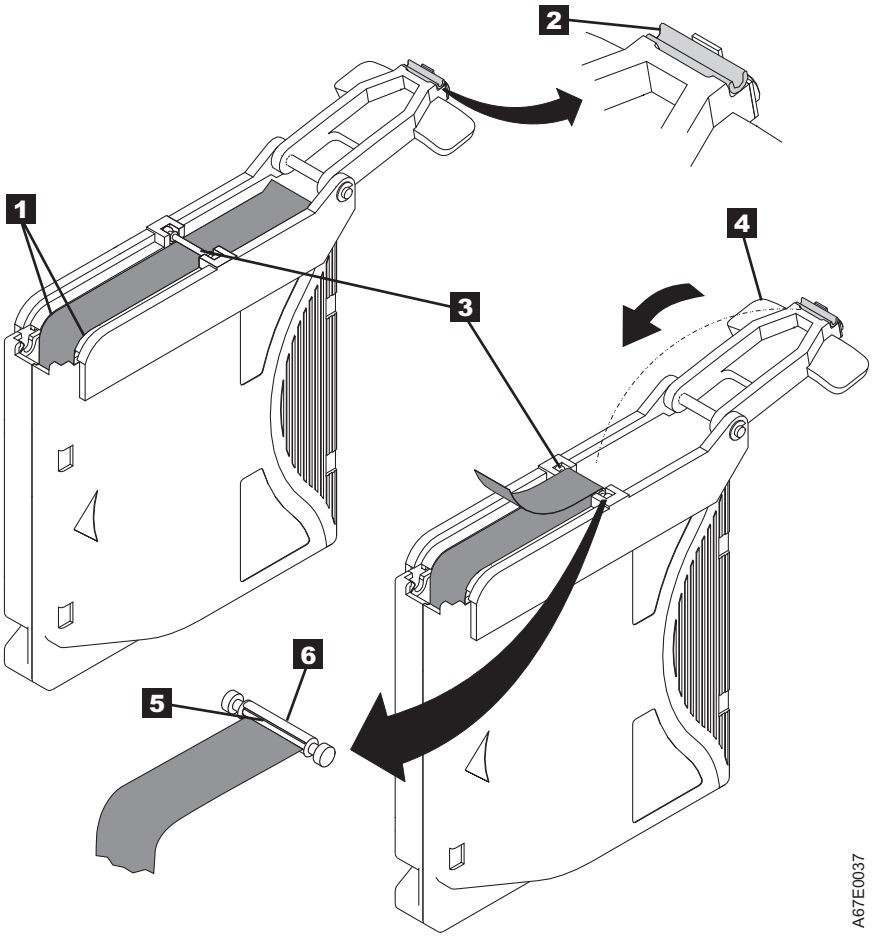


Figure 9-14. Attaching the leader pin to the tape

Chapter 10. Troubleshooting

Before a CRU replacement part is ordered, observe the LEDs on all library components to determine exactly which part is failing. See "Interpreting LEDs" on page 10-8 for information. If the LEDs on all components are functioning properly, see "Contacting IBM technical support" on page 10-21.

Important: This library has Tier 1 CRUs (customer replaceable units). The CRUs are parts of the library that must be added, removed, and replaced by the customer. If a customer chooses to have the CRU added or removed/replaced by an IBM service representative, there is a charge for the service.

Before a replacement CRU is ordered, ensure that the following criteria are met:

- The failure is repeatable.
- A log is captured for emailing to IBM service.
  - Use the ITDT tool for drive logs.
  - Use the Web User Interface (**Service Library** > **Capture Library Log** for library logs or **Service Library** > **Capture Drive Log** for drive logs).

If the library is in the process of capturing an automatic snapshot, you cannot manually capture a library log until the automatic snapshot is complete. If this process happens, an error message displays. Wait about 10 minutes and try again.

How the library reports problems

This library uses advanced problem detection, reporting, and notification technology to alert customers of problems as soon as they occur. It runs numerous self-tests to monitor the library's temperature, voltage and currents, and standard library operations. These self-tests are run each time that the library is powered ON, and during normal operation when the library is idle.

If the self-test detects a problem, the library generates a service report, or Operator Intervention, that identifies which component is likely causing the problem. The

library's LEDs can also turn ON, OFF, or flash to indicate an abnormal state. If the problem is not severe, the library continues to provide full functionality to all unaffected logical libraries.

When possible, the library provides instructions for resolving problems. These instructions display on the library's Operator Panel.

Note: If resolution of the problems includes instructions to open an access door, an access door must be opened and closed to clear the error and to enable the robotics to function properly.

Customers can frequently resolve a simple problem themselves with the information found in "Diagnosing a problem" on page 10-3. If the problem involves a field replaceable unit (FRU), the customer must contact IBM technical support (see "Contacting IBM technical support" on page 10-21). Only qualified service technicians can service FRUs.

Viewing, resolving, and closing Operator Intervention messages

From the `Tools` menu on the Operator Panel, you can view all of the library operator interventions. This view lists all of the library operator interventions in the order in which they were created starting with the most recent. Each message contains a Service Action Ticket (SAT) code (see "Service Action Tickets" on page 11-1) and an explanation of what error the library encountered. You can navigate resolution details from this screen as well (see "Diagnostic resolutions" on page 11-61). Before a library component is replaced, a ticket is closed, or IBM technical support is contacted, refer to "Diagnosing a problem" on page 10-3 for help about resolving the problem.

Important: It is recommended that Service Action Tickets are not allowed to accumulate in the Operator Intervention reports. After an incident is resolved or repaired, the Service Action Ticket must be closed.

Before a CRU replacement part is ordered, observe the LEDs on all library components to determine exactly which part is failing. See "Interpreting LEDs" on page 10-8 for information. If the LEDs on all components are functioning properly, see "Contacting IBM technical support" on page 10-21.

Viewing Operator Intervention messages

You can view operator intervention messages by choosing **Operator Interventions** from the `Tools` menu. You can also click the **Subsystem Status** buttons at the bottom of the graphical user interface home page to view all operator interventions for the subsystem you choose (Library, Drives, or Media). Operator Intervention messages are displayed in the order in which they were created, starting with the most recent. Click a column heading to sort the rows by that heading.

Resolving Operator Intervention messages

You can resolve and close operator intervention messages from the **Tools** > **Operator Interventions** screen. Identify the Operator intervention message that you want to resolve, click **Resolve**, and complete the steps that are listed in the `Library Resolution` window. It is possible to close the operator intervention message without resolving the reported issue.

Closing RAS tickets automatically

The library closes all currently open operator intervention messages when you reboot the library. If any errors occur during the reboot, the library

issues new operator intervention messages. In order for automatic ticket closure to occur, a user must intentionally initiate a reboot, by either restarting the library, shutting down the library, or upgrading library firmware. Automatic ticket closure does NOT occur if the library shuts down unexpectedly or if the power cord is unplugged. You can always view closed tickets on the Web client by selecting **Service Library** > **Operator Interventions** and clicking **Closed State**. Tickets that were auto-closed are designated as "Canceled." Automatic ticket closure is enabled by default. You can enable or disable this feature from the operator panel. The path to open the appropriate screen is: From the operator panel, select **Tools** > **System Settings**and then select or clear the **Auto-Ticket Closure** check box.

Closing all Operator Intervention messages

You can close all operator intervention messages without resolving them by clicking the **Close All Tickets** button. Be careful when all tickets are closed. It is recommended that each operator intervention is viewed, analyzed, and closed individually.

Diagnosing a problem

Problem Area	If...	Then...
Error Message	**Your library issues an Operator Intervention...** You know when an Operator Intervention is issued when **Library**, **Drives**, or **Media** at the bottom of the Operator Panel screen turns yellow or red. Operator Interventions are also indicated by the amber Operator Intervention Alert LED on the front panel of the library to the right of the **Power** button, or by email notifications, if this feature is enabled.	• Press **Library**, **Drives**, or **Media** at the bottom of the Operator Panel screen, then touch **Operator Interventions** to view the error message. • After an error message is read, press **Resolve** to display the suggested resolution for the problem. • Refer to Chapter 11, "Service Action Tickets (Txxx) and Diagnostic Resolutions (DRxxx)," on page 11-1 for information about the Service Action Ticket number (T*xxx*).

Problem Area	If...	Then...
	The resolution for an Operator Intervention suggests a CRU or FRU replacement...	Before IBM is called to order a replacement CRU or to request FRU replacement: • Refer to Chapter 11, “Service Action Tickets (Txxx) and Diagnostic Resolutions (DRxxx),” on page 11-1 for information on resolving the problem. • Observe the LEDs on all components (For more information, see “Interpreting LEDs” on page 10-8.). If the LEDs on a component indicate that there is a problem, reseat the component. • Visually check, and reseat if necessary, all of the cables that are connected to the failing FRU or CRU. For more information, see “Checking/reseating cables” on page 10-15. • If possible, power cycle the library. • If the error occurs again: – If the suspect component is a CRU, refer to Chapter 12, “Adding, removing, and replacing procedures,” on page 12-1 for detailed instructions. – OR - – If the suspect component is a FRU, see “Pre-call checklist” on page 10-20 and “Contacting IBM technical support” on page 10-21 to request FRU replacement service.
	A TapeAlert message was received...	Refer to Appendix B, “TapeAlert flags supported by the drive,” on page B-1.
	You are experiencing a problem with your library and no Operator Intervention was created...	If after all diagnostic procedures are tried you are unable to resolve the problem, refer to “Contacting IBM technical support” on page 10-21.
	The Operator Panel displays, "Error - cannot Determine Personality"...	1. Power cycle the library. 2. If the same message displays, replace the Compact Flash Card (see “Removing/replacing the Library Control Blade or Compact Flash card” on page 12-27.
	You get repeated errors, multiple functions surface failure messages, or Txxx codes...	Open and close an access door to ensure that all previous error handling is completed and to enable normal library robotic function.
	HTML error 404 appears on the computer screen when trying to launch the Web User Interface...	1. Verify that the Ethernet cable is properly connected at both ends. 2. Ping the library address to verify communication. 3. Verify network settings at host and library. 4. If the cable is properly connected, refer to “Removing/replacing the Library Control Blade or Compact Flash card” on page 12-27.

Problem Area	If...	Then...
Operator Panel	**The Operator Panel display is blank, hung, frozen, or a visual problem occurs (incorrect characters, missing characters, and so forth), dim display, or non-responsive touchscreen...**	1. Verify that power is being applied to the library. 2. Gather failure information by logging in to the Web User Interface and selecting **Service Library** > **Capture Library Log**. 3. Power cycle the library. 4. Verify that you are running the latest levels of library and drive firmware, then upgrade if necessary (see "Firmware upgrades" on page 8-23. 5. If the Operator Panel display is still failing, refer to "Contacting IBM technical support" on page 10-21.
Media	**A cartridge leader pin has detached from the cartridge...**	Reposition the leader pin (see"Reattaching a leader pin" on page 9-19 or "Repositioning a leader pin" on page 9-17).
	A cartridge is not ejecting from a drive...	1. Take the logical library to which the drive is assigned offline (refer to "Taking a logical library offline/online" on page 8-18). 2. Reset the drive (see "Resetting a drive" on page 8-30). If the cartridge does not eject, continue to the next step. 3. Open the I/O station door, then open the access door. 4. Locate the drive that does not eject the cartridge, then locate the blue **Unload** button on the drive. 5. Press **Unload** once. The Status light that is located to the left of **Unload** flashes green while the drive is rewinding and unload the cartridge. 6. If the cartridge does not eject from the drive, refer to "Contacting IBM technical support" on page 10-21.
	Tape is broken, stretched, folded over, or wrinkled inside the cartridge...	1. Replace the tape cartridge. 2. Ensure that the latest available drive code is installed (refer to "Updating drive firmware" on page 8-25). If the problem continues, replace the drive (refer to "Adding/removing/replacing a tape drive" on page 12-24).
Firmware	**A firmware problem is suspected...**	Verify that you are running the latest levels of library and drive firmware, then upgrade if necessary (see "Firmware upgrades" on page 8-23). If new firmware does not resolve the problem, refer to "Contacting IBM technical support" on page 10-21.
	The Library firmware does not complete the boot-up process and appears hung... Failure of the **Working** screen to display on the Operator Panel in 15 minutes indicates that the boot-up process is not completing.	1. Power OFF the library and wait at least 1 minute before the library is powered ON to recover the problem. 2. If a library firmware update was completed, try to repeat the update procedure. If the library firmware still fails to boot-up correctly, refer to "Contacting IBM technical support" on page 10-21.
	Library firmware is being updated...	More time is required by the library, including a blank screen then a backlit screen, before the **Working** screen displays.
	All firmware (library and drive) is not at the latest level...	Refer to "Firmware upgrades" on page 8-23 for instructions on updating all of the components that are not at the latest level. The procedure directs you to the IBM website to check for latest firmware levels.

Problem Area	If...	Then...
Logs	**You are required to capture a library log or a drive log...**	• For information on capturing a library log, refer to "Capturing a library log" on page 8-22. • For information on capturing a drive log, refer to "Capturing a drive log" on page 8-30.
	You need to acquire library or drive information at the host...	Refer to Appendix A, "Message retrieval at the host," on page A-1.
Diagnostics	**You need to run library diagnostic tests...**	Refer to "Library Verify diagnostic tests" on page 8-3.
Configuration	**Configuring the library resulted in fewer storage slots than are actually present.**	Verify that the Capacity Expansion license keys are applied as needed.
	You are reinstalling a feature requiring a License Key code.	1. From the Operator Panel, select **Setup** > **License**. 2. Reenter the license key code. If the license key code cannot be located, contact your IBM sales representative.
Power	**If the power supply power switch is ON and power indicator is OFF...**	1. Verify that the power switch is ON. 2. Verify that the power cable is properly seated on the power supply. 3. Analyze the problem by observing the power supply LEDs (see "Power supply LEDs" on page 10-12). 4. If necessary, replace the failing power supply (refer to "Removing/replacing a power supply (primary and redundant)" on page 12-34).
	If the blue LED on the power supply is ON, the power ON/OFF button on the front of the library is ON (button pushed IN), but the power indicator on the front of the library is OFF...	1. Suspect a failing power **ON/OFF** button on the front of the library, or a loose or broken cable. 2. See "Contacting IBM technical support" on page 10-21.

Problem Area	If...	Then...
Picker	**The Picker is stuck in one position and is making a clicking sound...**	1. Visually verify that all gear racks (front and rear) are properly aligned. If they are not aligned, refer to "Verifying front and rear gear racks alignment" on page 12-17. 2. Verify that the picker assembly is level. If it is not level, see "Contacting IBM technical support" on page 10-21. 3. Check for broken gear teeth on the Y motor. If there are broken teeth, see "Contacting IBM technical support" on page 10-21.
	The Picker assembly does not move within five minutes after Power ON...	1. Check cable connections from the cable spool to the Y-axis assembly and from the Y-axis assembly to the picker. 2. With access doors closed, note if the green LED on top of the picker is ON. • For a 5U library, open the I/O station door to view. • For a 14U library or larger, look through the expansion module window. 3. If the green LED is OFF, suspect the picker assembly, the Y-axis assembly, the module-to-module communication terminator, or an open door. 4. If the picker assembly is still not working, refer to "Contacting IBM technical support" on page 10-21.
Web User Interface	**A Web User Interface Help page is not opening...**	Verify that other help pages are not currently open. If other pages are currently open, close them and try again.
	You are unable to log in to the library from the Web User Interface (Web Browser cannot display the web page)...	One of the library security settings can be disabled. • From the Operator Panel: **Tools** > **Security** . • Ensure that the **Network Interface** and **Remote UI** options are enabled.
	You are unable to configure or use one of the internet traffic control parameters such as: • **ICMP (Internet Control Message Protocol or pinging the library)** • **SSH (Secure Shell) (iLink Services)** • **SNMP (Simple Network Management Protocol)** • **SMI-S (Storage Management Initiative Specification)**	One of the library security settings can be disabled. • From the Operator Panel: **Tools** > **Security** For information, refer to "Configuring library Security settings" on page 8-12.
Library Not Booting	• **There is a blank Operator Panel/display** • **Picker doesn't move** • **Display is stuck on IBM or initialization for more than 20 minutes** • **Lights are not correct on back of library.**	Suspect the LCB compact flash or the power supply.

Interpreting LEDs

Light emitting diodes (LEDs) provide a visual indication about the status of certain library components. LEDs can sometimes communicate that a problem exists when operator interventions cannot. For example, an LED can indicate a firmware problem that prohibits the library from generating operator interventions.

The following components of the library have LEDs:

- "Power button LEDs"
- "Library Control Blade LEDs" on page 10-9
- "Tape drive LEDs" on page 10-10
- "Power supply LEDs" on page 10-12
- "Picker LED" on page 10-13

Some of these components can also include a fibre port link LED.

Power button LEDs

Two LEDs are located to the right of the library 's **Power** button (**1**) on the front panel of the control module.

Figure 10-1. Power button LEDs

- Green power ON LED (**2**) - When lit, this LED indicates that the library power is ON.
- Amber Operator Intervention Alert LED (**3**) - When lit, this LED indicates that there is a Library, Drives, or Media Operator Intervention available. To view the Operator Intervention, select **Tools** > **Operator Intervention** from the Operator Panel.

Library Control Blade LEDs

The library contains a Library Control Blade (LCB). LEDs are used to indicate the status of the LCB.

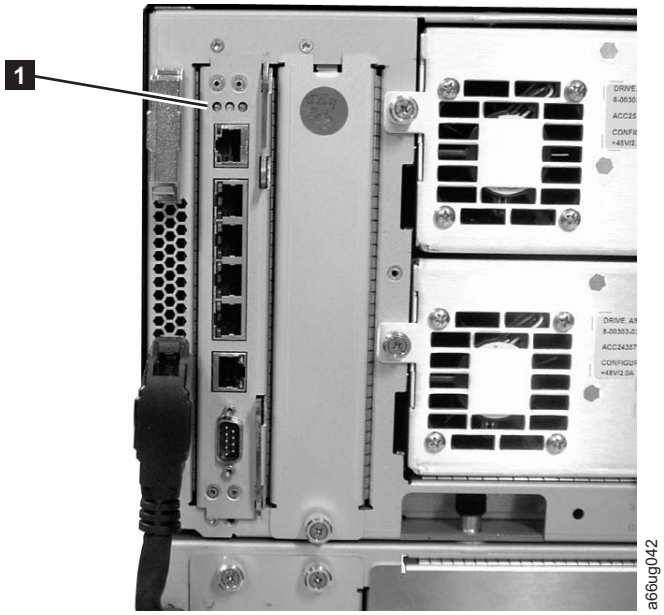


Figure 10-2. Library Control Blade LEDs

LCB LEDs (**1**) indicate status by the rate at which they flash. The color of the LED identifies the area of the component that is reported.

Use the following table to interpret the status of LCB LEDs:

Table 10-1. LCB LEDs

LED Color	Represents	Blade Status
Green	Processor status	• Solid ON - Processor not operating • Solid ON for 3 seconds, then flashes twice - LCB firmware is downloading • 1 flash per second - Normal: Processor operating • 10 flashes per second - Identify mode • Solid OFF - Processor not operating
Amber	Health status	• 1 flash per second - Main processor not operating • Solid OFF - Normal: Blade operational
Blue	Power control status	• Solid ON - Swap mode: LCB is powered down and can be removed • 1 flash per 10 seconds - Normal: LCB on • Solid OFF - LCB not receiving power

Note: If all three LEDs are solid ON for at least 20 minutes, suspect a bad or corrupted compact flash. See "Removing/replacing the Library Control Blade or Compact Flash card" on page 12-27.

Amber LED on Library Control Blade

Under normal operating conditions, the amber LED on a Library Control Blade (LCB) is not lit. If you see that the amber LED on an LCB is either flashing continuously or solidly lit for at least 20 minutes, service the LCB as soon as possible. The library can generate an operator intervention, depending on the source of the problem.

Attention: Never remove an LCB when its amber LED is solidly lit, unless it was solidly lit for at least 20 minutes.

The table indicates the actions that you can take, based on the condition of the LED.

Table 10-2. Amber LED on an LCB

State of Amber LED	Suggested Service Action
Solid ON for 20+ minutes	Replace the LCB.
1 flash per second	Check the firmware for the LCB and make sure that you have the most current firmware available (visit http://www.ibm.com/storage/lto. Do not replace the LCB. It is unlikely that the LCB hardware is the source of the problem. Observe LEDs on other components before you refer to "Contacting IBM technical support" on page 10-21.

Servicing a Library Control Blade based on LED status

When a blade is serviced based on the status of an LED:

1. Observe the flashing patterns of the LEDs for at least 30 seconds. Log in your observations both the operator intervention and the equipment failure report that you must return with the defective part. Accurate reporting of all LED states for the entire green, amber, and blue set of LEDs is critical for diagnosing the cause of the problem.
2. Generate a current log of the library, and send it to technical support for analysis.

Tape drive LEDs

Operator interventions typically report all problems that are related to tape drives, including error codes and tape alerts. By observing the flashing pattern of LEDs on tape drives, however, you can discern which operation the tape drive is running.

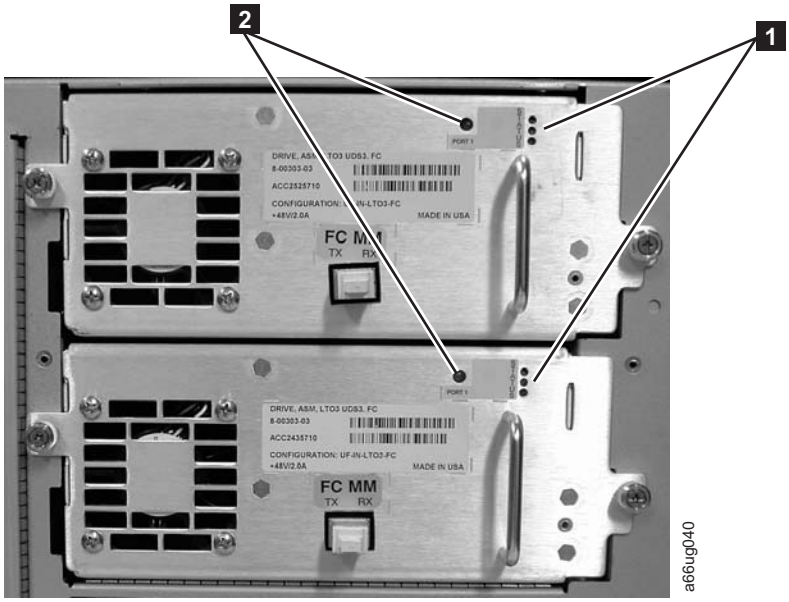


Figure 10-3. Tape drive LEDs

Use the table to interpret tape drive activity by observing tape drive LEDs (**1** in Figure 10-3).

Table 10-3. Tape Drive Activity

LED Color	Represents	Drive Status
Green	Processor activity	• Solid ON - Drive 's main processor is not operating • Solid ON for 3 seconds, then flashes twice - Drive firmware is downloading • 1 flash per second - Normal: Drive operational • Flashes 3 times in 3 seconds, then pauses (solid OFF), and then repeats - Drive is activating (varying online) • 10 flashes per second - Identify mode • Solid OFF - Drive 's main processor is not operating
Amber	Health of the drive	• Solid ON - Drive failed • Solid OFF - Normal: drive operational
Blue	Power control	• Solid ON - Drive is powered down and ready to be replaced or varied online • 1 flash per 10 seconds - Normal: Drive operational • Solid OFF - Drive is not receiving power

Fibre port link LED

The fibre port link LED (**2** in Figure 10-3) shows the current state of the Fibre Channel link and indicates whether the link is ready to transmit commands.

Use the table to interpret Fibre Channel link activity.

Table 10-4. Fibre port link LED on tape drive

LED Color	Represents	Fibre Port Link Status
Green	LIP and activity	• Solid ON - Loop Initialization Protocol (LIP) occurred. • Flashes at regular intervals - Host command/data activity is occurring.
Amber	Online and light detected	• Solid ON - The library enabled the drive data bus, and it can detect light through a fiber optic cable.
No color	No activity or no light detected	• Solid OFF - Either the drive is off or the drive cannot detect light through a fiber optic cable (which is equivalent to a missing fibre cable). If the drive is varied OFF, the blue status LED is solidly lit.

Power supply LEDs

Operator interventions typically report all problems that are related to power supplies. You can also observe the flashing pattern of LEDs on power supplies to see if they are functioning correctly.

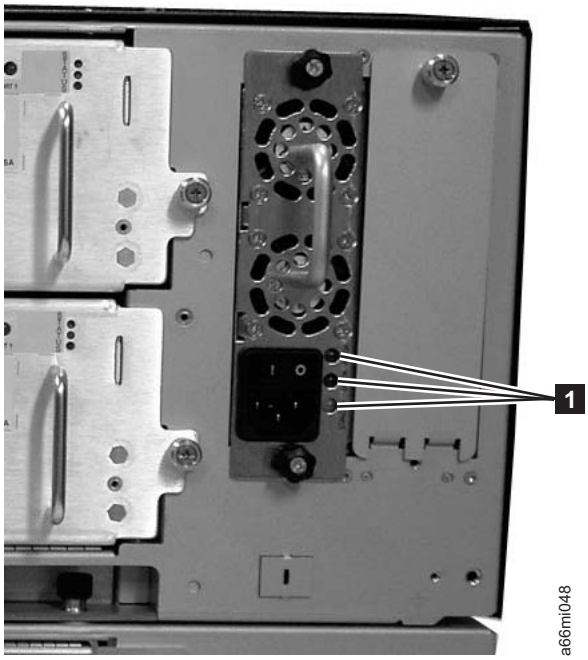


Figure 10-4. Power supply LEDs

Power supply LEDs indicate status by the rate at which they flash. The color of the LED identifies the area of the component that is reported.

Table 10-5. Power Supply LEDs

LED Color	Represents	Power Supply Status
Green	AC OK (top)	• Solid ON - The power supply 's AC input is above the minimum requirements to operate. • Solid OFF - The power supply 's AC input is below the minimum requirements to operate.
Green	DC OK (middle)	• Solid ON - The power supply 's output voltage is within regulation. • Solid OFF - The power supply 's output voltage is not within regulation.
Blue	Fault (bottom)	• Solid ON - Indicates that one of the following faults is detected: – Power supply is outside of specifications – Current limit is exceeded – Temperature limit is exceeded – Fan failed while AC input is present and above the minimum operating voltage – AC input is below the minimum operating voltage – The power supply is ON, the **Power** button ON, but the library 's indicator panel is OFF • Solid OFF - Normal: No faults that are detected

In the operator intervention that is associated with the defective power supply, record both the number of the module and the number of the power supply that is connected to that module.

Each module can have up to two power supplies. When viewed from the rear, the power supply on the left is considered to be #1, while the power supply on the right is #2.

Modules are numbered according to their position in relation to the control module (CM).

Picker LED

Both the Original and the M2 picker assembly have one green LED, seen in the images (**1** in Figure 10-5 on page 10-14) that must be ON for the picker to function properly. If the LED is not lit, the picker assembly must be investigated for problems. The module-to-module communication cable is not in place, module communication terminator is not in place, or an access door is open.

To observe the status of the picker LED:

1. Look through the viewing window on the front of an expansion module and determine whether the picker LED is ON.
2. If you cannot see the picker LED, power OFF the library. The picker moves to the bottom of the library.
3. Power ON the library.
4. Open the lowest I/O station door in your library. Looking through the opening to the left of the flap inside the I/O station, observe the picker LED.

Note: Do not open the access door to observe the picker LED. If the access door is opened, the picker LED is turned OFF.

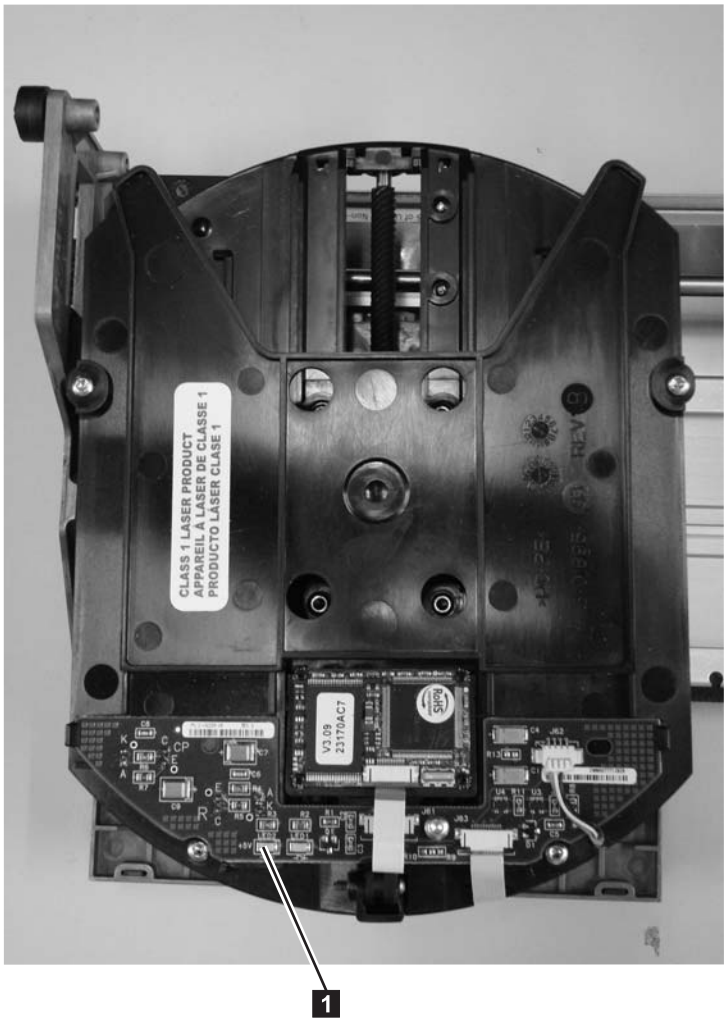


Figure 10-5. Location of Original picker assembly LED

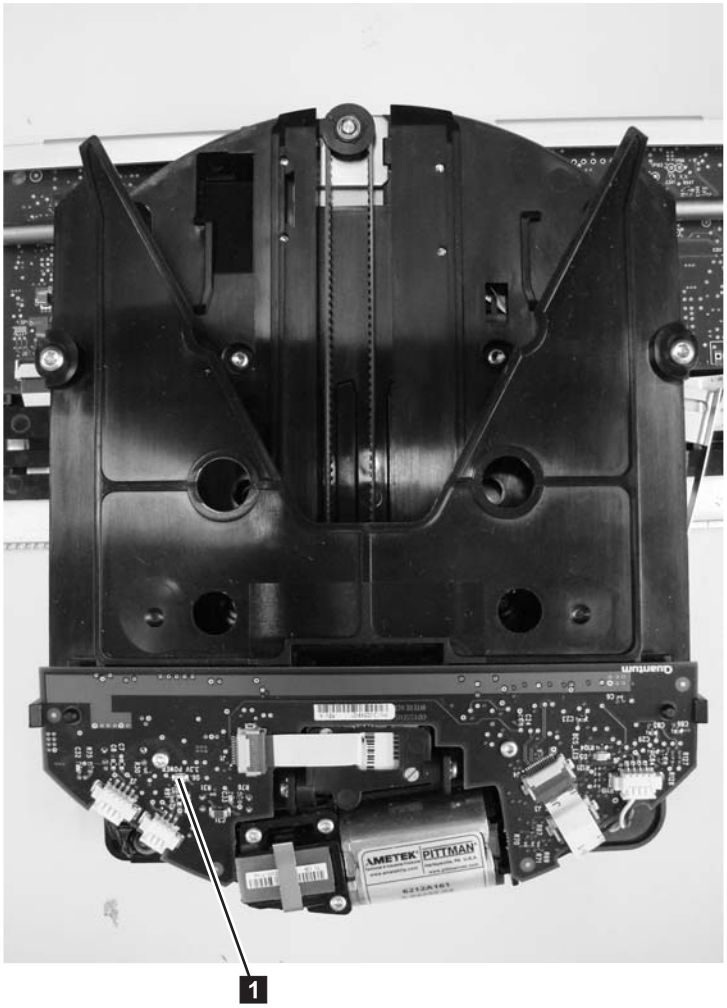


Figure 10-6. Location of M2 picker assembly LED

Checking/reseating cables

External cables

To check or reseat external library cables and terminators, complete the following steps:

1. Locate the cables and terminators by referring to the example figures.

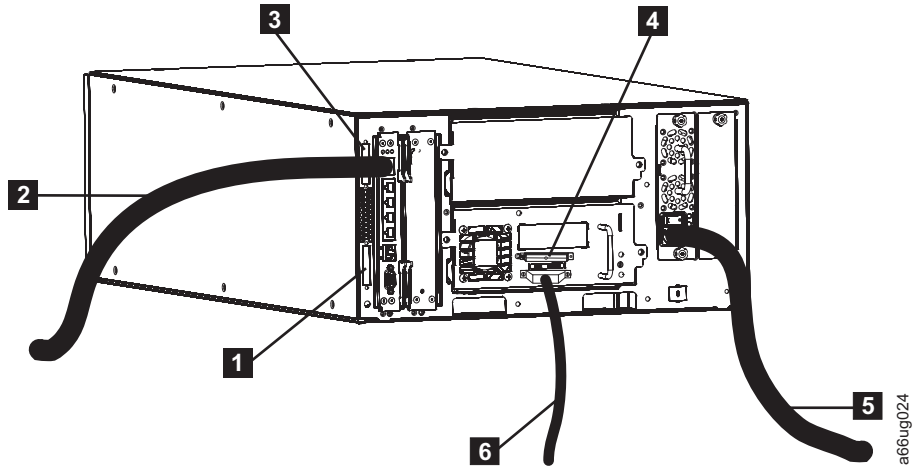


Figure 10-7. Cabling of a 5U library with SCSI drives

1	Module communication terminator	3	Module communication terminator	5	Power cord
2	Ethernet cable (customer supplied)	4	SCSI terminator	6	SCSI drive cable

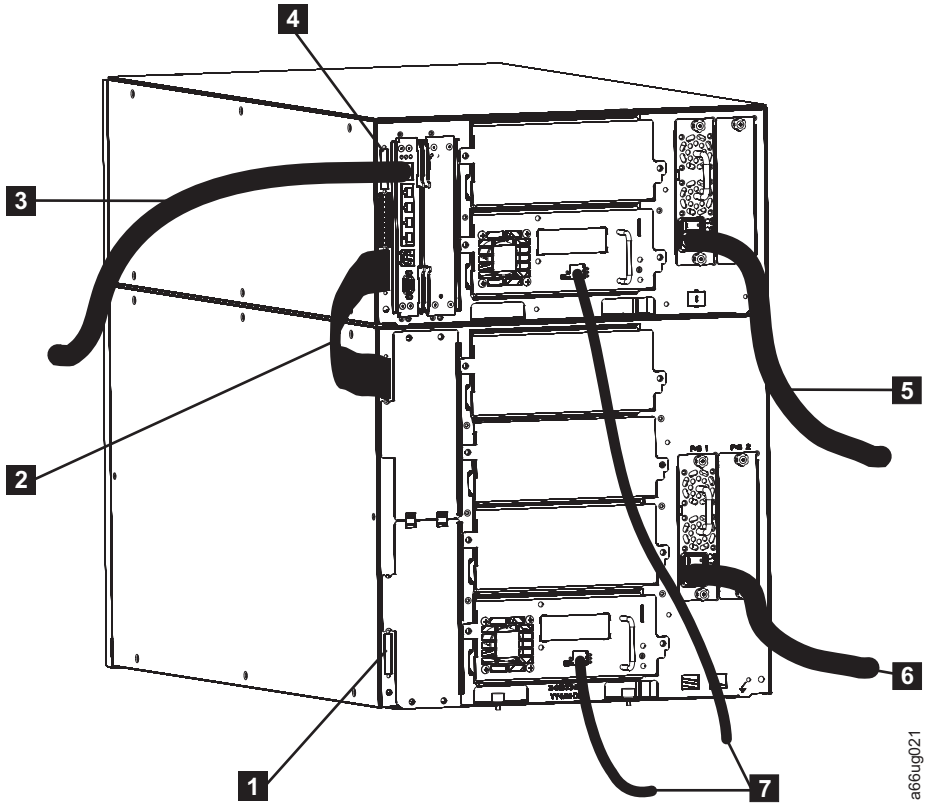


Figure 10-8. Cabling of a 14U library with Fibre Channel drives

1	Module communication terminator	4	Module communication terminator	7	Fibre drive-to-network cables
2	Module-to-module communication cable	5	Power cord (upper module)		
3	Ethernet cable (customer supplied)	6	Power cord (lower module)		

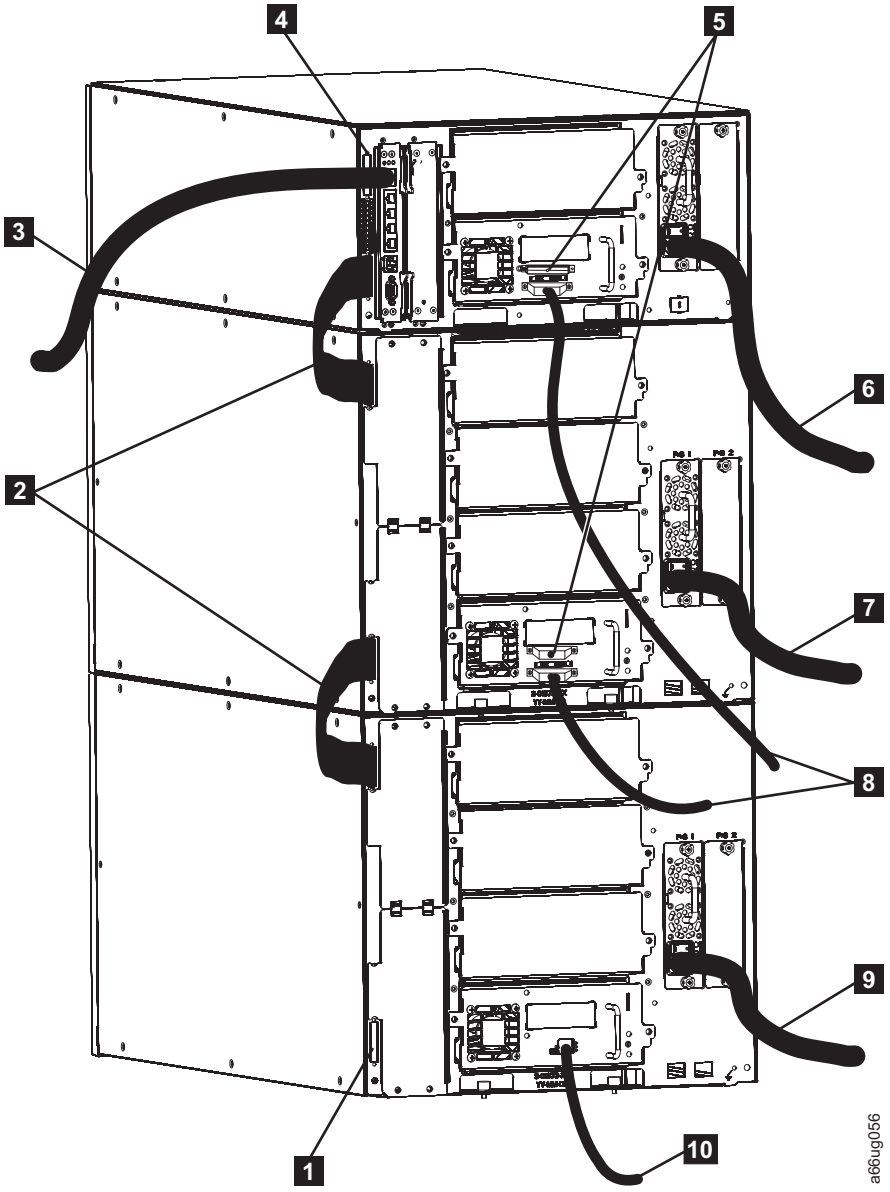


Figure 10-9. Cabling of a multi-module library with SCSI and Fibre Channel drives

1	Module communication terminator	5	SCSI terminators	8	SCSI drive cables
2	Module-to-module communication cable	6	Power cord (Control Module)	9	Power cord (Expansion Module)

3	Ethernet cable (customer supplied)	7	Power cord (Expansion Module)	10	Fibre drive-to-network cable
4	Module communication terminator				

2. Check and reseat, if necessary, all of the cables and terminators that are connected to your library.
3. Verify that there is no damage to any connector pins.

Troubleshooting "Library Not Ready" messages

The Operator Panel user interface includes a header that contains the company logo, product name, and the three main navigation buttons: **Home**, **Help**, and **Logout**. In addition, a message in the header alerts you when the library is not ready. (No message displays in the header when the library is in a ready state.)

On the operator panel, **LIBRARY NOT READY** flashes at regular intervals whenever the library robotics is not yet ready to run library functions. To view information about the library's condition, select **Tools** > **About Library**. The **State** field on the **About Library** screen displays **Not Ready**, followed, when applicable, by a brief explanation. For example, if the library door is open, the **State** field displays: **Not Ready, Door opened**.

"Library Not Ready" messages display in the header in the operator panel under the following circumstances:

- The robot is calibrating. When the robot finishes calibrating, the "Library Not Ready" message no longer displays.
- The robot cannot calibrate. For example, a fiducial label is missing, preventing the robot from calibrating.
- The robot requires manual intervention. For example, the picker contains a tape cartridge that it cannot unload.
- The library door is open. The robot does not operate if the door is open.

If none of the above situations apply, but the library is still not ready to operate, the header displays a "Library Not Ready" message without extra detail. The library generates an operator intervention message whenever the library enters a "not ready" state. The operator intervention message can provide information that helps you troubleshoot the problem. See Chapter 11, "Service Action Tickets (Txxx) and Diagnostic Resolutions (DRxxx)," on page 11-1 for information.

Emailing logs

Logs provide a summary of the status of the library, and include configuration settings and information that is provided in Operator Interventions.

To email current logs:

1. To capture a library log from the Web User Interface, select **Service Library** > **Capture Library Log**
2. When requested by IBM, attach the log to an email message and send it to IBM technical support for further diagnosis.

Manually recover cartridge from picker

The procedure to manually recover a cartridge from a picker is similar for both the robot assembly and the M2 robot assembly.

1. Manually rotate the picker to gain access to the appropriate component to eject the cartridge.
   - In the robot assembly, access the three drive gears, as shown in Figure 10-10.

Figure 10-10. Picker that is rotated for drive gears access

   - In the M2 robot assembly, access the thumbwheel on the front of the picker as shown in Figure 10-11 on page 10-20.

Figure 10-11. Access the M2 picker thumbwheel

2. Rotate the gear (**1** in Figure 10-10 on page 10-19 or the arrow in Figure 10-11) with your thumb or finger, in the direction that is shown by the arrow.
3. Continue rotating the gear or thumbwheel until the cartridge is ejected from the picker.

Pre-call checklist

If you have questions or problems with the library, complete these steps before a call to IBM technical support is placed.

Note: Where instructions refer you to the web, visit http://www.ibm.com/storage/support/lto.

1. Verify that you exhausted all troubleshooting options (refer to "Diagnosing a problem" on page 10-3.
2. Verify that the drive's firmware is at the most recent level (see "Viewing drive information" on page 8-28). To determine the latest release of firmware, visit the web.
3. Verify that your device drivers are at the most recent level (see your server (host) manual for instructions).
   - For the latest release of IBM device drivers, visit the web.
   - For the latest release of device drivers by independent software vendors (ISVs), visit the appropriate third-party website.
4. Verify whether your hardware and software configuration is supported. To determine the latest supported attachments, visit the web.
5. Perform a general checkup of the hardware and connections:
   - Ensure that the host interface cable connector does not contain bent or recessed pins.

- Ensure that all retention screws for the host interface cable and terminator are securely tightened.
- For SCSI attached systems, ensure that you are using the correct SCSI terminator and that you are not mistakenly using a SCSI wrap plug.

If you still have a problem after these steps are completed, see "Contacting IBM technical support."

Contacting IBM technical support

- Complete the steps in "Pre-call checklist" on page 10-20 before a call is placed to IBM technical support.
- Before IBM technical support is called, the customer is responsible for following IBM's published LTO diagnostic procedures, including any needed update to the latest level of firmware. For details, visit http://www.ibm.com/storage/support/lto.
- The IBM Support Center assists with problem determination and can initiate shipment of a replacement part, if needed, to the customer's location. Transportation costs, both ways, are paid by IBM. The replacement part becomes the property of the customer in exchange for the failed part, which becomes the property of IBM. The customer is responsible for packing the failed part into the shipping carton that contained the replacement part. Failure to return the failed part to IBM within 30 days results in a bill sent to the customer for the new list price. The customer is responsible for installing and setting up the CRU replacement part. All FRU replacement parts are installed by an authorized IBM service representative.
- Failure to use the carton in which the replacement part was received, or failure to properly pack the returned part, can result in charges that are incurred for damage to the failed part during shipment.
- Before you call technical support, follow these steps that help you take full advantage of your call:
  1. Be prepared to provide library and drive firmware levels currently installed.
     - Remotely (From the Web User Interface):
       - **Service Library** > **View/Update Library Firmware Level**
       - **Service Library** > **View/Update Drive Firmware Levels**
     - Physically on the Operator Panel:
       - **Tools** > **About Library**.
  2. Review all documentation carefully. (Experience demonstrates that most questions are answered in your documentation.)
  3. Be prepared to explain whether the software or hardware worked properly any time in the past. Have you changed anything recently?
  4. Pinpoint the exact location of your problem, if possible. Note the steps that led to the problem. Can you duplicate the problem or is it a one-time occurrence?
  5. Note any error messages displayed. Write down the exact error message.
  6. If at all possible, call while at your computer, with the library installed and turned ON.
  7. If the drive is running on a network, have all relevant information available (that is, type, version number, network hardware).
  8. Be prepared to provide:
     - Machine type and Model name

- Remotely: Go to **Viewing Library Information**, then click **Enclosure 0** to get this information from the Web UI.
- Physically: Go to the front of the control module on the label underneath the **Power** button.

See "Viewing library information" on page 8-22.

– Serial number of the library
- Remotely: Go to **Viewing Library Information**, then click **Enclosure 0** to get this information from the Web UI.
- Physically: Go to the front of the control module on the label underneath the **Power** button.
- Physically on the Operator Panel: Go to **Tools** > **About Library**.

See "Viewing library information" on page 8-22.

– Software version numbers
– Device driver information
– Host application name and version
– Hardware configuration, including firmware versions, date, and number
– Type of host, operating system version, clock speed, RAM, network type, network version, and any special devices installed
– A brief description of the problem, including Service Action Ticket number (Txxx).

Having this information available when you call for customer assistance enables support personnel to resolve your problem in the most efficient manner possible.

• To contact IBM technical support:
– In the US: 1-800-IBM_SERV (1-800-426-7378)
– All other Countries/Regions: http://www.ibm.com/planetwide/
– To open a Service Request online: Under **Get Support**, click **Open a Service Request**.

Chapter 11. Service Action Tickets (Txxx) and Diagnostic Resolutions (DRxxx)

Before a CRU replacement part is ordered, observe the LEDs on all library components to determine exactly which part is failing. See "Interpreting LEDs" on page 10-8 for information. If the LEDs on all components are functioning properly, see "Contacting IBM technical support" on page 10-21.

Service Action Tickets

When the library detects a problem, it generates an error code and displays it in the Operator Intervention report. A full description of the problem and suggestions for resolving it are also displayed.

The following sections offer more information than is displayed in an Operator Intervention on the Operator Panel. Refer to this information for help in resolving problems.

Check your host for Sense Data and refer to "Drive sense data" on page C-4.

Important: It is recommended that Service Action Tickets are not allowed to accumulate in the Operator Intervention reports. After an incident is resolved or repaired, the Service Action Ticket must be closed.

T001: Tape cartridge stuck in picker, motion OK

Description	GUI Description: A tape is stranded in the Picker assembly and must be removed to continue operations. Explanation: The robot is not logically expecting to see a tape in the picker, but the tape presence sensor indicates otherwise. The tape cannot legitimately be returned to a home slot nor can it be placed in a destination slot. The VOLSER can be unknown, the library can be full, or changing the host inventory is disruptive
Detection Scenarios	1. The picker becomes enabled after a door is opened or the library system boots up and discovers that the cartridge present sensor detects a cartridge. 2. The system tried to recover from a PUT failure and wants to return the cartridge to a home slot. However, the home slot recovery logic completes without recovery (home slot is a drive or the I/O station is open or the I/O station is full). 3. The cartridge present sensor and sensing circuit is falsely representing the presence of a cartridge.

Root Causes	1. Operator did not recover cartridge. 2. Operator put a cartridge in the picker. 3. Power loss during a move with media and the library logic cannot legitimately return it to the proper cell. 4. Physical contamination such as dust and debris on the sensor gives a "false full state". 5. Various electrical failures.
Possible CRU Replacements	• Tape cartridge • Library Control Blade
Possible FRU Replacements	• Picker assembly • Y-axis Cable Spool • Internal Cables and Boards Kit 3
Resolution	Complete “DR001: Resolving picker cartridge presence” on page 11-61.

T002: PUT operation failed, final cartridge position unknown, motion OK

Description	GUI Description: The robot failed to place a tape cartridge and cartridge recovery is required. Explanation: The library cannot successfully put a tape into a drive, storage slot, or I/O station and the final “resting place” of the tape is unknown. There are no additional recovery logic paths to be exercised. Fundamental servo control seems OK. If the operation was initiated by a host move media, the move media command failed with a SK/ASC/ASCQ `4h/15h/01h` (hardware mechanical positioning error).
Detection Scenarios	PUT is not successful. PUT recovery is not successful, and a cartridge is not known to be properly seated in the Picker or a storage slot.
Root Causes	1. Magazine is damaged. 2. Magazine is the wrong type for the cartridge. 3. A storage cell is blocked by foreign material or not clipped in and seated correctly. 4. Calibration problem that resulted in improper Picker position. 5. Picker offset problem. 6. Cartridge is damaged. 7. Unlabeled cartridge or intermittently readable cartridge label in destination slot. 8. Drive load mechanism is not working. 9. Various Picker problems such as slipping gears, encoder issues
Possible CRU Replacements	• Tape cartridge • Library Control Blade
Possible FRU Replacements	• Picker assembly • Y-axis Cable Spool • Internal Cables and Boards Kit 3

Resolution	Complete “DR002: Resolving tape cartridge recovery” on page 11-62. Before the ticket is closed: • If a storage cell is blocked by foreign material, remove the foreign material. • If the picker is improperly positioned, power cycle the library. • If the suspect cartridge is damaged, copy the data onto a new cartridge then destroy the suspect cartridge. If the data cannot be copied, replace the suspect cartridge. • If the suspect cartridge does not have a bar code label, apply a label. • If the suspect cartridge has a damaged bar code label, remove the damaged label and apply a new label. • If the problem persists, refer to “Diagnosing a problem” on page 10-3 for more diagnostic procedures.

T003: GET operation failed, final cartridge position unknown, motion OK

Description	GUI Description: The robot failed to pick a tape cartridge and cartridge recovery is required. Explanation: The library cannot successfully get a tape from a drive, storage, or I/O location. The final “resting place” of the tape is unknown. There are no additional recovery logic paths. Fundamental servo control appears to be OK. If the operation was initiated by a host move media, the move media command failed with an ASC/ASCQ of `4h/15h/01h` (hardware mechanical positioning error).
Detection Scenarios	GET is not successful, GET recovery is not successful, and the cartridge is not known to be properly seated in the picker or a storage slot.
Root Causes	1. Magazine is damaged. 2. Magazine is the wrong type for the cartridge. 3. A storage cell is blocked by foreign material or not clipped in and seated correctly. 4. Calibration problem that resulted in improper picker position. 5. Picker offset problem. 6. Cartridge is damaged. 7. Unlabeled cartridge or intermittently readable cartridge label in destination slot. 8. Drive load mechanism is not working. 9. Various picker problems such as slipping gears, encoder issues
Possible CRU Replacements	• Tape cartridge • Library Control Blade
Possible FRU Replacements	• Picker assembly • Y-axis Cable Spool • Internal Cables and Boards Kit 3

Resolution	Perform “DR002: Resolving tape cartridge recovery” on page 11-62. Before the ticket is closed: • If a storage cell is blocked by foreign material, remove the foreign material. • If the picker is improperly positioned, power cycle the library. • If the suspect cartridge is damaged, copy the data onto a new cartridge then destroy the suspect cartridge. Otherwise, replace the cartridge. • If the suspect cartridge does not have a bar code label, apply a label. • If the suspect cartridge has a damaged bar code label, remove the damaged label and apply a new label. • If the problem persists, refer to “Diagnosing a problem” on page 10-3 for more diagnostic procedures.

T004: PUT operation failed, tape back In source location, motion OK

Description	GUI Description: The robot failed to place a tape cartridge to a destination slot but recovered the cartridge to an alternative location. Explanation: The library cannot successfully put a cartridge into the intended target drive, storage, or I/O location. The library successfully returned the cartridge to the source location. Fundamental servo control appears to be OK.
Detection Scenarios	PUT is not successful and PUT recovery is not successful at the destination element. Recovery logic allowed the cartridge to be returned to the initial source location. If the operation was initiated by a host MOVE MEDIA, the MOVE MEDIA command failed with a Sense Key/ASC/ASCQ of `4h/15h/01h`.
Root Causes	1. Magazine is damaged, wrong type, cell is blocked by foreign material, or not clipped in and seated correctly. 2. Calibration problem. 3. Picker offset problem. 4. Destination cell full with labeled cartridge (invalid inventory). 5. Destination cell is full with cartridge with damaged label or is unlabeled or has an intermittently readable label. 6. Various picker problems such as slipping gears, encoder issues, Y-axis assembly not level
Possible CRU Replacements	• Tape cartridge • Library Control Blade
Possible FRU Replacements	• Picker assembly • Y-axis Cable Spool • Internal Cables and Boards Kit 3

Resolution	Complete “DR004: Resolving full destination element” on page 11-63. Before the ticket is closed, complete the following steps: 1. If a magazine cell is blocked by foreign material, remove the foreign material. 2. If a magazine is not clipped in and seated correctly, reseat the magazine. 3. If your library is reporting an invalid inventory, verify that you purchased and entered your Capacity Expansion key. To determine the number of available slots in your library: • From the Operator Panel, view the **Capacity View** home screen. • From the Web User Interface, select **Monitor System** > **System Summary**. If the number of available slots is incorrect, reenter your Capacity Expansion license key by selecting **Setup** > **License** from the Operator Panel. 4. If the destination cell contains a cartridge that has a damaged label or is unlabeled, remove the damaged label. If necessary, apply a new label to the cartridge. 5. Power cycle the library. 6. If the problem persists, refer to “Diagnosing a problem” on page 10-3 for more diagnostic procedures.

.

T005: X, Y, Theta motion profile failure, tape in picker, motion NOT OK

Description	GUI Description: The robot failed to move a tape cartridge because of an axis motion problem. Explanation: Any X, Y, Theta (θ) motion failure occurred that cannot be considered a complete obstruction. This problem occurs only during a move and NOT a get or put. Because the tape is in the picker, tape recovery must be a part of the resolution strategy. This ticket cause specifically excludes any Z-axis motion failures that are typically associated with get or put actions. Specifically included are motion failures that occur while pivoting, moving on the X-axis or moving on the Y-axis.
Detection Scenarios	1. A specified move in the X-axis cannot complete. 2. A specified move in the Y-axis cannot complete. 3. A specified movement in the Theta (θ)-axis cannot complete.
Root Causes	1. Many electrical hardware failures. Code or hardware detects that motion control is not occurring properly (encoder issues, motor driving circuit issues, motor-winding issues, cable connection issues, and so on). 2. A relatively small number of mechanical hardware errors that do not result in the detection of a complete obstruction but where motion control does not appear to be normal (contamination or damage to encoder wheel, high friction, and so on).
Possible CRU Replacements	• Tape cartridge • Library Control Blade

Possible FRU Replacements	• Robot assembly • Cable Spool • Y motor (only required for M1 robot) • Y-axis assembly • Internal Cables and Boards Kit 3
Resolution	• Complete “DR001: Resolving picker cartridge presence” on page 11-61 • Complete “DR005: Resolving motion failure” on page 11-64. If the problem persists, refer to “Diagnosing a problem” on page 10-3 for more diagnostic procedures.

T006: X, Y, Theta motion profile failure, no tape In picker, motion NOT OK

Description	GUI Description: The robot failed to move because an axis motion problem. Explanation: An unrecoverable motion failure occurs at an operational point where a cartridge is not in the picker. Because the cartridge is not in the picker, cartridge recovery is not necessary as part of the resolution to this issue. This cause specifically excludes any Z-axis motion failures. Included are motion failures that occur while pivoting, moving on the X-axis or moving on the Y-axis. If the ticket details indicate that the Y-axis has problems, then both the picker and the Y-carriage assembly must be replaced. Otherwise, only the picker must be replaced..
Detection Scenarios	1. A specified move in the X-axis cannot complete. 2. A specified move in the Y-axis cannot complete. 3. A specified movement in the Theta (θ)-axis cannot complete.
Root Causes	1. Many electrical hardware failures. Code or hardware detects that motion control is not occurring properly (encoder issues, motor-driving circuit issues, motor winding issues, cable connection issues, and so on). 2. A relatively small number of hardware errors that do not result in complete obstruction but where servo control does not appear to be normal.
Possible CRU Replacements	• Tape cartridge • Library Control Blade
Possible FRU Replacements	• Robot assembly • Cable Spool • Y motor (only required for M1 robot) • Y-axis assembly • Internal Cables and Boards Kit 3
Resolution	Complete “DR005: Resolving motion failure” on page 11-64. If the problem persists, refer to “Diagnosing a problem” on page 10-3 for more diagnostic procedures.

T007: X, Y, Theta motion obstruction, motion OK

Description	GUI Description: The robot is unable to properly move because of an obstruction in its motion path. Explanation: A complete physical obstruction exists in a motion path that precludes repeated attempts to move beyond a certain point in the range of motion. Servo control appears normal but a move profile cannot be completed. Cartridge might be returned to a home slot.
Detection Scenarios	1. A specified move in the X-axis cannot complete but motion control appears normal. 2. A specified move in the Y-axis cannot complete but motion control appears normal. 3. A specified move in the Theta (θ)-axis cannot complete but motion control appears normal.
Root Causes	1. Operator Intervention that results in foreign material or an obstructing object in a library motion path. 2. Picker locking mechanism left engaged in the library motion path (see Figure 3-7 on page 3-7). 3. Certain damaged hardware conditions that obstruct motion at a particular point along an axis.
Possible CRU Replacements	Tape cartridge
Possible FRU Replacements	• Robot assembly • Y-carriage assembly
Resolution	• Verify that no obstructions are present in the path of the picker. • Perform "DR028: Resolving motion obstruction" on page 11-73. • If the problem persists, refer to "Diagnosing a problem" on page 10-3 for more diagnostic procedures.

T008: Cannot home, motion OK

Description	GUI Description: The robot can move but cannot establish its home position correctly. Explanation: Robot motion and servo control appear normal but home sensors do not make the transition when the robot is moved through prescribed search distances and times.
Detection Scenarios	1. X home sensor does not make the transition while homing. 2. Y home sensor does not make the transition while homing. 3. θ home sensor does not make the transition while homing. 4. Z home sensor does not make the transition while homing.
Root Causes	1. Malfunctioning home sensors. 2. Missing or damaged mechanical flags that trigger home sensors. 3. Hardware failures that result in apparent normal motion according to encoders, but no actual motion (ex. slipping gears). 4. Robot parking tab is interfering with Y-axis travel of the robot. 5. Robot assembly is not placed properly into Y-climber rails, resulting in an unleveled robot when it is moving along the Y-rails. 6. Y-rails are not secured correctly, causing the robot Y-carriage to become unleveled when it is moving between modules.

Possible CRU Replacements	• Library Control Blade
Possible FRU Replacements	• Picker assembly • Y motor (only required for M1 robot) • Y-axis assembly • Internal Cables and Boards Kit 3
Resolution	• Verify that no obstructions are present in the path of the picker. • Complete "DR028: Resolving motion obstruction" on page 11-73. • If the problem persists, refer to "Diagnosing a problem" on page 10-3 for more diagnostic procedures.

T009: Drive load unsuccessful, motion OK

Description	GUI Description: An attempted drive load failed, but robotic motion appears normal. Explanation: The robot successfully completed all motion profiles that are associated with putting to a drive but the drive reports that the tape cartridge did not load.
Detection Scenarios	While the status of a drive is checked after a PUT motion profile to the drive is completed, the drive does not report back a loaded state.
Root Causes	1. Defective drive. 2. Defective tape cartridge. 3. Motion profile was successful as detected at motor encoders but cartridge did not get placed far enough. 4. Picker dragged cartridge back out of drive but not far enough to trigger picker cartridge present sensor.
Possible CRU Replacements	• Tape cartridge • Drive sled
Possible FRU Replacements	• Picker assembly
Resolution	Complete "DR030: Resolving drive load failure" on page 11-74. Before the ticket is closed, complete the following steps: • Inspect the suspect cartridge for damage. Copy data onto a new cartridge if the suspect cartridge is damaged, then destroy the suspect cartridge. If data cannot be copied onto a new cartridge, replace the suspect cartridge. • Before a drive is replaced, refer to "Diagnosing a problem" on page 10-3 for more diagnostic procedures.

T010: Drive unload failed

Description	GUI Description: A drive did not eject a tape. Explanation: The library is expecting the drive to achieve an unloaded state but the drive does not.

Detection Scenarios	1. After a move media is issued from a host that requires a get from a tape drive, the tape drive never achieves the unloaded state. 2. When GUI commands are issued that require a drive unload (manual drive unload, move media, and so on) and the drive never achieves the unloaded state. **Note:** This ticket cause interacts with "explicit unload" behavior. Since the library always issues an unload command, it is not possible to determine whether a host unload command failed first, followed by a subsequent failure of a library-issued unload command.
Root Causes	1. Drive is still busy with host application command execution. 2. Tape drive fails to unload after the library issues an unload command. 3. Defective tape cartridge.
Possible CRU Replacements	• Tape cartridge • Drive sled
Resolution	Complete "DR003: Resolving drive eject failure" on page 11-63.

T011: Drive over-eject condition

Description	GUI Description: A drive over-ejected a tape cartridge into the robot 's motion path. Explanation: The library is about to complete a get from a tape drive and checks the tape drive status to determine whether the tape cartridge is ejected. LTO tape drives demonstrated a specific failure mode where they eject a tape in an abnormal manner. Normally upon eject, the tape is in a particular position where it is clear of the robot motion path. It cannot be reloaded because of mechanical interlock within the tape drive load mechanism. The historical failure mode is that the tape slips an extra amount out of the tape drive throat that rearms the load mechanism of the tape drive. Two subsequent problems can occur. The over ejected tape can become an obstruction hazard for robot moves. In addition, the robot get operations can then retrigger the tape drive load mechanism by bumping the tape during a get. There can be a "tug of war" between robot and tape drive or the tape drive can win the tug of war, resulting in the loading of a phantom tape. When the tape drive loads a phantom tape, there are resulting tape drive errors. The goal of reporting this problem is to identify tape drives that over eject tapes to avoid these problems.
Detection Scenarios	Library checks drive status before it completes a GET. It is trying to determine whether the drive is in an unloaded state and if a cartridge is present. If a cartridge is not reported as present, the library can assume that it was "over ejected".
Root Causes	The drive eject process did not result in the correct positioning of the ejected cartridge.
Possible CRU Replacements	Drive sled

Resolution	Before the following steps are completed: 1. "Removing a tape drive" on page 12-24. 2. "Removing and replacing a tape drive" on page 12-25. refer to "Diagnosing a problem" on page 10-3 for more diagnostic procedures.

T012: Drive unload control prevented

Description	GUI Description: A host issued a SCSI Prevent/Allow Media Removal command that is preventing the drive from unloading a tape cartridge. Explanation: The library must issue a command to the drive (such as unload) but cannot complete the operation. The host issued a Prevent/Allow Medium Removal SCSI command, preventing media removal.
Detection Scenarios	1. Library tries to issue an unload command. 2. Library tries to issue a command that is associated with drive unload.
Root Causes	A host is either properly or improperly reserving the drive while a user or host is trying to properly or improperly complete some action on the drive.
Possible FRU Replacements	No library FRU is involved. Rather this is an indication that a host orphaned a reserve on the drive.
Resolution	Complete "DR016: Resolving prevent/allow media removal" on page 11-69.

T013: Invalid library SN label, library cannot initialize

Description	GUI Description: A library module serial number label cannot be read, preventing the library from correct initialization and operation. Explanation: The library logic learns the serial number of the system by reading an internal serial number label. This procedure is done at first bootup from a "cleared to ship" condition i to establish the serial number. It is also done on subsequent bootups to confirm that the LCB Compact flash memory card is in the correct library. The library reports a problem when it cannot read a serial number or detects an invalid serial number or another bar code on the module label when in this "cleared to ship" condition. When T013 is posted, the library cannot operate normally. Different tickets are posted if there are motion-related problems, scanner communication problems, or other problems.
Detection Scenarios	1. At first power ON during installation, the library must establish the serial number for the first time. There can be no serial number in system memory. 2. At any power up, system memory already has a serial number that is established for the Library Control Blade. 3. A Library Control Blade is improperly swapped into a different physical library and the system reads the physical library label.
Root Causes	1. Library Control Blades that are swapped between libraries. 2. Label is damaged, misaligned, or placed on the cartridge incorrectly. 3. Bar code scanner not working properly. 4. Entire communication path to bar code scanner is not working properly.
Possible CRU Replacements	Library Control Blade

Possible FRU Replacements	• Picker assembly • Y motor (only required for M1 robot) • Y-axis assembly • Y-axis Cable Spool • Internal Cables and Boards Kit 3 **Note:** The system serial number label is part of the enclosure FRU.
Resolution	. Before a library component is replaced, refer to “Diagnosing a problem” on page 10-3 for more diagnostic procedures.

T014: I/O station magazine missing

Description	GUI Description: A library I/O station is closed with a magazine that is missing. Explanation: There is a fixed bar code label location on the I/O station structure behind the removable magazines. It decodes as %XXX. The purpose of the label is to allow the library to detect that an I/O station magazine is not installed. This label is important on I/O station magazines because they are user removable. While an inventory of the I/O station magazines is completed, the library ends up verifying the presence of the magazine by NOT detecting this special fixed label.
Detection Scenarios	Any time the library attempts to inventory an I/O station magazine, it reads the fixed label if a magazine is missing. I/O station magazines are always expected to be present.
Root Causes	1. Missing I/O station magazine 2. A cartridge in an I/O station happens to have a label that decodes as “%XXX”. **Note:** The inability to communicate between the Library Control Blade and the bar code scanner results in a different ticket cause.
Resolution	Complete “DR023: Resolving missing I/O station magazine” on page 11-71.

T015: Drive sled fiducial read failure

Description	GUI Description: The robot is unable to scan the drive sled 's identification/fiducial label. Explanation: When the library is attempting to determine the type of a drive and verify its physical presence in the library, it cannot do so because it cannot read a label where it expects to find one.
Detection Scenarios	1. Installation of a drive into a library drive slot triggers the library to discover it. 2. Bootup causes the library to physically discover any drive that is electrically connected in the system.
Root Causes	1. Damaged label or marginal label that cannot be read 2. Drive with invalid label is present (earlier generation of plug compatible drive sled) **Note:** The inability to communicate between the Library Control Blade and the bar code scanner results in a different ticket cause.

Possible CRU Replacements	Drive sled
Resolution	Complete “DR007: Resolving bar code scanner issue” on page 11-65.

T016: Unexpected drive type

Description	GUI Description: A configured drive sled is replaced with a drive sled of different type. . Explanation: When the library is attempting to determine the type of a drive and verify its physical presence in the library, it detects a drive type that is not compatible with the logical library assignment of the drive slot (for example, an LTO-1 drive in an LTO-3 drive position).
Detection Scenarios	1. Installation of a tape drive into a library drive slot triggers the library to discover it. 2. Bootup causes the library to physically discover any tape drive that is electrically connected in the system.
Root Causes	1. User or CE mistakenly uses the actual wrong type of CRU (for example, LTO-1 drive sled in a slot that is defined as LTO-3). 2. Manufacturing defect has wrong label type for actual physical drive type (for example, LTO-1 label on an LTO-3 drive). **Note:** Inability to communicate between the LCB and the scanner results in a different ticket cause.
Possible CRU Replacements	Drive sled
Resolution	Before the following steps are completed: 1. “Removing a tape drive” on page 12-24 2. “Removing and replacing a tape drive” on page 12-25 refer to “Diagnosing a problem” on page 10-3 for more diagnostic procedures.

T017: Invalid storage or I/O position

Description	Calibration completes and the coordinates of each storage and I/O element are calculated. The calculated values are determined to be outside travel limits that are established for the robot.
Detection Scenarios	Calculated element positions fail validity check against travel limits.
Root Causes	1. Calibration targets not in position. 2. Calibration sensor detects edges but is not correctly finding calibration target edges.
Possible FRU Replacements	• Fiducial targets • Storage column • Y motor (only required for M1 robot) • Y-axis assembly • Y-axis Cable Spool • Picker assembly • Internal Cables and Boards Kit 3
Resolution	Before IBM technical support is contacted, refer to “Diagnosing a problem” on page 10-3 for more diagnostic procedures.

T018: Invalid drive position

Description	Calibration completes and the coordinates of each drive are calculated. The calculated values are determined to be outside travel limits that are established for the robot.
Detection Scenarios	Calculated element positions fail validity check against travel limits.
Root Causes	1. Drive calibration target is not in position. 2. Calibration sensor detects edges but is not correctly finding calibration target edges.
Possible CRU Replacements	Drive sled
Possible FRU Replacements	• Y motor (only required for M1 robot) • Y-axis assembly • Picker assembly • Y-axis Cable Spool • Internal Cables and Boards Kit 3
Resolution	Before a library component is replaced or IBM technical support is contacted, refer to “Diagnosing a problem” on page 10-3 for more diagnostic procedures.

T019: Drive calibration failure, motion OK

Description	GUI Description: The library is unable to calibrate the position of a drive. Explanation: The system electrically detects a drive and is able to scan the bar code label but cannot successfully calibrate the position of the drive. The calibration search pattern completes successfully.
Detection Scenarios	Calibration motion completes but edge-finding of one or more edges does not occur.
Root Causes	1. Damaged drive sled calibration fiducial. 2. Dust on picker assembly calibration sensor. 3. Calibration sensor not functioning properly. 4. Drive or picker position is so far off nominal that search pattern cannot locate target.
Possible CRU Replacements	Drive sled
Possible FRU Replacements	• Y motor • Y-axis assembly • Y-axis Cable Spool • Picker assembly • Internal Cables and Boards Kit
Resolution	1. Complete “DR082: Resolving library calibration failure” on page 11-87. 2. Use the 'Details' option in the RAS ticket to identify which tape drive is having trouble with calibration. Reseat the drive sled in another sled bay. 3. Reseat the picker and Y-climber to ensure that they are level. 4. Clear the RAS ticket and try the original operation again.

T020: Storage calibration failure, motion OK

Description	GUI Description: The library is unable to calibrate the position of a tape cartridge magazine. Explanation: The system cannot successfully calibrate the position of a storage magazine but the calibration search pattern completes successfully.
Detection Scenarios	Calibration motion completes but edge-finding of one or more edges does not occur.
Root Causes	1. Dust on picker assembly calibration sensor. 2. Calibration sensor not functioning properly. 3. Calibration target not functioning properly. 4. Fiducial target or robot position is so far off nominal that search pattern cannot locate target (unlevel picker). This action can also generate a T083: Picker assembly not level.
Possible FRU Replacements	• Column assembly • I/O Slide assembly
Resolution	1. Complete “DR082: Resolving library calibration failure” on page 11-87. **Note:** The picture that is shown in DR082 shows the location of the calibration sensor. If you are guiding a customer by phone, you might want to copy the picture and email it to them. 2. Open the doors on the all the modules in the library from the bottom to the control module. Lift the robot and bring it to rest on the parking tab. Check inside the library for any debris on the floor of the library that can interfere with picker movement. 3. Remove the robot from the library and carefully inspect the picker for any damage or obstruction on the face that can prevent a clear line of sight to the bar codes or fiducials. Place the robot back into the library. Ensure that the Y-rails are locked in the down position and that the robot is level. Close this ticket and resume normal operations. If this ticket recurs, go the next step. 4. Clear the RAS ticket and try the original operation again.

T021: Drive sled communication failure

Description	GUI Description: The library lost communication with the drive sled. Explanation: The library is communicating with a tape drive sled and considered it to be assigned to a logical library. Two-way communications no longer occur. This ticket is NOT caused by two scenarios: • Physical removal of a tape drive if the tape drive is not assigned to a logical library • Complete physical removal of a drive if it is turned offline with the library operator panel When the library detects loss of communication with a drive that is online, the library robot attempts to scan the bar code label on the drive. If the label is read and communication is not present, the ticket gets posted based on the fact that the drive is physically present but no communication is occurring. If the label is not read, the drive is assumed to be physically removed. Therefore communication is not expected.
Detection Scenarios	1. Routine polling of the sled can no longer occur. 2. Specific library to drive sled commands are not responded to.

Root Causes	1. Drive is physically remove/unplugged (intentional or not installed correctly). 2. Various hardware failures on the drive sled. 3. Various hardware failures in the library.
Possible CRU Replacements	• Module Terminators and Module-to-Module cables • Drive sled
Possible FRU Replacements	• Internal Cables and Boards Kit • Expansion module chassis
Resolution	Complete "DR029: Resolving drive sled communication loss" on page 11-73. Before the ticket is closed, complete the following steps: 1. If a drive is physically removed from the library, reinstall the drive (refer to "Adding/removing/replacing a tape drive" on page 12-24). 2. If a drive is unplugged, reconnect the drive. 3. Before a library component is replaced or IBM technical support is contacted, refer to "Diagnosing a problem" on page 10-3 for more diagnostic procedures.

T022: Tape drive communication failure

Description	GUI Description: Communication to the tape drive failed inside the drive sled assembly. Explanation: Internal to the drive, the sled control board can no longer communicate with the drive brick..
Detection Scenarios	1. Routine Polling between sled control board and drive brick can no longer occur. 2. Specific commands such as unload, reset, are not responded to.
Root Causes	1. Cable broken, unplugged, or damaged. 2. Drive brick failure.
Possible CRU Replacements	Drive sled
Possible FRU Replacements	1. Internal Cables and Boards Kit 3 2. Expansion module chassis
Resolution	Clear the operator intervention. If the library firmware is below 400G, upgrade the library firmware to 400G or later revision of code. A timing issue was addressed in the 400G library firmware, which was occasionally falsely reporting T022 operator interventions. If the library firmware is at 400G or later, or the problem persists after the library is upgraded to 400G or later revision code, complete the following steps. 1. "Removing a tape drive" on page 12-24 2. "Removing and replacing a tape drive" on page 12-25 Refer to "Diagnosing a problem" on page 10-3 for more diagnostic procedures.

T023: Drive sled fan failure

Description	GUI Description: The fan within the drive sled assembly is spinning too slowly or does not rotate at all.

Detection Scenarios	Regular polling/monitoring of the fan indicates a problem.
Root Causes	1. Hardware failure of fan. 2. Wiring or PCBA failure. 3. Blocked air paths. 4. Physical obstruction.
Possible CRU Replacements	Drive sled
Resolution	Before the following steps are completed: 1. “Removing a tape drive” on page 12-24 2. “Removing and replacing a tape drive” on page 12-25 3. Use the 'Details' option in the RAS ticket to identify which tape drive is generating the RAS ticket. If possible, check the front of the tape drive for error indications. Check the suspect drive sled to determine whether the fan is still spinning. Check for any obstructions. refer to “Diagnosing a problem” on page 10-3 for more diagnostic procedures.

T024: AC power loss

Description	GUI Description: AC power to a library power supply is turned off. Explanation: A power supply detected loss of AC power. AC power loss to a single power supply control module is unlikely to post this ticket because of the speed at which system shutdown occurs after an AC loss. This ticket is most likely to occur when there is AC loss to a redundant power supply in a control module or any supply in any expansion module.
Detection Scenarios	AC power status from the supply creates an interrupt that is managed by software.
Root Causes	1. AC supply is gone (cord is removed, customer side AC failure). 2. Individual on/off switch for the supply is set to off. 3. Hardware failure inside supply.
Possible CRU Replacements	• Power supply • Expansion module
Possible FRU Replacements	Internal Cables and Boards Kit
Resolution	Complete the following steps: • “DR009: Resolving AC failure” on page 11-65 Before the following steps are completed: • “Removing a primary power supply” on page 12-35. • “Reinstalling/replacing a power supply” on page 12-36. refer to “Diagnosing a problem” on page 10-3 for more diagnostic procedures.

T025: Power supply hardware failure

Description	GUI Description: A defective power supply is detected. Explanation: Power supplies report four failure conditions that are considered to be a hardware failure within the supply: Fan Fail, Over Temp, DC Fail and Over Current. These failures can occur in both single and redundant power supply control modules and any expansion module with a power supply.
Detection Scenarios	Regular polling between Library Control Blade and power supply is not successful.
Root Causes	1. Detected fan failure in the supply. 2. Detected over temp condition in the supply. 3. Detected DC failure in the supply. 4. Detected over current failure in the supply.
Possible CRU Replacements	• Power supply • Module Terminators and Module-to-Module cables
Possible FRU Replacements	Internal Cables and Boards Kit
Resolution	Before any remove/replace procedures are completed, refer to “Diagnosing a problem” on page 10-3 for more diagnostic procedures.

T026: Primary key server failover

Description	GUI Description: The library completed a successful communication failover to the secondary key server. Explanation: The key management feature of this library allows the user to connect 2 key servers for redundancy. If communication to the primary server is interrupted, the library automatically switches or failovers to the secondary server. This RAS ticket is generated to notify the user of this failover event.
Detection Scenarios	• When the library detects that it can no longer communicate with the primary key server and automatically switches to the secondary key server.
Root Causes	1. Primary key server is not connected properly. 2. Primary key server is not configured properly. 3. Library ethernet settings are not configured properly.
Resolution	1. Complete “DR079: Resolving key server communication issue” on page 11-85. 2. Complete EKM path diagnostic tests (**Tools** > **Diagnostics** > **EKM** > **EKM Path Diagnostics** in the Web User Interface). 3. If the "Ping" test is unsuccessful, look for physical connection problems and down servers. 4. If "Ping" is successful, do the following steps: a. Verify that EKM is running. b. Verify that the media is not from a different EKM environment. c. Verify that the key server is present. .

T027: Key server communication failure

Description	GUI Description: The library is unable to communicate with the configured key servers. Explanation: The key management feature of the library allows the user to connect to two key servers for redundancy. If communication to one of these servers fails and a communication failover is not possible or not successful, then this ticket is generated. A separate ticket is created for each key server that fails..
Detection Scenarios	Library detects that communication with a key server is not successful
Root Causes	1. Primary/secondary key server is not connected properly. 2. Primary/secondary key server is not configured properly. 3. Library ethernet settings are not configured properly.
Resolution	1. Complete “DR079: Resolving key server communication issue” on page 11-85. 2. Complete EKM path diagnostics (**Tools** > **Diagnostics** > **EKM** > **EKM Path Diagnostics** in the Web User Interface). 3. If the "Ping" test is unsuccessful, look for physical connection problems and down servers. 4. If "Ping" is successful, do the following steps: a. Verify that EKM is running. b. Verify that the media is not from a different EKM environment. c. Verify that the key server is present.

T028: Secondary key server failure

Description	GUI Description: The library completed a successful communication failover to the primary key server. Explanation: The key management feature of the library allows the user to connect two key servers for redundancy. If communication to the secondary server is interrupted, then the library automatically switches or failovers to the primary server. This RAS ticket is generated to notify the user that communication to the secondary key server failed and that the library completed a successful failover to the primary key server.
Detection Scenarios	When the library detects that it can no longer communicate with the secondary key server and automatically switches to the primary key server where it established successful communication.
Root Causes	1. Secondary key server is not connected properly. 2. Secondary key server is not configured properly. 3. Library ethernet settings are not configured properly.
Resolution	1. Complete “DR079: Resolving key server communication issue” on page 11-85. 2. Complete EKM path diagnostic tests (**Tools** > **Diagnostics** > **EKM** > **EKM Path Diagnostics** in the Web User Interface).

T029 - Key server communication warning

Description	The library is unable to successfully monitor the communication path and operation status of the configured key server. The key management feature of the library allows the user to connect two key servers for redundancy. If communication fails during background key server path testing, this operator intervention is generated. A separate operator intervention is created for each key server that fails.
Detection Scenarios	Library detects that communication with a key server is not successful
Root Causes	1. Primary/secondary key server is not connected properly 2. Primary/secondary key server is not configured properly 3. Library ethernet settings are not configured properly
Resolution	1. Complete "DR079: Resolving key server communication issue" on page 11-85. 2. Complete key path diagnostic tests (**Service Library** > **Key Path Diagnostics** in the Web User Interface).

T030: Excessive I/O station events

Description	GUI Description: An I/O station is reporting continuous door open or closure events although no close or open door state change is detected. Explanation: The library controller is receiving too many I/O station interrupts. The problem can be caused by a stuck interrupt line for the CM or EM door open and close indication. Door open and close state changes are detected properly, but the excessive I/O station state change interrupt notifications indicate a hardware problem, most likely because of a cabling/connection issue.
Detection Scenarios	Library firmware receives multiple or continuous I/O station open and close interrupts, but does not detect the required door open and close state change.
Root Causes	1. Internal module sensor line and cable connections shorted. 2. Module terminator pins that are bent or shorted. 3. Module-to-module cable pins that are bent or shorted.
Resolution	1. Complete "DR008: Resolving stuck I/O station interrupt" on page 11-65. 2. Inspect the module terminators and module-to-module cables for loose connectors or damage (bent or broken pins). If damaged, replace the part. Reseat the terminators and cables. 3. Power on the library and wait for the library to initialize. Open and close each I/O station door. If the problem is not fixed, you must replace the module.
Possible Replacement CRUs/FRUs	1. Module Terminators and Module-to-Module cables 2. Module (EM or CM)

T031: I/O station unlock failure

Description	GUI Description: An I/O station lock that failed to unlock. Explanation: System logic or external command is requiring I/O station lock to unlock but it does not.
Detection Scenarios	When unlock action is attempted, lock/unlock position sensor does not detect the proper state.

Root Causes	1. Lock mechanism not working properly. 2. Lock position sensor not working properly. 3. Mechanical binding or obstruction prevents correct motion and detection. 4. Mechanical failure of sensor flag.
Possible CRU Replacements	Library Control Blade
Possible FRU Replacements	• I/O station lock assembly • Display/Door and I/O PCB • Internal Cables and Boards Kit 3
Resolution	Complete the following steps: • "DR011: Resolving I/O station lock/unlock failure" on page 11-66 • Before a library component is replaced or IBM technical support is contacted, refer to "Diagnosing a problem" on page 10-3 for more diagnostic procedures.

T032: I/O station lock failure

Description	GUI Description: An I/O station lock that failed to lock when required. Explanation: System logic or external command is requiring I/O station lock to lock but it does not.
Detection Scenarios	When a lock action is attempted, the lock/unlock position sensor does not detect the correct state.
Root Causes	1. Lock mechanism not working properly. 2. Lock position sensor not working properly. 3. Mechanical binding or obstruction prevents correct motion and detection. 4. Mechanical failure of sensor flag.
Possible CRU Replacements	Library Control Blade
Possible FRU Replacements	• I/O station lock assembly • Display/Door and I/O PCB • Internal Cables and Boards Kit 3
Resolution	Complete the following steps: • "DR011: Resolving I/O station lock/unlock failure" on page 11-66 • Before a library component is replaced or IBM technical support is contacted, refer to "Diagnosing a problem" on page 10-3 for more diagnostic procedures.

T033: Drive TapeAlert 3 - Hard read or write error

Description	System determines that the drive issued a TapeAlert 3, indicating an unrecoverable read, write, or positioning error.
Detection Scenarios	Tape drive issues a Tape Alert 3 that is recognized by the library during the continuous 4-second polling cycle of drive status.
Root Causes	Drive determined that there is a problem per its internal algorithms.
Possible CRU Replacements	• Tape cartridge • Drive sled

Resolution	If the cartridge is managed by a host application, remove the cartridge with the host application. If the cartridge is managed by the library, complete the following steps: • Remove the suspect cartridge (see “Removing a data cartridge” on page 8-32 or “Removing a cleaning cartridge” on page 8-34). • Insert a new cartridge (see “Inserting data cartridges” on page 8-31 or “Inserting a cleaning cartridge” on page 8-33).

T034: Drive TapeAlert 4 - Media error

Description	GUI Description: A tape can no longer be written or read, or performance is severely degraded. Explanation: System determines that the drive issued a TapeAlert 4, indicating an unrecoverable read, write, or positioning error that the drive specifically isolates to the media. This ticket is generated only if accompanied by TA 39, to indicate a pulled leader pin.
Detection Scenarios	Tape drive issues a TapeAlert 4 that is recognized by the library during the continuous 4-second polling cycle of drive status.
Root Causes	Drive determined that there is a problem per its internal algorithms.
Possible CRU Replacements	Tape cartridge
Resolution	Complete “DR044: Resolving Drive TapeAlert 4 - media error” on page 11-79

T035: Drive TapeAlert 5 - Read failure

Description	GUI Description: The drive is having difficulty reading from a tape. Explanation: System determines that the drive issued a TapeAlert 5, indicating an unrecoverable read error where isolation is uncertain between drive and media.
Detection Scenarios	Tape drive issues a TapeAlert 5 that is recognized by the library during the continuous 4-second polling cycle of drive status.
Root Causes	Drive determined that there is a problem per its internal algorithms.
Possible CRU Replacements	Tape cartridge
Resolution	Complete “DR045: Resolving Driving TapeAlert 5, 6 - read/write failure” on page 11-79.

T036: Drive TapeAlert 6 - Write failure

Description	GUI Description: The drive can no longer write data to a tape. Explanation: System determines that the drive issued a TapeAlert 6, indicating an unrecoverable write error where isolation is uncertain between drive and media.
Detection Scenarios	Tape drive issues a TapeAlert 6 that is recognized by the library during the continuous 4-second polling cycle of drive status.
Root Causes	Drive determined that there is a problem per its internal algorithms.
Possible CRU Replacements	Tape cartridge
Resolution	Complete “DR045: Resolving Driving TapeAlert 5, 6 - read/write failure” on page 11-79.

T037: Drive TapeAlert 8 - Not data grade

Description	GUI Description: The drive cannot use a tape because it is not of required data grade. Explanation: System determines that the drive issued a TapeAlert 8, indicating that the tape cartridge in the drive is not a data grade tape.
Detection Scenarios	Tape drive issues a TapeAlert 8 that is recognized by the library during the continuous 4-second polling cycle of drive status.
Root Causes	Drive determined that there is a problem per its internal algorithms.
Possible CRU Replacements	Tape cartridge
Resolution	Complete “DR046: Resolving Drive TapeAlert 8 - suspect data grade tape” on page 11-80.

T038: Drive TapeAlert 9 - Write protected

Description	GUI Description: The drive was requested to write to a write-protected tape. Explanation: System determines that a write was attempted on a write-protected tape.
Detection Scenarios	Tape drive issues a TapeAlert 9
Root Causes	Write-protect feature on tape is protecting the tape but the user is trying to write to it.
Possible CRU Replacements	Tape cartridge
Resolution	Complete “DR014: Resolving write-protected tape cartridge” on page 11-68. To remove the write protection feature from the cartridge, refer to “Write-protect switch” on page 9-3.

T039: Drive TapeAlert 12 - Unsupported format

Description	GUI Description: The tape cartridge format is incompatible with the drive. Explanation: System determines that the drive issued a TapeAlert 12, indicating that the media loaded is an unsupported format. With the IBM LTO family of drives, full backward read and write compatibility is stopped when LTO 3 was introduced. LTO 3 cannot write in LTO 1 format. Therefore, an LTO 1 tape is an unsupported format when the library tries to write to it with an LTO 3 drive.
Detection Scenarios	Tape drive issues a TapeAlert 12 that is recognized by the library during the continuous 4-second polling cycle of drive status.
Root Causes	Drive determined that there is a problem per its internal algorithms.
Possible CRU Replacements	Tape cartridge
Resolution	Complete “DR015: Resolving unsupported tape format” on page 11-68.

T040: Drive TapeAlert 15 - MIC chip failure

Description	GUI Description: The memory in the tape cartridge failed. Explanation: System determines that the drive issued a TapeAlert 15, indicating that MIC (memory in cassette) of the loaded media is not working properly. The MIC is the memory that is part of the cartridge, also called LTO CM.
Detection Scenarios	Tape drive issues a TapeAlert 15 that is recognized by the library during the continuous 4-second polling cycle of drive status.
Root Causes	Drive determined that there is a problem per its internal algorithms.
Possible CRU Replacements	Tape cartridge
Resolution	Complete “DR047: Resolving Drive TapeAlert 15 - cartridge memory failure” on page 11-80

T041: Drive TapeAlert 16 - Forced eject

Description	GUI Description: The tape is ejected from a drive while it is read or written. Explanation: System determines that the drive issued a TapeAlert 16, indicating that a drive unload was triggered while the drive was actively reading or writing. The source of the unload is either an operator initiated manual push button on the drive itself or a GUI initiated command.
Detection Scenarios	Tape drive issues a TapeAlert 16 that is recognized by the library during the continuous 4-second polling cycle of drive status.
Root Causes	Drive determined that there is a problem per its internal algorithms.
Possible CRU Replacements	Tape cartridge
Resolution	Complete “DR048: Resolving Drive TapeAlert 16 - forced eject” on page 11-80.

T045: Drive TapeAlert 20 - Clean now

Description	GUI Description: The drive is requesting cleaning before it is used again. Explanation: System determines that the tape drive issued a TapeAlert 20, indicating that the tape drive requires cleaning before it is used again. This message is coincident with a "C" on the drive seven segment display.
Detection Scenarios	Tape drive issues a TapeAlert 20 that is recognized by the library during the continuous 4-second polling cycle of drive status.
Root Causes	Drive determined that there is a problem per its internal algorithms.
Possible CRU Replacements	No library CRU or FRU is involved. Rather, this message is an indication that the tape drive requires a cleaning tape to continue. Use a known good cleaning tape to clean the tape drive.
Resolution	Complete “DR018: Resolving drive cleaning requirement” on page 11-69.

T046: Drive TapeAlert 21 - Clean periodic

Description	GUI Description: The drive is requesting cleaning at the next convenient opportunity. Explanation: System determines that the drive issued a TapeAlert 21, indicating that the drive requires cleaning. This message is coincident with a "C" on the drive seven segment display..
Detection Scenarios	Tape drive issues a TapeAlert 21 that is recognized by the library during the continuous 4-second polling cycle of drive status.
Root Causes	Drive determined that a normal cleaning cycle occurred.
Possible CRU Replacements	No library CRU or FRU is involved. Rather, this message is an indication that the tape drive requires a cleaning tape to continue. Use a known good cleaning tape to clean the tape drive.
Resolution	Complete “DR018: Resolving drive cleaning requirement” on page 11-69.

T047: Drive TapeAlert 22 - Expired cleaning media

Description	GUI Description: The cleaning tape was used too many times. Explanation: System determines that a cleaning media is expired.
Detection Scenarios	• Tape drive issues a TapeAlert 22 • Code that manages library-based cleaning determines that a cartridge is used up based on actively managing the use count.
Root Causes	Cleaning tape is used up.
Possible CRU Replacements	No library CRU or FRU is involved. Rather, this message is an indication that the cleaning tape media is expired and must be replaced.
Resolution	If the cartridge is managed by a host application, export the cartridge with the host application. If the cartridge is managed by the library, complete the following steps: • Remove the suspect cartridge (see “Removing a cleaning cartridge” on page 8-34). • Insert a new cartridge (see “Inserting a cleaning cartridge” on page 8-33).

T048: Drive TapeAlert 23 - Invalid cleaning tape

Description	GUI Description: The tape drive requires cleaning, but a non-cleaning tape was loaded. Explanation: System determines that the drive issued a TapeAlert 23, indicating that the drive was expecting a cleaning tape but the loaded cartridge is not a cleaning tape.
Detection Scenario	Tape drive issues a TapeAlert 23 that is recognized by the library during the continuous 4-second polling cycle of drive status.
Root Causes	• User or library attempts to mount a cleaning tape but the tape is not actually a cleaning tape. • User mistakenly loads a data tape as a cleaning tape • Inventory or application issue results in data tape that is loaded when drive expects cleaning tape
Possible CRU Replacements	• Tape cartridge

Resolution	If the cartridge is managed by a host application, export the cartridge with the host application. If the cartridge is managed by the library, complete the following steps: • Remove the suspect cartridge (see “Removing a cleaning cartridge” on page 8-34). • Insert a new cartridge (see “Inserting a cleaning cartridge” on page 8-33).

T049: Drive TapeAlert 30 - Hardware A

Description	GUI Description: The tape drive detected an internal hardware problem. Explanation: System determines that the drive issued a TapeAlert 30, indicating a hardware error that requires a drive power cycle before the drive recovers to a usable state.
Detection Scenario	Tape drive issues a TapeAlert 30 that is recognized by the library during the continuous 4-second polling cycle of drive status.
Root Causes	Drive determined that there is a problem per its internal algorithms.
Possible CRU Replacements	Drive sled
Resolution	Before the following steps are completed: • “Removing a tape drive” on page 12-24. • “Removing and replacing a tape drive” on page 12-25. refer to “Diagnosing a problem” on page 10-3 for more diagnostic procedures. • Complete “DR049: Resolving Drive TapeAlert 30, 31 - drive hardware error” on page 11-81. • From the Operator Panel, select **Tools** > **Service** > **Drives** to run the drive diagnostic test. A blank, scratch cartridge is required for this test.

T050: Drive TapeAlert 31 - Hardware B

Description	GUI Description: The tape drive detected an internal hardware problem. Explanation: System determines that the drive issued a TapeAlert 31, indicating a hardware error that requires a drive power cycle before the drive recovers to a usable state.
Detection Scenario	Tape drive issues a TapeAlert 31 that is recognized by the library during the continuous 4-second polling cycle of drive status.
Root Causes	Drive determined that there is a problem per its internal algorithms.
Possible CRU Replacements	Drive sled
Resolution	Before the following steps are completed: • “Removing a tape drive” on page 12-24 • “Removing and replacing a tape drive” on page 12-25 refer to “Diagnosing a problem” on page 10-3 for more diagnostic procedures.

T051: Drive TapeAlert 32 - Interface

Description	GUI Description: The tape drive reported an external data interface problem Explanation: System determines that the drive issued a TapeAlert 32, indicating a tape drive detected a problem with the application client interface.
Detection Scenarios	Tape drive issues a TapeAlert 32 that is recognized by the library during the continuous 4-second polling cycle of drive status.
Root Causes	Drive determined that there is a problem per its internal algorithms.
Possible CRU Replacements	Drive sled(only if all cables are OK and host communication to other drives works)
Resolution	1. Complete “DR012: Resolving Drive TapeAlert 32 - host interface” on page 11-67. 2. Use the "Details" option in the RAS ticket to identify which tape drive reported the RAS ticket. 3. Clear the RAS ticket. 4. Check the cabling from the back of the tape drive to the host and reseat all the cables. 5. If RAS ticket persists, swap cables between drives to isolate a bad cable. If this test works and you can detect the drive, replace the bad cable. 6. If swapping cables did not fix the problem, upgrade the tape drive to the latest drive firmware.

T052: Drive TapeAlert 33 - Media eject required

Description	GUI Description: The tape drive has an error that requires the tape cartridge to be ejected for error recovery. Explanation: System determines that the drive issued a TapeAlert 33, indicating that the drive requires a cartridge to be ejected to resolve a problem.
Detection Scenarios	Tape drive issues a TapeAlert 33 that is recognized by the library during the continuous 4-second polling cycle of drive status.
Root Causes	Drive determined that there is a problem per its internal algorithms.
Possible CRU Replacement	Drive sled
Resolution	1. Complete “DR037: Resolving media eject” on page 11-77. 2. From the Operator Panel, select **Tools** > **Service** > **Drives** to run the drive diagnostic test. A blank, scratch cartridge is required for this test.Before the following steps are completed: • “Removing a tape drive” on page 12-24 • “Removing and replacing a tape drive” on page 12-25 refer to “Diagnosing a problem” on page 10-3 for more diagnostic procedures.

T053 - Unload timeout

Description	A tape drive did not successfully unload a tape cartridge within the allotted time frame, preventing the robot from picking and moving the cartridge. The library is expecting the drive to achieve an unloaded state within 3 to 5 minutes of initiating the unload request, but the drive is still rewinding and unthreading the tape. This operator intervention is ONLY displayed if the tape drive was instructed to complete an unload operation and the drive did not respond with a successful or failed to unload response within the allotted time frame. If the library controller code is determining that the drive is still busy for a defined wait time period and the unload request is not sent to the tape drive, this operator intervention is not generated, but rather the request to unload is denied as an illegal request. **Note:** The library does not wait for the maximum unload time that is defined by the drive. Drives can take up to 18 minutes before action on the unload or eject operation. The library waits only for 3 minutes before the unload request fails.
Detection Scenarios	• A SCSI Move Medium was issued but the drive does not achieve an unload or eject state within the allotted time frame after it is instructed to unload and eject. • A UI command was issued to unload or move from a drive, but the drive does not achieve an unload or eject state within the allotted time frame after it is instructed to unload and eject.
Root Causes	The tape drive was instructed to unload the tape cartridge but did not complete the request within the allotted time frame.
Resolution	1. Complete DR006 - Resolve unload timeout “DR006: Resolving unload timeout” on page 11-64. 2. If possible, check the front of the tape drive for error indications.
Possible CRU Replacements	Drive sled

T055: Drive TapeAlert 37 - Drive detects voltage problem

Description	GUI Description: The drive exceeded one of its voltage limits. Explanation: System determines that the drive issued a Tape Alert 37, indicating that the drive brick detected a voltage problem.
Detection Scenario	The library determines there is a Tape Alert 37 through its Event Message exchange with the drive sled. The drive sled detects the Tape Alert 37 by its periodic polling of the drive brick.
Root Causes	1. Drive determined that there is a voltage problem per its internal algorithms. 2. Drive detected a momentary voltage drop when a separate drive was being activated. 3. System power supply failure or fault.
Possible CRU Replacements	• Drive sled • Power module
Resolution	1. Complete “DR083: Resolving drive voltage problem” on page 11-87.

T060: Main access door open

Description	GUI Description: A library access door is open. Explanation: At boot time or run time, the library detects that at least one main door is open. The main access door switches are physically wired in series and the system firmware cannot distinguish which switch/door is open. In addition, the health of the module-to-module connection and termination affects the series wiring of the switches. Firmware logic does not report this ticket if the module-to-module termination is totally missing or not correct.
Detection Scenario	Constant monitoring of the switch electrical circuit (hardware interrupt) detects a door open. This detecting is true at run time or boot up.
Root Causes	1. Any main access door is open. 2. A number of electrical hardware failures in the door switch circuit (includes intermittent issues). 3. Mechanical issues where the door switch is not being made even though door is closed (includes intermittent issues). 4. Disconnected module terminator or module-to-module cable. 5. Damaged module terminator or module-to-module cable with bent or broken pins.
Possible CRU Replacements	• Module-to-Module communication cable • Module communication terminator • Display/Door and I/E PCB
Possible FRU Replacements	• Door Interlock Switch • Internal cables and boards kit
Resolution	Complete “DR019: Resolving open access door” on page 11-69.

T061: Tape Alert 55 - Loading fail

Description	GUI Description: The tape drive encountered a problem while a tape cartridge is loaded. Explanation: When a tape is loaded into the drive, a hardware malfunction can prevent the tape from being loaded in the drive. Or, the tape can get stuck in the drive.
Detection Scenarios	After a drive is loaded, the drive generates a Tape Alert 55, which is noticed by the library.
Root Causes	1. A drive hardware error that prevents the tape from being loaded. 2. A damaged tape that cannot be loaded into the drive.
Possible FRU Replacements	• Drive sled

Resolution	1. Complete “DR078: Resolving tape load/unload failure” on page 11-85. 2. Use the "Details" option in the RAS ticket to identify which tape drive reported the RAS ticket. Check for lock block condition. If possible, check the front of the tape drive for error indications. Clear the RAS ticket. 3. Open the main door and inspect the tape drive or path for obstruction. 4. Isolate the media that are used during the load operation and verify that it is not damaged. 5. Finally, pull the drive sled from the sled bay and reseat it in another sled bay and retry the load operation. Additionally, if 400G library firmware or later is used, run the IVT - Drive test from the Library Tests option that is accessed through the Operator Panel. **Note:** IVT is optimized for library firmware versions 520G and above and libraries that are built after July 1, 2008 (serial numbers with last 4 digits 8609 and above). • If your library was built on or before July 1, 2008, and you are running firmware version 520G or above, you are not able to run the IVT test, even though the selection is available. • If your library was built on or before July 1, 2008, and you are running firmware version 500G or below, you can run the test, but it is not recommended because it might produce erroneous results.

T062: Module configuration problem

Description	GUI Description: The library cannot determine its module configuration because of module-to-module cable connection or a module termination failure. Explanation: At boot time or run time, the library physical frame configuration is not valid. The configuration is determined with address bits and module count bits that are routed through the module to module cabling and termination.
Detection Scenarios	1. Code determines that there is greater than one control module that is based on geographic address bits. 2. Code detects five frames or greater above the control module per the geographic address bits. 3. Code detects five frames or greater below the control module per the geographic address bits. 4. Code detects that one or more geographic address bit patterns do not match a valid configuration. 5. The code detects/communicates with a device (I/O stations, power supplies, drives, blades, fan blades) that must not exist per the detected frame count and frame configuration. 6. Code determined frame configuration that is based on frame count and geographic address bit pattern does not match hard stops that are found by Y motion tests.
Root Causes	1. Greater than one control module exists in a stack of frames that are wired together. 2. Five frames or greater are above the control module. 3. Five frames or greater are below the control module. 4. Hardware failure results in one or more invalid geo bit patterns. 5. Hardware failure results in one or more valid but incorrect geo bit patterns when compared to frame count (more or fewer frames detected than actual count).

Possible CRU Replacements	• Module-to-Module communication cable • Module communication terminator • Library Control Blade
Possible FRU Replacements	• Internal Cables and Boards Kit • Expansion module enclosure
Resolution	Complete “DR010: Termination and connectivity diagnostic tests” on page 11-66.

T063: WWNN label change

Description	GUI Description: The robot cannot read or detected a new library worldwide node name (WWNN). Explanation: The library logic learns the library WWNN of the system by reading an abbreviated base WWNN base volume serial number label. This action is done at first boot up from a "cleared to ship" condition to establish the WWNN. It is also done on subsequent boot ups to verify that the persisted information on the library compact flash file system matches the physical library module. The library reports a problem when it cannot read the WWNN or it reads a WWNN value that does not match the persisted library configuration. A different motion-related problem is reported if motion is preventing the correct reading of the WWNN.
Detection Scenarios	1. At first boot up from clear to ship, the library must establish the WWNN for the first time. There can be no WWNN in system memory. 2. Any power up. System memory already has a WWNN established for the Library Control Blade. 3. The Library Control Blade is improperly swapped into a different physical chassis and the system reads the physical chassis WWNN label. 4. The compact flash from a system already in use is placed into a new replacement module.
Root Causes	1. The Library Control Blade was swapped between libraries. 2. WWNN label is damaged. 3. Bar code scanner is not working properly. 4. Entire communication path to bar code scanner is not working properly. 5. Library module is replaced.
Possible CRU Replacements	Library Control Blade
Possible FRU Replacements	• Picker • Internal Cables and Boards Kit 3
Resolution	Complete “DR007: Resolving bar code scanner issue” on page 11-65. Before you replace a library component, refer to “Diagnosing a problem” on page 10-3 for more diagnostic procedures.

T064: LCB hardware failure

Description	GUI Description: The Library Control Blade experienced a hardware failure. Explanation: The library encounters an error that appears to be isolated to hardware on the Library Control Blade itself.
Detection Scenarios:	Code detects a board level voltage problem.

Root Causes:	Board level voltage problems.
Possible CRU Replacements:	1. Library Control Blade 2. Display/Door and I/E PCB (DIEB)
Resolution	• Observe library component LEDs (refer to "Interpreting LEDs" on page 10-8. • Refer to instructions to remove and replace the Library Control Blade (see "Removing/replacing the Library Control Blade or Compact Flash card" on page 12-27).

T065: Robot over-current condition

Description	GUI Description: Robot power is interrupted because of an over-current condition. Explanation: The library detects that the 42 V picker supply circuit on the LCB is not at an acceptable voltage. Field data indicates that it is more likely an issue with the LCB rather than a picker assembly issue.
Detection Scenarios	Monitoring of voltage divider indicates partial or complete voltage drop
Root Causes	1. The 48 V to 42 V conversion power supply on the LCB shutdown because of excessive current draw. 2. Board level hardware failures 3. Permanent or temporary short in cables, connectors, picker 4. Various hardware failures in picker that causes too much current to be drawn. 5. Shorted module terminators or module-to-module cable pins.
Possible CRU Replacements	• Y- carriage assembly • Library Control Board
Possible FRU Replacements	Picker
Resolution	Complete "DR035: Resolving robot power interruption" on page 11-76

T066: Drive power fuse (F1) blown

Description	GUI Description: Drive power is interrupted because of a blown fuse. Explanation: The library detects that an F1 drive fuse on a Drive Sled Interface Board (DSIB) failed. Each module has a DSIB card to provide an electrical connection point for the drive sleds. Each DSIB has a replaceable fuse for the overall drive power bus. This fuse protects the core library hardware components from some type of short or over-current problem in one or more drives.
Detection Scenarios	• Monitoring of voltage divider indicates partial or complete voltage drop
Root Causes:	1. Board level hardware failure 2. Permanent or temporary short circuit conditions in drives, drive sleds, docking connectors
Possible CRU Replacements	Drive sled
Possible FRU Replacements	• DSIB fuse, 5U or 9U
Resolution	See "Contacting IBM technical support" on page 10-21.

T067: Display assembly hardware failure

Description	GUI Description: A local display assembly hardware failure is detected. Explanation: The library encounters an error that appears to be isolated to Operator Panel hardware, including the Operator Panel board.
Detection Scenarios	No communication with Operator Panel board.
Root Causes	1. Blown DIEB fuse. 2. Rare power supply problem where too much voltage is transferred to the display. 3. DIEB temperature limit that exceeds threshold. 4. LCB failure.
Possible FRU Replacements	• Operator Panel • Internal Cables and Boards Kit 3
Resolution	Remove and replace the Operator Panel (see “Contacting IBM technical support” on page 10-21).

T068: Destination element full

Description	GUI Description: The robot determined that a destination location for a tape cartridge move operation is already full. Explanation: The robot attempted to put to a drive, I/O, or storage element and determined that the element is full. This problem is distinctly NOT a SCSI illegal request situation. At the beginning of the move media, the library inventory indicated that the destination element was in an empty state to allow it to be a valid destination. During recovery operations, the library concluded that the cell is obstructed by a piece of media. Any failure that is not thought to be a piece of media in the destination must not be mapped to this ticket.
Detection Scenarios	• The destination element for a move media is full with a labeled cartridge. Library inventory does not know that the cell is full. • The destination element for a move media is full with an unlabeled cartridge. As part of recovery, the library attempts to run a get from the cell. If the get succeeds and a tape cartridge is detected in the picker by the tape present sensor, then the slot is designated as full with an unlabeled tape present.
Root Causes	• Inventory did not occur since the cartridge was placed in element by some manual operator intervention. • An unlabeled tape is placed in a slot by a user (not by the robot).
Possible CRU Replacements	Tape cartridge
Resolution	Complete “DR020: Resolving library inventory mismatch” on page 11-70.

T069: Source element empty

Description	GUI Description: The robot determined that a source location for a tape cartridge move operation is empty. Explanation: The robot attempted to get from a drive, I/O, or storage element and determined that the element is empty. This problem is distinctly NOT a SCSI illegal request situation. At the beginning of the move media, the library inventory indicated that the source element was not in an empty state and it was a valid source for a move media command. During recovery operations, the library concluded that the cell is genuinely empty. Empty is defined as NOT containing a cartridge with a readable volume serial number.
Detection Scenarios	The library fails to successfully get a cartridge during a move media. The cartridge present sensor in the picker indicates no cartridge at the conclusion of a GET. A subsequent inventory scan of the cell indicates that no cartridge is present.
Root Causes	Inventory was manually changed since last robotic inventory. Cartridge was removed from or moved within the system.
Possible CRU Replacements	Tape cartridge
Resolution	Complete “DR020: Resolving library inventory mismatch” on page 11-70.

T070: Library control path failure

Description	GUI Description: The library control command path through a tape drive failed. Explanation: The library media changer control path through a drive failed. The host that owns and runs the logical library can no longer be expected to control the library. The control path must be fixed or a user can choose to switch the control path to a different drive within the same logical library.
Detection Scenarios	1. The loss of communications between the library and the drive sled 2. The loss of communications between the drive sled controller board and the drive brick.
Root Causes	1. Various hardware problems inside the drive sled. 2. Tape drive (brick) firmware problem 3. Drive sled firmware problem 4. Library communication firmware problem 5. Drive Sled Interface Board (DSIB) hardware problem 6. Loss of power to sled (DSIB 48 V fuse)
Possible CRU Replacement	Drive sled
Resolution	• Update drive firmware (see “Updating drive firmware” on page 8-25. • Update library firmware (see “Updating library firmware” on page 8-24. • If the problem still exists, replace the drive sled (see “Adding/removing/replacing a tape drive” on page 12-24).

T071: Missing power supply

Description	GUI Description: A previously installed power supply is missing. The library can no longer detect the presence of a power supply that was previously physically installed and logically added to the system.
Detection Scenarios	Regular polling between LCB and power supply checks for presence of the power supply.
Root Causes	1. Power supply was physically removed after it was added to a powered ON system. 2. Hardware failure inside supply 3. Hardware failure in library side connector of other electronics. 4. Disconnected module terminator or module-to-module cable. 5. Damaged module terminator or module-to-module cable with bent or broken pins.
Possible CRU Replacements	1. Module Terminators and Module-to-Module cables 2. Power supply
Resolution	Complete “DR022: Resolving missing power supply” on page 11-70.

T072: Unmanaged system fault

Description	GUI Description: The library encountered an unmanaged fault. Explanation: Library firmware reported a problem that is not associated with a specific ticket and corresponding diagnostic resolution. This problem cannot be resolved without escalation to tech support and engineering.
Resolution	Complete “DR021: Contacting IBM service” on page 11-70.

T073: I/O storage door open

Description	GUI Description: An I/O station door that is configured for storage is open. Explanation: Certain I/O station doors can be designated as storage slots. When one of these doors is open, the system cannot become operational because these storage slots are not available to the robot. The ticket is posted to inform the user that the library cannot become operational and that the door must be closed so the system can lock it and start the library.
Detection Scenario	1. When the main doors are closed and the robot attempts to initialize, the state of “I/O Storage Doors” is checked. 2. When the library powers up and the robot attempts to initialize, the state of the “I/O Storage Doors” is checked.
Root Causes	1. I/O storage door is left open by user. 2. Hardware failure in the I/O door open/closed sensing. 3. Stuck lock assembly sensor switches.
Possible FRU Replacements	• I/O lock assembly • I/O magazine slide assembly
Resolution	Complete “DR034: Resolving open storage I/O door” on page 11-75.

T074: Drive sled auto-leveling failure

Description	GUI Description: The drive sled assembly failed to automatically update its firmware to the correct version. Explanation: The normal auto-level process for a sled did not work. When a drive sled is inserted into a powered ON library or when a library powers ON, the firmware level of the drive sled is checked to be consistent with the level required by the main library firmware. If the level is not correct, the sled is up-leveled or down-leveled accordingly. Failure in this process to set the correct firmware level in the sled results in this ticket.
Root Causes	1. Physical interruption of the firmware download process. 2. Firmware problems. 3. Hardware failures that result in intermittent or failed communication between library and drive sled.
Possible CRU Replacements	• Firmware • Drive sled
Possible FRU Replacements	Internal Cables and Boards Kit
Resolution	Complete “DR033: Resolving drive sled auto-level failure” on page 11-75.

T075: Unsupported module configuration

Description	GUI Description: The installed library firmware does not support the detected module configuration. Explanation: The current level of library firmware does not support the module configuration as detected by scanned module serial number labels. The firmware allows 5U, 14U, 23U, 32U, and 41U configurations. It does not run with anything greater than 41U or with a 10U configuration.
Detection Scenario	During initialization, the robot reads serial numbers on the modules that are present.
Root Causes	1. The system really is an invalid configuration and all modules are labeled correctly. 2. A chassis module is not labeled correctly. 3. The firmware level that is loaded on the library does not support a valid configuration. 4. Bar code reader is not scanning the labels correctly.
Possible CRU Replacements	Firmware
Possible FRU Replacements	**Note:** Read and complete all resolution steps before any parts are sent. Dispatch the first part that is listed for replacement. If this part does not solve the problem, dispatch the second part, and so on, in order. Dispatch only one part (or set of parts) at a time. • Picker assembly • Module (EM or CM) - dispatch only this FRU if the label is missing or damaged
Resolution	Complete “DR026: Resolving unsupported module configuration” on page 11-72.

T076: Robot initialization failure

Description	GUI Description: The robot did not initialize properly. Explanation: This ticket is designed to notify the user if the robot cannot initialize at all. The problem most likely lies with the cable spool, so it is replaced first, unless examination of the module terminator and module to module cables reveal a defect. The robot assembly is replaced second, since it has the next greatest probability of resolving the problem. No other parts must be dispatched until after these parts are replaced.
Detection Scenario	1. Any time the main door closes and the robot goes through an initialization sequence. 2. At power up of the library if the main door is closed.
Root Causes	1. Complete loss of connection to robot (that is, unplugged cable spool or equivalent). 2. Broken connection to Y-motor 3. Numerous hardware failures on the picker assembly
Possible CRU Replacements	Library Control Blade
Possible FRU Replacements	• Module Terminators and Module-to-Module cables • Cable Spool • Robot assembly
Resolution	Complete “DR031: Resolving robot initialization failure” on page 11-74.

T077: I/O station partially open

Description	GUI Description: The I/O station is in a partially open state or a cable connection failed. Explanation: This ticket is designed to report the problem that occurs if the cable that connects any of the I/O stations is unplugged. Hardware limitations make it such that unplugged or partially open I/O stations cannot be distinguished from one another. The default state of the open and closed door sensors is such that only the partially open state looks like the unplugged state (door not open + door not closed). The detection logic checks for this condition at bootup only to avoid triggering the ticket during any operational door open /close sequence.
Detection Scenario	Any time the library boots up it checks for the state of the I/O open and close sensors to see whether there is a not open and not closed condition.
Root Causes	1. I/O station safety flap broken or loose. 2. I/O station is unplugged at boot up 3. I/O station is left in a not open and not closed state at boot up
Possible FRU Replacements	• I/O station lock assembly • I/O station safety flap • Internal Cables and Boards Kit
Resolution	Complete “DR036: Resolving partially open I/O station” on page 11-76.

T079: Get operation failed, motion OK

Description	GUI Description: The robot failed to pick a tape cartridge. Explanation; The library cannot successfully get a tape from a drive, storage, or I/O location. The tape is still resting in the source location. The robot is not obstructed in any way and can continue operations (unlike the case for T003). If the operation was initiated by a host move media, the move media command failed with an ASC/ASCQ of `4h/15h/01h` (hardware mechanical positioning error).
Detection Scenario	The picker cannot get a tape from the source location. It can scan or touch the tape to verify that it is present.
Root Causes	1. Picker has broken fingers. 2. Picker has bad calibration so it is not positioned correctly. 3. Picker has bad **'y'** gears so it is not at the height it needs to be. 4. An obstruction that prevents the picker fingers from getting into the tape grooves. 5. A damaged tape that is jammed and stuck in the slot. 6. A damaged slot or drive that does not release the tape.
Possible CRU Replacements	• Cartridge
Possible FRU Replacements	• Picker • Y-axis assembly • Column assembly
Resolution	Complete “DR076: Resolving GET failure” on page 11-84.

T080: Module SN change

Description	GUI Description: The library detected the removal of an expansion module or a replacement of the control module. Explanation: When the library powers ON and the robot initializes, the bar code serial number (SN) labels in each module are scanned by the robot, beginning at the bottom of the library (closest to the y-axis home) and then working up. The library uses the control module (CM) SN and any expansion module SN to establish key operational properties and characteristics of library storage slots and partitions. A change in the CM SN or the removal of an EM (even if it is replaced with another EM) can “break” an established partition in such a way that it must be deleted. This ticket was designed to notify the user that a condition exists that requires the deletion of a partition and allow the user to assess whether human error is involved, such as mixing the Library Control Blade 's compact flash memory between libraries.
Detection Scenario	At library boot up time, the robot attempts to scan all module SN 's. When SNs are discovered, they are compared to persisted data on the system compact flash.

Root Causes	1. An LCB is improperly swapped into a different physical module and the system reads the physical module label. 2. A CM chassis FRU is replaced in an already configured system 3. A previously detected and configured EM is removed completely from a vertical stack of modules. 4. A previously detected and configured EM is removed completely from a vertical stack of modules and replaced with another EM of similar OR different size and location. 5. Bar code reader is not scanning the labels correctly. 6. Scratched or damaged label.
Possible FRU Replacement	• Picker assembly
Resolution	Complete "DR039: Resolving logical library deletion" on page 11-77.

T081: Incorrect module brand

Description	GUI Description: The library detected an incompatible module brand that does not match the library configuration. Explanation: The branding of a system is accomplished in two different ways. The firmware uses information that is saved on the compact flash to determine what brand the firmware and GUIs present to the user. There is also physical branding of the system in the form of different cosmetic skins, badging, paint, or external labels.on each module. Each module has a machine-readable bar code label that carries a module serial number (SN) and branding information that must match the physical branding of the module. The library manufacturing process installs a machine-readable bar code label that matches the external, user visible branding of the module. Because the library robot can read this bar code label, it can check the branding of the physical modules against the branding of the firmware and GUIs. This ticket is a defensive tool that is used to notify the user that there is a mismatch in the branding mechanisms. The root cause of a mismatch can be manufacturing defects, logistical errors (shipping the wrong spare part), or user errors such as moving parts between systems.
Detection Scenario	At library power ON, the robot attempts to scan all module bar code labels. When the OID number on each label is read, the embedded branding information is compared to persistent data on the system compact flash.
Root Causes	1. Various manufacturing defect errors, mislabeling, or part mix ups. 2. Spare part logistics error where wrong module FRU or compact flash FRU is sent to a customer site. 3. Users or service personnel that mix and match hardware from multiple systems of different branding in the field. 4. Malicious intent where customers attempt to buy and combine hardware from different sources. 5. Bar code reader is not scanning the labels correctly.
Possible FRU Replacement	• Picker assembly
Resolution	Complete "DR040: Resolving incompatible module branding" on page 11-77.

T082: Volume serial scanner failure

Description	GUI Description: The library volume serial scanner is not operating properly. Explanation: The volume serial scanner is detected to be in a state where the library control logic cannot use it. Library robot power is known to be applied (door is closed and robot is detected to be functioning enough to confirm power is applied) and yet scanner communication cannot be established at all or is intermittent.
Detection Scenario	1. During any library power ON or door close operation, picker power is applied and bar code scanner communication is established. 2. During run time operations such as inventory where the bar code scanner is used.
Root Causes	1. Scanner is physically disconnected 2. Various electrical hardware failures that prevent correct communication between the Library Control Blade and bar code scanner. 3. Bar code reader is not scanning the labels correctly.
Possible CRU Replacements	Library Control Blade
Possible FRU Replacements	**Note:** Read and complete all resolution steps before any parts are sent. Dispatch the first part that is listed for replacement. If this part does not solve the problem, dispatch the second part, and so on, in order. Dispatch only one part (or set of parts) at a time. • Picker assembly • Cable Spool • Y- carriage assembly
Resolution	Refer to "DR100: Resolving bar code scanner malfunction" on page 11-92.

T083: Unlevel robot assembly not level

Description	GUI Description: The robot assembly is not horizontally level and might be installed improperly. Explanation: The firmware detected a condition that indicates the robot assembly (Y-carriage and picker) is not installed level within the system. The robot assembly has drive gears that mate with rack gears inside the library modules. Field assembly problems and hardware failure problems can cause the robot assembly to be not level and therefore not function properly.
Detection Scenario	1. The robot cannot move to its Y-axis parking position after homing in Y because the front of the Y carriage hits the floor. Parking position is below homing position. 2. Front and back magazine fiducial positions on the left side are not at the same Y level. This test algorithm can detect non-level conditions in both directions (front high or back high). **Note:** There are a few known false detection scenarios: Certain specific size obstructions that are sitting on the floor of the library. Magazines that are not seated correctly. Damaged fiducials that are detected as mis-positioned because they are damaged.

Root Causes	1. Robot drive gears not installed in Y racks at the same time. This action results in the two ends of the Y carriage 1 - 2 teeth out of synchronization. 2. Y racks that are not seated properly/evenly. Both the front and rear Y rack are intended to be released from their shipping latches and lowered such that the racks in the bottom module rest on the floor of the unit. 3. Hardware failure and assembly failure modes can result in the front and rear drive gears on the Y carriage becoming excessively out of phase with each other. 4. Robot lock mechanism is out of position and interfering with the robot Y-axis travel.
Possible FRU Replacements	• Y-axis assembly • Internal Cables and Boards Kit
Resolution	1. Complete “DR041: Resolving robot installation” on page 11-78. 2. This RAS ticket appears almost exclusively for a picker and Y-carriage assembly climber not being level. Clear the RAS ticket. Remove these components from the unit and then reseat them to ensure that they are level. 3. Inspect the picker rails inside the unit and make sure that they are level, flush with the unit, and properly locked into place. 4. Ensure that the entire library is level in the rack. 5. Dispatch only the above FRU after all efforts are exhausted to get the unit and picker/Y-carriage assembly level.

T084: Missing cleaning tape

Description	GUI Description: A cleaning tape cartridge, which is configured for automatic library-initiated cleaning, is missing. Explanation: When the library is used to manage drive cleaning, the cleaning cartridges that are imported into the library are not visible to any host and are not part of any logical library. Rather, they are in the “system” logical library. Under all circumstances, the user must use theinsert and remove cleaning cartridge functions to move cleaning cartridges into and out of the cleaning slots in this “system” logical library. If, during inventory a system cleaning cartridge was removed manually (through an open door or with the power OFF), this ticket is used to notify the user that this cleaning resource is missing. Because the cartridge is missing, the library cleaning functionality is no longer intact. It is either degraded (fewer cartridges available) or totally absent (no cleaning cartridge in the library).
Detection Scenario	1. When library inventory occurs during robot initialization from a power ON. 2. When library inventory occurs during robot initialization from a door close.
Root Causes	1. User removes cartridge manually instead of with Remove cleaning media GUI command. 2. Bar code label on a system cleaning cartridge is not read during inventory. 3. Any scenario where a properly inserted system cleaning cartridge that is not properly removed is detected to be missing based on library inventory operations.
Possible CRU Replacements	Cleaning cartridge

Resolution	1. Complete “DR042: Resolving missing cleaning cartridge” on page 11-78. 2. If auto-cleaning is enabled, ensure that a cleaning tape is loaded in the correctly specified cleaning slot in the library.

T085: Unknown cartridge in cleaning slot

Description	GUI Description: A configured cleaning slot contains an unknown tape cartridge that is not used for automatic library-initiated drive cleaning operations. Explanation: When the library is used to manage drive cleaning, the cleaning cartridges that are inserted into the library are not visible to any host and are not part of any logical library. Rather, they are in the “system” logical library. Under all circumstances, the user must use the insert and remove cleaning cartridge functions to move cleaning cartridges into and out of the cleaning slots in this “system” logical library. If, during inventory, an unexpected (non-inserted) cartridge is inserted into a cleaning slot manually (through an open door or with the power OFF) this ticket is used to notify the user that this slot contains a cartridge that cannot be used for cleaning. Because the cartridge was not inserted as a cleaning cartridge, the library cleaning functionality is no longer intact. It is either degraded (fewer valid cartridges available) or totally absent (no valid cleaning cartridge in the library).
Detection Scenario	1. When library inventory occurs during robot initialization from a power ON. 2. When library inventory occurs during robot initialization from a door close.
Root Causes	1. User adds a cartridge manually instead of with the insert cleaning media GUI command. 2. Any time a cleaning slot is defined with the GUI and there is a rogue, labeled cartridge in the slot. This issue can occur under door open conditions or covers off. 3. Any scenario where a bar code labeled cartridge ends up in a cleaning slot by means other than with the correct insert GUI command.
Possible CRU Replacements	Cleaning cartridge
Resolution	Complete “DR043: Resolving invalid cleaning cartridge” on page 11-79.

T086: Inaccessible tape cartridge

Description	GUI Description: A tape cartridge is in a storage location that is not accessible by the library robot. Explanation: In library configurations of 23U or more, the top storage slot in each of the two columns on the top row of the right side of the library (columns 4 and 5) are inaccessible to the library robot. When the vertical stacks of library modules are 23U or higher, the robot is no longer adequately supported by the y-racks to get and put tape cartridges from these two storage slots. All other storage slots in the library remain accessible. This ticket is produced when a user manually inserts a cartridge into one of these slots and the library detects the cartridge during inventory. The library itself does not load a cartridge into one of these slots with host or Operator Panel commands. The slots that themselves are not presented as usable in logical libraries. Although the library cannot reliably get and put tapes from these storage locations, the library can still discover volume serial labeled tapes in these slots during normal inventory operations. Because these slots are inaccessible, they are not part of the library 's inventory and the ticket does not list their locations in the details. The ticket lists "None."
Detection Scenario	In libraries of 23U or greater, the library discovers a bar code labeled cartridge in the top slot of either column 4 or 5 during inventory.
Root Causes	A user manually places a cartridge in the top slot of either column 4 or 5 during inventory in a library that is at least 23U or greater.
Possible CRU Replacements	Cartridge
Resolution	Complete “DR050: Resolving invalid tape location” on page 11-81.

T087: Invalid library SN label warning

Description	GUI Description: The library 's serial number bar code label cannot be read by the robot but the library is able to initialize and continue operation. Explanation: The library logic learns the serial number of the system by reading an internal serial number label. The service tag is on the same label as the serial number. This action is done at first bootup from a "clear to ship" condition to establish the serial number. It is also done on subsequent bootups to confirm that the compact flash memory card is in the correct library. The library reports this operator intervention message when it cannot read the library serial number but it confirms the functionality of the bar code reading system by successfully reading other bar code labels in the library. It also has the library serial number that is stored in memory from a previous successful read. When this operator intervention message is posted, the user can be confident that at least one other bar code label is read. For example, bar codes that can be used the check functionality are: • WWN or SN (in control modules) • OID (in expansion modules) Different tickets are posted if there are motion-related problems, or scanner communication problems.
Detection Scenario	Any power-up. System memory already has a valid SN established for the LCB.

Root Causes	• Label is damaged. • Label is missing. • Label is physically obstructed. • Label is readable but does not meet minimum criteria to be considered a library SN label. • Scanner cannot read the serial number label.
Possible CRU Replacements	• LCB flash memory • LCB
Possible FRU Replacement	• Module (EM or CM) - dispatch only this FRU if the label is missing or damaged. • Picker assembly • Y- carriage assembly
Resolution	1. Complete "DR051: Resolving library SN label detection" on page 11-81. 2. Inspect the label inside the unit for damage. 3. Clear the RAS ticket. 4. Upgrade the library firmware to 400G or later and run the IVT - Picker test with the Library Tests option accessed through the Operator Panel. If the test passes, the issue is most likely not the picker. **Note:** IVT is optimized for firmware to firmware versions 520G and above and libraries that are built after July 1, 2008 (serial numbers with last 4 digits 8609 and above). • If your library was built on or before July 1, 2008, and you are running firmware version 520G or above, you are not able to run IVT test, even though the selection is available. • If your library was built on or before July 1, 2008, and you are running firmware version 500G or below, you can run the test, but it is not recommended because it can produce erroneous results.

T089: Email notification error

Description	GUI Description: A library-initiated email notification did not reach its destination. Explanation: The user can configure the library to send an email to a specified address whenever an operator intervention message is generated or a configured Advanced Reporting log notification is sent. This email includes a description of the operator intervention message and optionally includes the library current log. The library reports this operator intervention message if it receives any error codes when it tries to send out this email. This operator intervention message indicates that there is something wrong with the customer 's internal network or its settings, but there is no error on the library side. The library cannot detect all errors that can occur on a network, but can determine whether the email was successfully sent to the mail server on the network.
Detection Scenario	• Any time a RAS ticket is generated and the library is configured to generate a RAS email. • Any time an Advanced Reporting Notification is configured and the scheduled sending of such logs experiences an error.

Root Causes	• Email settings on the library are not correct. • The library is not connected to the network. • Library is plugged into the wrong network port. • Network cable is damaged. • Email server is down. • Some other configuration error on the customer 's network.
Resolution	Complete “DR053: Resolving network configuration issue” on page 11-82.

T090: Invalid cleaning tape

Description	GUI Description: A non-cleaning tape cartridge was used to attempt to clean the drive. System determines that the tape used to attempt to clean a drive is not a cleaning tape. This ticket differs from the Tape Alert 23 ticket (T048) in that this ticket is generated anytime a non-cleaning tape is used to clean a drive, not just in the case where the drive requires cleaning.
Detection Scenario	After a tape is loaded to clean a drive, the system notices that cleaning did not begin within 30 seconds.
Root Causes	• User or library attempts to mount a cleaning tape but the tape is not a cleaning tape. • User mistakenly loads a data tape as a cleaning tape. • Inventory or application issue results in data tape that is loaded when drive expects cleaning tape.
Resolution	Complete “DR077: Resolving invalid cleaning tape” on page 11-85.

T091: TapeAlert 56 - Unload failure

Description	GUI Description: The tape drive encountered a problem while a tape cartridge was unloading. Explanation: When an attempt is made to unload a tape, a drive brick hardware malfunction can prevent the tape from ejecting. The tape can be stuck in the drive.
Detection Scenario	After an unsuccessful attempt to unload a tape, the drive generates a TapeAlert 56, which is noticed by the library.
Root Causes	• A drive hardware error that prevents the tape from unloading. • A damaged tape that cannot be unloaded from the drive.
Possible FRU Replacements	• Drive sled
Resolution	Complete “DR078: Resolving tape load/unload failure” on page 11-85.

T092: Unreadable branding identifier

Description	GUI Description: The library cannot read the branding identifier. Explanation: The library logic learns the branding of the system by reading an internal label. The branding identifier is on the same label as the serial number. This action is done at first boot up from a "cleared to ship" condition to establish the library personality. It is also done on subsequent bootups to confirm that the Compact flash memory card is in the correct library. The library reports this ticket when it cannot read the library branding code but it confirmed functionality of the bar code reading system by successfully reading some other bar code label in the library. When T092 is posted, the user can be confident that at least one other bar code label was read. For example, bar codes that can be used to check functionality are WWN or SN (in CM cases). Different tickets are posted if there are motion-related problems, or scanner communication problems.

Detection Scenario	Picker cannot accurately read the OEM identifier bar code on the control module label.
Root Cause	Label might be damaged or missing.
Possible FRU Replacements	• Module (EM or CM) - dispatch only this FRU if the label is missing or damaged. • Picker assembly
Resolution	Complete "DR080: Resolving unreadable branding" on page 11-86.

T093: Automatic cleaning failure

Description	GUI Description: The library detected a problem during an automatic cleaning operation. Explanation: When the library is set up for Auto Clean, all the normal tickets for cleaning issues are disabled, since the auto clean mechanism resolves any RAS tickets automatically. There is, however, one case where a ticket must be posted: If the auto clean mechanism itself fails, this is the only ticket that is produced.
Detection Scenario	Auto Clean mechanism fails.
Root Cause	1. Auto Clean setup error (such as a user manually removing a cleaning cartridge) 2. Any tape, motion, or driver error for which there exists a RAS ticket
Resolution	Complete "DR081: Resolving autoclean failure" on page 11-86.

T094: Drive bay open

Description	GUI Description: A library drive bay in the rear of the library is open. Explanation: At boot time or run time, the library detects that at least one of the unoccupied drive bays does not have a cover on it. For safety reasons, if a drive bay is not occupied by a drive and does not have a cover plate that is installed, the robot is slowed to half speed to minimize the risk of having someone put their hand inside the library and the robot run into it at full speed. Library operations take twice as long in this state. As users normally remove the drive bay covers to insert or move drives, the library waits between 30 seconds and 10 minutes after this condition is detected to post the operator intervention message. The library is not capable of displaying the location of the open drive bay.
Detection Scenario	• Missing drive cover plate • Drive cover is loose or ajar and not electrically connected
Root Causes	• User removed the panel and forgot to put it back. • Cover plate was not put on securely and the electrical connection is not solid. • The cover plate is damaged in such a way that the electrical connection cannot be made. • Drive that is pulled back.
Possible CRU	Drive cover plate.
Resolution	Complete “DR054: Resolving open drive bay” on page 11-82.

T095: Installation and verification test (IVT) failure

Description	GUI Description: A subtest failed during the Installation & Verification Test. Explanation: The library contains a verification test that can be run to validate that the system is installed correctly and is running. Errors can occur during this test. The library posts this ticket whenever an error occurs during the Installation & Verification Test, but does not affect the overall library functionality. The ticket is a warning that a problem might be developing.
Detection Scenario	During the Installation & Verification Test run, any library error occurs that is not already handled by an existing RAS ticket.
Root Causes	Any function that is run by the Installation & Verification Test that does not complete successfully.
Resolution	Complete “DR021: Contacting IBM service” on page 11-70.

T096: Module communication error

Description	GUI Description: An error occurred while the library was trying to communicate with a module. Explanation: The system is having a problem with finding or communicating with all the modules in the library.
Detection Scenario	At boot up, the library cannot determine the status of all modules.
Root Causes	• Bent pin on a terminator or a module-to-module cable. • I/O station sensor error. • I2C bus error.

Possible CRU Replacements	• LCB • Module-to-module cable • CAN Bus terminator
Possible FRU Replacement	• CM or EM module • I/O station assembly • I/O Lock assembly
Resolution	Complete “DR056: Resolving module communication” on page 11-82.

T108: Incompatible drive brand

Description	GUI Description: An incompatible drive sled installation is detected. Explanation: Different library configurations support different drives. The drive sleds contains certain configuration information that the library uses to validate that the drive is configured properly. If a drive 's configuration data does not match what the library expects, the drive is not usable and this ticket is generated.
Detection Scenario	When the drive is installed, the configuration data does not match what is expected.
Root Causes	• User installed a drive from a different brand library. • User did not purchase the drive from an official TS3310 sales channel. • Drive sled does not have the correct configuration information programmed.
Possible FRU Replacement	Drive sled
Resolution	Complete “DR068: Resolving incompatible tape drive” on page 11-83.

T109: Drive firmware update failure

Description	GUI Description: A tape drive firmware update failed. Explanation: Tape drive firmware can be upgraded by using an FMR tape or by downloading the firmware to a drive through the web user interface, or by using a host utility. After the upgrade process is complete, the library checks to verify that the drive reports the new firmware version. If not, this ticket is generated. This ticket is generated only when the user upgrades the drive firmware manually.
Detection Scenario	After a drive firmware updated, the new version from the drive does not differ from the old version.
Root Causes	• The firmware image that was used to update the drive was the same as what was already installed on the drive. • A firmware upgrade cartridge with an incompatible firmware version (wrong generation, drive type) was used. • The firmware upgrade cartridge used did not have valid firmware. • The firmware image was successfully transferred to the drive, but was corrupted or incomplete. • Error in drive communication or other drive-specific error.
Possible FRU Replacement	Drive sled
Resolution	Complete “DR069: Resolving drive firmware update failure” on page 11-83.

T110: Drive firmware mismatch detected

Description	GUI Description: A mismatch in tape drive firmware versions is detected. Explanation: Each drive that is installed in the library is programmed with firmware from the drive manufacturer. All drives in the library must have the same firmware version. The library checks the library firmware version upon initialization and again when a new drive is inserted. If the drive does not have the same firmware, a ticket is generated. Rather than listing all the differences, the ticket instructs the user to look at the System Information screen to identify which drives must be updated.
Detection Scenario	On initialization, the library detects that not all drives have the same firmware version.
Root Causes	A drive was installed that had a different firmware version than other drives in the library.
Possible FRU Replacement	Drive sled
Resolution	Complete “DR070: Resolving tape drive firmware mismatch” on page 11-83.

T112: Invalid tape drive firmware image

Description	GUI Description: A stored tape drive firmware image is not usable for auto-leveling of a tape drive. Explanation: During initialization or when a drive is inserted while the library is operating, the library checks the product firmware level of the installed tape drive (brick). Then, it compares that version to the version that it stores internally in its file system. If they are not the same, the library automatically updates the tape drive (brick) with this internally stored code image.
Detection Scenario	The automatic update of the tape drive firmware fails.
Root Causes	The tape drive firmware image that is stored on the library 's file system is corrupted.
Resolution	Complete “DR072: Resolving tape drive auto-level failure” on page 11-84.

T114: Unassigned tape cartridge

Description	GUI Description: A tape cartridge is detected in a storage location that is not assigned to any partition. Explanation: At bootup, or after a door open event, the picker runs an inventory of the entire library. If a cartridge is in a slot that is not part of a logical library, the cartridge is inaccessible to the user and must be manually removed. This ticket is generated upon the first occurrence of such a cartridge. A separate ticket is not generated for each cartridge found.
Detection Scenario	During inventory, a cartridge is found in a slot that does not belong to a logical library.
Root Causes	• Tape was manually placed into the slot. • A partition was deleted that contained media and the library was power-cycled or the main door was opened.
Resolution	Complete “DR074: Resolving unassigned inaccessible tape cartridge” on page 11-84.

T115: Installation & Verification Test (IVT) warning

Description	GUI Description: A marginal, but still operable, assembly condition was found during the Installation & Verification Test (IVT). Explanation: The library contains a verification test that can be run to validate that the system was installed correctly and is running. Errors can occur during this test. The library posts this ticket whenever an error occurs during this Installation & Verification Test that does not affect the overall functionality of the library. It is more of a warning that a problem might be developing.
Detection Scenario	During the Installation & Verification Test, when an error occurs that is not serious enough to limit library functionality.
Root Causes	Any function that is run by the Installation & Verification Test that does not complete successfully.
Resolution	Complete "DR075: Resolving Installation & Verification Test warning" on page 11-84.

T116: Robotics firmware image error

Description	This ticket occurs with **Model 2** robots only. GUI Description: The robotics firmware auto-level process cannot be run because necessary files are missing or corrupted. Explanation: The library is unable to attempt the robotics firmware auto-level process. In this case, the robotics firmware auto-level is not attempted and the robotics subsystem is left in the 'not ready' state.
Detection Scenario	1. A necessary auto-level file is missing in the library firmware. 2. A necessary auto-level file failed validation.
Root Causes	Firmware corruption.
Possible FRUs	Library firmware
Resolution	Complete "DR084: Resolving robotics firmware image error" on page 11-88.

T117: Robotics auto-level failure

Description	This ticket occurs with **Model 2** robots only. GUI Description: The robotics firmware auto-level process failed to update either the robot flash image or the scanner flash image. Explanation: The normal firmware auto-level process for robotics was not successful. Each time the robot is initialized, the firmware level of the robot is checked to be consistent with the level required by the main library firmware. If the level is not correct, the robotics firmware is up-leveled or down-leveled accordingly. Failure in this process to update to the correct robotics firmware level results in the generation of this ticket.
Detection Scenario	The Robot Controller Board did not complete one of the following operations: 1. Validate the received flash image 2. Program its flash with the robot flash image. A necessary auto-level file failed validation.

Root Causes	1. Flash Image CRC failure on the received file. 2. Hardware failures that result in unsuccessful flash programming.
Possible FRUs	• Picker assembly • Robot assembly
Resolution	Complete “DR085: Resolving robotics auto-level failure” on page 11-88.

T118: Degraded robotics flash

Description	This ticket occurs with **Model 2** robots only. GUI Description: The robotics firmware auto-leveling process was completed but failed to update one of the redundant robot controller flash partitions. Explanation: The library was not able to update one of the robotics flash parts (but the other was successfully updated). The robotics subsystem can still become ready, but the flash is in a degraded mode and the backup image is unavailable. This is a warning ticket.
Detection Scenario	The robotics firmware auto-level process was unable to update one of the Robot Controller Board 's flash parts.
Root Causes	One of the Robot Controller Board 's flash partitions is bad.
Possible FRUs	Robot assembly
Resolution	Complete “DR086: Resolving robotics degraded flash warning” on page 11-88.

T120: Robotics Y-axis motion failure, tape in picker

Description	GUI Description: A Y-axis motion error occurred while the robot was moving a tape cartridge. Explanation: A Y-axis motion error that cannot be considered a complete obstruction is reported by robotics. Because a tape is in the picker, tape recovery must be a part of the resolution strategy. This ticket occurs only during a robotics move, not during a robotics get or put..
Detection Scenario	1. A specified move in the Y-axis cannot complete. 2. Robotics firmware reports a Y-axis error condition.
Root Causes	1. A physical obstruction in the path of the robot 's motion. Examples include tape cartridges that are extending from the picker assembly or from a storage location, or tape cartridges or debris that collected on the floor of the library. 2. Many electrical hardware failures. Firmware or hardware detects that motion control is not occurring properly (encoder issues, motor-driving circuits, motor-winding issues). 3. A relatively small number of mechanical hardware failures that do not result in the detection of a complete obstruction, but where motion control generates robotics firmware error codes (contamination or damage to encoder wheel, high friction).
Possible FRUs	• Y-carriage assembly (if Model 1 robot is installed) or Robot assembly (if Model 2 robot is installed) • Cable Spool
Resolution	Complete “DR088: Resolving robotics Y-axis motion failure” on page 11-89.

T121: Robotics Y-axis motion failure, no tape in picker

Description	GUI Description: A Y-axis motion error occurred, which does not seem to be the result of robotic obstruction. Explanation: A Y-axis motion error that cannot be considered a complete obstruction is reported by robotics. Because a tape is not in the picker, tape recovery is not necessary as part of the resolution strategy. This ticket occurs only during a robotics move, not during a robotics get or put.
Detection Scenario	1. A specified move in the Y-axis cannot complete. 2. Robotics firmware reports a Y-axis error condition.
Root Causes	1. A physical obstruction in the path of the robot 's motion. Examples include tape cartridges that are extending from the picker assembly or from a storage location, or tape cartridges or debris that collected on the floor of the library. 2. Many electrical hardware failures. Firmware or hardware detects that motion control is not occurring properly (encoder issues, motor-driving circuits, motor-winding issues). 3. A relatively small number of mechanical hardware failures that do not result in the detection of a complete obstruction, but where motion control generates robotics firmware error codes (contamination or damage to encoder wheel, high friction).
Possible FRUs	Robot assembly
Resolution	Complete “DR088: Resolving robotics Y-axis motion failure” on page 11-89.

T122: Robotics X, Z, Theta axis motion failure, tape in picker

Description	GUI Description: An X, Z, or Theta axis motion error occurred while the robot was moving a tape cartridge. Explanation: An X, Z, or Theta axis motion error that cannot be considered a complete obstruction is reported by robotics. Because a tape is in the picker, tape recovery must be a part of the resolution strategy. This ticket can occur during a robotics move or during a robotics get or put.
Detection Scenario	1. A specified move in the X, Z, or Theta axis cannot complete 2. Robotics firmware reports an X, Z, or Theta axis error condition.
Root Causes	1. A physical obstruction in the path of the robot 's motion. Examples include tape cartridges that are extending from the picker assembly or from a storage location, or tape cartridges or debris that collected on the floor of the library 2. Many electrical hardware failures. Firmware or hardware detects that motion control is not occurring properly (encoder issues, motor-driving circuits, motor-winding issues). 3. A relatively small number of mechanical hardware failures that do not result in the detection of a complete obstruction, but where motion control generates robotics firmware error codes (contamination or damage to encoder wheel, high friction).
Possible FRUs	Robot assembly
Resolution	Complete “DR089: Resolving X, Z, Theta axis motion failure” on page 11-89.

T123: Robotics X, Z, Theta axis motion failure, no tape in picker

Description	GUI Description: An X, Z, or Theta axis motion error occurred, which does not seem to be the result of a robotic obstruction. Explanation: An X, Z, or Theta axis motion error that cannot be considered a complete obstruction is reported by robotics. Because a tape is not in the picker, tape recovery is not necessary as part of the resolution strategy. This ticket can occur during a robotics move or during a robotics get or put.
Detection Scenario	1. A specified move in the X, Z, or Theta axis cannot complete 2. Robotics firmware reports an X, Z, or Theta axis error condition.
Root Causes	1. A physical obstruction in the path of the robot 's motion. Examples include tape cartridges that are extending from the picker assembly or from a storage location, or tape cartridges or debris that collected on the floor of the library. 2. Many electrical hardware failures. Firmware or hardware detects that motion control is not occurring properly (encoder issues, motor-driving circuits, motor-winding issues) 3. A relatively small number of mechanical hardware failures that do not result in the detection of a complete obstruction, but where motion control generates robotics firmware error codes (contamination or damage to encoder wheel, high friction).
Possible FRUs	1. Picker assembly (if Model 1 or Model 2 robot is installed) 2. Robot assembly (if Model 2 robot is installed) 3. Cable Spool
Resolution	Complete “DR089: Resolving X, Z, Theta axis motion failure” on page 11-89.

T124: Robotics hardware error - RCB

Description	This ticket occurs with **Model 2** robots only. GUI Description: A servo hardware error is isolated to the Robot Controller Board.
Detection Scenario	Robotics firmware reports a specific hardware error that identifies the Robot Controller Board as the source.
Root Causes	Electrical hardware failure.
Possible FRUs	1. Robot assembly 2. Cable Spool
Resolution	Complete “DR090: Resolving robotics hardware error - RCB” on page 11-89.

T125: Robotics hardware error - picker

Description	GUI Description: A servo hardware error is detected in the picker mechanism. Explanation: A servo hardware error is isolated to the robotics picker mechanism.
Detection Scenario	Robotics firmware reports a specific hardware error that identifies the picker assembly electronics as the source.

Root Causes	Electrical hardware failure.
Possible FRUs	• Picker assembly (if Model 1 or Model 2 robot is installed) • Robot assembly (if Model 2 robot is installed)
Resolution	Complete "DR091: Resolving robotics hardware error - picker" on page 11-90.

T126: Robotics hardware error - scanner

Description	GUI Description: A hardware error is isolated to the bar code scanner. Explanation: A hardware error is isolated to the robot 's scanner device.
Detection Scenario	Robotics firmware reports a specific hardware error that identifies the Imager component of the picker assembly as the source.
Root Causes	1. Obstructions in the view path of the robot Imager. 2. Electrical hardware failure.
Possible FRUs	• Picker assembly (if Model 1 or Model 2 robot is installed) • Robot assembly (if Model 2 robot is installed)
Resolution	Complete "DR092: Resolving robotics hardware error - scanner" on page 11-90.

T127: Robotics communication error

Description	This ticket occurs with **Model 2** robots only. GUI Description: The library controller firmware lost communication with the robotics subsystem. Explanation: The library is not able to communicate with the Model 2 robotics subsystem. This ticket is generated if the library previously established a communication link with the robotics subsystem, but that link is now lost and cannot be reestablished.
Detection Scenario	The library firmware did establish communication with the robotics subsystem but encountered a communication failure during operation and communication cannot be reestablished.
Root Causes	1. Damaged module terminator or module-to-module cable with bent or broken pins. 2. An intermittent door-open condition that disconnects power from the robot. 3. A cable spool or connection problem. 4. A picker assembly hardware failure. 5. A Y-carriage assembly connection problem. 6. A robot controller board hardware or software failure. 7. An LCB serial communication link failure.
Possible FRUs	• Cable Spool • Robot assembly (replace entire unit)
Resolution	Complete "DR093: Resolving robotics communication error" on page 11-90.

T128: Incompatible robot installation

Description	GUI Description: The library control firmware detected that an incompatible robot is installed. Explanation: The library has an incompatible robot installed. This issue can happen when a GA-style (Model 1) robot is replaced with the Model 2 robot, or vice versa.
Detection Scenario	Library firmware detects a change in robot model, which is incompatible with the current library configuration.
Root Causes	The robot was replaced with an incompatible robot type.
Possible FRUs	• Robot assembly
Resolution	Complete "DR094: Resolving incompatible robot installed" on page 11-90.

T129: Drive sled firmware image error

Description	GUI Description: Drive sled firmware cannot be auto-leveled because of a missing or corrupted drive sled firmware image. Explanation: During an attempt to autolevel the drive sleds, the library detected a missing or corrupted UDS.lif (drive sled firmware) file.
Detection Scenario	Main library firmware that controls and runs drive sled firmware updates detects that the drive sled firmware update file is missing or corrupted.
Root Causes	The drive sled firmware update file is missing or corrupted.
Possible FRUs	Library firmware
Resolution	Complete "DR095: Resolving drive sled auto-level failure" on page 11-91.

T130: Tape drive cleaning failure

Description	GUI Description: A tape drive was cleaned but continues to request cleaning. Explanation: After a drive is cleaned and the cleaning tape is removed from the drive, the drive continues to request cleaning.
Detection Scenario	A drive continues to request a cleaning after successful cleaning cycles are applied.
Root Causes	Tape drive malfunction.
Possible CRUs	Drive sled.
Resolution	Complete "DR096: Resolving drive cleaning failure" on page 11-91.

T132: Hardware clock failure

Description	GUI Description: The hardware real-time clock (RTC) failed. The library system time can appear to be set correctly, but accurate time is lost following a power cycle or reboot. Explanation: While the library time is set, the library detected an error in the hardware real-time clock (RTC). This type of error allows the library system time to be changed, but the time is not set correctly following a power cycle or reboot.

Detection Scenario	Main library firmware determined that setting the hardware clock failed, though the system time appears to be set correctly.
Root Cause	The hardware clock on the LCB failed.
Possible CRUs	LCB
Resolution	Complete “DR098: Resolving hardware clock failure” on page 11-91.

T133: Bar code label mapping failure

Description	GUI Description: The library control firmware cannot map bar code labels to respective slots during an inventory operation. Explanation: The library is attempting to map bar code labels during inventory and is prevented from doing so because one or more bar code labels are improperly attached, or a magazine is improperly seated/installed.
Detection Scenario	The library cannot complete an inventory and there are no indications of hardware failure.
Root Causes	1. Obstructions in the view path of the robot Imager. 2. Improper installation of magazines. 3. Improper bar code label on tape cartridges. 4. User interface operations were completed while the robot was scanning bar code labels.
Resolution	Complete “DR099: Resolving bar code label mapping” on page 11-91.

T134: Bar code scanner malfunction

Description	GUI Description: The library bar code scanner cannot read bar code labels. Explanation: The bar code scanner is unable to detect target information. The bar code scanner cannot detect any bar codes within the library.
Detection Scenario	The library was unable to detect bar codes when target columns are scanned at startup.
Root Causes	1. Bar code scanner illumination is insufficient. 2. Bar code scanner view is obscured (blocked). 3. Bar code scanner failed.
Possible FRU Replacements	1. Picker assembly 2. Cable Spool
Resolution	Complete “DR100: Resolving bar code scanner malfunction” on page 11-92.

T135: Tape drive type change

Description	GUI Description: An assigned tape drive is replaced with a tape drive of a different type. Explanation: A tape drive that is assigned to a partition is replaced with a tape drive of a different type, where *type* is defined by the tape drive 's vendor, generation, and interface. This RAS ticket is generated to notify the user of the tape drive type change.

Detection Scenarios	1. Installation of a tape drive into a library drive slot triggers the library to discover it. 2. Boot up causes the library to physically discover any tape drive that is electrically connected in the system.
Root Cause	User replaced an assigned tape drive with a tape drive of a different generation, interface, or vendor.
Possible CRU	Drive sled
Resolution	Complete "DR101: Resolving tape drive type change" on page 11-92.

T136: Robotics Z-axis motion failure

Description	GUI Description: An unrecoverable robot motion failure occurred in the Z-axis. Explanation: An unrecoverable motion failure occurred in the z-axis. Because a tape cartridge might or might not be present in the picker, tape recovery must be part of the resolution strategy.
Detection Scenarios	A specified motion in the Z-axis cannot complete.
Root Cause	1. Many electrical hardware failures. Code or hardware detects that motion control is not occurring correctly (encoder issues, motor-driving circuit issues, motor-winding issues, cable connection issues). 2. A relatively small number of hardware errors that do not result in complete obstruction but where servo control does not appear to be normal.
Possible FRU Replacement	• Picker assembly
Resolution	Complete "DR102: Resolving robotics Z-axis motion failure" on page 11-92.

T137: Display assembly communication failure

Description	GUI Description: A local display assembly communication failure is detected. Explanation: The library encountered an error that appears to be caused by a communication link failure to the display assembly (DIEB).
Detection Scenarios	1. Failed I2C communication with the DIEB. 2. Failed GPIO communication with the DIEB.
Root Cause	1. Board level hardware failures. 2. Display not plugged in. 3. Cable failure or not plugged in. 4. LCB failure. 5. Rare power supply problem where too much voltage is transferred to the display.
Possible CRUs	• LCB • Display/Door and I/E PCB
Possible FRU Replacement	• Module (EM or CM) • Display (Operator Panel)
Resolution	Complete "DR103: Resolving display assembly communication failure" on page 11-93.

T139: Robotics communication loss

Description	This ticket occurs with **Model 1** robots only. GUI Description: The library controller firmware lost communication with the robotics subsystem. Explanation: The library lost communication with the Model 1 robotics subsystem. This ticket is generated if the library previously established a communication link with the robotics subsystem, but that link is now lost and cannot be reestablished.
Detection Scenarios	The library firmware established communication with the robotics subsystem but encountered a communication failure during operation and communication is not reestablished.
Root Cause	1. An intermittent door-open condition that disconnects power from the robot. 2. Damaged module terminator or module-to-module cable with bent or broken pins. 3. A cable spool or connection problem. 4. A picker assembly hardware failure. 5. A Y-carriage assembly connection problem. 6. An LCB serial communication link failure.
Possible CRUs	• Robot assembly (replace entire unit)
Possible FRU Replacement	• Module Terminators and Module-to-Module cables • Cable Spool
Resolution	1. Complete “DR093: Resolving robotics communication error” on page 11-90. 2. Check whether there is a main door open condition, which can be caused by an open door, defective or loose module terminator or module-to-module cable. 3. Inspect the module terminators and module-to-module cables for loose connectors or damage (bent or broken pins). If damaged, replace the part. Reseat the terminators and cables.

T141: Unknown picker calibration offsets

Description	GUI Description: Library firmware is unable to read robotics picker calibration offsets. Explanation: The picker 's EEPROM/FLASH that contains calibration offset values that are required for picker calibration and fiducial size evaluation, does not contain valid calibration offsets. If such offsets are missing and cannot be read, the robot fails calibration and cannot operate.
Detection Scenarios	Attempts to read the stored calibration offsets from EEPROM/FLASH of the Robotics Controller Board failed.
Root Cause	1. Defective EEPROM/FLASH area to read offsets. 2. Calibration offsets not stored during manufacturing process.
Possible FRU Replacement	Picker assembly
Resolution	Contact service for picker assembly installation or replacement.

T142: Robotics Y-axis hardware failure

Description	GUI Description: The robotic Y-axis gear failed to complete proper motion. Explanation: Movement of the robot assembly along the Y-axis is accomplished with the Y-carriage assembly, which contains the Y-motor. The Y-motor has a gear that is attached directly to the motor shaft. Failure or degradation of this Y-motor gear is the failure mode for this ticket.
Detection Scenarios	Robotics firmware reports a specific hardware error that identifies the Y-carriage assembly or Y-motor hardware as the source.
Root Cause	Failure or degradation of the Y-motor gear that drives the robot assembly along the y-axis.
Possible FRU Replacement	Y-carriage assembly (if Model 1 robot is installed) or Robot assembly (if Model 2 robot is installed)
Resolution	Contact service for picker assembly installation and/or replacement.

T143: Unlabeled cartridge detected

Description	GUI Description: An unlabeled tape cartridge or unreadable tape cartridge bar code label is detected. Explanation: During library initialization, or after a main door closure event, the library runs an inventory of the entire library. An inventory of respective magazines is also run each time an I/O station closes. These inventory operations use scanner reported bar code label information to determine element full and empty status. If the library is configured to run an "EMPTY SLOT" detection, it uses the teach sensor to determine whether an empty element can hold a cartridge that might not have a scanner readable bar code label. If such an unlabeled cartridge is found, this RAS ticket is generated to alert of the condition and allow the user to correct the issue. The system is able to report full status and also allow the cartridge to be moved. But any cartridge label reference lists "NO_LABEL" on the user interface screens and a SCSI READ ELEMENT STATUS response does not list label or VOLSER information at all. A RAS ticket is generated upon the first occurrence of such unlabeled cartridge detection; a separate ticket is not generated for each tape found.
Detection Scenarios	During "touch" inventory, the teach sensor indicates the cartridge presence, but the scanner was unable to read the cartridge bar code label.
Root Cause	A tape cartridge does not have a bar code label that is attached, or the bar code label is damaged and unreadable.
Possible FRU Replacement	None
Resolution	Remove and replace the unlabeled tape cartridge.

T144: I/O station door sensor stuck

Description	GUI Description: An I/E (or I/O) station sensor switch is reporting incorrect sensor status and might be stuck. Explanation: The library controller detected that an I/O station sensor is not reporting a valid status. The problem can be caused by a stuck sensor in the I/O station lock assembly with a control module or expansion module. Door open and close state changes are not detected reliably. Premature I/O station teach operations can occur, or no teach and inventory operation is triggered at all.

Detection Scenarios	When a state change is processed on either of the two sensor switches, or if the sensor switch that is causing the interrupt is activated, the opposite sensor switch is checked to see whether it is activated too. If they are both active, one sensor switch is stuck.
Root Cause	• A sensor switch is obstructed by foreign material. • A sensor switch is binding or sticking. • A sensor switch is broken.
Possible FRU Replacement	I/O station lock assembly
Resolution	See "DR025: Resolving stuck I/O station sensor" on page 11-71.

T145 - Media removal notification

Description	The library detected an expected cartridge removal from a configured I/E (or I/O) area element.
Explanation	The library is configured for Media Security Notification and detected an expected removal of media. Media removal is expected whenever an exported cartridge is physically removed by an operator from an I/O area element.
Detection Scenarios	After I/O elements are inventoried, the library determined that a previously exported cartridge is no longer present.
Root Causes	An exported cartridge was removed from the library.
Resolution	Complete "DR106 - Resolving media security notification" on page 11-93.

T146 - Media removal warning

Description	The library detected an unexpected cartridge removal from the library.
Explanation	The library is configured for Media Security Notification and detected an unexpected removal of media. Media removal is not expected if the cartridge is no longer found in previously configured storage and drive elements, and the medium changer (picker) element itself. Media removal is also not expected from configured I/O area elements, unless the tape cartridge is moved to such element by robotic motion.
Detection Scenarios	After an inventory operation, the library determined that a previously configured, but not exported, tape cartridge is no longer present.
Root Causes	A tape cartridge is removed from the library without being correctly exported by the robot.
Resolution	Complete "DR106 - Resolving media security notification" on page 11-93.

T149 - Key path diagnostic delay

Description	The library is unable to initiate a background Key Path Diagnostic test to an EKM server.
Explanation	The library attempted to run a Key Path Diagnostic test to an EKM server, but a tape drive is not available with the correct prerequisites, such as being ready and unloaded. This ticket conveys the fact that the test cannot be run within the selected test time period. This time period is determined by the configured test time interval that is multiplied by the configured test warning threshold.

Detection Scenarios	The library attempted to run a Key Path Diagnostic test but did not succeed in initiating the test within the configured test warning threshold. A tape drive is not available to allow the test to run.
Root Causes	• IBM LTO tape drive or drives are still loaded, preventing the library from initiating a Key Path Diagnostic test with a tape drive. • IBM LTO tape drive or drives are not ready, preventing the library from initiating a Key Path Diagnostic test with a tape drive.
Resolution	Complete "DR118 - Resolving EKM path diagnostic delay" on page 11-94.

T153: Drive encryption control failure

Description	GUI Description: A tape drive failed to enable or disable Library Managed Encryption (LME). Explanation: The drive sled controller firmware commanded the drive to enable or disable library managed encryption for the drive, yet the drive failed to complete the requested operation.
Detection Scenarios	• Library control firmware received a drive sled event, `E_DDC_LME_ENABLED`, indicating that the tape drive enabled Library Managed Encryption, but the library requested that the drive configure for Application Managed Encryption (AME). • Library control firmware received a drive sled event, `E_DDC_LME_DISABLED`, indicating that the tape drive did not enable Library Managed Encryption, but the library requested that the drive configure for LME.
Root Cause	Library control firmware was informed by drive sled of a tape drive command failure.
Possible FRU Replacement	Drive sled
Resolution	Complete "DR110: Resolving drive encryption control failure" on page 11-93.

T154: Drive encryption monitoring warning

Description	GUI Description: A tape drive request to initiate a library managed encryption key exchange did not provide the required request details to service the encryption key exchange request. Explanation: The drive sled controller firmware suspended Encryption Service Request (ESR) monitoring of the tape drive. The tape drive indicated an ESR, but when the drive sled controller firmware requested details from the tape drive, no data was provided. If this issue is encountered twice in a row, ESR monitoring is suspended during the drive mount session and is re-enabled when a new tape cartridge is mounted.
Detection Scenarios	Library control firmware received a drive sled event that indicated that the tape drive reported an ESR, but details are not reported by the tape drive.
Root Cause	Tape drive firmware can incorrectly report an ESR when none is outstanding, or have a valid ESR, but not have the correct encryption key request details available upon drive sled controller request.
Possible FRU Replacement	Drive sled
Resolution	Complete "DR111: Resolving drive encryption service request monitoring" on page 11-94.

T177: EEB lost ethernet/CAN connectivity

Description	GUI Description: A connection failure is detected for the Ethernet Expansion Blade (EEB). Explanation: The library detected a connection failure with an Ethernet Expansion Blade (EEB). Depending on the failure, communication to one or more connected tape drives can be affected.
Detection Scenarios	The library firmware encountered a communication failure during EEB operation and communication cannot be reestablished.
Root Cause	• Cable not plugged in. • Cable is faulty. • Port on EEB is not functioning. • Port on LCB is not functioning. • EEB is not functioning.
Possible FRU Replacement	• Ethernet Expansion Blade • Ethernet cable
Resolution	1. Note the ticket details to determine the EEB location and failure reason. 2. If the EEB is removed intentionally or moved to a new location within the library, select the **Service Library** > **Ethernet Expansion Blade Control** menu to remove the EEB 3. If the EEB is not removed and CAN and ethernet connection failures are reported, ensure that the EEB is installed properly, fully latched, secured, and powered ON. Reseat the EEB if necessary. 4. If the ticket informs of a CAN connection issue only, EEB power control is not operational. However, if the EEB is powered up, ethernet communication is still functional. Reseat the EEB at an opportune time when drive operations and drive connectivity interference is tolerable. 5. If the ticket informs of an ethernet connectivity issue only, ensure that the EEB is properly connected: • Check for correct connection of the ethernet cable between any one of the four internal ethernet ports of the Library Control Blade (LCB) and the ethernet port marked LOWER in the 9U expansion module that contains the EEB. • Inspect the ethernet cable for damage and reconnect as needed. 6. If the problem persists, contact service for further assistance.

Diagnostic resolutions

Diagnostic resolutions are accessed with wizard screens on the Operator Panel. When an Operator Intervention occurs, a diagnostic resolution wizard is available to help you resolve the problem.

Important: It is recommended that Service Action Tickets are not allowed to accumulate in the Operator Intervention reports. After an incident is resolved or repaired, the Service Action Ticket must be closed.

DR001: Resolving picker cartridge presence

Problem: The library has a tape in the picker assembly but cannot recover without user intervention to remove the tape.

Troubleshooting Steps:

1. Take all library partitions offline.
2. Open the library main access doors.
3. Rotate the picker assembly by hand so that the opening faces the drives.
4. Use the gear thumbwheel on the right side of the picker assembly base closest to you to manually drive the tape cartridge out of the picker assembly towards the tape drives.
5. Remove the tape cartridge and close the library main access doors. Wait for the library to initialize.
6. Insert the tape into the appropriate logical library.
7. If a tape cartridge was removed, continue operations.
8. If there was no tape cartridge in the picker assembly, it is most likely that the tape presence sensor in the picker assembly is malfunctioning. Contact service for assistance.
9. Choose one of the following options:
   - Select **Close** to close the ticket.
   - Select **Exit** to leave the ticket open for future troubleshooting.
   - Select **Back** to return to the Diagnostic Resolution.

If there is no cartridge in the picker when you investigate, it is likely that the cartridge present sensor in the picker is malfunctioning.

Before IBM technical support is contacted, refer to "Diagnosing a problem" on page 10-3 for more diagnostic procedures.

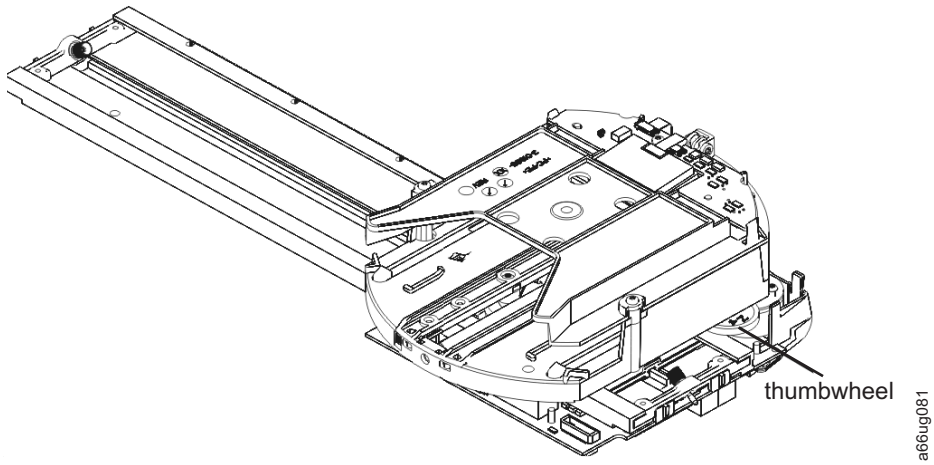


Figure 11-1. Gear thumbwheel

DR002: Resolving tape cartridge recovery

Problem

The library robot stopped working during a move media operation. The tape cartridge must be manually recovered before operations can continue.

Troubleshooting Step:

1. Open the main access door and find the cartridge. It might be stranded between the picker and the source or destination of the move.
2. Recover the cartridge.
3. Inspect slots for any obstruction.
4. Close the main access doors and wait for the system to complete initialization.
5. Use the **Tools** > **Service** > **Library** > **Robot Test** to verify whether the robot is operational.
   - If the test fails, refer to "Diagnosing a problem" on page 10-3.
   - If the test passes, close the Operator Intervention message and continue operations and monitor for reoccurrence.
6. Choose one of the following options:
   - Select **Close** to close the ticket now.
   - Select **Exit** to leave the ticket open for future troubleshooting.
   - Select **Back** to return to the Diagnostic Resolution.

DR003: Resolving drive eject failure

Problem:

The library received a request to unload and eject a tape cartridge from a tape drive but the operation failed.

There are two cases to consider:

- The tape drive is busy servicing host commands.
- The tape drive cannot physically unload and eject the tape cartridge.

Troubleshooting Steps:

1. View the ticket details to determine whether the tape drive is busy reading or writing data.
2. If the drive was busy servicing host commands, wait for the host application to finish drive operations. Then, repeat the command request to unload the tape drive.
3. If the drive was not busy servicing host commands, try the failing command request again.
4. If the requested command succeeds, observe for future occurrences and contact Service if the issue repeats.
5. If the requested command fails, open the library main access door and use the drive pushbutton on the front of the drive to initiate a tape cartridge eject operation. Press and hold the button continuously for 10 seconds. If the tape is ejected, leave the cartridge in the tape drive, close the library access doors and continue operation. Observe for future occurrences of such issue and contact Service if the issue repeats.
6. If the drive fails to unload and eject the tape cartridge, contact Service for assistance.
7. You have three options:
   a. Close the Operator Intervention now.
   b. Exit to leave it open for future troubleshooting.
   c. Return to the Diagnostic Resolution now.

DR004: Resolving full destination element

Problem:

The library attempted to put a cartridge in a drive, storage, or the I/O station. The destination location appears to be blocked or partially blocked. The library successfully returned the cartridge to the source location.

Troubleshooting Steps:

1. Identify the coordinate that is provided in the details of the ticket.
2. Open the library bulk load doors *(access doors)* and locate the problem location.
3. Inspect it for the presence of unlabeled media, or other contamination or damage that prevented the library robot from placing the cartridge.

DR005: Resolving motion failure

Problem:

The picker failed to complete a motion. The detected failure is likely to be a genuine hardware failure.

Troubleshooting Step:

1. Open the I/O station door, then the access door. Look for any obvious problems such as unplugged cables or damage to the picker assembly.
2. Remove any tapes from the picker or from the path of the picker.
3. Close the doors and wait for the system to complete initialization.
4. Select **Tools** > **Service** > **Library** > **Robot** to determine if the failure is permanent.
   - If the test fails, contact IBM technical support (see "Contacting IBM technical support" on page 10-21).
   - If the test passes, monitor for reoccurrence.

DR006: Resolving unload timeout

This tape drive diagnostic test requires a blank, scratch cartridge.

Problem:

A drive is suspected of having a problem.

Troubleshooting Steps:

1. From the Operator Panel, select **Tools** > **Service** > **System**.
2. Press **Yes** to take all logical libraries offline.
3. Select **Drives**.
4. Select **Drive Tests**.
5. Select **Wrap Test**.
6. Select the interface to be tested.
7. Select the module and drive to be tested.
8. Place a scratch cartridge in the top slot of the top I/O station, then close the I/O door.
9. When the **Assign I/O** screen is displayed, press **System**, then **Apply** to continue.
10. Attach the wrap tool to the Fibre Channel port on the back of the drive.
11. Select the drive test to be completed. The cartridge is loaded and the test begins.
12. The scratch cartridge is returned to the top slot of the top I/O station and the results of the test are displayed.
13. Press **Exit** to return to the **Library Verify** screen.
14. Press **Back** to return to the **System Diagnostics** screen.
15. Press **Back** to return to the **Library Offline** screen.
16. Press **No** to return to the **Service Menu** screen.
17. Press **Exit** to return to the **Tools** menu.
18. Press the **Operations** tab, then press **Logical Library Mode** to bring the logical libraries back online.

DR007: Resolving bar code scanner issue

Problem:

The library failed to scan one of the following system bar code labels:

- system serial number
- Worldwide name
- drive identification label
- module serial number

This problem IS NOT associated with failure to read a tape cartridge bar code label.

Troubleshooting Steps:

1. Select **Tools** > **Service** > **Library** > **Barcode Test** to help isolate the problem and determine whether it is intermittent.
2. Run the test several times and note the results.
   - If the test passes, the failure is most likely with a particular bar code label.
   - If the test fails, the failure is most likely with the picker assembly that contains the bar code scanner. Contact IBM technical support (see "Contacting IBM technical support" on page 10-21).

DR008: Resolving stuck I/O station interrupt

Problem:

The library control firmware receives continuous I/O station door state change events. Actual door open and closure state changes can still be detected and cartridge inventory operations are still working properly, but library performance is affected.

Troubleshooting Steps:

1. Close the RAS ticket and power off the library.
2. Inspect the top and bottom library module terminators for bent or shorted connector pins. Reattach if no problem is found.
3. If the library consists of multiple modules, inspect all module-to-module cables for bent or shorted connector pins. Reattach if no problem is found.
4. If a defective connector is found, call service for part replacement.
5. If no issue is found, power on the library and wait for the library to initialize. Open and close each I/O station door. If the RAS ticket is displayed again, contact service.

DR009: Resolving AC failure

Problem:

The facility AC power failed on a power supply. The facility power might be OFF. The power switch on the power supply is turned OFFor, the power supply failed.

Troubleshooting Steps:

1. Check the facility AC power and make sure that the power supply is properly seated and the power switch is on.
2. Inspect all module terminators for any broken or bent pins.
3. If the library consists of multiple modules, inspect all module-to-module cables for any broken or bent pins.
4. If the facility AC power and the power supply power switch are OK, contact IBM technical support. See "Contacting IBM technical support" on page 10-21.

DR010: Termination and connectivity diagnostic tests

Problem:

The library requires two terminators to be plugged into two specific ports on the rear of the library to automatically detect its configuration. In a multi-module system, these terminators are placed in the expansion modules at the top and bottom of the vertical stack. In addition, cables must connect all modules together.

Troubleshooting Steps:

Are the terminators and all module to module cables plugged in properly?

- **No** - You reported that the cables and terminators were not plugged in correctly. Select **Continue**, then power down the library, plug the cables in and power the library back on. When the library powers up, it detects the presence of the cables and terminators and properly configures itself. The library determined that the problem is fixed and it closes the ticket.
- **Yes** - Place both terminators on the CM to isolate the problem. You can back up or proceed with the Self Test.
  - **Self Test Failed** - Inspect the module connectors and terminators for bent or broken pins. Contact service to order replacement terminators. Refer to your product documentation to determine how to order parts.
  - **Self Test Passed** - Self Test passed. Continue to isolate the failure by plugging the terminator into the next upper expansion module and connecting the modules with the module-to-module cable. When the terminators and cables are installed, complete the self test again. If there is no additional upper expansion module, select **Next**.
    - **Self Test Failed** - Inspect the module connectors and module-to-module cables for bent or broken pins. Contact service to order replacement cable or expansion module. Refer to your product documentation to determine how to order parts.
    - **Self Test Passed** - Upper expansion module Self Test passed or there was no upper expansion module. Continue to isolate the failure by plugging the terminator into the first lower module and installing the module-to-module communication cable. When the terminator and cables are installed, complete the Self Test again.

      If there is no lower module, select **Next**.
      - **Self Test Failed** - Self Test failed. Contact IBM service to order replacement cable or lower expansion module. See product documentation to determine how to order parts.
      - **Self Test Passed** - Proceed to next step.
      - The library must be power-cycled for the module configuration to be fully started as the intended operating configuration.

DR011: Resolving I/O station lock/unlock failure

Problem:

An I/O station lock failed to operate properly. It is possible for a user to interfere with lock and unlock operations by trying to open/close an I/O station door while the lock is attempting to engage or disengage.

Troubleshooting Steps:

To proceed with troubleshooting, take the library out of service.

- If the user opened or closed the I/O station at the time the problem was reported. Close this operator intervention message and try operations again.
- If the problem is reported again, contact service.
- If there was no user interaction with the I/O station at the time the problem was reported, defective hardware is likely. Contact service to resolve the problem.
- Choose one of the following options:
  - Select **Close** to close the ticket now.
  - Select **Exit** to leave the ticket open for future troubleshooting.
  - Select **Back** to return to the Diagnostic Resolution.

It can take several minutes to achieve an offline state for all partitions, depending on host commands in progress.

Do you want to set all logical libraries to offline currently?

- **No** - You elected to troubleshoot later. Ticket remains open.
- **Yes** - Open all I/O station doors. Select **Self Test** to trigger the library to verify that all doors are open.
  - **Self Test Failed** - Test failed. Door *X* is not detected open. Replace I/O station lock assembly.
  - **Self Test Passed** - Door open test passed.

    Close all I/O station doors. Select **Self Test** to trigger the library to verify all I/O station doors are closed.
    - **Self Test Failed** - Test failed. Door *X* is not detected closed. Replace I/O station lock assembly.
    - **Self Test Passed** - Door closed test passed.

      Select **Self Test** to trigger the library to verify that all I/O station locks can be locked and opened.
      - **Self Test Failed** - Test failed. Lock *X* is not opening and closing properly. Replace I/O station lock assembly.
      - **Self Test Passed** - Lock test passed.

        Attempt to open all I/O station doors to confirm that the doors are locked.

        Did any of the doors open?
        - **Yes** - I/O station door *X* opened when the lock should have prevented it. Replace I/O station lock assembly.
        - **No** - Doors locked shut test passed.

          The system attempts to locate the I/O station magazines with the robotics.
          - **Self Test Failed** - I/O station magazine *X* in I/O station *Y* cannot be properly calibrated. Replace I/O station lock assembly and magazine.
          - **Self Test Passed** - All self tests passed. The original problem is resolved.

            Ticket is closed.

            Monitor for reoccurrence.

DR012: Resolving Drive TapeAlert 32 - host interface

Problem:

A tape drive detected and reported a problem with its host interface connection. This problem can be caused by a loose or disconnected cable, bad termination, or other FC, SAS, or SCSI communication issues.

Troubleshooting Step:

1. If the drive is SCSI -
   - Check for correct termination
   - Check cable length meets SCSI limits
   - Check host and drive connectors for bent or broken pins
   - Secure host and drive connectors
2. If the drive is Fibre Channel -
   - Check cable connections are secure
   - Check for broken or pinched cables
   - Check for cable bend radius too sharp
   - Check cable connections are clean
3. If the drive is SAS -
   - Check cable connections are secure.
   - Check for broken or pinched cables.
   - Check cable connections are clean.
4. Check all hardware components between host and drive are communicating correctly.
5. Check host HBA and components are communicating correctly.
6. If problem remains unresolved, before IBM technical support is contacted, refer to “Diagnosing a problem” on page 10-3 for more diagnostic procedures.

DR014: Resolving write-protected tape cartridge

Problem:

A backup application attempted to write data to a write-protected or WORM cartridge.

Troubleshooting Step:

Determine whether the cartridge is write-protected.

If not, export the cartridge with your backup application. Correct the problem by manually changing the write-protect switch on the cartridge.

If the cartridge is correctly set as a "read only" tape, investigate your host application to determine why a write was attempted.

DR015: Resolving unsupported tape format

Problem:

A cartridge that is not a correct format is loaded into a drive. There are several common scenarios:

1. FMR update cartridge that is loaded as a data cartridge
2. Cleaning cartridge that is loaded as a data cartridge
3. Data cartridge that is loaded as an FMR cartridge
4. Data cartridge that is loaded as a cleaning cartridge
5. Wrong generation of tape in a drive.

Troubleshooting Step:

If the cartridge was loaded to the drive with the Library GUI, remove the cartridge with the library **Operations** > **Media** > **Move** function. Insert the correct type of cartridge for the wanted operation and continue.

If the cartridge was loaded to the drive with a host application, remove the cartridge with the host application. Insert the correct type of cartridge for the wanted operation and continue.

DR016: Resolving prevent/allow media removal

Problem:

The library is commanded to complete a cartridge move from a drive, but the drive is preventing any media removal because it received a SCSI Prevent/Allow Media Removal command to prevent a tape cartridge removal. The library cannot unload and eject the tape cartridge from the drive until the host application issues a SCSI Prevent/Allow Media Removal command to allow a tape cartridge unload operation.

Troubleshooting Step:

Determine which host currently has a prevent media removal set. Use the host application or OS functionality to clear the Prevent mode.

DR018: Resolving drive cleaning requirement

Problem:

A drive reported that it requires cleaning. The drive cannot be used for normal operations again until it is successfully cleaned. This problem is addressed differently based on your system setup.

Troubleshooting Steps:

There are two cases to consider:

1. Library-controlled or host-controlled cleaning is enabled.
   - Before the tape drive requested cleaning, the cleaning process was triggered already when the tape drive recommended cleaning. However, since the tape drive is now requesting to be cleaned, a valid, non-expired cleaning tape might not be available for library-initiated or host controlled cleaning. Verify that cleaning tapes are properly configured and not expired.
   - Complete a manually initiated cleaning operation for the tape drive as specified in the user documentation.
2. Library-controlled automatic cleaning is disabled.

   Since automatic library initiated tape drive cleaning operations are not enabled, complete a manually initiated drive-cleaning operation for the tape drive as specified in the user documentation. In the case of RAS ticket "T045: Drive TapeAlert 20 - Clean now" on page 11-23, the drive might require multiple drive cleaning operations.
3. Choose one of the following options:
   - Select **Close** to close the ticket now.
   - Select **Exit** to leave the ticket open for future troubleshooting.
   - Select **Back** to return to the Diagnostic Resolution.

DR019: Resolving open access door

Problem:

A library main access door appears to be open. Either an access door is opened, or module termination is interrupted.

There are two basic scenarios to recover from:

1. Door open DID NOT interrupt a library MOVE MEDIA.
2. Door open DID interrupt a library MOVE MEDIA.

Resolutions:

1. Door open DID NOT interrupt a library MOVE MEDIA.

   If the door opening was planned and completed when the picker was idle, recovery consists of closing the door. The library reinventories and triggers backup applications to resynchronize inventory.
2. Door open DID interrupt a library MOVE MEDIA.

   If the door opening was not planned, MOVE MEDIA operations might be interrupted. Check backup applications to make sure that no jobs were interrupted. Follow the **Resolve** instructions for any other problems.

DR020: Resolving library inventory mismatch

Problem:

The library encountered a problem that indicates a mismatch between the library's physical and logical inventory.

Troubleshooting Steps:

1. View the ticket details to determine the source and destination element locations.
2. Open a main access door and inspect the destination element for tape cartridge presence.
3. If a labeled tape cartridge is present, the robot is not reading that label reliably. Inspect the label, replace if needed and close the main access door to trigger an inventory of the library.
4. If the source element is empty, close the main access door to trigger an inventory of the library.
5. Wait for the library to initialize and then restart the host applications to continue operation.
6. If the robot does not inventory the library after the door is closed, contact service for further assistance.
7. Choose one of the following options:
   - Select **Close** to close the ticket now.
   - Select **Exit** to leave the ticket open for future troubleshooting.
   - Select **Back** to return to the Diagnostic Resolution.

DR021: Contacting IBM service

This Operator Intervention requires technical assistance from IBM. Contact an IBM service representative by phone or web to open a Service Request.

In the US: 800-IBM-SERV (1-800-426-7378)

All other countries/regions: http://www.ibm.com

To open a Service Request online: http://www.ibm.com

At the direction of IBM technical support, you might be asked to complete the following functions:

- Capture a snapshot (From the Web User Interface, select **Service Library** > **Capture Library Log**
- Close Operator Intervention.

  You can select **No** to leave this problem open for future review.

DR022: Resolving missing power supply

Problem:

A power supply is detected to be missing in the system. This issue is most likely caused by an actual removal of a power supply.

Troubleshooting Step:

If you recently removed a power supply from the library, replace it and close this Operator Intervention.

If you want to permanently remove a power supply, close this operator intervention and power-cycle the library with the power supply removed.

If all power supplies appear to be present, see "Contacting IBM technical support" on page 10-21 for possible power supply hardware replacement.

DR023: Resolving missing I/O station magazine

Problem:

An I/O station is closed with a missing cartridge magazine. The library can still complete most operations. However, any attempt to export a cartridge to this I/O station location fails.

Troubleshooting Step:

1. If the magazine was intentionally removed, close this operator intervention.
2. If the magazine was removed by mistake, open the I/O station and reinstall the magazine. Close the operator intervention.
3. If the magazine was installed when this problem was detected, refer to "DR021: Contacting IBM service" on page 11-70.

DR024: Closing I/O door

Problem:

An I/O station door is open but the library requires it to be closed to continue operation.

Troubleshooting Step:

Close the I/O station door and close the Operator Intervention.

DR025: Resolving stuck I/O station sensor

Problem:

The library control firmware detected an invalid I/O station door sensor state. Actual I/O station door closure events can be detected prematurely, resulting in premature I/O station calibration attempts and calibration failures. Or, they might not be detected at all, skipping any calibration and inventory operations.

Troubleshooting Steps:

1. Identify the library module that is listed in the RAS ticket and open its I/O station door.
2. Close the RAS ticket.
3. Open the main access door to view the I/O station lock assembly of the opened I/O station.
4. Inspect both I/O station lock assembly sensor switches, which are in the front and rear of the I/O station lock assembly.
5. Look for obstructions or misalignment, causing the rear sensor switch actuator lever to be held down.
6. Open and close the I/O station safety door multiple times to view operation of the front sensor switch.
7. If no issue is found, or interference was identified and corrected, close the I/O station and main access door. Wait for the library to complete initialization.
8. Open and close the I/O station door and verify that the I/O station is calibrated and scanned.
9. If the I/O station is not being calibrated and inventoried, or the RAS ticket is displayed again, refer to "DR021: Contacting IBM service" on page 11-70.
10. Choose one of the following options:
    - Select **Close** to close the ticket now.
    - Select **Exit** to leave the ticket open for future troubleshooting.
    - Select **Back** to return to the Diagnostic Resolution.

DR026: Resolving unsupported module configuration

Problem:

The library detected a configuration of expansion module frames that is not supported by the current firmware. There are two possible scenarios:

- The configuration is valid and your system requires newer firmware to support the configuration.
- The EM configurations are not valid.

Troubleshooting Steps:

In all cases, contact service to determine a course of action. Be prepared to describe the number of modules in your system.

DR027: Resolving unknown library SN label

Problem:

The library cannot read one of the module serial number labels but already validated that the bar code scanning system is working properly. There are four likely scenarios:

1. Line of sight from the scanner to the module serial number bar code label is blocked by foreign material such as a media bar code label.
2. The module serial number bar code label is damaged and the bar code scanner cannot read it reliably.
3. One or more module terminators or module-to-module cables has bent or broken pins.
4. The module terminators or module-to-module cables are not installed in the correct locations and exclude a module.

Troubleshooting Steps:

1. Power off the library and inspect all module terminators and module-to-module cables for any bent or broken pins. Contact service to replace any damaged parts.
2. Ensure that the module terminators are connected to the extreme top and bottom connectors of the library and that the module-to-module cables are connected correctly per the library documentation.
3. Open the main library access doors and look for any damage to the module serial number. Check for obstructions in front of the module serial number bar code labels.
4. If no obvious foreign material is found, the module serial number is damaged and the EM or CM must be replaced. The library is not operational until it can successfully read the bar code label. Close the ticket and close all main access doors to allow the library to initialize again.
5. If the issue recurs, contact service for possible CM or EM replacement.

DR028: Resolving motion obstruction

Problem:

The library robot failed to complete a motion. Apparently the motion is obstructed by a foreign object or a misplaced cartridge.

Troubleshooting Steps:

1. Open the main access door and look for interference by the parking tab, any obvious foreign objects, or tape cartridges that are obstructing motion.
2. Check for packing material and robot shipping posts, which are large plastic screws that protrude from the top of the robot. Make sure that the Y-rails are secured properly and the robot is moving horizontally level along the Y-rails.
3. Look under the robot to make sure that there is no tape or other hidden obstruction on the floor of the library.
4. Verify that the robot parking tab is in the unparked position and not interfering with the robot Y-axis travel.
5. Close the doors and wait for the system to complete initialization.
6. Use the **Tools** > **Service** > **System** > **Library** > **Robotics** to exercise the robot and verify that the obstruction is cleared.
   - If the test fails, contact IBM technical support for further troubleshooting. Refer to "Contacting IBM technical support" on page 10-21.
   - If the test passes, the obstruction is cleared. Monitor for reoccurrence.

DR029: Resolving drive sled communication loss

Problem:

The system can no longer communicate with a drive sled.

A few scenarios create this problem.

1. A user removed a drive sled
2. A hardware failure that results in the drive that appears to be disconnected.

Troubleshooting Steps:

1. If the drive was intentionally removed, close this ticket.
2. Check for T021 tickets posted against other drives in the same module, if present. If other tickets exist, skip to step #7.
3. Close this ticket and remove and reseat the drive. Check the thumb screws on the drive to make sure that they are tight and the drive is mounted flush to the library chassis.
4. If this ticket reappears, close it again and move the drive to an empty slot in the same module. If no ticket appears after this action, contact service to replace the chassis.
5. Otherwise, close the ticket and move the drive to an empty slot in an adjacent module, if applicable. Check for ticket recurrence.
6. If the ticket is posted yet again, contact service for drive replacement If the ticket is posted yet again, contact service for drive replacement.
7. Check the power supply in the back of the module to verify that it is turned on and plugged in properly. If not, correct the problem, close all the T021 tickets for the module, and verify that they do not get posted again.
8. If the tickets do reappear, check further for T021 tickets posted against drives in other modules, if applicable. If there is none, contact service for chassis replacement.
9. If T021 tickets do exist for drives in other modules, close them, turn off the library, remove and reseat the LCB, and turn the library back on. Check to see whether any T021 tickets reappear.
10. If so, then check for other causes. There are other problems such as T066 - Drive power fuse blown or a module terminator or module-to-module cable with bent or broken pins that can cause communication loss. Resolve these problems, if found.
11. If not, contact service for further assistance.

DR030: Resolving drive load failure

Problem:

The robot was unable to load a tape drive. The robot motion completed normally but the drive did not report that it successfully loaded the tape. The problem can be caused by defective drive hardware or a defective picker mechanism.

Two possible scenarios that can lead to this problem:

1. The drive hardware is not functioning properly.
2. The robot hardware is not functioning properly.

Troubleshooting:

1. The problem is most likely isolated to the specific drive referenced under the **Details** button. However, check for the same problem that is reported for other drives in the system.
2. If this same problem is reported on multiple drives, contact IBM technical support.
3. If this problem is isolated to an individual drive, replace the drive. Refer to “Adding/removing/replacing a tape drive” on page 12-24.

DR031: Resolving robot initialization failure

Problem:

During a power ON or after library main access doors are closed, the robot did not initialize properly.

A common cause for this problem is an unplugged cable that leads to the robot. Other permanent hardware failures that result in loss of connection to the robot can also be a root cause.

Troubleshooting Steps:

1. Open the library main access doors. This action allows access to the robot and removes power from the robot. Check for any obvious disconnected cables that lead to the robot.
2. If any disconnected cables are discovered, plug them in and close all main access doors. The robot automatically attempts to initialize.
3. If no problem is found or the robot still fails, contact IBM technical support.

DR032: Resolving drive control path failure

Problem:

A control path to a library failed. It is likely that a drive sled failure is being reported as a separate problem.

It might be possible to reestablish the control path by resetting the drive sled. In libraries with more than one drive, you can use an alternate drive as the control path if your host connection architecture permits it.

Changing the control path can be a temporary work-around until the original drive problem is corrected OR a permanent change in your setup.

Procedure:

1. Reset the drive. For information, refer to"Resetting a drive" on page 8-30.
2. Close this ticket and attempt to reestablish the control path. Pull the drive sled out of the library, wait for the robot to scan the drive location, then reinsert the drive sled and secure the thumbscrews.
3. Wait for the drive to initialize and become ready
4. If this ticket recurs, continue to step 4 to switch the control path, otherwise, the problem is resolved and no further action is required.
5. Use the functions under the **Setup** > **Control Path** menu to switch the control path.
6. Whether you change the control path or not, you can close this problem.
7. Any associated drive problem must be resolved separately.

DR033: Resolving drive sled auto-level failure

Problem:

The library attempted to change the firmware level in a drive sled but the process failed.

Troubleshooting Steps:

1. With the drive coordinate from the problem Details, identify the drive sled that failed.
2. After the drive is located on the rear of the library, unscrew the thumbscrews and pull the drive out completely for at least 30 seconds. Reinsert the drive and tighten the thumbscrews.
3. Close the ticket, reinsert the drive sled, and tighten the thumbscrews.
4. The library now attempts to discover and initialize the drive again.
5. If this second attempt to establish the drive firmware level fails, contact IBM technical support. See "Contacting IBM technical support" on page 10-21.

DR034: Resolving open storage I/O door

Problem:

This library has an I/O station door that is configured to function as tape storage. This door was detected to be open at a time when the library needed it to be closed. The library cannot access these tape storage locations until this I/O door is closed and locked by the library.

Troubleshooting Steps:

There are two scenarios:

1. An I/O station door is genuinely open. If any I/O station doors are open, close them. When the I/O station doors are closed, the library automatically locks doors that are designated as storage. Close this operator intervention and monitor for reoccurrence.
2. A hardware failure makes it appear that an I/O station door is open. If all doors are closed, use the I/O station test under **Tools** > **Service** > **System** > **Library** to test the function of the I/O station.

DR035: Resolving robot power interruption

Problem:

The robot momentarily pulled too much current. Circuit protection occurred: a blown fuse or an internal power supply that is temporarily powered off.

Troubleshooting Steps:

1. Close this RAS ticket.
2. Open a library main access door, wait 10 seconds, and then close the main access door.
3. Observe library initialization.
4. If the robot does not initialize and a RAS ticket is displayed again, contact service for further assistance.
5. Choose one of the following options:
   - Select **Close** to close the ticket now.
   - Select **Exit** to leave the ticket open for future troubleshooting.
   - Select **Back** to return to the Diagnostic Resolution.

DR036: Resolving partially open I/O station

Problem:

An I/O station cannot be accessed.

Possible Causes:

1. The I/O station safety flap is broken
2. The I/O station flap is partially open. If so, close it.
3. The control cable to the I/O station is unplugged.
4. A hardware failure makes it appear that an I/O station door is partially open.

Troubleshooting Steps:

1. If any of the I/O station safety flaps are broken, replace them.
2. If any of the I/O station flaps are partially open, close them.
3. If none of the flaps are partially open, open the access door and look for an unplugged cable on the back of the lock assembly.
4. If none of the flaps are partially open and cables are connected, use the I/O station test under the **Tools** > **Service** > **Library** menu to test the function of the I/O station.
5. If the problem persists, refer to “Contacting IBM technical support” on page 10-21.

DR037: Resolving media eject

Problem:

A drive reported a problem that requires the currently loaded tape to be ejected from the drive in order for the drive to recover. With the drive coordinate from the problem Details, identify the drive sled.

Possible Causes:

1. The I/O station safety door is broken
2. The I/O station door is partially open. If so, close it.
3. The control cable to the I/O station is unplugged.
4. A hardware failure makes it appear that an I/O station door is partially open.

Troubleshooting Steps:

1. Eject the tape from the drive and remove it from the library.
2. Inspect the tape and retire the tape if problems are found.
   - Damaged cartridge shell
   - Misplaced bar code labels or foreign material
   - Snapped tape/disconnected leader
3. If the tape appears good, try operations with the tape again.
4. If the problem persists, refer to "Contacting IBM technical support" on page 10-21.

DR039: Resolving logical library deletion

Problem:

The system detected a change in module configuration, such as a new control module serial number or a removed expansion module that invalidates any existing logical library. Although a logical library is visible on the user interface, the assignment of storage slots and drives is broken because of the new module configuration.

Troubleshooting Steps:

1. With the Operator Panel, go to **Setup** > **Logical Library** and delete any existing logical libraries.
2. Refer to "Creating logical libraries" on page 8-3 for information.

DR040: Resolving incompatible module branding

Problem:

The library detected a branding mismatch. This issue is most likely caused by a manufacturing-labeling error or a user that mixes incompatible parts from multiple library systems.

Troubleshooting Steps:

1. If this problem was reported following a field upgrade, or the replacement of a defective part, the new part might be incorrect or mislabeled. Refer to "DR021: Contacting IBM service" on page 11-70.
2. If this problem occurred following the swapping of chassis, control boards, or compact flash cards between libraries, the two libraries have incompatible parts and the parts must be returned to their original libraries.
3. If neither of these scenarios apply or the problem remains unresolved, refer to "DR021: Contacting IBM service" on page 11-70.
4. **Close** the ticket or **Exit** to leave the ticket open for future troubleshooting.

DR041: Resolving robot installation

Problem:

The library detected a condition that indicates the robot assembly was installed incorrectly. The robot travels on rack gears, Y-rails, at the front and rear of the library. If the robot is installed into the rack gears with one end higher or lower than the other, the robot assembly cannot function properly.

Troubleshooting Steps:

1. The installation of the robot assembly must be done again to correct the problem. Close the ticket and power off the library.
2. Reference the user documentation for removing and installing the robot's Y-carriage assembly.
3. Remove the robot assembly from the library.
4. Make sure that the Y-rails are secured properly and verify that the left-side Y-rail columns are fully settled to the lowest positions.
5. Verify that the robot parking tab is in the unparked position and does not interfere with the robot Y-axis travel.
6. Install the robot assembly and assure that it is moving horizontally level along the Y-rails.
7. Power up the library and monitor for reoccurrence of the ticket.
8. If the ticket is not displayed again, the problem is corrected.
9. If the ticket is displayed again, the problem still exists, requiring further inspection of the Y-rail and Y-carriage assembly motion.
10. Choose one of the following options:
    - Select **Close** to close the ticket now.
    - Select **Exit** to leave the ticket open for future troubleshooting.
    - Select **Back** to return to the Diagnostic Resolution.

DR042: Resolving missing cleaning cartridge

Problem:

While the inventory is run, the library determined that a cleaning cartridge is missing.

This cleaning cartridge was originally inserted with the library operator interface specifically for the library to use for cleaning tape drives. This cartridge is not managed by any host applications.

It is likely that this cartridge was manually removed while the library was powered OFF or when the main access door was opened.

Troubleshooting Steps:

1. You can determine the bar code label of the missing cleaning cartridge and the coordinate where it used to be stored by selecting **Details**.
2. A valid cleaning cartridge must be inserted into the library to allow cleaning operations to function properly.
3. If inspection of the cartridge slot shows the cartridge to be present, the bar code label is not being read reliably by the library. Replace the bar code label or the cartridge.

DR043: Resolving invalid cleaning cartridge

Problem:

While the inventory is run, the library determined that an invalid cartridge is occupying a cleaning slot.

In order for a cartridge to be a valid cleaning cartridge, it must be imported as a cleaning cartridge with the library operator interface.

It is likely that this invalid cartridge was manually inserted while the library was powered OFF or when the main access door was opened.

Troubleshooting Steps:

1. You can determine the bar code label of the invalid cleaning cartridge and the coordinate where it is located by selecting **Details**.
2. Open the library main access door and remove this cartridge.
3. A valid cleaning cartridge must be imported into the library to allow cleaning operations to function properly.

DR044: Resolving Drive TapeAlert 4 - media error

Problem:

The tape cartridge is suspected because of failing tape operations. Data can be at risk, which is based on the condition of the tape.

This problem can be caused by:

- The specific tape
- The specific drive
- The interaction of the tape and drive

Troubleshooting Steps:

1. Determine the specific cartridge and drive that is involved in the problem by selecting**Details**.
2. Try the operation again with the same cartridge in the same drive.
3. If the attempt fails, copy data to a new cartridge.
4. Restart the current operation with a different cartridge.
5. If the problem remains unresolved, contact service.

DR045: Resolving Driving TapeAlert 5, 6 - read/write failure

Problem:

A drive detected a problem reading from or writing to a tape.

This problem can be caused by:

- The specific tape
- The specific drive
- The interaction of the tape and drive

Troubleshooting Steps:

1. Determine the specific cartridge and drive that is involved in the problem by selecting **Details**.
2. Try the operation again with the same cartridge in the same drive.
3. If the attempt fails, try the operation to the same cartridge in a different drive.
4. If the cartridge fails in more than one drive, retire the cartridge.
5. If the cartridge tests OK, use a known good cartridge to test the drive by running read/write operations from a host, or by using a drive-specific utility. Contact service for information on a drive utility for your specific drive type.
6. If the problem persists, gather a drive log after the next occurrence of a TapeAlert 5 or 6. Drive logs are captured by using the **Service Library** > **Capture Drive log** menu selection from the Web User Interface. Contact service and provide the drive log.

DR046: Resolving Drive TapeAlert 8 - suspect data grade tape

Problem:

A drive determined that a tape is not data grade and therefore data must not be written to it.

There can be several possible causes of this problem. Not all of the causes are genuine bad tapes, but in some cases a cartridge must be retired.

Troubleshooting Steps:

1. Attempting invalid operations with a cleaning cartridge can cause this problem. If the cartridge is a cleaning cartridge, remove it from the host application inventory of valid data cartridges.
2. If the cartridge is new, the tape might not be formatted by the cartridge manufacturer. The drive automatically attempts to format the tape. If successful, all other operations to the tape continue without incident and this problem can be closed.
3. On LTO cartridges, the cartridge memory chip might be corrupted. With host application utilities, force a read of the entire tape. When the tape is unloaded, the drive repairs the memory chip corruption. Monitor this cartridge for reoccurrence of a Tape Alert 8. Retire this cartridge if the problem occurs again.

DR047: Resolving Drive TapeAlert 15 - cartridge memory failure

Problem:

A drive determined that a memory in cassette (MIC) failed. This issue reduces performance. The cartridge memory might be repairable.

Troubleshooting Steps:

1. Attempt to repair the cartridge memory by using host backup application utilities to read the entire tape. When the tape is unloaded, the cartridge might be able to repair the tape memory.
2. To verify that the cartridge memory is repaired, attempt to use the cartridge again for normal read/write operations. If this cartridge fails again, retire the cartridge.

DR048: Resolving Drive TapeAlert 16 - forced eject

Problem:

A cartridge was manually ejected from a drive while it was actively reading or writing. This action typically occurs when a user is servicing the drive and did not stop all host operations to the drive.

Troubleshooting Steps:

1. Reload the tape cartridge into the drive.
2. Restart the failed host application.

DR049: Resolving Drive TapeAlert 30, 31 - drive hardware error

Problem:

The tape drive detected an internal hardware error that requires a power cycle of the drive to recover.

Troubleshooting Steps:

1. Stop all additional host operations to this drive.
2. If a cartridge is still mounted in the drive, unload it with the host application or library operator interface.
3. With the local library operator interface, take the drive offline with the **Operations** > **Change Drive Mode** command (on the web client, the path is **Operations** > **Drive** > **Change Mode**).
4. When the drive is offline, the blue LED on the rear of the drive must be turned ON solid blue. Remove the drive completely from the library for at least 1 minute.
5. Reinstall the drive and wait for the normal drive LED states to be established -
   - green flash once per second
   - amber OFF
   - blue ON solid (drive is offline)
6. With the local library operator interface, take the drive online with the **Operations** > **Change Drive Mode** command (on the web client, the path is **Operations** > **Drive** > **Change Mode**).
7. Attempt host operations again. If the drive fails immediately or the problem becomes chronic, contact service.

DR050: Resolving invalid tape location

Problem:

While the inventory is running, the library determines that a cartridge is in an invalid location. In early level libraries that are 23U or taller, the top slot in each of storage columns 4 and 5 cannot be accessed by the robot. Therefore, it cannot be used for cartridge storage. It is likely that this cartridge was placed into the slot manually by a user. The library does not place cartridges into these slots that are based on host or user commands.

Troubleshooting Steps:

1. Select **Details** to determine the bar code label of the cartridge and the coordinate where it is located.
2. Open the main access door and remove this cartridge. Columns 4 and 5 are on the right side of the library as you face it.
3. Close the door and resume operations.

DR051: Resolving library SN label detection

Problem:

The library cannot read one of the module serial number labels but already validated that the bar code scanning system is working properly.

Troubleshooting Steps:

1. Open the main library doors, and look for any obstructions in front of the module serial number bar code labels.
2. If no obvious foreign material is found, the module SN is damaged and the EM or CM must be replaced. The library is still operational, but the replacement must be scheduled as soon as possible.
3. Contact service for possible CM or EM replacement.

DR053: Resolving network configuration issue

Problem:

The library attempted to send an email to the specified address, but encountered an error with the network configuration.

Troubleshooting Steps:

1. Check the email and mail server settings on the library to ensure that all values are correct.
2. Check to make sure that the library is properly connected to the network.
3. Make sure that the network cable is not damaged.
4. If there is no problem with these items, there is a configuration problem with your network. Contact your network administrator for assistance with troubleshooting this issue.

DR054: Resolving open drive bay

Problem:

The library detected that a drive bay was opened in the rear of the library, and a cover plate was not installed. For safety reasons, the robot runs at a slower speed until a drive sled or a drive cover plate is installed.

Troubleshooting Steps:

1. If the cover removal was intentional, reinstall the cover plate to resolve this issue. The robot again moves at full speed.
2. If a drive sled or drive bay cover plate removal was not intentional, check the back of the library for any unsecured drive sleds and loose, missing, or damaged drive bay cover plates.
3. Secure all drive sleds and drive cover plates. Contact service if any drive cover plates are damaged or missing, or drive sleds or cover plates cannot be secured.

DR055: Resolving Installation & Verification Test error

Problem:

A problem was detected while the system validation test is running.

<Description added at runtime>.

Check the IVT logs for further details.

Troubleshooting Steps:

<Description added at runtime>.

1. Close the ticket now.
2. Exit to leave it open for further troubleshooting.
3. Return to the Diagnostic Resolution now.

DR056: Resolving module communication

Problem:

The library encountered an error when it tried to initialize its modules.

Troubleshooting Steps:

1. Turn the library OFF.
2. Remove both the top and bottom terminators and carefully inspect them for bent pins. If any are found, contact service for replacement.
3. Remove all module-to-module connectors and carefully inspect them for bent pins. If any are found, contact service for replacement.
4. If no bent pins are found on any of these parts, contact service for further assistance.

DR068: Resolving incompatible tape drive

Problem:

The installed drive is not compatible with the library.

Troubleshooting Steps:

1. View the ticket details to see which drive is not compatible and remove that drive from the library.
2. Replace the drive cover plate.
3. Contact service for assistance with resolving this issue.

DR069: Resolving drive firmware update failure

Problem:

An attempt to update the firmware of a drive was not successful.

Troubleshooting Steps:

1. Verify that the version that is used for the upgrade is different from what the drive is using. If not, close this ticket and try the upgrade again with the correct firmware version.
2. If the upgrade is completed with a firmware upgrade cartridge, ensure that the cartridge contains the correct firmware for the type and generation of the drive that is updated. Also, check that the firmware upgrade cartridge is not corrupted. If so, close the ticket and upgrade again with the correct firmware upgrade cartridge.
3. If the update was not done with a firmware upgrade cartridge, ensure that the file that contains the firmware image is not corrupted or incomplete. If so, close the ticket and upgrade again with the correct firmware upgrade file.
4. If none of these conditions apply, close this ticket and attempt the upgrade a second time.
5. If this ticket reappears after the upgrade is tried again, contact service for assistance with resolving this issue.

DR070: Resolving tape drive firmware mismatch

Problem:

The library detected that all drives do not have the same firmware version.

Troubleshooting Steps:

1. Go to the **Tools** > **Drive Info** screen on the Control Panel, or **Service Library** > **Update Drive Firmware** on the Web User Interface to view the firmware version that is installed on each drive.
2. Note the drives that do not have the latest version of firmware and upgrade those drives. See “Updating drive firmware” on page 8-25.

DR072: Resolving tape drive auto-level failure

Problem:

The automatic update of drive brick firmware failed. The code image that is stored on the library appears to be invalid.

Troubleshooting Steps:

1. Download a new drive brick firmware image through the Web UI.
2. Close this ticket and reboot the library so that the drive brick upgrade is run again upon initialization.
3. If this ticket reappears, contact service for further assistance.

DR074: Resolving unassigned inaccessible tape cartridge

Problem:

At least one cartridge is detected in a slot that is not assigned to any logical library. It is therefore not accessible by the library or by any host application.

Troubleshooting Steps:

1. Go to the **Monitor System** > **Library Map** screen in the Web User Interface to view the logical library map.
2. Open the main library door and look for cartridges in slots that are not included in any logical library per the Library Map.
3. Manually remove any of these cartridges and, if wanted, insert them back into the library.

DR075: Resolving Installation & Verification Test warning

Problem:

The Installation & Verification Test returned a result that indicated that one of the tests was not successful. The library is still functional and can be used normally. However, this warning might be an indication of a developing problem.

Troubleshooting Steps:

1. Review the ticket details and the Installation & Verification Test logs to determine which library component failed.
2. Check whether any new RAS tickets were generated against the failed component. If so, contact service for further assistance in resolving this issue.
3. Monitor the library for any further problems with this component. If no further RAS tickets are generated, the library can continue to be used normally.

DR076: Resolving GET failure

Problem:

The library robot failed during a move media, while it was trying to get a tape. Operations can continue, but the tape must be manually removed.

Troubleshooting Steps:

1. Open the library main door and inspect the picker for damaged fingers or any other obstruction. If found, remove the obstruction or contact service for picker replacement.
2. View the ticket details for the tape location. Inspect the tape and slot for any damage that might cause the tape to get stuck in the slot. If the tape is damaged, replace the tape with a good one. If the slot is somehow damaged, contact service for replacement.
3. If the tape is in a drive, inspect the drive for any damage that would prevent tape ejection. If found, contact service for drive replacement.
4. If the problem persists, refer to "Contacting IBM technical support" on page 10-21.

DR077: Resolving invalid cleaning tape

Problem:

The system detected that a non-cleaning tape was used to clean a drive.

Troubleshooting Steps:

1. With the bar code listed in the ticket details, locate the tape in the library.
2. If the cartridge is configured for automatic library-initiated cleaning operations, consult your user guide to export a cleaning tape from the library and import a valid cleaning cartridge for future use.
3. If the cleaning tape was configured for application use, consult your user's guide to export the tape cartridge and import a valid cleaning tape for future use.
4. If a manual drive cleaning was completed, replace the tape cartridge with a valid cleaning tape and repeat the drive cleaning operation.

DR078: Resolving tape load/unload failure

Problem:

A tape drive did not load a tape correctly. Library automatic recovery was not successful and user intervention is required.

Troubleshooting Steps:

1. Attempt to unload the tape from the drive with the host backup application that is using the drive, or with the remote or local UI.
2. Open the library main access doors and use the blue pushbutton on the front of the drive to trigger an unload. Press and hold the button continuously for 10 seconds.
3. If the tape is ejected, retrieve it and inspect it for any damage. If found, discontinue use of the tape.
4. If the tape is not ejected, contact service for further assistance in resolving this issue.

DR079: Resolving key server communication issue

Problem:

The library is not able to communicate with a key server. This message does not indicate a problem with the library, but rather a configuration or setup issue.

Troubleshooting Steps:

1. Ensure that the library is properly connected to the network, and that the network cable is not damaged.
2. Ensure that the library's Library Managed Encryption settings are correct. Ensure that the settings contain the correct key server IP address and port number.
3. Verify that the key server is powered ON, operational, and that it is also properly connected to the network.
4. Ensure that the key server's IP configuration is set properly, that the ports are configured correctly, and that they are active. Ensure that the Key Manager is running on the key server.
5. Run the **Service Library** > **Key Path Diagnostics** to help in isolating the problem. This diagnostic procedure consists of four tests:
   a. Drive Test - A drive communication test to ensure that the Library-Drive Interface (LDI) is functioning properly.
   b. Ethernet Test - A key server 'ping' test of all IP addresses associated with LME configured drives.
   c. EKM Path Test - A communication test that is used to establish a link to a key manager. The test ensures that the communication paths between each drive and the EKM are correctly installed and set up.
   d. EKM Config Test - A final test to establish a link to a key manager and request a default key. This test ensures that the drive is correctly configured in the EKM to service key requests
6. If there is no problem with any of these items, there is a configuration problem with your network. Contact your network administrator for assistance with troubleshooting this issue.

DR080: Resolving unreadable branding

Problem:

The library cannot read the module-branding identifier, but already validated that the bar code-scanning system is working properly.

There are two likely scenarios:

1. Line of sight from the scanner to the module-branding label is blocked by foreign material, such as a media bar code label.
2. The module branding label is damaged and the bar code scanner cannot read it reliably.

Troubleshooting Steps:

1. Open the CM main library door. Look for any obstructions in front of the module branding bar code labels.
2. If no obvious foreign material is found, the module branding label is damaged and the CM must be replaced.
3. Contact service for further assistance in resolving this issue.

DR081: Resolving autoclean failure

Problem:

The library's AutoClean feature encountered an error and did not clean a drive.

Troubleshooting Steps:

1. View the **Monitor System** > **Library Map** report to locate the configured cleaning slots.
2. Open the main library door and inspect these cleaning slots. Verify that all the tapes that are occupying the cleaning slots are valid cleaning tapes, particularly the tape with the VOLSER mentioned in the ticket details.
3. This issue might be caused by an error elsewhere in the library. Check for and resolve other unopened RAS tickets.
4. If this ticket persists, contact service for further assistance in resolving this issue.

DR082: Resolving library calibration failure

Problem:

The library encountered a problem during calibration. This ticket can be caused by a blocked or obscured line of sight of the calibration sensor or a damaged white calibration target. This ticket can also be caused by a brightly colored tape cartridge located in a slot immediately above a white I/O station calibration target.

Troubleshooting Steps:

1. Note the ticket details to determine the library module and also any I/O or storage column, or drive location; then close the ticket.
2. If the ticket details identified an I/O station column of a module, complete the following steps -
   a. Ensure the I/O station in the identified module was firmly closed to allow correct calibration.
   b. If it was properly closed, open the I/O station and inspect the white I/O station calibration target for any damage, such as scratches in the white calibration target square.
   c. If no damage is found, inspect the slot above the I/O station calibration target for a brightly colored tape cartridge (yellow or orange). If such brightly colored tape cartridge is present, ignore this ticket and continue.
3. If the ticket details identified a storage location, complete the following steps:
   a. Open the access door that is identified in the ticket details and locate all white calibration targets of the identified storage column and inspect them for any damage.
   b. If no damage is found, open the bottom main access door of the module and gently move the picker assembly towards the door opening. Then, rotate it gently as far clockwise as possible.
   c. Open and fully extend the bottom I/O station door, then reach through the main access door. Locate the picker assembly recessed calibration sensor in the picker base, slightly to the right of the center line. Gently wipe the surface of the calibration sensor with a soft, lint-free cloth.
4. If the ticket details identify a drive sled, remove the identified drive and inspect the calibration bracket horizontal white stripe for any damage.

Note: This graphic shows the location of the calibration sensor. If you are guiding a customer by phone, you might want to copy the graphic and email it to them.

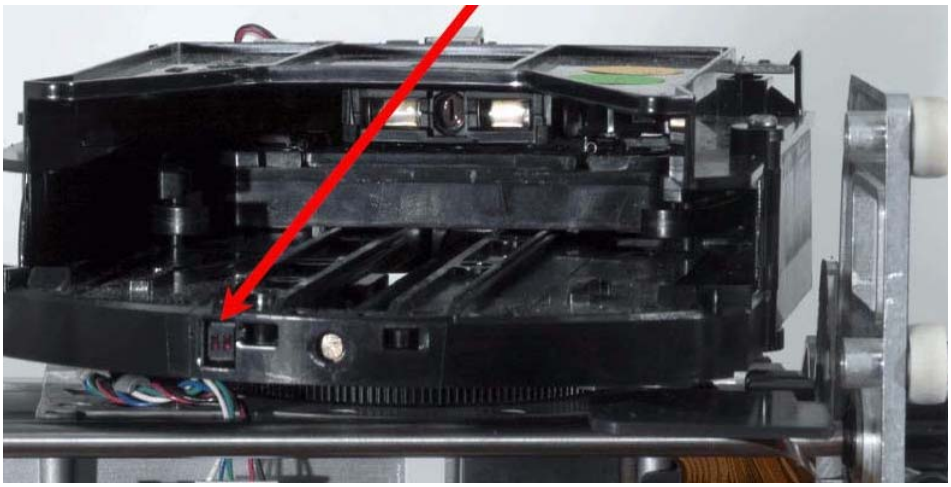


Figure 11-2. Calibration sensor

DR083: Resolving drive voltage problem

Problem:

A tape drive detected a voltage problem. This problem can occur when a separate drive is activated.

Troubleshooting Steps:

1. Close this ticket, then remove and reinsert the drive sled to clear the fault.
2. If this ticket recurs, ensure that the facility AC power cable is secured to the power supplies. Ensure that no fault condition is indicated on the power supply LEDs. If a fault is present, contact service for possible power supply replacement.
3. If no power supply faults are indicated, and this ticket recurs against the same drive, contact service for possible drive replacement.

DR084: Resolving robotics firmware image error

Problem:

The normal robotics firmware auto-level process was not attempted. This problem is caused by a missing or corrupted robotics firmware update file.

Troubleshooting Steps:

1. Close this ticket, then run a library firmware upgrade to the current firmware revision.
2. If this ticket recurs following the library firmware upgrade, contact service for more diagnostic steps.

DR085: Resolving robotics auto-level failure

Problem:

The normal robotics firmware auto-level process did not complete successfully. This problem can be caused by one of the following conditions -

1. A robotics flash image failed validation by the Y-axis/picker assembly Controller Board.
2. A flash programming error occurred on the Y-axis/picker assembly Controller Board.
3. An error occurred when the picker imager flash was updated.

Troubleshooting Steps:

1. View the ticket details and note which firmware image failed.
2. Close this ticket.
3. Try the auto-level process again by reinitializing the robot (open and close the main access door).
4. If this ticket recurs during the retry, continue to Step 5. Otherwise, no further action is required.
5. If 'Robot' firmware is identified in Step 1, contact service for Y-axis picker assembly Controller Board replacement. If 'Imager' firmware is identified in Step 1, contact service for picker assembly replacement.
6. Close this ticket, then run a library firmware upgrade to the current firmware revision.
7. If this ticket recurs following the library firmware upgrade, contact service for more diagnostic steps.

DR086: Resolving robotics degraded flash warning

Problem:

One of the Y-axis/picker assembly's flash partitions was not updated. Because one of the two flash partitions is properly functioning, auto-level can still occur and the robotics subsystem can go ready. This is a Warning ticket. Flash is in a degraded mode and the backup image is unavailable.Service must be contacted as soon as possible.

Troubleshooting Steps:

1. Contact service for Y-axis/picker assembly replacement.
2. Close this ticket and monitor for recurrence.

DR088: Resolving robotics Y-axis motion failure

Problem:

The library robot failed to complete a motion in the Y-axis. The detected failure is likely to be a genuine hardware failure.

Troubleshooting Steps:

1. Open the main access door and look for any obvious problems such as damage to the robot assembly, or tape cartridges and debris that collected on the floor of the library.
2. Reposition any tape cartridges found extending from storage locations.
3. Remove any tape cartridges that are found in the picker assembly.
4. Inspect any recovered tape cartridges for damage.
5. Close the doors and wait for the system to complete initialization. Use the **Tools** > **Service** > **Library** > **Robot** test to determine whether the failure is permanent.
6. If the test fails, contact service for robot assembly replacement.
7. If the test passes, continue to close this Ticket.
8. Make sure that the logical libraries are online and continue normal library operations. Monitor for recurrence of the problem.

DR089: Resolving X, Z, Theta axis motion failure

Problem:

The library robot failed to complete a motion in the X, Z, or Theta axis. The detected failure is likely to be a genuine hardware failure.

Troubleshooting Steps:

1. Open the main access door and look for any obvious problems such as damage to the robot assembly, or tape cartridges and debris that collected on the floor of the library.
2. Reposition any tape cartridges found extending from storage locations.
3. Remove any tape cartridges that are found in the picker assembly.
4. Inspect any recovered tape cartridges for damage.
5. Close the doors and wait for the system to complete initialization. Use the **Tools** > **Service** > **Library** > **Robot** test to determine whether the failure is permanent.
6. If the test fails, contact service for robot assembly replacement.
7. If the test passes, continue to close this Ticket.
8. Make sure that the logical libraries are online and continue normal library operations. Monitor for recurrence of the problem.

DR090: Resolving robotics hardware error - RCB

Problem:

Robotics firmware reported a specific hardware error that identifies the Robot Controller Board as the failed component. This problem might be caused by an electrical hardware failure.

Troubleshooting Steps:

1. Close this ticket and reinitialize the robot by opening and closing the main access door.
2. If this ticket recurs after the robot reinitializes, contact service for Y-axis/picker assembly replacement.

DR091: Resolving robotics hardware error - picker

Problem:

The robotics firmware reported a specific hardware error that identifies the picker assembly as the failed component. This problem might be caused by an electrical hardware failure at the picker assembly or at the Robot Controller Board.

Troubleshooting Steps:

1. Close this ticket and reinitialize the robot by opening and closing the main access door.
2. If this ticket recurs after the robot reinitializes, contact service for picker assembly replacement.

DR092: Resolving robotics hardware error - scanner

Problem:

The robotics firmware reported a specific hardware error that identifies the robot scanner as the failed component. This problem might be caused by one or more of the following conditions.

1. An obstruction in the viewing path of the robot scanner.
2. Electrical hardware failure at the picker assembly or at the Robot Controller Board.

Troubleshooting Steps:

1. Open the main access door and check for any obvious obstruction that is blocking the view of the robot scanner.
2. Close this ticket and reinitialize the robot by opening and closing the main access door.
3. If this ticket recurs after the robot reinitializes, contact service for robot controller board or picker assembly replacement.

DR093: Resolving robotics communication error

Problem:

The library firmware detected a communication failure with the robotics subsystem. This problem might be caused by one or more of the following conditions:

1. Power loss to the robot assembly.
2. Y-axis Cable Spool or connection failure.
3. Electrical hardware failure.

Troubleshooting Steps:

1. Ensure that the main access doors are closed.
2. Ensure that all module terminators and Box to Box cables are properly connected.
3. Determine the robot location within the system. Then, open the I/O station closest to the robot position to determine whether the green LED on top of the picker is on.
4. If the picker LED is not on, open the main access door and verify that the Y-axis Cable Spool is properly attached and not damaged.
5. Close this ticket and reinitialize the robot by opening and closing the main access door.
6. If this ticket recurs after the robot reinitializes, contact service for further assistance.

DR094: Resolving incompatible robot installed

Problem:

The library firmware detected that an incompatible robot was installed. This problem occurs when a robot assembly was replaced with an incorrect type.

Troubleshooting Steps:

1. Replace the installed robot assembly with the required, originally installed, robot assembly model type.
2. Call service for complete robot assembly replacement that includes -
   - Robot Controller Board
   - Y- carriage assembly
   - Picker assembly

DR095: Resolving drive sled auto-level failure

Problem:

The library is not able to auto-level any of the drive sleds. This problem might be caused by a missing or corrupted firmware update image file.

Troubleshooting Steps:

1. Close this ticket and run a library firmware upgrade to the current production firmware revision.
2. If this ticket recurs following the library firmware upgrade, contact service for more diagnostic steps.

DR096: Resolving drive cleaning failure

Problem:

After the drive was cleaned and the cleaning tape was removed from the drive, the drive continues to request drive cleaning. This issue can indicate a problem with the drive.

Troubleshooting Steps:

1. Close this ticket and run a manual drive cleaning with a different cleaning tape.
2. If this ticket recurs following the manual cleaning, take the drive offline.
3. Contact service for more diagnostic steps.
   Note: The drive must not be used for read/write operations because continued cleaning requests can exhaust the cleaning tape supply.

DR098: Resolving hardware clock failure

Problem:

The library firmware detected that the hardware clock (RTC) failed. The library system time might appear to be set correctly, but accurate time is lost following a power cycle or reboot.

Troubleshooting Steps:

1. The hardware clock (RTC) is part of the LCB hardware. Call service for replacement of the LCB.

DR099: Resolving bar code label mapping

Problem:

There was a bar code scanning error that is detected during an attempt to inventory the library. There are two possible scenarios -

1. Improper application of bar code labels.
2. Magazines improperly seated.

Troubleshooting Steps:

1. Verify that all library and tape bar code labels are properly attached and that no overlapping bar code labels are visible.
2. Ensure that all magazines are properly installed and that all bar code labels are visible.
3. Open and then close the access door to cause the library to run another inventory.
4. If the problem persists after the library attempts to re-inventory, then contact service for more diagnostic steps.

DR100: Resolving bar code scanner malfunction

Problem:

The bar code scanner is communicating properly but cannot read any bar codes. There are two likely scenarios -

1. Line of sight from the scanner to the module branding label is blocked by foreign material such as a media bar code label.
2. The bar code scanner is damaged and the Y-axis/picker assembly must be replaced.

1)

Troubleshooting Steps:

1. Open the library door to gain access to the robot. Look for any obstructions in front of the bar code scanner (inside the mouth of the picker).
2. If no foreign material is found, the bar code scanner is damaged and the Y-axis/picker assembly must be replaced. Contact service for assistance with Y-axis/picker assembly replacement.

DR101: Resolving tape drive type change

Problem:

The library firmware detected that a tape drive assigned to a partition is replaced with a tape drive of a different type. A tape drive's type is defined by its vendor, generation, and interface. Complete one of the following options to activate the new tape drive.

Troubleshooting Steps:

- Replace the new tape drive with one that is of the exact type as the original tape drive.

OR

- Remove the original tape drive from the partition's configuration, then add the new tape drive to the partition's configuration. To do this procedure, follow these steps:
  1. From the main menu, select **Manage Library** > **Logical Libraries**.
  2. From the `Logical Libraries` menu, select the partition to be modified. Select **Modify** from the drop-down selection list, then select **Go**.
  3. From the `Modify Logical Library` menu, click the **Select Drives to Assign to Logical library** link. Clear the original tape drive from the drives list and select **Apply**.
  4. From the `Modify Logical Library` menu, click the **Select Drives to Assign to Logical library** link. Select the new tape drive from the drives list and select **Apply**.

DR102: Resolving robotics Z-axis motion failure

Problem:

The library Y-axis/picker assembly failed to complete a motion in the Z-axis. The detected failure is likely to be a genuine hardware failure.

Troubleshooting Steps:

1. Open the main access door and look for any obvious problems such as unplugged cables or damage to the picker.
2. Remove any tape cartridges from the picker or the path of Y-axis/picker assembly motion. Close the doors and wait for the system to complete initialization.
3. Use the **Tools** > **Service** > **Library** > **Robot** test to determine whether the failure is permanent.
4. If the test fails, contact service for hardware replacement. If the test passes, monitor for reoccurrence.

DR103: Resolving display assembly communication failure

Problem:

A problem is detected and isolated to a communication link failure to the library's local display assembly. The nature of the problem indicates that replacement of the display assembly might be required. Your library can remain operational from the remote browser interface.

Troubleshooting Steps:

1. If this ticket and T064 - LCB hardware failure are generated within a few minutes of each other, the problem lies with one of the power supplies in the CM. Contact service for replacement of a power supply.
2. Examine all cabling at the back of the display assembly and within the CM for correct connectivity. Inspect for damage.
3. If no cabling problems are found, and no concurrent tickets are posted against the LCB, contact service for replacement of the display assembly.

DR106 - Resolving media security notification

Problem: The library is configured to inform of unexpected cartridge removal, expected tape cartridge removal or both:

- Media removal is expected whenever an exported cartridge was physically removed by an operator from an I/O area element.
- Media removal is not expected if a cartridge was previously detected in a storage, drive, or I/O element without being exported or moved by the robot to a respective I/E area element for operator access and removal.

Troubleshooting Steps:

- If the media removal was expected, I/O area elements might be available for operator initiated cartridge insert operations, import operations or both.
- If the media removal was unexpected, cartridge removal authorization might need to be validated.

1. To view which cartridges are removed, go to **Service Library** > **Media Security Log** and select **Media Security Log**.
2. You have three options:
   - Select **Close** to close the operator intervention.
   - Select **Exit** to leave the operator intervention open for future troubleshooting.
   - Select **Back** to return to the Diagnostic Resolution.

DR110: Resolving drive encryption control failure

Problem:

A tape drive reported that the requested drive encryption method cannot be enabled.

Troubleshooting Steps:

1. Note the drive sled coordinate from the RAS ticket and close the ticket.
2. Make sure that the referenced tape drive is not loaded with a tape cartridge. Unload the drive if a tape cartridge is present.
3. Verify that the tape drive firmware version is at least at the firmware version that is referenced in the release notes for the currently installed library firmware version. Update the tape drive firmware if a newer version is required.
4. Consult your user documentation about removal and replacement of a drive sled.
5. Remove the drive sled identified in the RAS ticket, wait for 1 minute, and then reinsert and secure the same drive sled into its drive bay location.
6. Wait for the drive to initialize and become ready.
7. Make sure that the logical library partition is configured for the correct encryption method and no RAS ticket is generated against the drive.
8. From the remote user interface, view the library configuration by selecting **Reports** > **Library Configuration**.
9. Click the respective drive coordinate and verify the drive encryption method setting.
10. Contact service if an issue remains.
11. Choose one of the following options -
    - Select **Close** to close the ticket now.
    - Select **Exit** to leave the ticket open for future troubleshooting.
    - Select **Back** to return to the Diagnostic Resolution.

DR111: Resolving drive encryption service request monitoring

Problem:

A tape drive reported that an encryption request needed to be serviced, but the drive did not indicate required encryption key request details. The drive sled controller suspended encryption key exchange request monitoring until the tape cartridge is unloaded.

Troubleshooting Steps:

1. Note the drive sled coordinate from the RAS ticket and close the ticket.
2. Unload the tape cartridge from the drive.
3. Reload the tape cartridge and restart the host application.
4. If the RAS ticket opens again, close the ticket and unload the drive.
5. Consult your user documentation to reset the drive.
6. When the drive is operational again, reload the tape cartridge and restart the host application.
7. If the problem persists, contact service for further assistance.
8. Choose one of the following options:
    - Select **Close** to close the ticket now.
    - Select **Exit** to leave the ticket open for future troubleshooting.
    - Select **Back** to return to the Diagnostic Resolution.

DR118 - Resolving EKM path diagnostic delay

This diagnostic resolution provides customer resolution steps for “T149 - Key path diagnostic delay” on page 11-59.

Problem	The library attempted to run a Key Path Diagnostic test with an available encryption-capable tape drive per the test interval setting. However, all configured tape drives are either loaded, unavailable, or otherwise busy. They cannot initiate the Key Path Diagnostic test to determine correct EKM server connectivity and operability.

Troubleshooting Steps	1. View the operator intervention details to determine which EKM server cannot be tested because the drives are not available to initiate a Key Path Diagnostic test. 2. Determine whether all tape drives that are configured for such EKM server access are currently mounted or otherwise unavailable and therefore cannot initiate a Key Path Diagnostic test. 3. If none of the configured tape drives are available to initiate a Key Path Diagnostic test, ignore and close this operator intervention. If applicable, configure the testing interval time or warning threshold to a less frequent testing period to avoid drive access contention and operator intervention generation. 4. If a tape drive is available to initiate a test, consult your user documentation to initiate a Key Path Diagnostic test: a. If the test succeeds, close this operator intervention and observe for further occurrences. b. If the test fails, analyze the issue and correct the problem or contact service for further assistance. 5. You have three options: • Select **Close** to close the operator intervention. • Select **Exit** to leave the operator intervention open for future troubleshooting. • Select **Back** to return to the Diagnostic Resolution.

Chapter 12. Adding, removing, and replacing procedures

Important: This library has Tier 1 CRUs (customer replaceable units). The drive sled and the power supply are Tier 1 CRUs. These CRUs are parts of the library that must be added, removed, and replaced by the customer. If a customer chooses to have the CRU added or removed/replaced by an IBM service representative, there is a charge for the service.

Before a replacement CRU is ordered, ensure that the following criteria is met:

- The failure is repeatable.
- A memory dump is captured for emailing to IBM Service.
  - Use the ITDT tool for drive memory dumps.
  - Use the Web User Interface (**Service Library** > **Capture Log**) for library memory dumps.

Required library state

Adding, removing, and replacing library components usually requires you to power OFF the entire library. There are a few components, however, that you can service without powering OFF the library. Instead, you might need to take only a certain logical library offline or you might not need to impact the status of the library at all.

Use the following table to determine the state that the library must be in before you service it.

Table 12-1. Library state required when library components are serviced

Library Component	Required Library State
Library Control Blade	Power OFF

Table 12-1. Library state required when library components are serviced (continued)

Library Component	Required Library State
Power Supply	ON/Normal
Storage Column	Power OFF
Drive	Power ON
Ethernet Expansion Blade (EEB)	Power OFF

Required tools

Servicing the library requires the following tools:

- T10 TORX screwdriver with a static safe handle
- #1 and #2 Philips screwdrivers
- Small flat blade screwdriver
- Electrostatic Discharge (ESD) kit (P/N 93F2649)
- Safety glasses

Electrostatic discharge

Important: A discharge of static electricity can damage static-sensitive devices or microcircuitry. Correct packaging and grounding techniques are necessary precautions to prevent damage.

To prevent electrostatic damage, observe the following precautions:

- Transport products in static-safe containers such as conductive tubes, bags, or boxes.
- Keep electrostatic-sensitive parts in their containers until they arrive at static-free stations.
- Cover the unit with approved static-dissipating material. If available, provide a ground strap that is connected to the work surface and properly grounded tools and equipment. If a ground strap is not available, touch a metal surface to discharge any static electricity in your body.
- Keep the work area free of non-conducting materials, such as ordinary plastic assembly aids and foam packing.
- Make sure that you are always properly grounded when you touch a static-sensitive component or assembly.
- Avoid touching pins, wires, or circuitry.
- Use conductive field service tools.

Preparing a library or library module for repairs

1. Ensure that all drives are empty.
2. Power OFF the library.
   - If the library is idle:
     a. Press **Power** on the front panel of the control module.
     b. Toggle each power supply switch to the OFF (O) position.
   - If the library is processing:
     a. From the Operator Panel, select **Operations** > **Shutdown** to end the current library task and shut down the library 's operating system.

b. When the library becomes idle, press **Power** on the front panel of the control module.
c. Toggle each power supply switch to the OFF (O) position.

Returning a library or library module to normal operations after repairs

1. Power ON the library.
   a. Toggle each power supply switch to the ON (|) position.
   b. Press **Power** on the front of the library.
2. If necessary, replace all tape cartridges in the library or library module.
3. If necessary, vary drives and logical libraries online.

Removing/replacing a control module

The control module enclosure (chassis) is not available as a FRU. If the Service Action Ticket (T code) or Diagnostic Resolution procedure specifies replacement of the enclosure, it is necessary to replace the internal cables and boards kit instead.

To make repairs to a control module, choose and complete one of these procedures:

- "Removing a 5U library (control module) from a rack"
- "Replacing a 5U library (control module) in a rack"
- "Removing a control module from a stand-alone or rack-mounted library (14U or larger)" on page 12-4
- "Replacing a control module in a stand-alone or rack-mounted library (14U or larger)" on page 12-9

Removing a 5U library (control module) from a rack

1. Complete "Preparing a library or library module for repairs" on page 12-2.
2. Unplug the customer-supplied ethernet cable from the Library Control Blade (**2** in Figure 12-27 on page 12-29).
3. Remove these components from the control module to reduce the weight of the module.
   a. Power supplies (see "Removing/replacing a power supply (primary and redundant)" on page 12-34)
   b. Drive sleds (see "Adding/removing/replacing a tape drive" on page 12-24)
4. Loosen the thumb screws that secure the library to the rear flange on each rack kit rail.
5. Open the I/O station door, then the access door on the control module.
6. From the front of the control module, remove the rack ears (see "Removing the rack ears" on page 12-16).
7. With a person standing on each side of the library, pull the control module out of the rack.
8. Place the library on a sturdy work surface.

Replacing a 5U library (control module) in a rack

1. With a person on each side of the library, pick it up from the work surface and slide it onto the rack kit rails of your rack.
2. Tighten the thumb screws that secure the library to the rear flange of each rack kit rail.

3. Install the rack ears on the front of the library to secure it to the rack (see "Replacing the rack ears" on page 12-17.
4. Reconnect the customer-supplied ethernet cable to the Library Control Blade (**2** in Figure 12-27 on page 12-29).
5. Reinstall the following components that are removed for weight reduction.
   a. Drive sleds (see "Adding/removing/replacing a tape drive" on page 12-24)
   b. Power supplies (see "Removing/replacing a power supply (primary and redundant)" on page 12-34)
6. Complete "Returning a library or library module to normal operations after repairs" on page 12-3.

Removing a control module from a stand-alone or rack-mounted library (14U or larger)

1. Perform "Preparing a library or library module for repairs" on page 12-2.

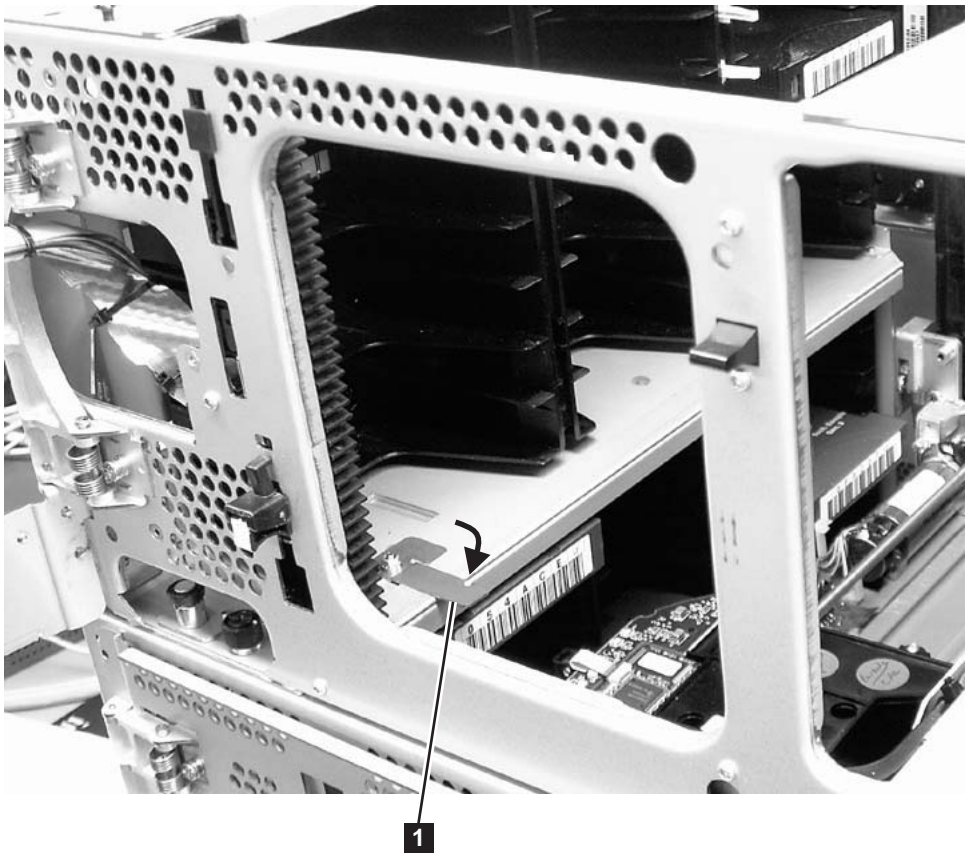


Figure 12-1. Picker locking mechanism

2. Move the Picker into the control module.
   a. Gently push the Picker up until it is in the control module.
   b. Engage the Picker locking mechanism (**1** in Figure 12-1).

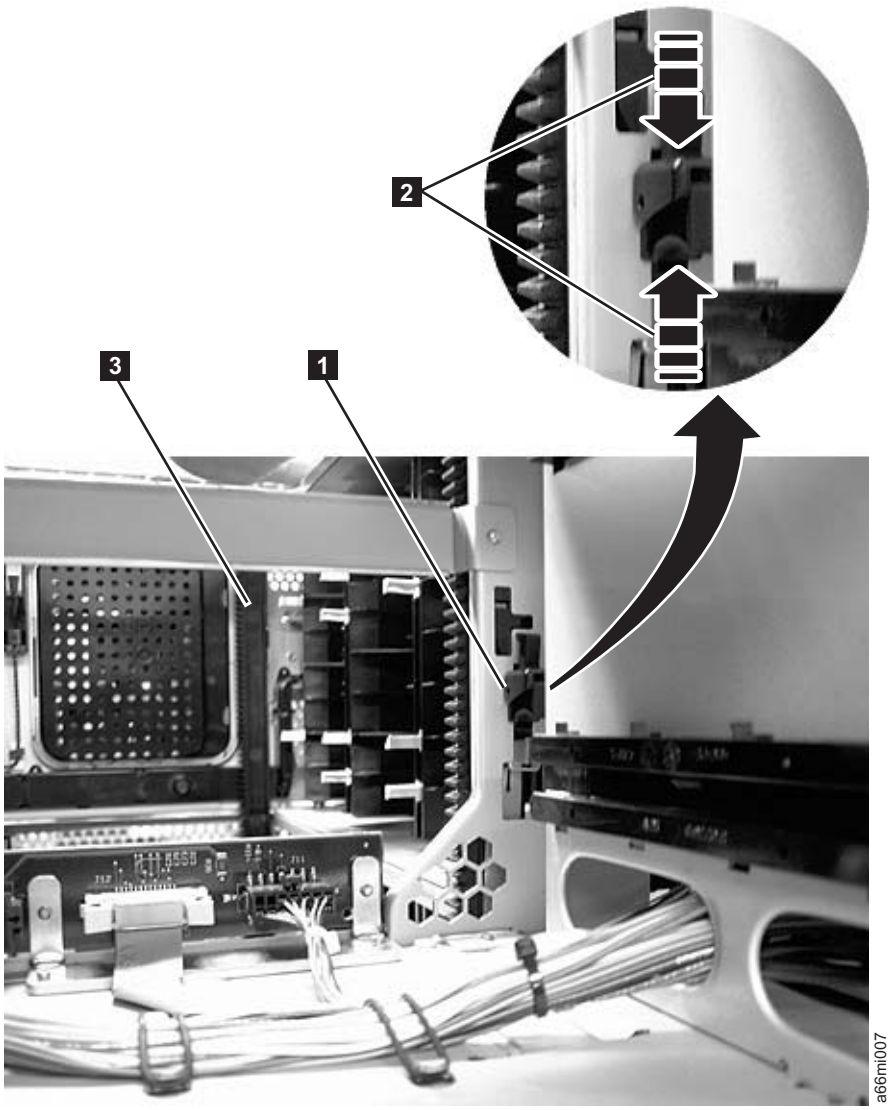


Figure 12-2. Gear racks and gear rack locking mechanism

3. Disengage the rear (**1** in Figure 12-2) and front (**3** in Figure 12-2) gear racks in the control module. While pinching the gear rack locking mechanism (**2** in Figure 12-2), push the gear rack up until it locks in place. To release the gear rack and move it up, perform the following steps.

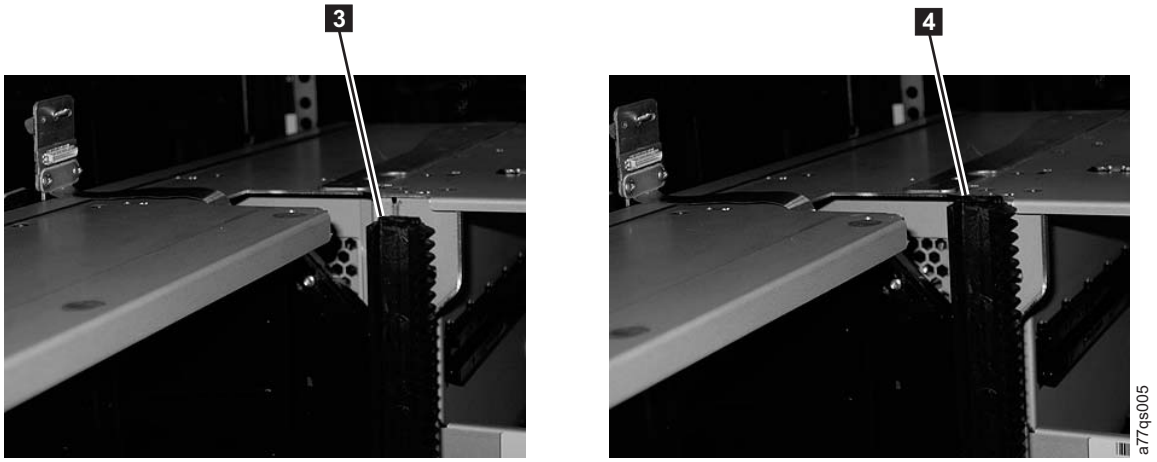


Figure 12-3. Gear racks in the up and down positions

a. Disengage the Y-rails so the module can be unstacked safely.

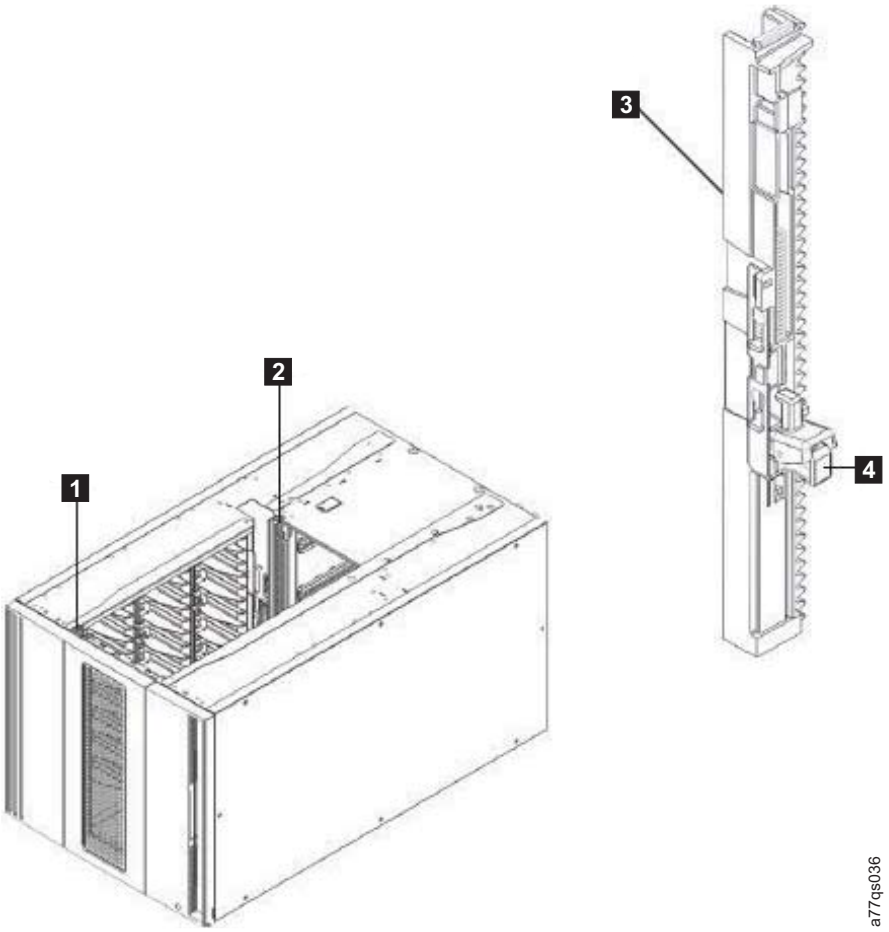


Figure 12-4. Placing gear rack in Up position

1	Front Y-rail	3	Y-rail (this end up)
2	Rear Y-rail	4	Squeeze here to release

b. From the front of the library, find the Y-rail release mechanism, which is located on the left side of the control module. Squeeze the handle of the Y-rail release mechanism, lift it, and release it so it locks in place.

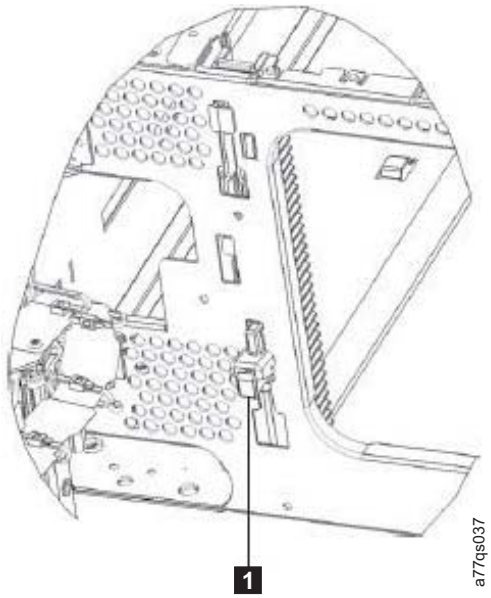


Figure 12-5. Releasing the Y-rail

1 Y-rail in unlocked, functional position

c. From the rear of the library, find the rear Y-rail release mechanism located in the interior of the right side of the module. Squeeze the handle of the Y-rail release mechanism, lift it, and release it so that it locks in place.

4. Unplug the customer-supplied Ethernet cable from the Library Control Blade (**2** in Figure 12-27 on page 12-29).
5. Unplug the module-to-module communication cable from the control module (**4** in Figure 12-27 on page 12-29).
6. Remove the following components from the control module to reduce the weight of the module.
   a. Power supplies (see "Removing/replacing a power supply (primary and redundant)" on page 12-34).
   b. Drive sleds (see "Adding/removing/replacing a tape drive" on page 12-24).

      Note: If not already done, remove all tape cartridges from the module being removed.

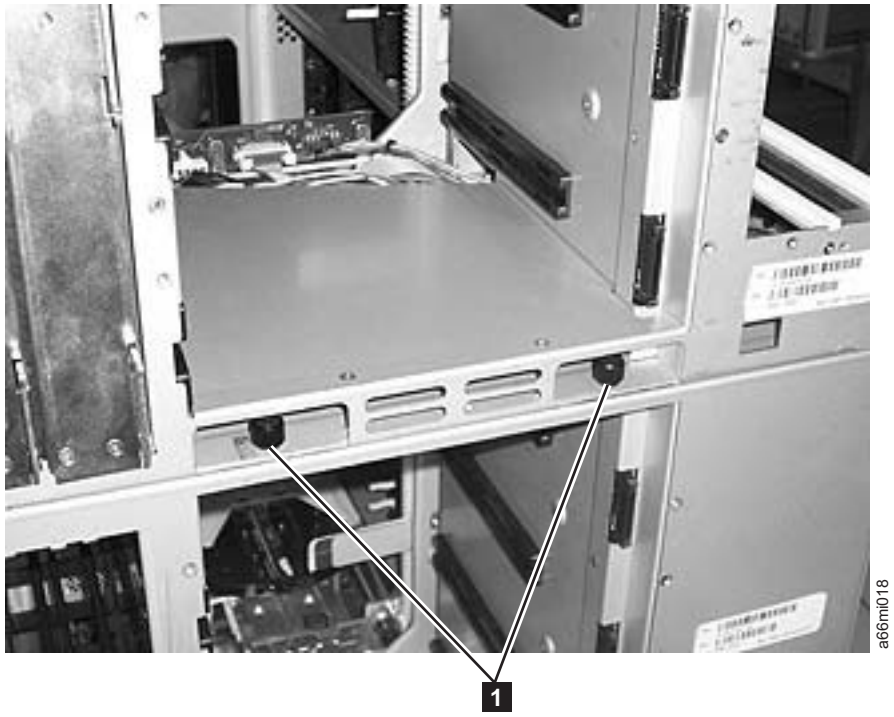


Figure 12-6. Control module rear thumb screws

7. Loosen the rear thumb screws (**1** in Figure 12-6) securing the control module to the lower expansion module.
8. If your library is installed in a rack, remove the rack ears (see "Removing the rack ears" on page 12-16) from the front of the control module.

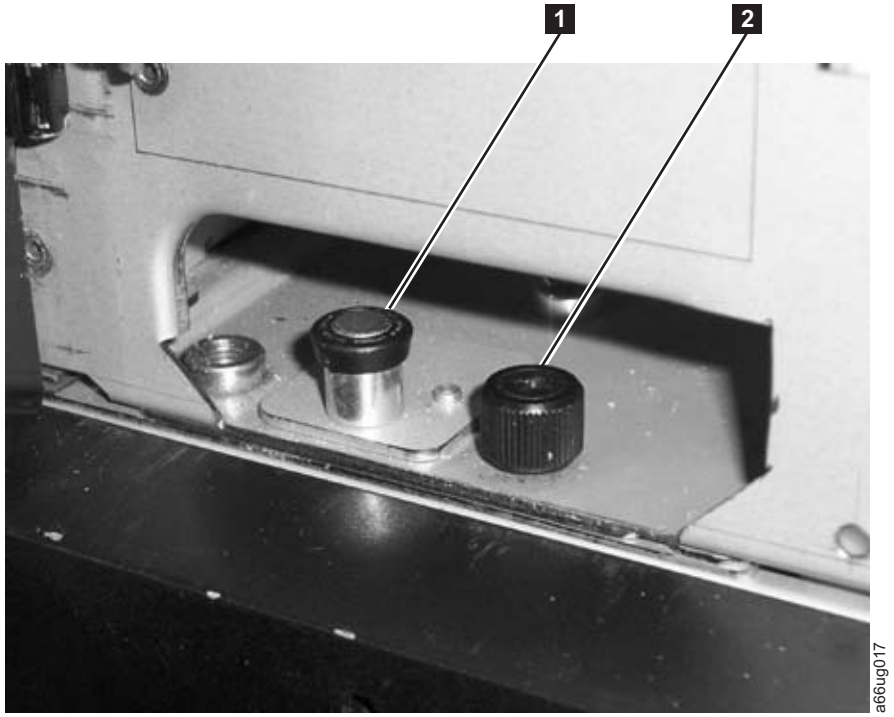


Figure 12-7. Alignment pin and front thumb screw

9. Open the I/O Station door, then open the Access Door of the control module to expose the control module alignment pin (1 in Figure 12-7 on page 12-8) and front thumb screws (2 in Figure 12-7 on page 12-8) behind the Access Door and behind the I/O Station door.
10. Loosen the front thumb screws.
11. Lift and rotate the control module alignment pin to lock the pin in an up position.
12. With a person standing on each side of the control module, pull it out of the rack.
13. Place the control module on a sturdy work surface.

Replacing a control module in a stand-alone or rack-mounted library (14U or larger)

1. Ensure that the front and rear gear racks are in the upper position (see 2 in Figure 12-8).

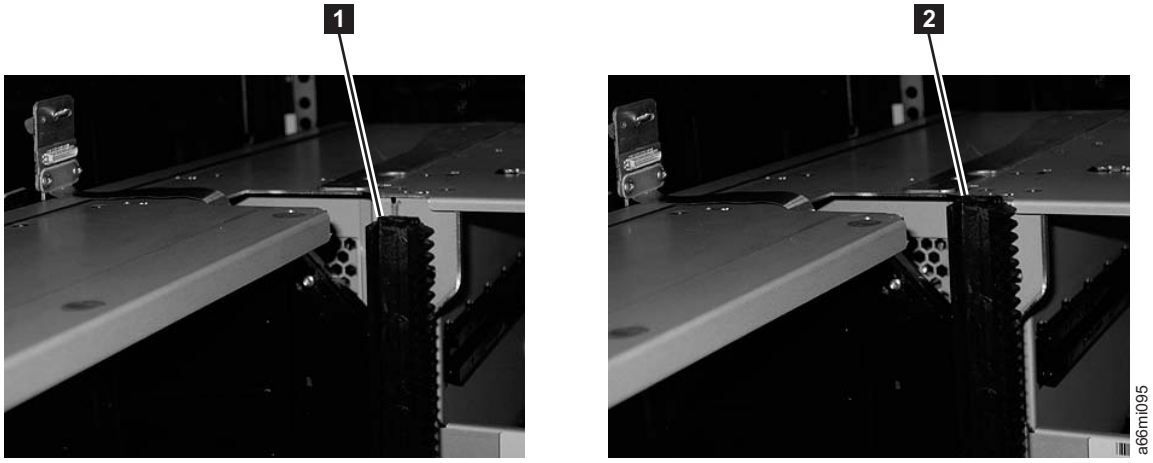


Figure 12-8. Gear racks (down and up)

2. Ensure that the module-to-module alignment pin (1 in Figure 12-7 on page 12-8) is in the raised position. If necessary, raise the pin and rotate it half a turn to lock it in the raised position.
3. With a person on each side of the control module, pick up the control module from the work surface and slide it partway onto the expansion module in the rack along the guide slots on the top of the expansion module and the bottom of the control module.

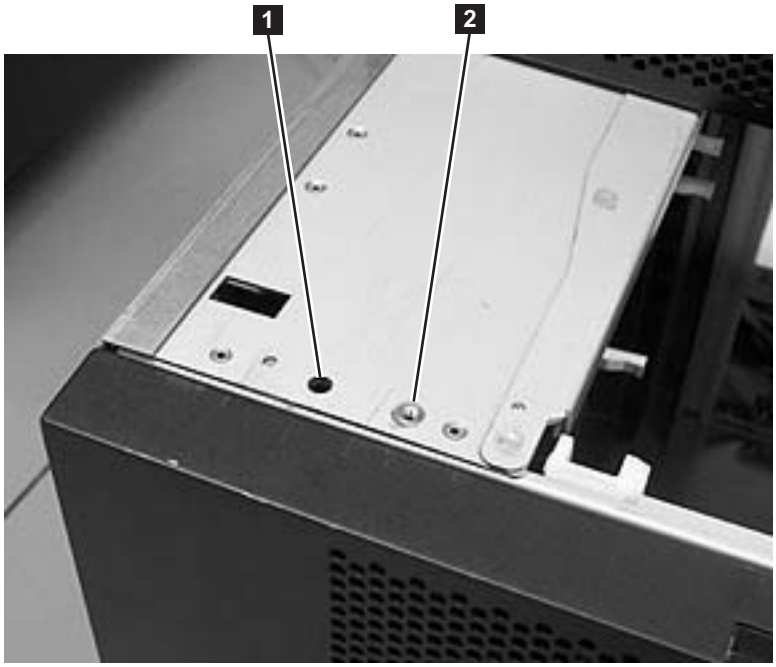


Figure 12-9. Alignment pin and front thumb screw receptacles

4. Open the I/O station door, then open the access door of the control module to expose the control module alignment pin behind the access door.
5. Push the control module onto the lower expansion module.
6. Twist the control module alignment pin (**1** in Figure 12-7 on page 12-8) to unlock it from the up position.
7. Adjust the control module 's position on top of the expansion module until the control module alignment pin drops into the alignment pin receptacle (**1** in Figure 12-9) in the lower expansion module.
8. Tighten the front thumb screw (**2** in Figure 12-7 on page 12-8) to secure the front of the control module to the lower expansion module (**2** in Figure 12-9).
9. Open the I/O station door and tighten the other front thumb screw.

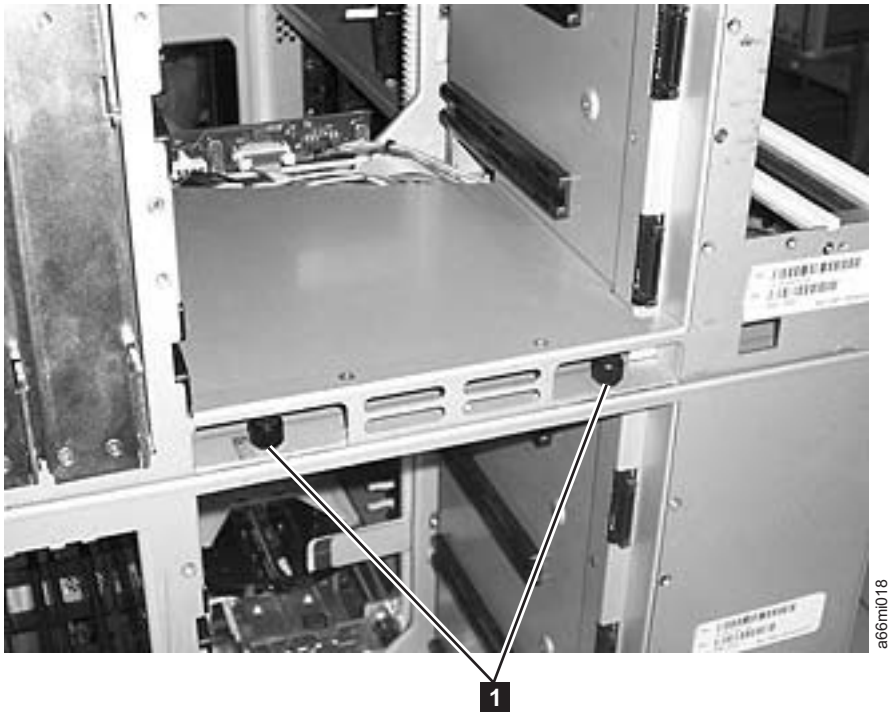


Figure 12-10. Control module rear thumb screws

10. Tighten the rear thumb screws (**1** in Figure 12-10) that secure the control module to the lower expansion module.
11. If your library is installed in a rack, reinstall the rack ears on the front of the control module to secure it to the rack (see "Replacing the rack ears" on page 12-17).

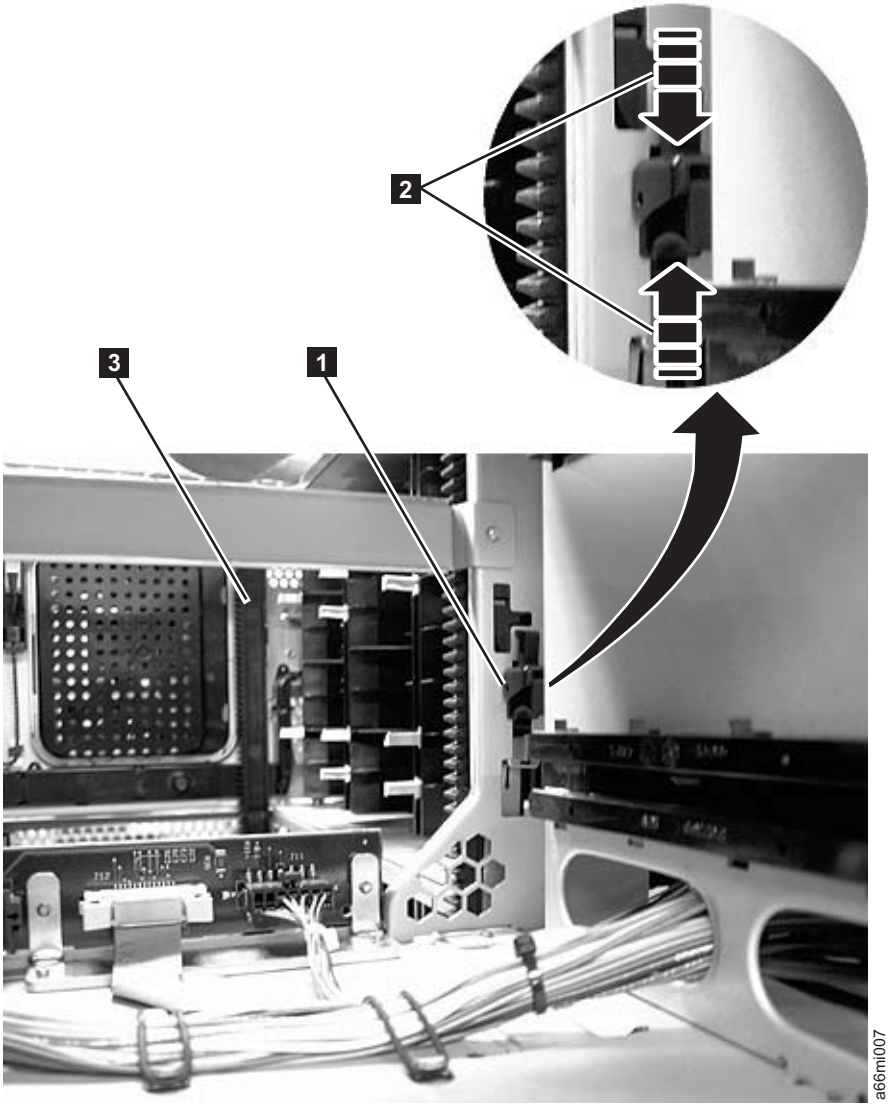


Figure 12-11. Gear racks and gear rack locking mechanism

Important: If the control module is at the bottom of the library, the gear racks should remain locked in the UP position. Skip step 12 and step 13 if the control module is at the bottom of the library. If the control module is not at the bottom of the library, complete step 12 and step 13.

12. Engage the rear (**1** in Figure 12-11) and front (**3** in Figure 12-11) gear racks in the control module. While pinching the gear rack locking mechanism (**2** in Figure 12-11), push the gear rack down until it locks in place and no gaps appear between the front and rear gear racks in the control module and expansion module.
13. To release the gear rack and move it down, follow these steps.
    - Engage the Y-rails of each module in your library configuration. Ensure that the Y-rails are properly aligned and the thumbscrews are tightened.

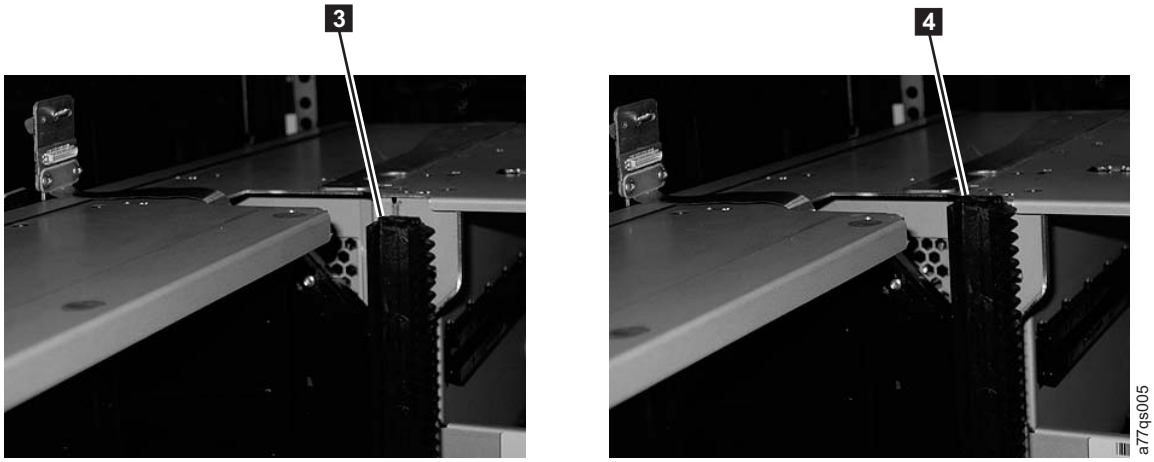


Figure 12-12. Gear racks in the up and down positions

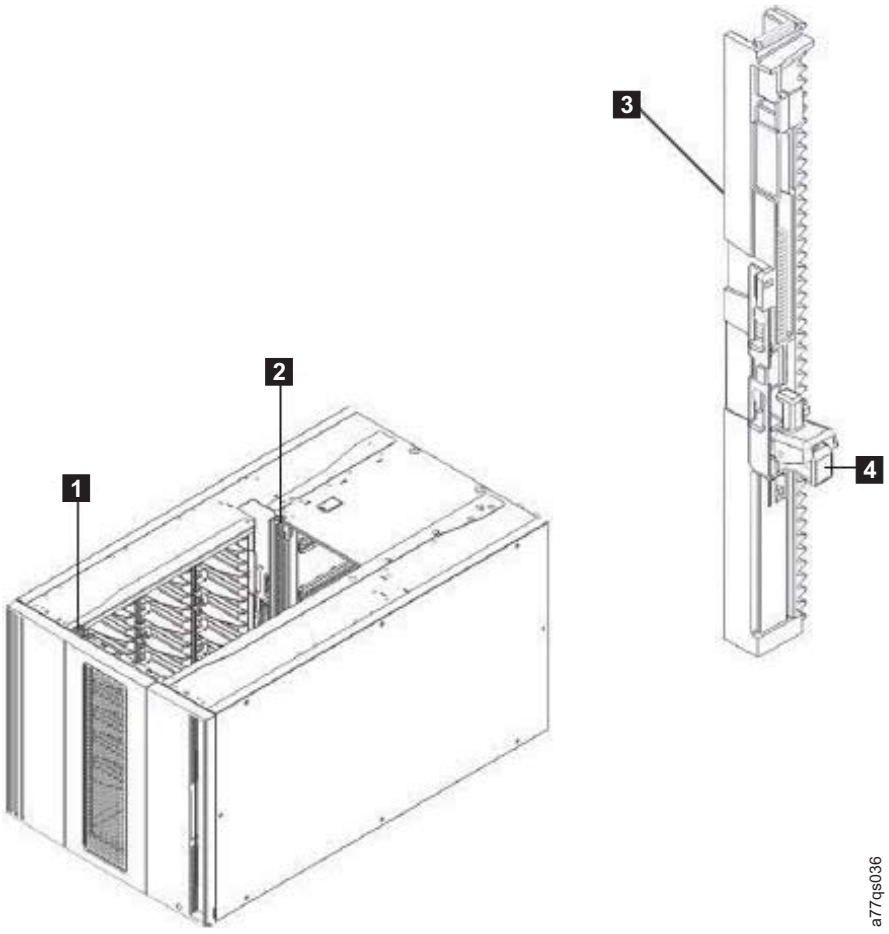


Figure 12-13. Placing gear rack in the Down position

1	Front Y-rail	3	Y-rail (this end up)
2	Rear Y-rail	4	Squeeze here to release

- From the front of the library, open the I/O station and access door of the 9U expansion module. Squeeze the handle of the Y-rail release mechanism,

lift it out of its locked position, and slide it downward as far as it goes.

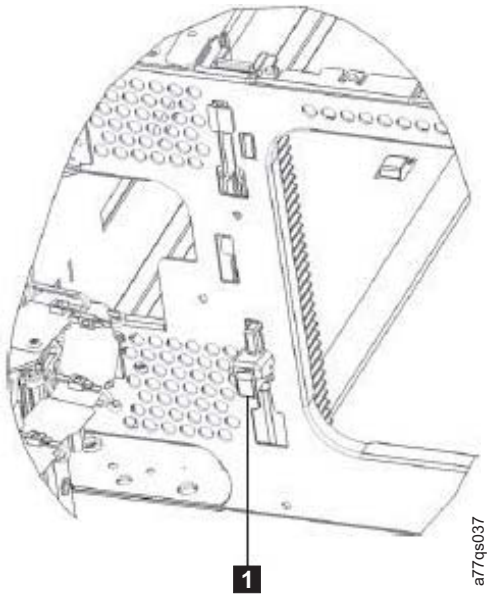


Figure 12-14. Releasing the Y-rail

1 Y-rail in unlocked, functional position

- From the back of the library, find the rear Y-rail release mechanism, which is in the interior of the right side of the module. Squeeze the handle of the Y-rail release mechanism, lift it out of its locked position, and slide it downward as far as it goes. Doing this procedure aligns the Y-rails with the Y-rails of the module beneath it.

  CAUTION:
  Ensure that there is no gap between the top and bottom Y-rails on both the front and back of the library. If a gap exists, the library cannot mechanically initialize.

14. Gently push the picker assembly up high enough to release the picker locking mechanism (see **1** in Figure 12-1 on page 12-4).
15. Release the picker assembly and allow it to slowly drop to the bottom of the library.
16. Reinstall all control module components that are removed for weight reduction.
    a. Drive sleds (see "Adding/removing/replacing a tape drive" on page 12-24)
    b. Power supplies (see "Removing/replacing a power supply (primary and redundant)" on page 12-34)
17. Reconnect the customer-supplied Ethernet cable to the Library Control Blade (for cable location, see **2** in Figure 12-27 on page 12-29).
18. Reconnect the module-to-module communication cable from the control module to the expansion module (**4** in Figure 12-27 on page 12-29).
19. Perform "Returning a library or library module to normal operations after repairs" on page 12-3.

Removing/replacing an expansion module

An expansion module increases the number of drives and data cartridge storage slots available within your library.

To make repairs to an expansion module, complete one of the following procedures.

- "Removing an expansion module from a library"
- "Replacing an expansion module in a stand-alone or rack-mounted library (14U or larger)"

Removing an expansion module from a library

1. Remove the following components from the expansion module for weight reduction:
   a. All power supplies (see "Removing/replacing a power supply (primary and redundant)" on page 12-34)
   b. All drive sleds (see "Adding/removing/replacing a tape drive" on page 12-24)

   Note: If not already done, remove all tape cartridges from the module that is removed.
2. Loosen the thumb screws that secure the expansion module to the rear flange on each rack kit rail, or to the module.
3. Open the I/O station door, then the access door on the expansion module.
4. From the front of the expansion module, remove the rack ears. See "Removing the rack ears" on page 12-16.
5. Raise the gear racks. See Figure 12-11 on page 12-12.
6. Raise the locating pin. See Figure 12-7 on page 12-8.
7. Loosen the thumb screw in the front.
8. Disconnect the module to module cables.
9. With a person on each side of the expansion module and a person in front of the expansion module, pull the module out of the rack.
10. Place the module on a sturdy work surface.

Replacing an expansion module in a stand-alone or rack-mounted library (14U or larger)

1. If your library is to be reinstalled into a rack, complete the following steps:
   a. With a person on each side of the expansion module and one person in front of the expansion module, pick up the module from the work surface and slide it onto the rack kit rails installed in your rack.
   b. Lower the locating pin. See Figure 12-7 on page 12-8.
   c. Tighten the front thumb screws.
   d. Lower the gear racks. See Figure 12-11 on page 12-12.

      Important: If the expansion module is at the bottom of the library, the gear racks must remain locked in the UP position. Skip step d. if the expansion module is at the bottom of the library. If the expansion module is not at the bottom of the library, complete step d.
   e. Install the module to module cables and terminators.

f. Tighten the rear thumb screws.

g. Tighten the thumb screw that secures the expansion module to the rear flange of each rack kit rail.

h. Open the I/O station door, then the access door on the expansion module.

i. Reinstall the rack ears on the front of the expansion module to secure it to the rack (see "Replacing the rack ears" on page 12-17).

2. Reinstall the following expansion module components:
   a. All drive sleds (see "Removing and replacing a tape drive" on page 12-25).
   b. All power supplies (see "Reinstalling/replacing a power supply" on page 12-36).
3. Complete "Replacing a control module in a stand-alone or rack-mounted library (14U or larger)" on page 12-9.

Removing/replacing rack ears

Rack ears are installed on each module in a rack-mounted library for weight distribution.

Removing the rack ears

Complete these steps to remove the rack ears on all units of the library.

1. Grasp the I/O station handle and pull it toward you until it locks in the open position.
2. Remove the right rack ear (**1** in Figure 12-15).

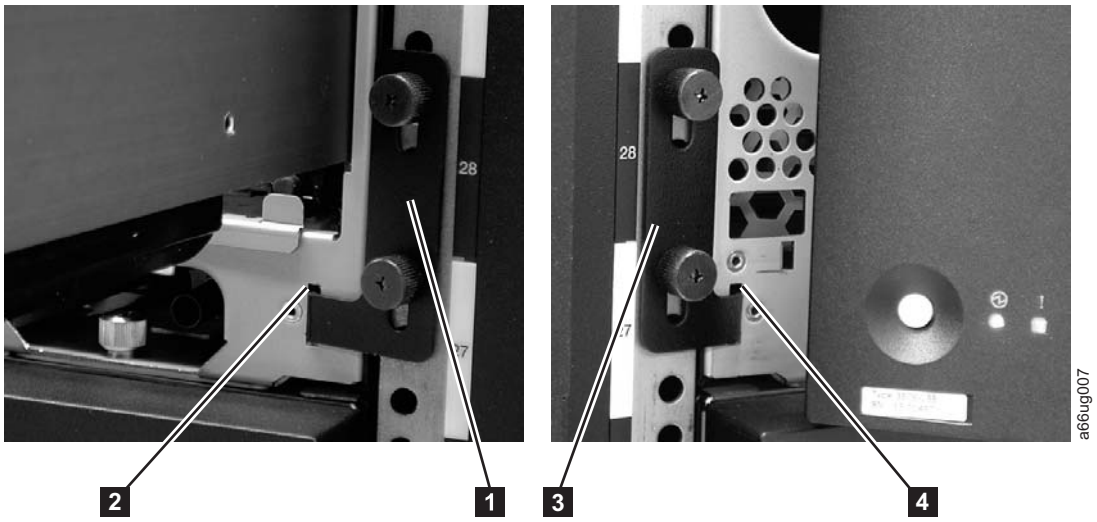


Figure 12-15. Removing the rack ears (control module shown)

   a. Remove the right rack ear thumb screws. If the screws are tight, use a #2 Phillips screwdriver to loosen them.
   b. Remove the right rack ear.
3. Remove the left rack ear (**3** in Figure 12-15).
   a. Open the left door of the library unit slightly.
   b. Grasp the hinged side of the door and, while you are pulling on the door, push right to expose the left rack ear.
   c. Remove the left rack ear thumb screws.

d. Remove the left rack ear.

4. Repeat this process for all units in the library, if necessary.

Replacing the rack ears

Complete these steps to replace the rack ears on all units of the library.

1. Grasp the I/O station handle and pull it toward you until it locks in the open position.
2. Replace the right rack ear (**1** in Figure 12-15 on page 12-16).
   a. At the lower right of the I/O station position on each library unit, there is a slot (**2** in Figure 12-15 on page 12-16). Insert the right rack ear into the slot.
   b. Position the right rack ear flush with the rack rail.
   c. Install and tighten the right rack ear thumb screws.
3. Replace the left rack ear (**3** in Figure 12-15 on page 12-16).
   a. Open the left door of the library unit slightly.
   a. Grasp the hinged side of the door and, while you are pulling on the door, push right to expose the slot for the left rack ear.
   b. Insert the left rack ear into the slot (**4** in Figure 12-15 on page 12-16).
   c. Position the left rack ear flush with the rack rail.
   d. Install and tighten the left rack ear thumb screws.
4. Repeat this process for all units in the library, if necessary.

Verifying front and rear gear racks alignment

For the picker to move from one unit to the next in a multi-module library, the front (**3** in Figure 12-16 on page 12-18) and rear (**1** in Figure 12-16 on page 12-18) gear racks in the control module must be properly aligned with the gear racks in the expansion module.

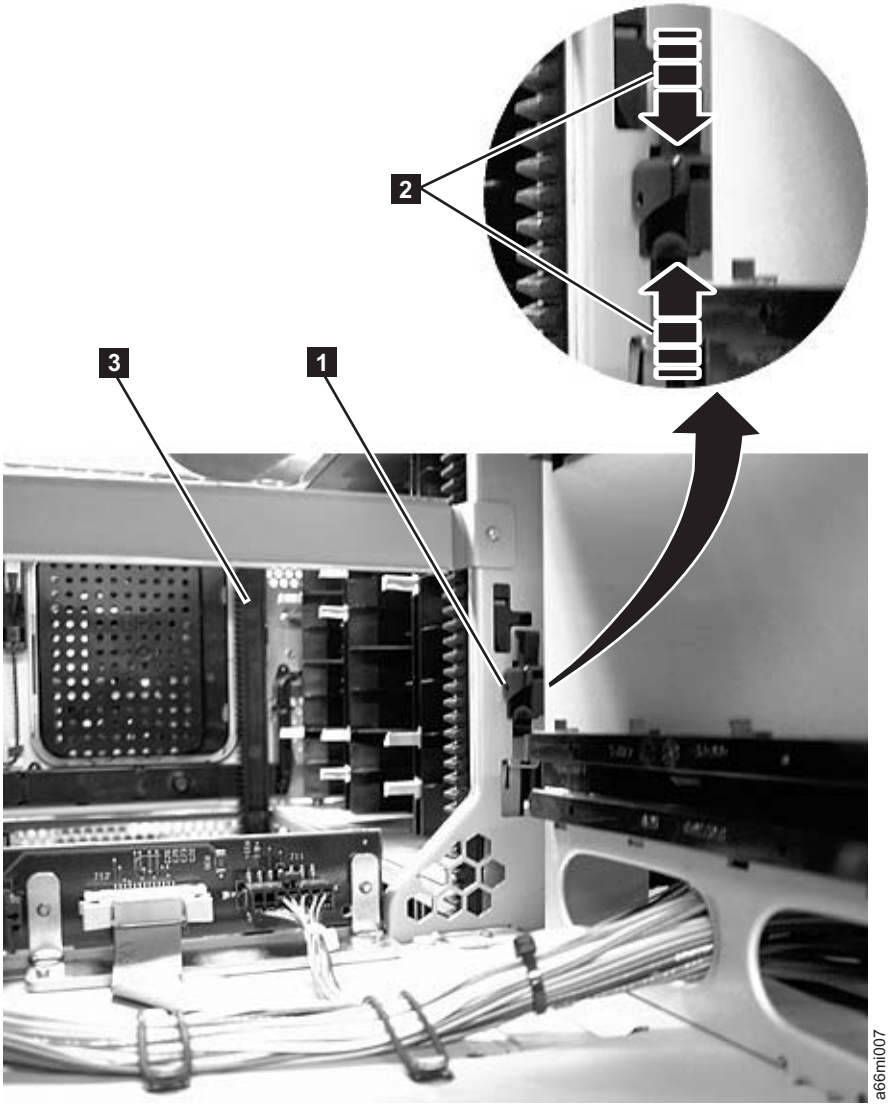


Figure 12-16. Gear rack

1	Rear gear rack-locking mechanism	2	Magnification of rear gear rack-locking mechanism	3	Front gear rack

Verify that the front (3 in Figure 12-16) and rear (1 in Figure 12-16) gear racks are properly aligned and positioned.

- In the bottom module of the library, verify that the gear racks are in the down position. Pinch the gear rack-locking mechanism (2 in Figure 12-16) and push the gear rack down. Ensure that the lock is **not** engaged in the hole in the frame.
- In all the modules above the bottom module:
  - Verify that the gear racks are in the down position. Pinch the gear rack-locking mechanism (2 in Figure 12-16) and push the gear rack down. Ensure that the lock is **not** engaged in the hole in the frame.
  - Verify that there are no gaps in the gear racks between library units.

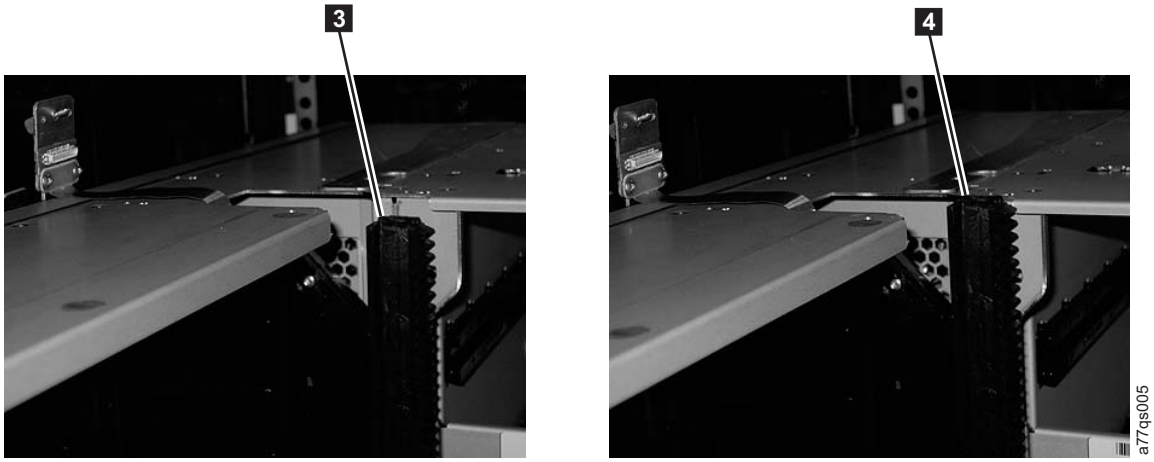


Figure 12-17. Gear racks in the up and down positions

To release the gear rack and move it down, follow these steps.

1. Engage the Y-rails of each module in your library configuration. Ensure that the Y-rails are properly aligned and the thumbscrews are tightened.

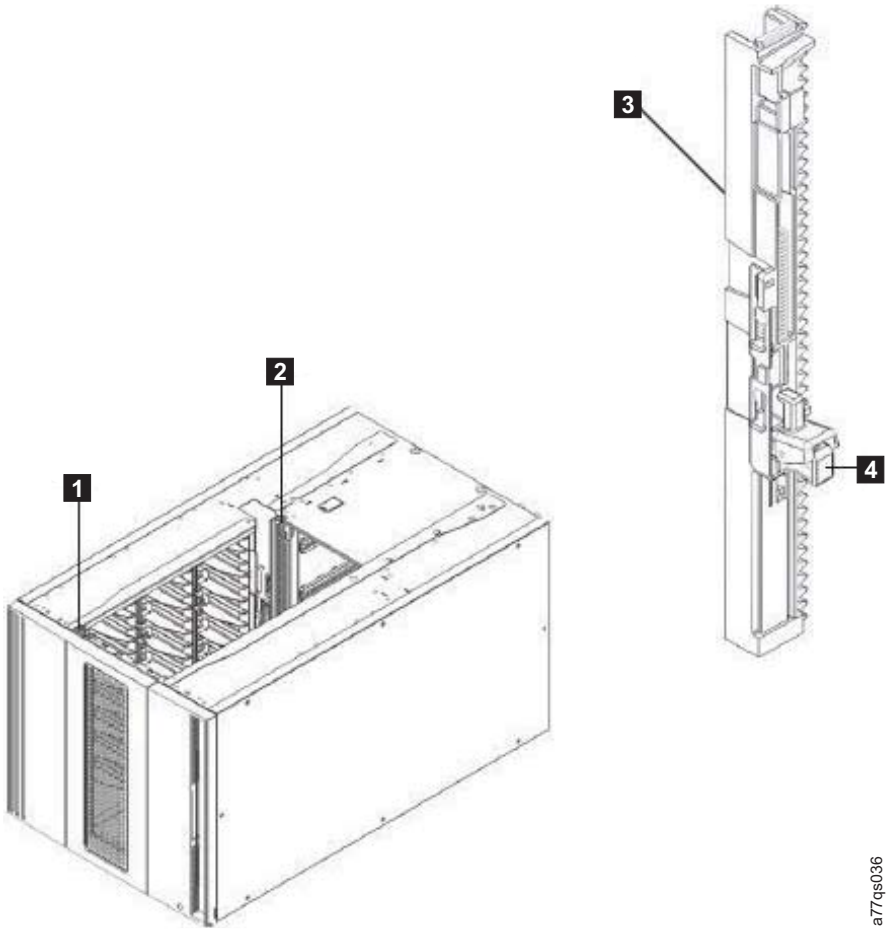


Figure 12-18. Placing gear rack in the Down position

1	The front Y-rail	3	The Y-rail (this end up)

2 The rear Y-rail 4 Squeeze here to release

2. From the front of the library, open the I/O station and access door of the 9U expansion module. Squeeze the handle of the Y-rail release mechanism, lift it out of its locked position, and slide it downward as far as it goes.

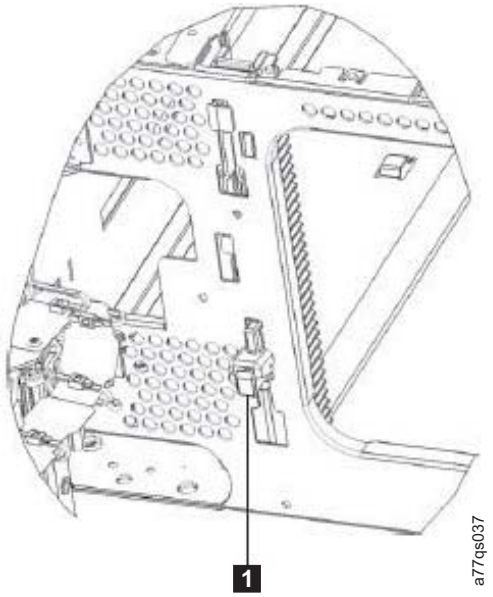


Figure 12-19. Releasing the Y-rail

1 Y-rail in unlocked, functional position

3. From the back of the library, find the rear Y-rail release mechanism, which is in the interior of the right side of the module. Squeeze the handle of the Y-rail release mechanism, lift it out of its locked position, and slide it downward as far as it goes. Doing this procedure aligns the Y-rails with the Y-rails of the module beneath it.

   CAUTION:
   Ensure that there is no gap between the top and bottom Y-rails on both the front and back of the library. If a gap exists, the library cannot mechanically initialize.

To align the gear racks in a multi-module library:

1. Slightly push up and pinch the gear rack-locking mechanism (1 in Figure 12-16 on page 12-18) to unlock the gear rack in the control module.
2. While you are pinching the gear rack-locking mechanism (2 in Figure 12-16 on page 12-18), push the gear rack down until it aligns with the gear rack in the expansion module, then release your hold on the locking mechanism.
3. Manually inspect the track to ensure that there are no gaps.
4. Repeat Steps 1 through 3 for the other gear rack.
5. Manually raise the picker and disengage the picker-locking mechanism (1 in Figure 12-20 on page 12-21) if necessary. If the gear racks are properly aligned, the picker slowly moves to the bottom of the library.

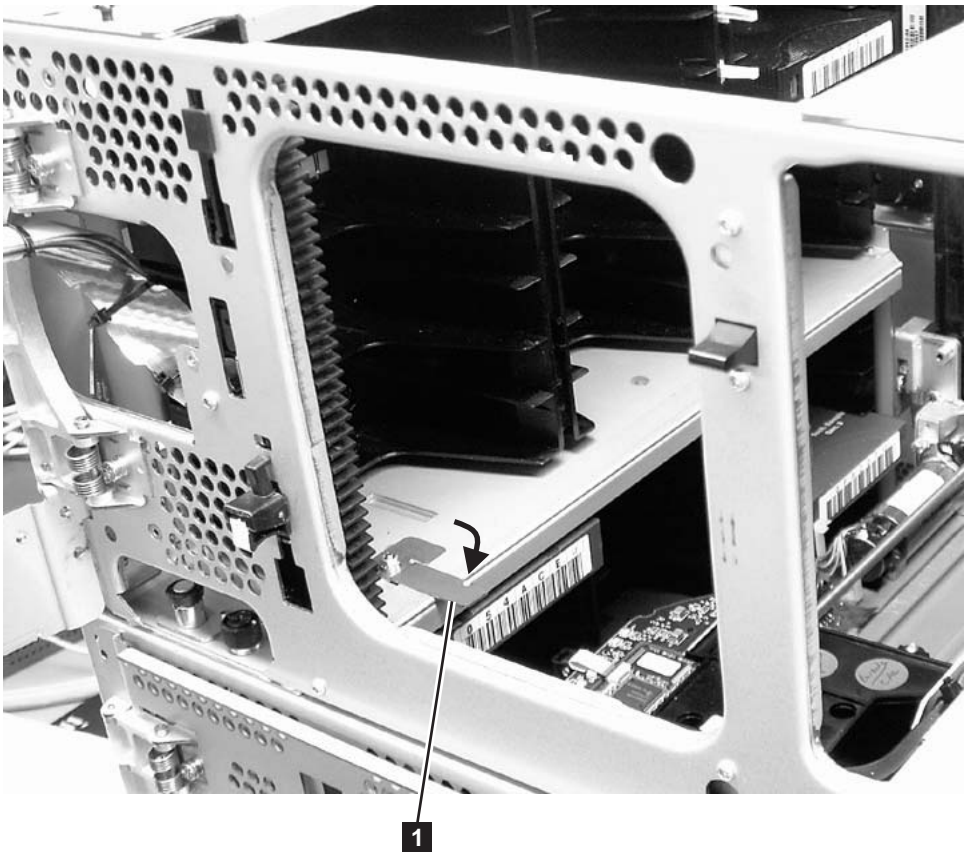


Figure 12-20. Picker assembly locking mechanism

I/O station

Each control and expansion module has an I/O station on the right side of the front of the unit. It is used for inserting/removing data and cleaning cartridges into and out of the library.

Figure 12-21. 14U library with control module I/O station open

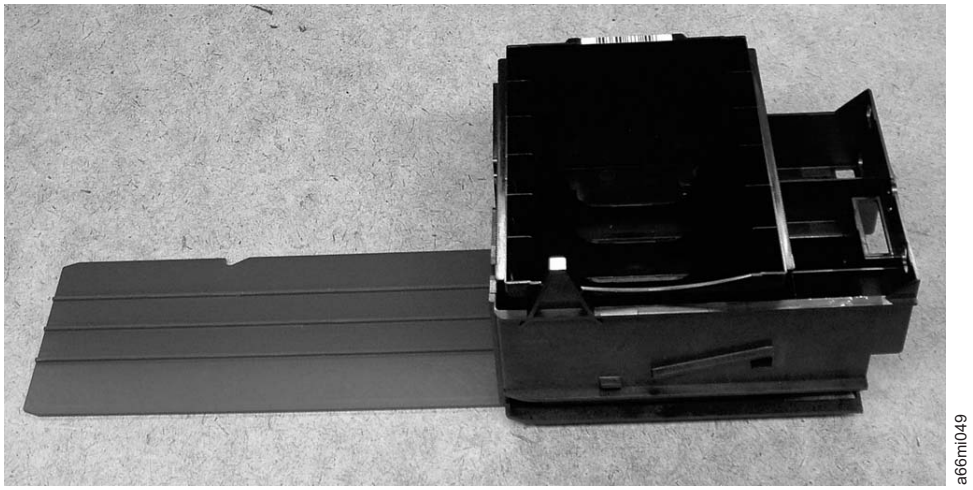


Figure 12-22. Control module I/O station

Each module 's I/O station must be locked for the library to function properly. When the library is busy running a task, such as retrieving a cartridge, the library locks all I/O station doors. The doors cannot be opened until the library is no longer busy. If the library detects that an I/O station door is either open or unlocked, the library cannot operate normally.

Manually unlocking the I/O station door

If the I/O station door fails to unlock, you can unlock it manually.

There are two styles of I/O station lock mechanism. The early style uses a T10 Torx wrench to rotate the lock mechanism. The new style has a large push-button type mechanism behind the hole (**1** in Figure 12-23) in the I/O station door.

Manually unlocking the early style I/O station door

If the I/O station door fails to unlock, you can unlock it manually.

To manually unlock the early style I/O station lock, follow these steps:

1. Insert a T10 Torx wrench in the hole (**1** in Figure 12-23) on the front of the I/O station door of the library module you want to open.
2. Turn the wrench one-quarter turn counterclockwise to unlock the door.

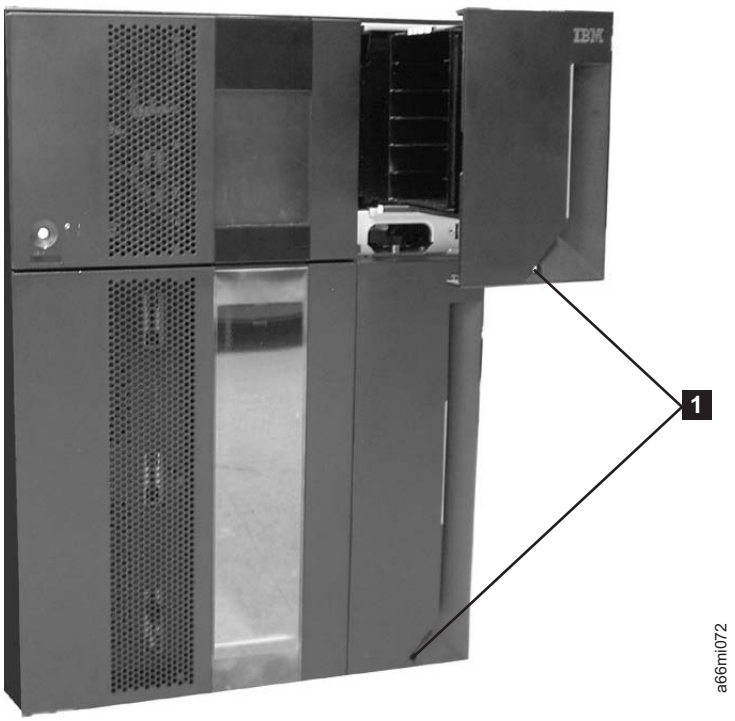


Figure 12-23. Access holes for manually unlocking I/O station doors

3. To manually relock the I/O station door:
   - From the Operator Panel, select **Operations** > **Lock I/O Station**
   - From the Web User Interface, select **Manage Cartridges** > **Lock/Unlock I/O Station Doors**

Manually unlocking the new style I/O station door

If the I/O station door fails to unlock, you can unlock it manually.

To manually unlock the new style I/O station lock, follow these steps:

1. Insert any straight tool (screwdriver, Torx wrench, and so on) into the hole (**1** in Figure 12-23) in the front cover of the I/O station.

2. Push the tool in to unlock the I/O station door. There is a large, flat pushbutton type mechanism behind the hole in the cover. When pushed toward the rear of the library, it releases the I/O station lock mechanism.
3. To manually relock the I/O station door:
   - From the Operator Panel, select **Operations** > **Lock I/O Station**
   - From the Web User Interface, select **Manage Cartridges** > **Lock/Unlock I/O Station Doors**

Rear panel components

The library has the following rear panel customer replaceable units (CRUs):

- Tape drive sled
- Library Control Blade (LCB)
- Library power supply
- Ethernet Expansion Blade (EEB)

Adding/removing/replacing a tape drive

Tape drives mounted in sleds are installed into tape drive slots in the rear of the library.

Removing a tape drive

Important: If you remove more than one tape drive at a time, record the locations of each drive before they are removed. Ensure that the drives are reinstalled in the correct location.

1. Vary all drives offline from the host.
   - From the Operator Panel, select **Operations** > **Change Drive Mode**.
   - From the Web User Interface, select **Service Library** > **Service Drives**.

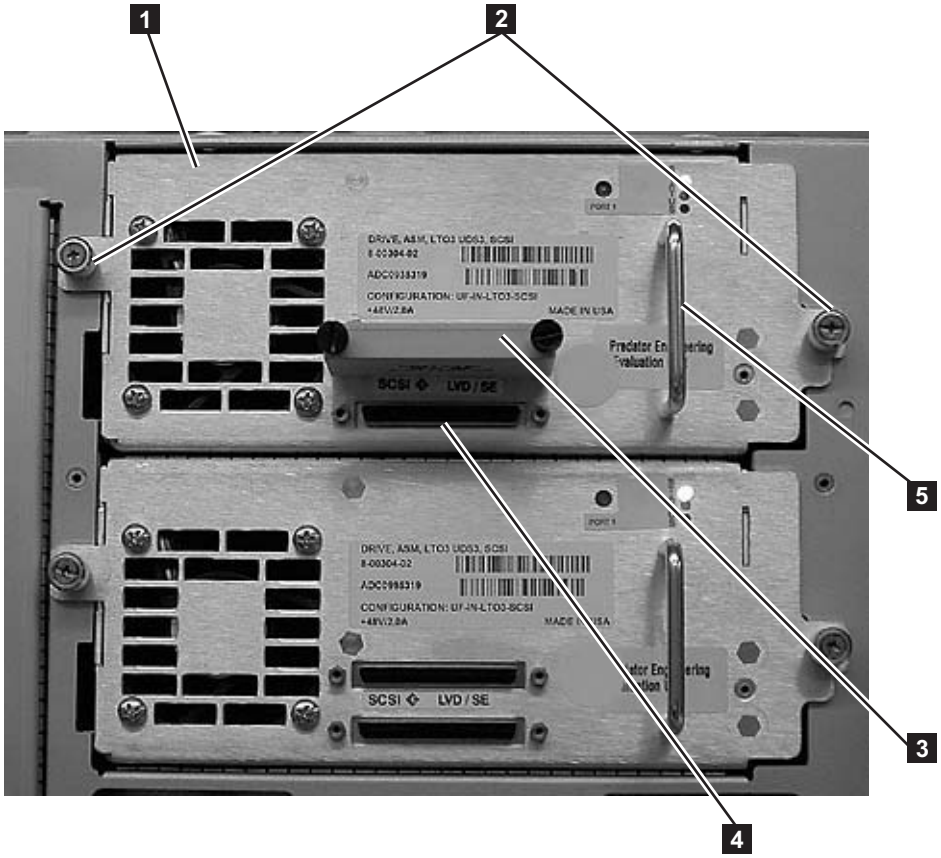


Figure 12-24. Tape drive (detail)

2. Disconnect the drive cable and place it on a flat surface in a secure location to avoid damaging the cable.
   a. For a SCSI drive, loosen the two thumb screws that hold the SCSI cable and terminator in place by turning them counterclockwise. Disconnect the cable and terminator from the drive that is being removed.
   b. For a Fibre Channel or SAS drive, unplug the host interface cable.
3. Loosen the two thumb screws (**2** in Figure 12-24) that hold the drive in place by turning them counterclockwise.
4. Slide the drive out of the library module. Grasp the handle (**5** in Figure 12-24) and slowly pull the drive toward you, while the tape drive is supported from underneath.

   Note: Removing a tape drive with power ON generates a Service Action Ticket T012.

Removing and replacing a tape drive

Attention: NEVER install a tape drive when a cartridge is in the drive in the eject position. Remove the cartridge first.

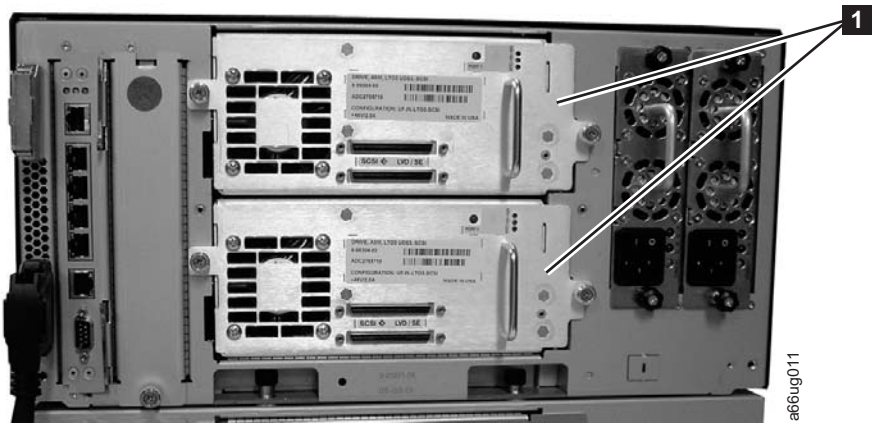


Figure 12-25. Control module tape drive

Attention: These instructions explain how to remove a tape drive and replace it with a new one. You must replace a tape drive if you are experiencing problems with one that is in use. You can remove a tape drive while the library is powered on. Do not, however, remove a tape drive that is in use. The new tape drive replaces the old tape drive in the logical library. You do not need to delete the old tape drive or add the new tape drive to the logical library, unless the replacement tape drive is of a different type (generation or interface) than the original. If the original tape drive is in a logical library, and the replacement tape drive is of a different type, the library generates an RAS ticket and does not activate the tape drive. If this issue happens, you must either replace the tape drive with one of the same types, or delete the old tape drive from the logical library. Then, add the new tape drive to the logical library. NEVER install a tape drive when a cartridge is in the drive in the eject position. Remove the cartridge first.

1. Prepare host applications for tape drive removal.
   a. From the Operator Panel, select **Operations** > **Change Drive Mode**.
   b. From the Web User Interface, select **Service Library** > **Service Drives**.
2. Save the library configuration.
3. If there is a tape cartridge in the target tape drive, use the Web User Interface to eject it.
4. Disconnect the drive cable and place it on a flat surface in a secure location to avoid damaging the cable.
   a. For a SCSI drive, loosen the two thumb screws that hold the SCSI cable and terminator in place by turning them counterclockwise. Disconnect the cable and terminator from the drive that is being removed.
   b. For a Fibre Channel or SAS drive, unplug the host interface cable.
5. Loosen the two thumb screws (**2** in Figure 12-24 on page 12-25) that hold the drive in place by turning them counterclockwise.
6. Slide the drive out of the library module. Grasp the handle (**5** in Figure 12-24 on page 12-25) and slowly pull the drive toward you, while the drive sled is supported from underneath.
7. Align the drive with the guide rails and guide slots along the tracks (**3** in Figure 12-26 on page 12-27) in the open drive sled slot (**2** in Figure 12-26 on page 12-27). Grasp the handle (**5** in Figure 12-24 on page 12-25) and slowly slide the tape drive into the library, while the drive is supported from underneath.

Note: The thumb screws must be aligned with the screw holes in the module. If they are not aligned, the tape drive was not inserted correctly.

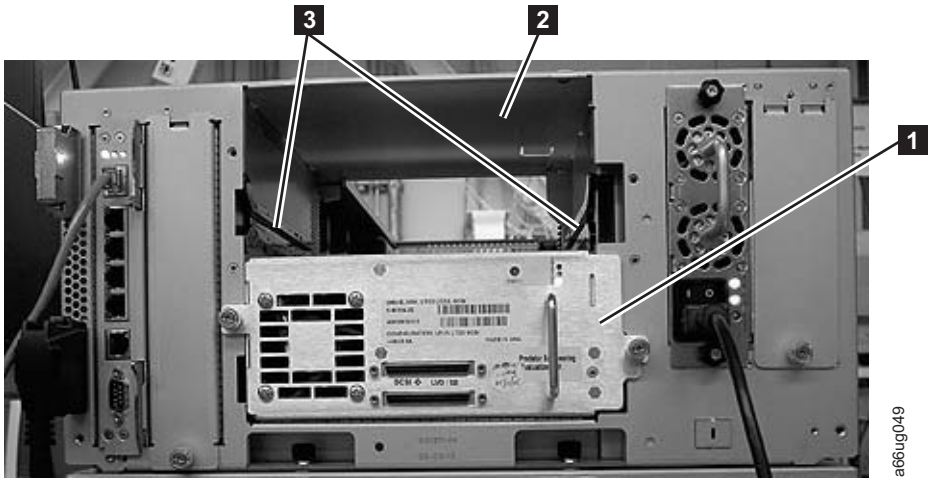


Figure 12-26. Tape drive slot

8. Tighten the 2 thumb screws (**2** in Figure 12-24 on page 12-25) that hold the drive sled in place by turning them clockwise.
9. Reconnect the tape drive cable.
   a. For a SCSI tape drive, plug the cable and terminator into the drive. Tighten the thumb screws that hold the SCSI cable (**4** in Figure 12-24 on page 12-25 shows the SCSI receptacle) and terminator (**3** in Figure 12-24 on page 12-25) in place by turning them clockwise.
   b. For a Fibre Channel or SAS tape drive, connect the host interface cable.
10. Repeat this procedure for all drives to be reinstalled in the library.
11. Ensure that all new drives that are being installed have the correct firmware level. New drive CRUs from stock might not have the latest version of the firmware. All drives of a specific interface and drive type requires the same firmware level.
    a. From the operator panel: **Tools** > **Drive Info**.
    b. From the Web user interface: **Service Library** > **View/Update Drive Firmware Levels** .
12. Update the drive firmware, if necessary. See "Updating drive firmware" on page 8-25.
13. Vary all drives online from the host.
14. If a new drive is installed in place of the removed drive, it is necessary that the host application is reconfigured to recognize the Vital Product Data (VPD) of the new drive. This procedure prevents possible communication and backup application disruptions.

    Note: This procedure does not require completion if Logical serial number addressing was implemented at a prior date.

Removing/replacing the Library Control Blade or Compact Flash card

The Library Control Blade (LCB) manages the entire library, including the Operator Panel and picker assembly. It also runs system tests to ensure that the library is functioning properly.

The Compact Flash (CF) card is housed on the LCB and contains the library firmware and vital product data (VPD) such as configuration settings.

Replacement of either the LCB or the CF requires the removal of the LCB/CF assembly from the library.

Important: Before the LCB/CF Assembly is removed from the library, ensure that you complete "Saving/restoring system configuration" on page 8-15 and that the saved file is available. If the CF card is replaced, you need this file to reconfigure the library.

A partial list of the configuration items that are saved:

- Current library firmware
- Network settings:
  - IP address
  - Subnet Mask & Gateway addresses
- Feature code licenses keys
- Logical library configuration
- Cartridge slot assignments
- Cleaning slot configuration
- I/O station configuration
- Drive IDs:
  - SCSI ID
  - Fibre Loop ID
  - SAS ID
- Encryption method selections
- Administrator and user account information

Removing the Library Control Blade/Compact Flash assembly

Important: Before the LCB/CF Assembly is removed from the library, ensure that you have the current library configuration data available. If the CF card is replaced, you need the following information to reconfigure the library:

- IP address
- Subnet mask address
- Gateway address
- Library firmware level
- License keys, if applicable

See "Saving/restoring system configuration" on page 8-15. Also, see Appendix E, "Library configuration form," on page E-1.

Important: When the LCB is handled, you must wear an ESD anti-static wrist strap, or touch the library frame to discharge any static electricity in your body. Do not handle the LCB without taking appropriate ESD precautions.

1. Complete "Preparing a library or library module for repairs" on page 12-2.
2. On the LCB (Figure 12-27 on page 12-29), disconnect the ethernet cable (**2** in Figure 12-27 on page 12-29) by pinching the tab to disengage the cable. Then, pull the connector out of the LCB.

Note: Six slots reside below the ethernet cable. The four topmost slots can access tape drive Ethernet connectivity directly via the library control blade. The two bottommost slots are designated as ethernet (5 in Figure 12-27) and serial (6 in Figure 12-27) ports, and are reserved for use by IBM service personnel.

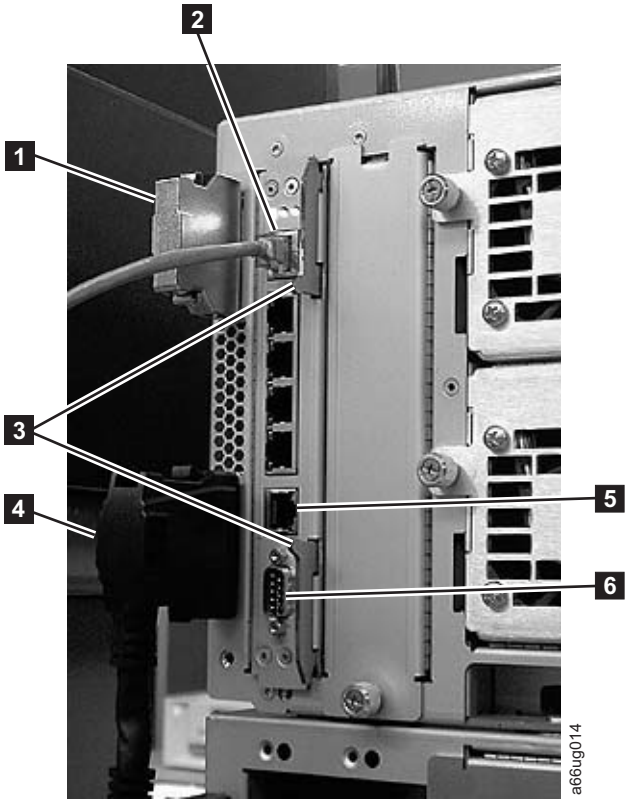


Figure 12-27. Library Control Blade (LCB)

1	Module communication terminator	4	Module-to-module communication cable
2	Ethernet cable (customer supplied)	5	Ethernet port (for IBM service personnel use)
3	Latches	6	Serial port (for IBM service personnel use)

3. Grasp the pair of latches (3 in Figure 12-27) near the top and bottom of the LCB. Simultaneously push the latches to the left, and then pull them out and away from the LCB.
4. Simultaneously grasp the same pair of latches again, and slowly pull them toward you. As the LCB begins to slide out of the control module, be sure to support the LCB from underneath, being careful to touch only the metal cover and the ground plane.

   Important: DO NOT touch any components on the LCB firmware board. Hold it by the metal cover and support it by the metal ground plane along the bottom edge.
5. When the LCB is removed from the control module, carefully lay it (Figure 12-28 on page 12-30) on a clean, flat surface.

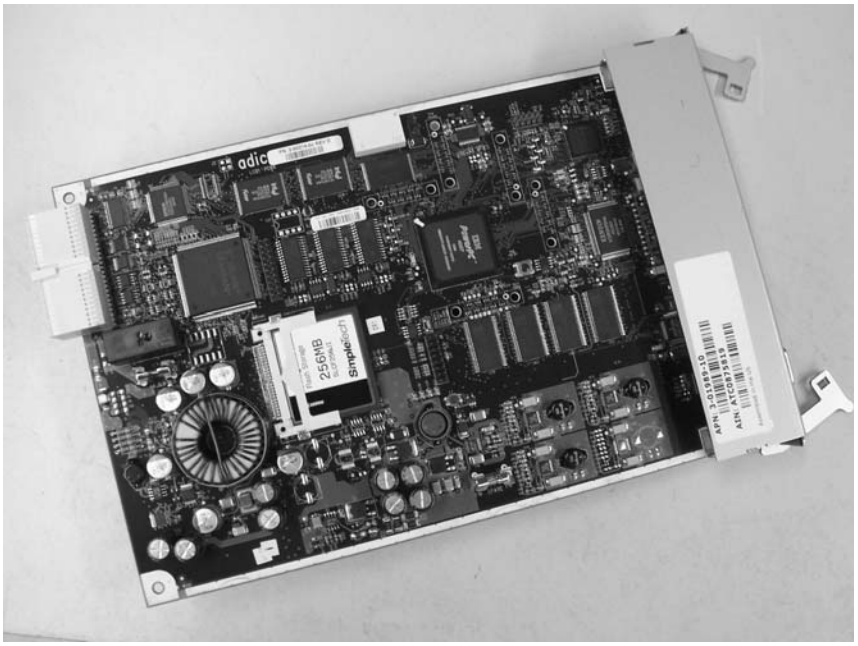


Figure 12-28. Library Control Blade (LCB)

6. Use one of the following procedures to complete the repair:
   - If you are replacing the LCB only, it is necessary to transfer the CF card from the old LCB to the new LCB. Continue with "Removing/replacing the Compact Flash card."
   - If you are replacing the CF card only, it is necessary to remove the failing CF card from the LCB, replace it with the new CF card, and upgrade the CF card firmware. Continue with Step 3 of "Removing/replacing the Compact Flash card".

Removing/replacing the Compact Flash card

Important: When the Compact Flash card is handled, you must wear an ESD anti-static wrist strap, or touch the library frame to discharge any static electricity in your body. Do not handle the Compact Flash card without taking appropriate ESD precautions.

Selections that are made during library configuration reside on the Compact Flash card.

Before the LCB/CF Assembly from the library is removed, ensure that you complete"Saving/restoring system configuration" on page 8-15 and that the saved file is available. If the CF card is replaced, you need this file to reconfigure the library.

Following is a partial list of the configuration items that are saved:

- Current library firmware
- Network settings:
  - IP address
  - Subnet Mask & Gateway addresses
- Feature code licenses keys
- Logical library configuration

- Cartridge slot assignments
- Cleaning slot configuration
- I/O station configuration
- Drive IDs:
  - SCSI ID
  - Fibre Loop ID
  - SAS ID
- Encryption method selections
- Administrator and user account information

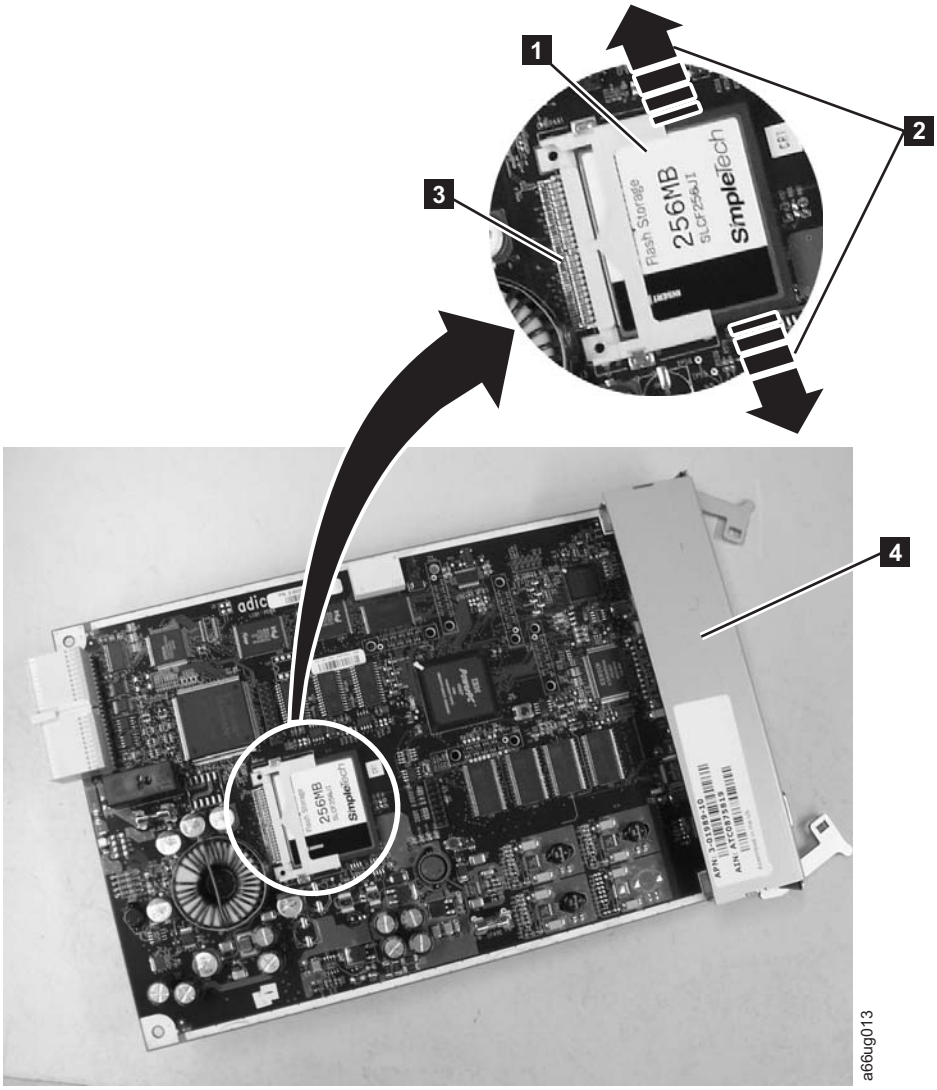


Figure 12-29. Removing the Compact Flash card from the Library Control Blade

1. Locate the compact flash card component on the LCB board (**1** in Figure 12-29).
2. Without touching any other components on the LCB firmware board, carefully grasp the compact flash card and wiggle it using a gentle, side-to-side motion (**2** in Figure 12-29) until the pins on the compact flash card become

disconnected from the pins on the LCB board (3 in Figure 12-29 on page 12-31). Then, slowly slide the compact flash card out of the guide slots.

3. Carefully lift the compact flash card out of the LCB board.
4. If you are installing a new LCB, continue by transferring the old CF to the new LCB. If you are installing a new CF card, continue by installing the new CF card in the old LCB. In either case, install the appropriate compact flash card to the LCB board you are installing with the label up, and pins aligned. Without touching any other components on the LCB board, carefully grasp the compact flash card, and slowly slide it into the guide slots. Continue to push the compact flash card into the guide slots until the pins start to connect. Then, hold the LCB board metal connector shield (4 in Figure 12-29 on page 12-31) with one hand and push the compact flash card into the connector with your other hand. The compact flash card must be firmly seated against the connector (3 in Figure 12-29 on page 12-31).

   Note: The card is properly connected when no gold pins are visible.

Replacing the Library Control Blade (LCB)

Important: When the LCB is handled, you must wear an ESD anti-static wrist strap, or touch the library frame to discharge any static electricity in your body. Do not handle the LCB without taking appropriate ESD precautions. DO NOT touch any components on the LCB firmware board (see Figure 12-28 on page 12-30). Hold it by the metal cover and support it by the metal ground plane only.

1. Locate the empty LCB slot on the rear panel of the control module (CM). Then, carefully line up the new LCB board along the guide slots, and gently slide it into the control module until the connector seats.

   Important: As the LCB begins to slide into the control module, be sure to support the circuit board from underneath, being careful to touch only the metal cover and the ground plane along the bottom edge.
2. Grasp the pair of latches near the top and bottom of the LCB (3 in Figure 12-30 on page 12-33) by pushing them in until they click into place.

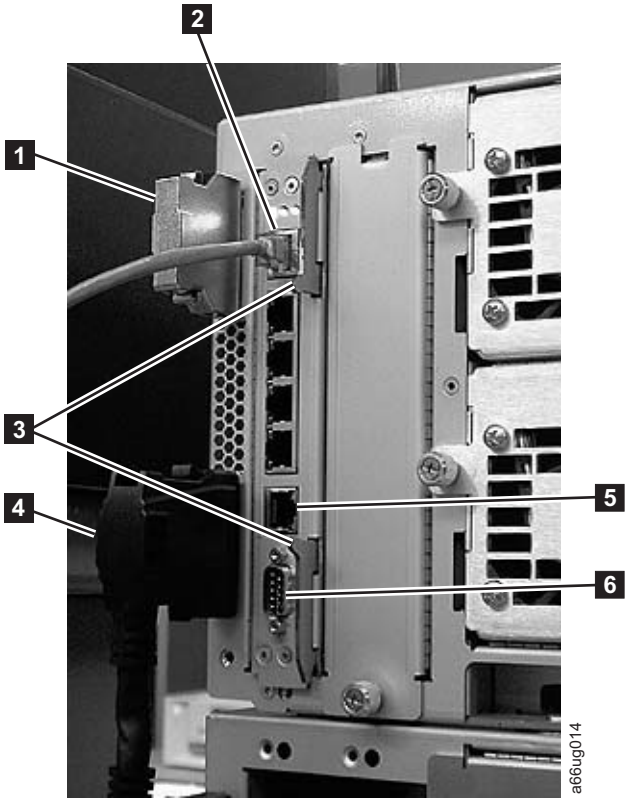


Figure 12-30. Library Control Blade (LCB)

1	Module communication terminator	4	Module-to-module communication cable
2	Ethernet cable (customer supplied)	5	Ethernet port (for IBM service personnel use)
3	Latches	6	Serial port (for IBM service personnel use)

3. Reconnect the ethernet cable (2 in Figure 12-30) by pinching the tab and pushing the connector into the LCB.

   Note: Six slots reside below the ethernet cable. The four topmost slots can access tape drive ethernet connectivity directly with the library control blade. The two bottommost slots are designated as ethernet (5 in Figure 12-30) and serial (6 in Figure 12-30) ports, and are reserved for use by IBM service personnel.
4. Power ON the library and wait for it to initialize. This procedure can take from 2 to 10 minutes, depending on the level of firmware on the Library. If the Compact Flash card is new and was never initialized, see "Upgrading the Compact Flash card firmware."
5. Complete "Returning a library or library module to normal operations after repairs" on page 12-3.

Upgrading the Compact Flash card firmware

If the Compact Flash card is new and is not initialized, it contains a minimal level of library firmware that allows the library to boot up and display an **Upgrade Notification** message. To use the library, you must upgrade to the latest level of library firmware. Use the following steps to upgrade firmware the first time you use a new Compact Flash card.

1. Log on to the local operator panel as ADMIN. The "Network Configuration" screen displays.
2. Turn OFF the DHCP selection.
3. Enter the IP address, Subnet Mask, and Default Gateway selections.
4. Verify the Library Name selection.
5. Select **Apply**.
6. When the **SUCCESS** message is displayed, select **CANCEL**. This message logs OFF from the local Operator Panel.
7. Log on to the remote web browser as **ADMIN**. The **Upgrade Notification** message displays on the web console.
8. Click the upgrade firmware link that is provided, then browse to locate the firmware file. See "Updating library firmware" on page 8-24 for instructions.
9. Restore the system configuration data to the Compact Flash card.
   - See "Saving/restoring system configuration" on page 8-15.
   - See Appendix E, "Library configuration form," on page E-1

Removing/replacing a power supply (primary and redundant)

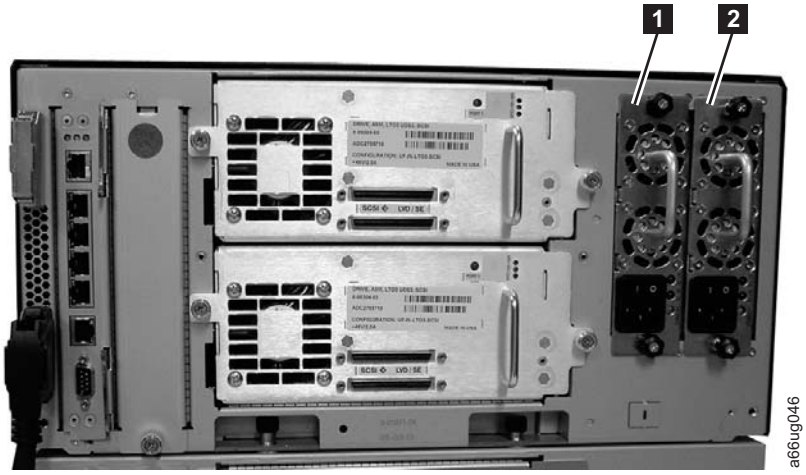


Figure 12-31. Power supplies in a control module

1 Primary power supply **2** Redundant power supply

Library power is controlled at the individual power supplies and at the front panel of the library. The switch on the rear of each power supply controls power for the module in which the power supply is installed. The button on the front of the control module controls power for all library modules in the library.

A second (redundant) power supply helps ensure that your library does not lose power (and become inaccessible) if the primary power supply happens to fail. The library automatically switches to the redundant power supply if the primary power supply fails for any reason.

A redundant power supply is connected to a different AC circuit from the primary power supply. Even better, the redundant power supply is connected to a separate power distribution source. If the primary power supply fails or becomes unstable, the redundant power supply automatically powers the library if it is turned ON.

If your library has a redundant power supply, you can replace the primary power supply without powering OFF the library. If your library does not have a redundant power supply that is installed, the empty slot is covered by a metal plate.

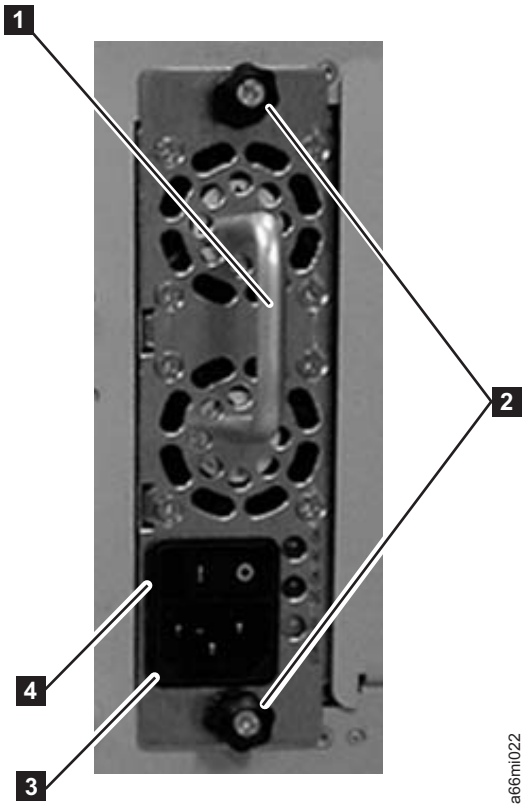


Figure 12-32. Power supply

1	Handle	3	Power cord receptacle
2	Thumb screws	4	Power switch

Removing a primary power supply

1. Complete "Preparing a library or library module for repairs" on page 12-2.

   Note: It is not necessary to power off the library if there is a redundant power supply installed.
2. Unplug each end of the power cord in the correct sequence.

   Attention: First, disconnect the power cord from the power source. Then, disconnect the power cord from the power supply receptacle (3 in Figure 12-32).
3. Loosen the two thumb screws (2 in Figure 12-32) by turning them counterclockwise.
4. Grasp the handle (1 in Figure 12-32) and slowly pull the power supply toward you, while it is supported from underneath.
5. Install a metal cover plate over the vacant power supply slot if you are not immediately installing a replacement.

Reinstalling/replacing a power supply

1. Grasp the power supply handle (1 in Figure 12-32 on page 12-35) while it is supported from underneath. Then, line up the power supply with the guides in the slot, and carefully push the power supply into the library.
2. Tighten the two thumb screws (2 in Figure 12-32 on page 12-35) on the power supply by turning them clockwise.
3. Connect the power supply by plugging in each end of the power cord in the correct sequence.

   Attention: First, connect the power cord to the power supply component (3 in Figure 12-32 on page 12-35). Then, connect the power cord to the power source.
4. Toggle the power switch (4 in Figure 12-32 on page 12-35) on the power supply to the | (ON) position.
5. If there is no redundant power supply, power ON the library with the **Power** button on the front of the library.

Removing a redundant power supply

1. Locate the slot for the redundant power supply to be removed on the back of the library.
2. Toggle the redundant power supply power switch (4 in Figure 12-32 on page 12-35) to the **O** (OFF) position.
3. Unplug the power cord from the redundant power supply receptacle (3 in Figure 12-32 on page 12-35).
4. Loosen the two thumb screws (2 in Figure 12-32 on page 12-35) by turning them counterclockwise.
5. Grasp the handle (1 in Figure 12-32 on page 12-35) and pull the power supply toward you. Support the component from underneath with your other hand.
6. Install a metal cover plate over the vacant redundant power supply slot if you are not immediately installing a replacement.

Replacing a redundant power supply

1. Locate the slot for the redundant power supply on the back of the library module.
2. Remove the cover plate over the vacant redundant power supply slot, if necessary.
3. Insert the redundant power supply by gripping the handle (1 in Figure 12-32 on page 12-35), sliding it into the guide slots, and pushing it into the empty slot.
4. Tighten the two thumb screws (2 in Figure 12-32 on page 12-35) that hold the redundant power supply in place.
5. Connect the power cord to the power supply (3 in Figure 12-32 on page 12-35) and to its source.
6. Turn ON power to the redundant power supply, with the switch (4 in Figure 12-32 on page 12-35) on the power supply.

Removing/replacing the Ethernet Expansion Blade (EEB)

For libraries greater than 5U, IBM provides the Ethernet Expansion Blade (EEB). The EEB facilitates direct ethernet connectivity between IBM Ultrium 5 and 6 Fibre

Channel tape drives and the library's internal ethernet. The customer, or a support person, can download drive logs and update drive firmware at high speeds with this interface.

Removing the Ethernet Expansion Blade (EEB)

Important: Before the EEB assembly is removed from the library, ensure that you completed "Saving/restoring system configuration" on page 8-15 and that the saved file is available.

1. Prepare the library for removing the EEB. From Web User Interface, select **Service Library** > **Ethernet Expansion Blade Control** > **Remove**.
2. Complete "Preparing a library or library module for repairs" on page 12-2.
3. On the EEB, disconnect the ethernet cables by pinching the tab to disengage the cables.

Figure 12-33. Ethernet cables removed

4. Grasp the pair of latches near the top and bottom of the EEB. Simultaneously push the latches to the left, and then pull them out and away from the EEB.
5. Simultaneously grasp the same pair of latches again, and slowly pull them toward you. As the EEB begins to slide out of the expansion module, be sure to support the EEB from underneath. Be careful to touch only the metal cover and the ground plane.

Figure 12-34. EEB with small cover plate to the right removed

Important: DO NOT touch any components on the EEB firmware board. Hold it by the metal cover and support it by the metal ground plane along the bottom edge.

6. When the EEB is removed from the expansion module, carefully lay it on a clean, flat surface.

Figure 12-35. EEB seen from above

7. If you are replacing the EEB, continue with "Adding or replacing the Ethernet Expansion Blade (EEB)" on page 12-42.
8. If you are not replacing the EEB, remove the small cover plate (P/N 35P3057) that covers the area to the right of the EEB (see Figure 12-34 on page 12-39). Install a large metal cover plate (P/N 35P2982) over the vacant slots and tighten the two thumb screws by turning them clockwise.

Figure 12-36. EEB removed - vacant slots

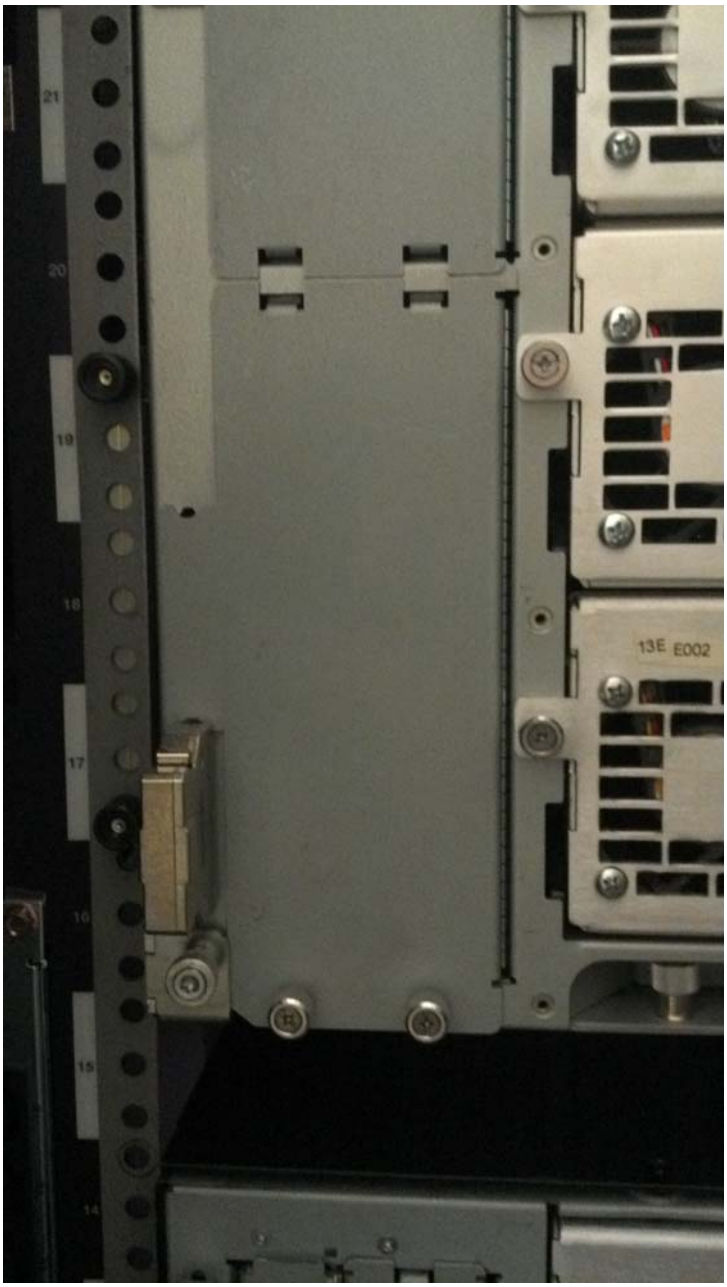


Figure 12-37. EEB removed and large cover plate installed

9. Complete "Returning a library or library module to normal operations after repairs" on page 12-3.

Adding or replacing the Ethernet Expansion Blade (EEB)

- Only one Ethernet Expansion Blade can be installed per expansion module.
- Library firmware must be at version 630G or later. See "Updating library firmware" on page 8-24.
- IBM Ultrium 5 tape drive firmware must be at version CB10 or later. IBM Ultrium 6 tape drive firmware must be at version CB20 or later. Update the drive firmware, if necessary. See "Updating drive firmware" on page 8-25.
- 5U libraries do not support an Ethernet Expansion Blade. For 5U libraries, request Feature code (FC)-6001 to connect the IBM Ultrium 5 and Ultrium 6

Fibre Channel tape drive to one of the internal ethernet ports on the Library Control Blade.

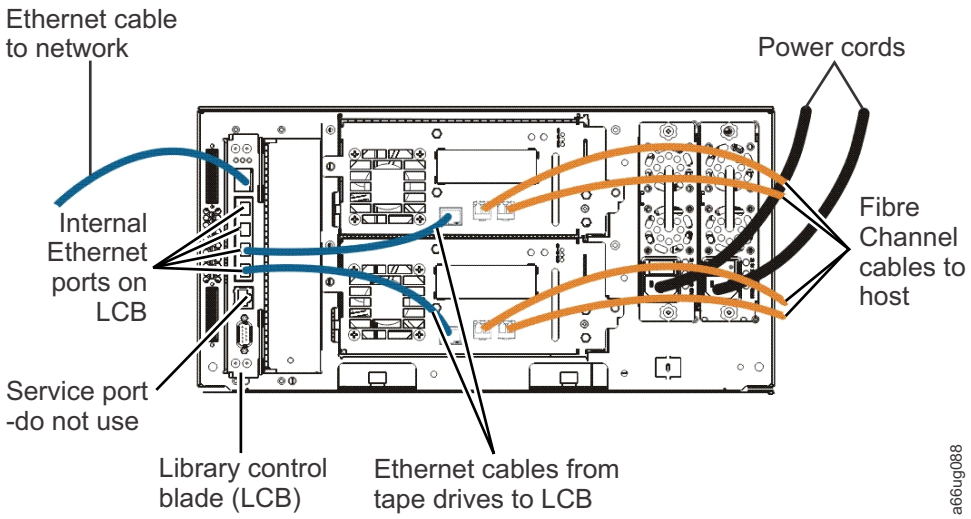


Figure 12-38. Ethernet connectivity on 5U libraries

- It is recommended that all IBM Ultrium 5 and 6 Fibre Channel tape drives greater than 5U are connected to an Ethernet Expansion Blade (FC-3470).
- The Ethernet Expansion Blade is not in the data path and does not affect tape drive control paths.

Important: Before the EEB assembly is removed from the library, ensure that you completed "Saving/restoring system configuration" on page 8-15 and that the saved file is available.

The Ethernet Expansion Blade must be installed in the lower left vertical bay in an expansion module.

1. Complete "Preparing a library or library module for repairs" on page 12-2..
2. Locate the lower left metal cover plate on the rear panel of the expansion module. In some cases, the Module Communication Terminator might be in the way of the cover plate. Remove the Module Communication Terminator, then remove the metal cover plate that covers the two slots. Loosen the two thumb screws by turning them counterclockwise, then pull outward on the plate. Save the cover plate in case you must use it later.

Figure 12-39. Module Communication Terminator is removed

3. Remove the new Ethernet Expansion Blade from the protective anti-static bag.

Figure 12-40. Ethernet Expansion Blade - horizontal view

4. Hold the Ethernet Expansion Blade upright with the latch hooks on the left side and the status LEDs at the bottom. Carefully line up the new EEB board along the guide slots, and gently slide it into the control module until the connector seats.

Figure 12-41. Ethernet Expansion Blade - installation

Important: Forcing the blade into the bay can cause the pins to bend.

Important: As the EEB begins to slide into the expansion module, be sure to support the circuit board from underneath. Be careful to touch only the metal cover and the ground plane along the bottom edge.

5. Grasp the pair of latches near the top and bottom of the EEB by pushing them in until they click into place.
6. The empty bay to the right of the Ethernet Expansion Blade must be covered by a cover plate (P/N 23R2604).

Figure 12-42. Cover plate to the right of the EEB

7. Reconnect the Module Communication Terminator.

Figure 12-43. Replaced Module Communication Terminator

8. Each Ethernet Expansion Blade has six ethernet ports to attach up to six IBM Ultrium 5 and 6 Fibre Channel drives. Do not attach tape drives of any other type to the Ethernet Expansion Blade.
9. Do not connect the Ethernet Expansion Blade to an external ethernet source. The Ethernet Expansion Blade is for internal ethernet connectivity within the library.
10. Connect up to six IBM Ultrium 5 and 6 Fibre Channel drives with the Ethernet Drive interface to the Ethernet Expansion Blade.

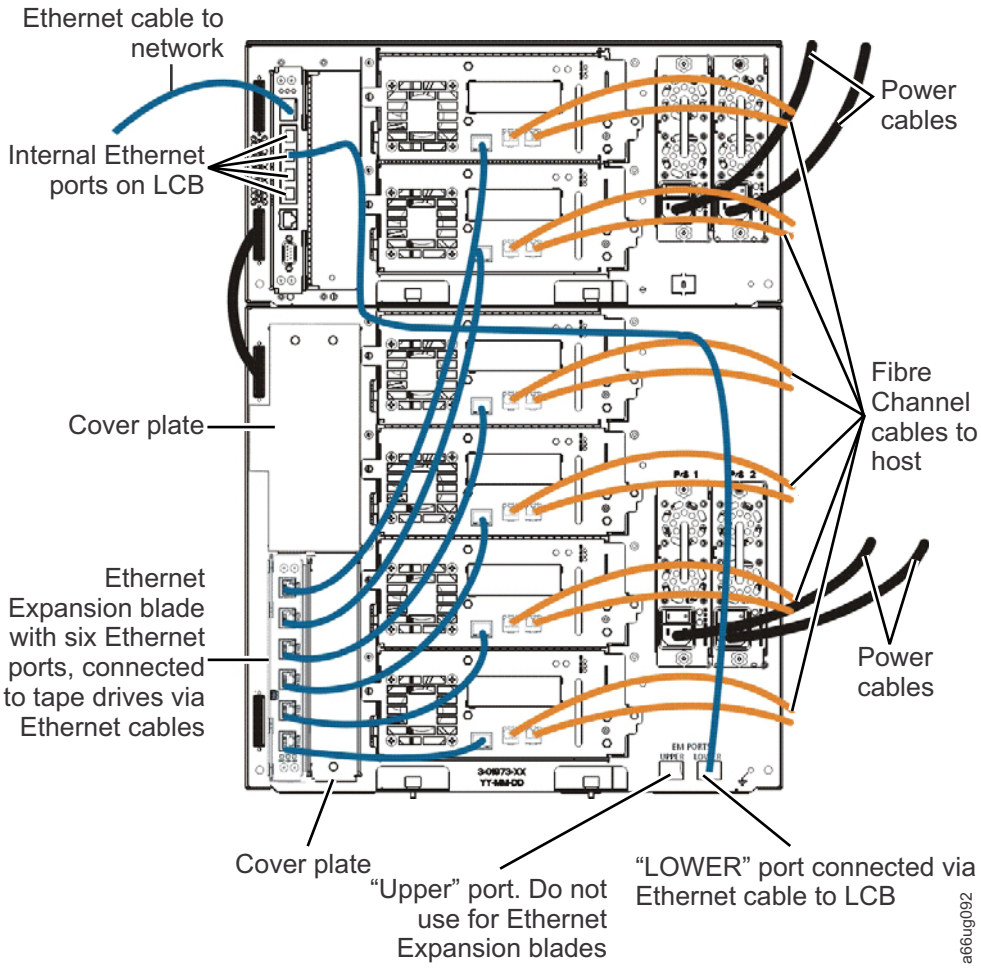


Figure 12-44. Ethernet connectivity on 14U and higher libraries

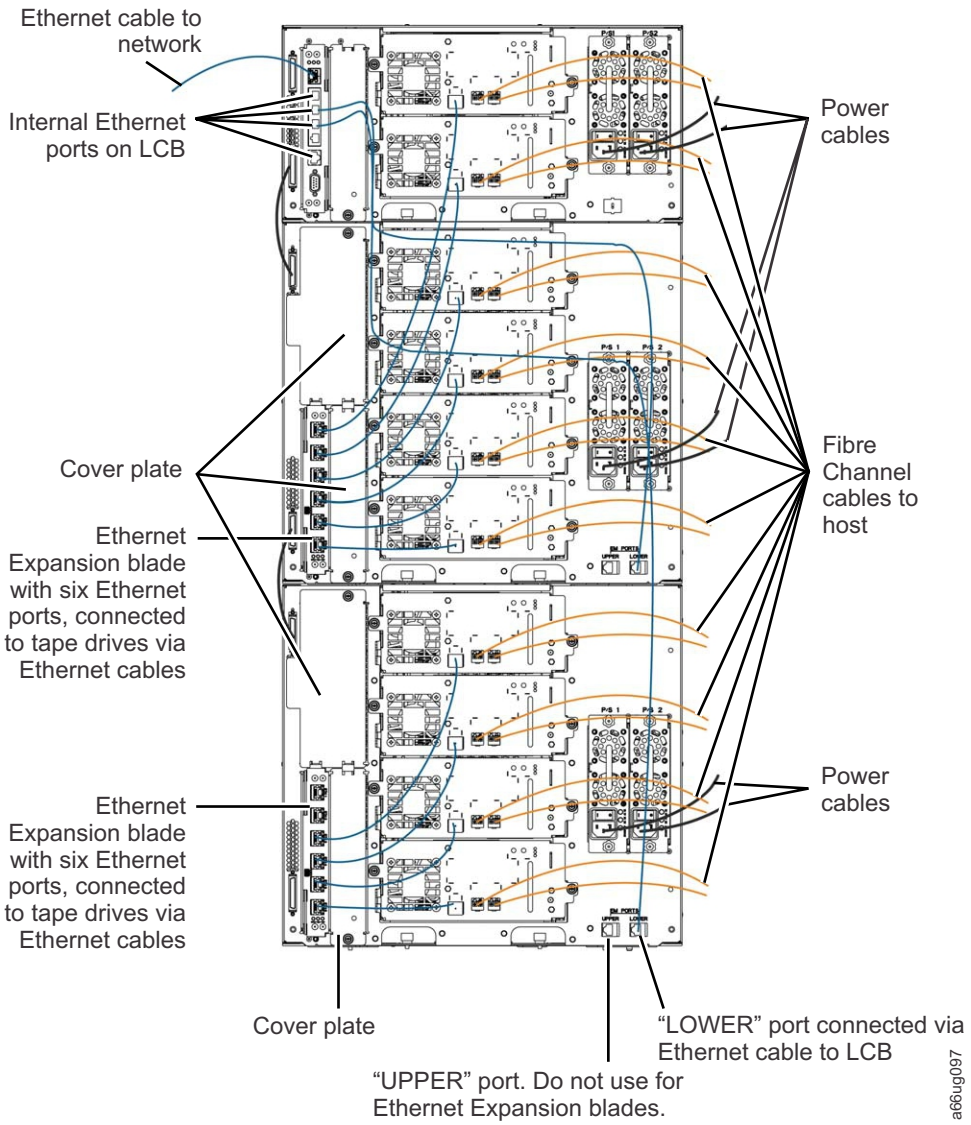


Figure 12-45. Ethernet connectivity on 14U and higher libraries

11. For every expansion module that contains an Ethernet Expansion Blade, connect with an ethernet cable from one of the four internal ethernet ports on the library control blade (LCB) to the ethernet port marked "LOWER" on the lower right of the expansion module in which the Ethernet Expansion Blade is installed. There are two ports, marked "UPPER" and "LOWER." Since the Ethernet Expansion Blade must be installed in the lower bay of the expansion module, you must use the ethernet port marked "LOWER." The "LOWER" port is on the right. See Figure 12-44 on page 12-49.
12. Complete "Returning a library or library module to normal operations after repairs" on page 12-3.
13. Verify that the Ethernet Expansion Blade is in the "Ready" state by checking the LEDs on the Ethernet Expansion Blade. The green LED flashes once per second, the blue LED flashes once every 10 seconds, and the amber LED is off. See Figure 12-46 on page 12-51.

Replacing the Ethernet Expansion Blade:

Follow the “Removing the Ethernet Expansion Blade (EEB)” on page 12-37 and “Adding or replacing the Ethernet Expansion Blade (EEB)” on page 12-42 procedures.

Ethernet Expansion Blade status LEDs

The status LEDs for the Ethernet Expansion Blade are at the bottom of the Ethernet Expansion Blade below ETH 6.

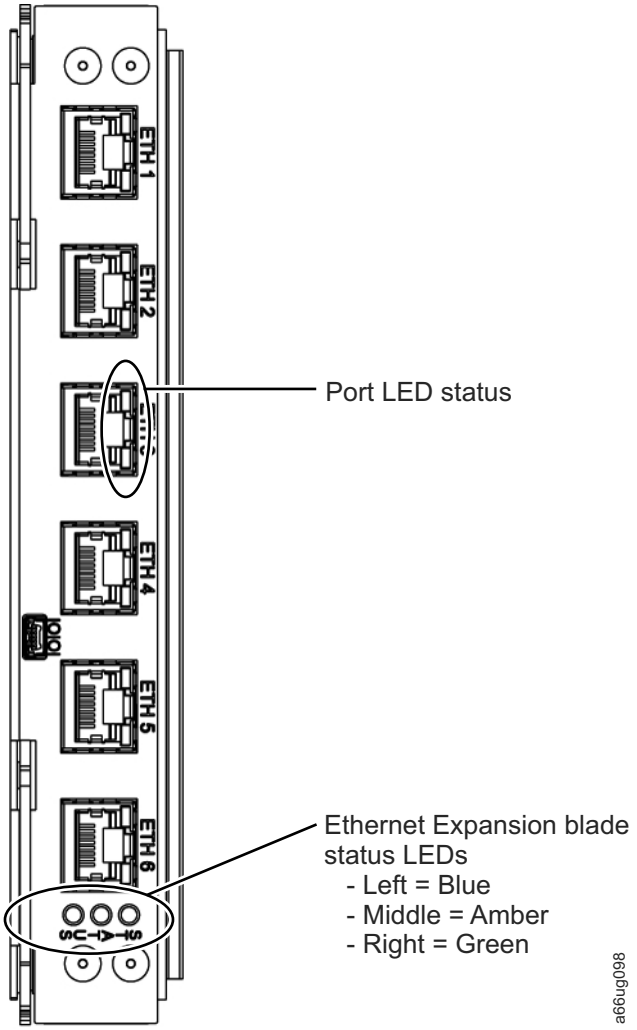


Figure 12-46. Ethernet Expansion Blade LEDs

Table 12-2. Ethernet Expansion Blade status LED Descriptions

LED Color	Represents	Blade Status
Green	Processor status	• Solid OFF - Blade’s main processor is not operating (or blade is booting). • Solid ON - Blade’s main processor is not operating. • Flashes once per second (1 Hz) - Normal.

Table 12-2. Ethernet Expansion Blade status LED Descriptions (continued)

LED Color	Represents	Blade Status
Amber	Health status	• Solid OFF - Normal. • Solid ON - Failure or blade is auto-leveling. With the blue LED flashing once very 10 seconds, this act is a normal condition. Auto-leveling takes about 3 minutes per blade, and blades auto-level in series. Never remove a blade when the amber LED is solid ON unless it is on continuously for at least 10 minutes.
Blue	Power control status	• Solid OFF - Blade is not receiving power. • Solid ON - Blade is not operational. • Flashes once every second (1 Hz) - Powered off. Ready to remove. • Flashes once per 10 seconds (flash) - Normal. Blade is powered on.

Table 12-3. Explanation of Ethernet Expansion Blade ethernet port LED states

LED Color	Blade Status
Green	• Solid ON - Link is up; data can be sent or received through the ethernet port. • Solid OFF - Link is down; data cannot be sent or received through the ethernet port.
Amber	• Flashes at irregular intervals - Data activity is occurring through the ethernet port. • Solid OFF - No data activity is occurring through the ethernet port.

Library conversions

Refer to the following sections for library conversion instructions:

- "Desktop to rack-mounted library conversion"
- "Rack-mounted to desktop library conversion" on page 12-53

Desktop to rack-mounted library conversion

Complete the following to convert your library from a desktop unit to a rack mounted unit.

1. Complete "Preparing a library or library module for repairs" on page 12-2.
2. Disconnect library cables.
   a. Disconnect all power cords from the power source and the library.
   b. Disconnect all drive cables.
   c. Disconnect the ethernet cable from the Library Control Blade.
3. Remove the library foot pads. For instructions, see "Removing/installing library foot pads" on page 12-54.
4. Install the library in the rack. For instructions, see Chapter 3, "Installing a new library in a rack," on page 3-1.
5. Cable the library. For instructions, see "Cabling the library" on page 3-35.
6. Complete "Returning a library or library module to normal operations after repairs" on page 12-3.

Rack-mounted to desktop library conversion

Complete the following to convert your library from a rack mounted unit to a desktop unit.

1. Complete “Preparing a library or library module for repairs” on page 12-2.
2. Disconnect library cables.
   a. Disconnect all power cords from the power source and the library.
   b. Disconnect all drive cables.
   c. Disconnect the ethernet cable from the Library Control Blade.
3. Reduce library weight. For instructions, see “Reducing library weight” on page 3-5.
4. Remove rack ears from all library modules.
   a. Grasp the I/O station handle and pull it toward you until it locks in the open position.
   b. Remove the right rack ear (**2** in Figure 12-47).

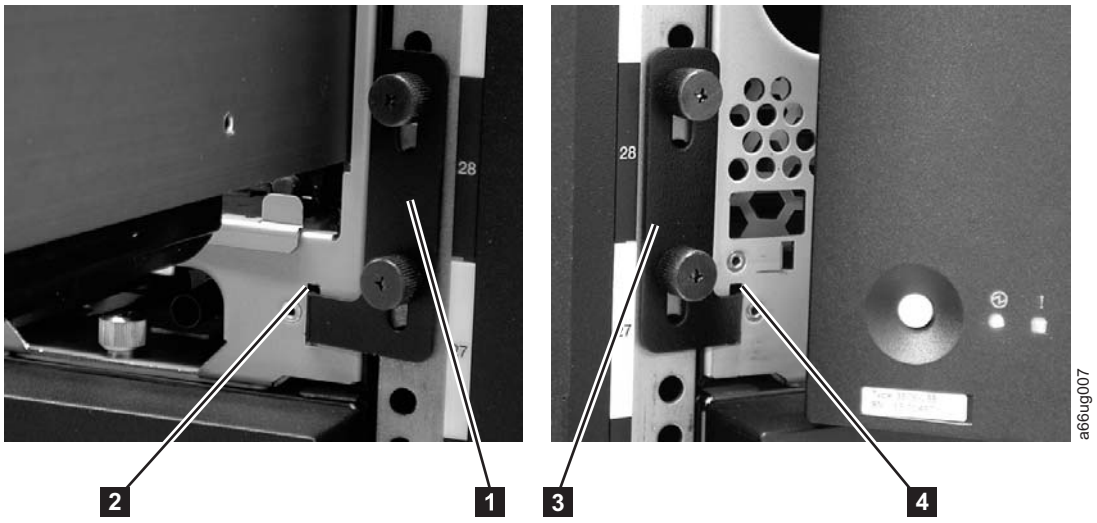


Figure 12-47. Removing the rack ears on a control module

      1) Loosen the right rack ear thumb screws.
      2) Remove the right rack ear.
   c. Remove the left rack ear (**3** in Figure 12-47).
      1) Open the left door of the library unit slightly.
      2) Grasp the hinged side of the door and, while you are pulling on the door, push right to expose the left rack ear.
      3) Loosen the left rack ear thumb screws.
      4) Remove the left rack ear.
   d. Repeat this process for all modules in the library.
5. Remove the library from the rack.

   Note: Without drive sleds and power supplies, a 5U library (control module) weighs approximately 50 lbs, and a 14U library (control module + 9U expansion module) weighs approximately 110 lbs.

   a. With a person on each side of the library, slide it out of the rack. You might prefer to slide each unit of a multi-unit library out of the rack separately.

b. Place the unit on a sturdy work surface to repair.

6. Install library foot pads. For instructions, see “Removing/installing library foot pads.”
7. Install the library components that are removed for weight reduction. For instructions, see “Installing library components removed for weight reduction” on page 3-32.
8. Cable the library. For instructions, see “Cabling the library” on page 3-35.
9. Complete “Returning a library or library module to normal operations after repairs” on page 12-3.

Removing/installing library foot pads

If your library is rack-mounted, foot pads must be installed on the bottom of the library chassis before the library can be used as a desktop unit. If your library is used as a desktop unit, foot pads are installed on the bottom of the library. Foot pads must be removed before the library can be installed in a rack.

Removing library foot pads

To remove the library foot pads:

1. Place the sling that was shipped with your library underneath the library halfway between the front and back feet. Ensure that both sling handles are an equal distance from the sides of the library. Use of the sling is recommended for a 9U module. A 5U module is much lighter in weight, and it might not be necessary to use the sling.
2. Carefully lay the library on its side.
3. With a #2 Phillips screwdriver, remove the foot pads that are attached to the bottom of the library. Store these parts for future use.
4. Carefully return the library to an upright position on top of the sling.

Installing Library Foot Pads

For a desktop installation, foot pads must be installed on the bottom module of your library. To install the library foot pads:

1. Being very careful, lay the module on its side.
2. Using a #2 Phillips screwdriver, install the foot pads on the bottom of the library chassis. See Figure 12-48 on page 12-55 for foot pad locations.

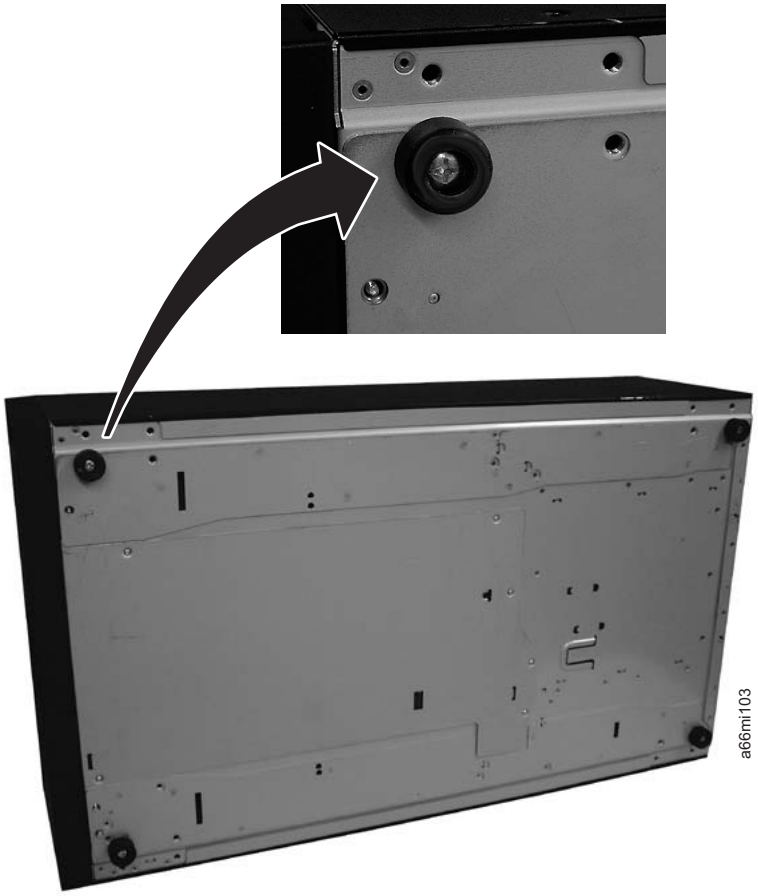


Figure 12-48. Foot pad Locations

3. Carefully return the library to an upright position.
4. Use the lifting sling to place the library module in the desktop location.
5. When you finish these desktop installation steps, store the installation sling in a secure location for possible future use.

Chapter 13. Parts list

Customer replaceable unit (CRU) parts list

To order CRU parts, contact your IBM sales representative.

For information about ordering media, refer to "Ordering media supplies" on page 9-14.

Important: This library has Tier 1 CRUs (customer replaceable units). These CRUs are parts of the library that must be added, removed, and replaced by the customer. If a customer chooses to have the CRU added or removed/replaced by an IBM service representative, there is a charge for the service.

Before a replacement CRU is ordered, ensure that the following criteria are met:

- The failure is repeatable.
- A dump is captured for emailing to IBM service.
  - Use the Web User Interface (**Service Library** > **Capture Library Log**) for library dumps.
  - Use the Web User Interface (**Service Library** > **Capture Drive Log**) for drive dumps.

CRU Type	Description	Feature Code	CRU Part Number
Assemblies	LTO Ultrium Gen 3 LVD Ultra160 drive sled	8037	23R6182
	LTO Ultrium Gen 3 2 Gb Fibre drive sled	—	23R2601
	LTO Ultrium Gen 3 4 Gb Fibre drive sled	8042	23R6450
	LTO Ultrium Gen 4 Fibre drive sled	8142	95P4824
	LTO Ultrium Gen 4 SAS drive sled	8139	95P4825
	LTO Ultrium Gen 5 Fibre drive sled	8242	46X4440
	LTO Ultrium Gen 6 Fibre drive sled	8342	35P2599
	Power Supply	1900	23R2582
	Library Control Blade (LCB) (7clll) without Compact Flash (CF) Card	—	35P3087
	Library Control Blade (LCB) with Compact Flash (CF) Card Includes: Library Controller Board (7cIII), Parts Failure Report Sheet, Compact Flash, 3576 LCB Kit Pubs, Label	—	35P2781
	Ethernet Expansion Blade (EEB) Includes: EEB, 6 short ethernet cables (1 m), 1 long ethernet cable (3.2 m), and 1 small cover plate.	3470	35P2832
	Compact Flash Card	—	45E3170
	Rack Mount Kit	7003	—

CRU Type	Description	Feature Code	CRU Part Number
License Keys	Capacity Expansion	1640	—
	Advanced Reporting	1650	—
	Path Failover	1682	—
	Transparent LTO Encryption	5900	—
Terminators & Wrap Plugs	Terminator, LVD multi-mode	—	23R5841
	Terminator, Module Communication (Qty 2 per P/N)	—	45E8321
	LVD SCSI Wrap Tool	—	23R5840
	Fibre Wrap Tool	—	12R9314
Interposers	Interposer, LC-SC fibre cable	5096	12R9321
	Interposer, VHDCI/HD68 SCSI cable	—	12R9321
	Interposer, SAS/MiniSAS 4x (2.0m max. cable length)	5400	95P4994
	Interposer, MiniSAS/MiniSAS 4x (2.0m max. cable length)	5500	95P4996
Miscellaneous	Cable, Module-to-Module Communication	—	23R2602
	Cable, RJ45 Ethernet Crossover	—	23R3663
	Cover, top for control module and expansion module	—	23R2594
	Cover, side for 5U control module	—	23R2595
	Covers, side for 9U expansion module	—	23R2596
	Fan Bay Cover, cover plate for empty slot next to LCB	—	23R2604
	Power Supply Cover, cover plate for empty Power Supply slot	—	23R2606
	Drive Bay Cover, cover plate for empty drive slot	—	23R2605
	Cover plate for empty slot next to the EEB	—	35P3057
	Cover plate for empty slots after EEB is removed	—	35P2982
	Library and Drive Firmware Update (by an IBM Service Representative)	0500	—
	Rack ears kit	—	23R3349
	Rack Power Distribution Unit (PDU) power cord	9848	39M5378
	Foot pads kit	—	23R2599
Ethernet Cables	Qty 2 per P/N 0.3 m	6001	45E3349
	Qty 1 per P/N 3.2 m	—	95P4759
SCSI Cables, HD68/HD68	0.4 m	8037	23R6408
SCSI Cables, VHDCI/ HD68	2.5 m	5602	23R3841
	4.5 m	5604	23R3594
	10 m	5610	23R3593
Fibre Cables, LC-LC	5 m	6005	39M5700
	13 m	6013	39M5701
	25 m	6025	12R9915
SAS Cables, SAS to MiniSAS 1x	2 m	5402	95P4587
	5.5 m (Do not use with 4x interposer, FC 5400)	5406	95P4588

CRU Type	Description	Feature Code	CRU Part Number
SAS Cables, Mini SAS to MiniSAS 1x	2 m	5502	95P4488
	5.5 m (Do not use with 4x interposer, FC 5500)	5506	95P4494

Power cords and receptacles

Figure 13-1 shows the plugs that are used by the power cords in Table 13-1 on page 13-4. Match the index number that is beside each plug to the index number in the table.

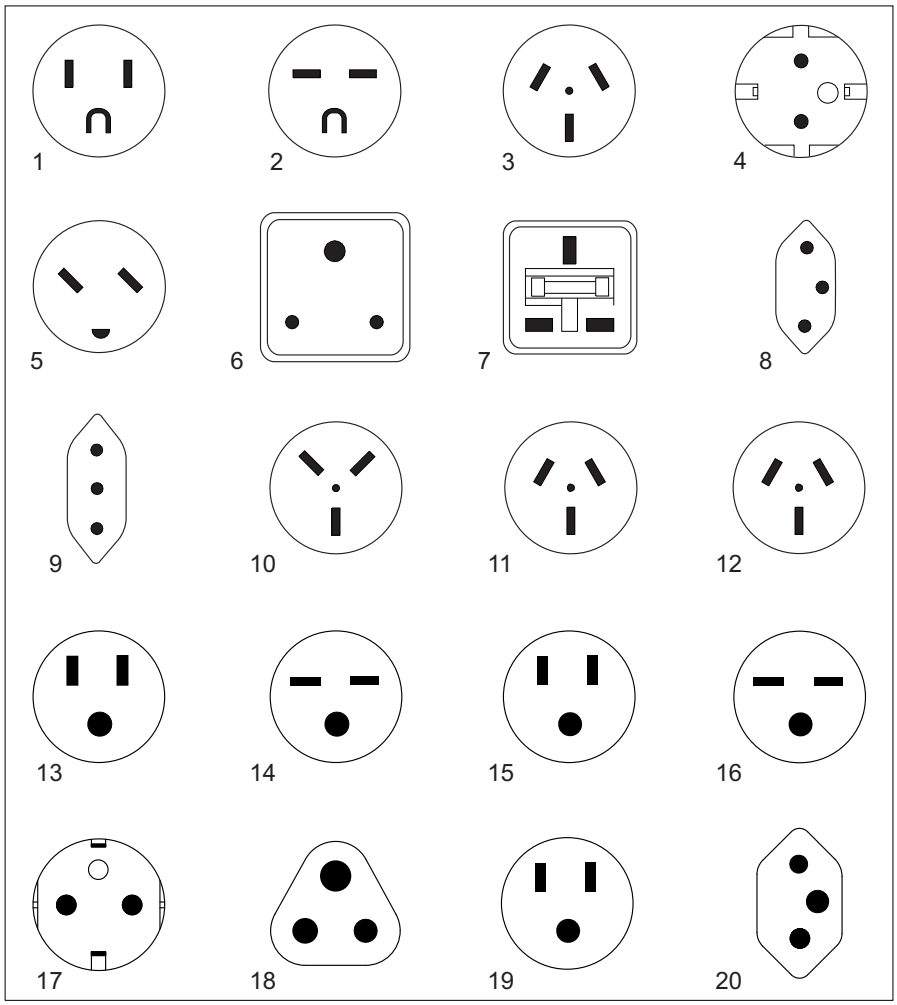


Figure 13-1. Types of power cord receptacles

Table 13-1. Power cords

Description, Feature Code (FC), and Part Number (PN)	Plug Standard Reference	Country or Region	Index Number in Figure 13-1 on page 13-3
US/Canada • 2.8 m, 125V • FC 9800 • PN 39M5081 • (See Note)	NEMA 5-15P	Aruba, Bahamas, Barbados, Bermuda, Bolivia, Brazil, Canada, Cayman Islands, Colombia, Costa Rica, Curacao, Dominican Republic, Ecuador, El Salvador, Guatemala, Guyana, Haiti, Honduras, Jamaica, Japan, Liberia, Mexico, Netherlands Antilles, Nicaragua, Panama, Peru, Philippines, Saudi Arabia, South Korea, Suriname, Taiwan, Trinidad Tobago, Venezuela, US	1
Chicago • 1.8 m, 125 V • FC 9986 • PN 39M5080	NEMA 5-15P	Chicago, U.S.A.	1
US/Canada • 2.8 m, 250 V • FC 9833 • PN 39M5095	NEMA 6-15P	Aruba, Bahamas, Barbados, Bermuda, Bolivia, Brazil, Canada, Cayman Islands, Costa Rica, Curacao, Dominican Republic, Ecuador, El Salvador, Guatemala, Guyana, Haiti, Honduras, Jamaica, Japan, Liberia, Netherlands Antilles, Nicaragua, Panama, Peru, Philippines, Suriname, Taiwan, Thailand, Trinidad Tobago, Venezuela, US	2
Australia • 2.8 m, 250V • FC 9831 • PN 39M5102	AS 3112 NZS 198	Argentina, Australia, China, Colombia, New Zealand, Papua New Guinea, Paraguay, Uruguay, Western Samoa	3

Table 13-1. Power cords (continued)

Description, Feature Code (FC), and Part Number (PN)	Plug Standard Reference	Country or Region	Index Number in Figure 13-1 on page 13-3
France, Germany • 2.8 m, 250V • FC 9820 • PN 39M5123	CEE 7 - VII	Afghanistan, Algeria, Andorra, Angola, Aruba, Austria, Belgium, Benin, Brazil, Bulgaria, Burkina Faso, Burundi, Cameroon, Central African Republic, Chad, Congo-Brazzaville, Curacao, Czech Republic, Democractic Republic of Congo, Denmark, Egypt, Finland, France, French Guiana, Germany, Greece, Guinea, Hungary, Iceland, Indonesia, Iran, Ivory Coast, Jordan, Kenya, Korea, Lebanon, Luxembourg, Macau, Malagasy, Mali, Martinique, Mauritania, Mauritius, Monaco, Morocco, Mozambique, Netherlands, Netherlands Antilles, New Caledonia, Niger, Norway, Poland, Portugal, Romania, Russia, Saudi Arabia, Senegal, Spain, Sweden, Sudan, Syria, Togo, Tunisia, Turkey, Yugoslavia, Zaire, Zimbabwe, Vietnam	4
Denmark • 2.8 m, 250V • FC 9821 • PN 39M5130	DK2-5A	Denmark	5
South Africa • 2.8 m, 250V • FC 9829 • PN 39M5144	SABS 164	Bangladesh, Burma, Pakistan, South Africa, Sri Lanka	6
United Kingdom • 2.8 m, 250V • FC 9825 • PN 39M5151	BS 1363	Antigua, Bahrain, Bermuda, Brunei, Channel Islands, China (Hong Kong S.A.R.), Cyprus, Fiji, Ghana, Guyana, India, Iraq, Ireland, Jordan, Kenya, Kuwait, Malaysia, Malawi, Malta, Nepal, Nigeria, Oman, Polynesia, Qatar, Sierra Leone, Singapore, Tanzania, Uganda, UK, United Arab Emirate (Dubai), Yemen, Zambia	7

Table 13-1. Power cords (continued)

Description, Feature Code (FC), and Part Number (PN)	Plug Standard Reference	Country or Region	Index Number in Figure 13-1 on page 13-3
Switzerland • 2.8 m, 250V • FC 9828 • PN 39M5158	SEV SN 416534	Liechtenstein, Switzerland	8
Italy • 2.8 m, 250V • FC 9830 • PN 39M5165	CEI 23- 16	Chile, Ethiopia, Italy, Libya, Somalia	9
Israel • 2.8 m, 250V • FC 9827 • PN 39M5172	S11-32-1971	Israel	10
Argentina • 2.8 m, 250V • FC 9834 • PN 39M5068	IEC 83-A5	Argentina, Brazil, Colombia, Paraguay, Trinidad Tobago, Uruguay	11
China • 2.8 m, 250V • FC 9840 • PN 39M5206	CCEE	People's Republic of China	12
Taiwan LV* • 2.8 m, 125V • FC 9835 • PN 39M5247	CNS 10917-3	Taiwan	13
Taiwan HV** • 2.8 m, 250V • FC 9841 • PN 39M5254	CNS 10917-3	Taiwan	14
Japan LV* • 2.8 m, 125V • FC 9842 • PN 39M5199	JIS C8303, C8306	Japan	15
Japan HV** • 2.8 m, 250V • FC 9843 • PN 39M5186	JIS C8303, C8306	Japan	16
Korea HV** • 2.8 m, 250V • FC 9844 • PN 39M5219	KS C8305, K60884-1	Korea	17

Table 13-1. Power cords (continued)

Description, Feature Code (FC), and Part Number (PN)	Plug Standard Reference	Country or Region	Index Number in Figure 13-1 on page 13-3
India HV** • 2.8 m, 250V • FC 9845 • PN 39M5226	IS 6538	India	18
Brazil LV* • 2.8 m, 125V • FC 9846 • PN 39M5233	InMetro NBR 6147	Brazil	19
Brazil HV** • 2.8 m, 250V • FC 9847 • PN 39M5240	InMetro NBR 14136	Brazil	20
* Low Voltage ** High Voltage			

Appendix A. Message retrieval at the host

Retrieving messages from different hosts is described in this appendix.

Obtaining error information from a System p® (RS/6000)

IBM device drivers for the System p system logs error information when an error occurs on a tape drive or library.

The error information includes:

1. Device VPD
2. SCSI command parameters
3. SCSI sense data (if available)

The AIX tape and Media Changer device driver for the System p provides logging to the system error log for various errors. You can view the error log by following this procedure.

1. At the AIX command line, type `errpt |pg` to display a summary report, or type `errpt -a |pg` to display a detailed report. Press **[Enter]**.

   Note: In most cases, you can use the summary report to find the date and time of any errors that are related to library devices, then use the detail report to obtain the sense data that is needed to identify the cause of the error.
2. Press **[Enter]** to scroll through the error log.
3. Type `q` and press **[Enter]**, to quit the error log at any time.

To correct a problem you noticed in the **errpt** report, determine the type of error by using the examples that follow:

- For library errors [Resource Name = **smc**n (for example, smc0) and Resource Type = 3576]), refer to "Library error log example" on page A-2 and locate the SCSI sense data.
- For drive errors [Resource Name = **rmt**n (for example, rmt0) and Resource Type = LTO], refer to "Drive error log example" on page A-3 and locate the SCSI sense data.
- For SCSI bus errors (not SCSI adapter errors), refer to "SCSI bus error: Example 1" on page A-4 and "SCSI bus error: Example 2" on page A-5 to determine which host adapter, SCSI bus, and device or devices are affected.
- For Fibre Channel errors (not Fibre Channel adapter errors), determine which host adapter and device are affected.
- For SCSI adapter errors (not SCSI bus errors), use the maintenance package for the host.

Note: See "Drive sense data" on page C-4 for further details on sense data.

Library error log example

```
LABEL: TAPE_ERR2
IDENTIFIER: 476B351D
Date/Time: Wed Oct 11 11:42:17
Sequence Number: 25265
Machine ID: 000D090D4C00
Node ID: tsm
Error Class: H
Error Type: PERM
Resource Name: smc0
Resource Class: tape
Resource Type: 3576
Location: 40-60-00-6,0
VPD:
Manufacturer................IBM
Machine Type and Model......ULT3576-TL
Serial Number...............IBM7810698
Device Specific . (FW) .....x.xx (Firmware Level)
Description
TAPE DRIVE FAILURE
Probable Causes
TAPE DRIVE
Failure Causes
TAPE
TAPE DRIVE
Recommended Actions
PERFORM PROBLEM DETERMINATION PROCEDURES
Detail Data
SENSE DATA
0C00 0000 A500 0001 1009 0101 0000 0000 0000 0000 7000 0400 0000 0046 0000 0000
4400 8100 0000 0000 0000 0000 0000 0200 4801 E300 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
```

Figure A-1. AIX ERRPT library error log example

Table A-1. AIX ERRPT Library Sense Data

Hex	Description
A5	SCSI Command
0001, 1009, 0101	Command Parameters
70	Byte 0 of Library Sense Data
04	Sense Key
4400	ASC/ASCQ (Additional Sense Code/Additional Sense Code Qualifier)
81	Library SAT (Service Action Ticket) Code

Drive error log example

```
LABEL: TAPE_ERR1
IDENTIFIER: 4865FA9B
Date/Time: Wed Oct 10 11:39:43
Sequence Number: 25264
Machine ID: 000D090D4C00
Node ID: tsm
Class: H
Type: PERM
Resource Name: rmt2
Resource Class: tape
Resource Type: LTO
Location: 40-60-00-2,0
VPD:
Manufacturer................IBM
Machine Type and Model......ULT3576-TD3
Serial Number...............1300015078
Device Specific.(FW)........xxxx (Firmware Level)
Description
TAPE OPERATION ERROR
Probable Causes
TAPE
User Causes
MEDIA DEFECTIVE
DIRTY READ/WRITE HEAD
Recommended Actions
FOR REMOVABLE MEDIA, CHANGE MEDIA AND RETRY
PERFORM PROBLEM DETERMINATION PROCEDURES
Detail Data
SENSE DATA
0602 0000 0100 0000 0200 0000 0000 0000 0000 0000 7000 0300 0000 001C 0000 0000
5200 0700 20B0 0000 0000 0000 0000 0000 0000 0000 058A 0212 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
```

Figure A-2. AIX ERRPT drive error log example

Table A-2. AIX ERRPT Drive Sense Data

Hex	Description
01	SCSI Command
0000, 0200, 0000	Command Parameters
70	Byte 0 of Tape Drive Sense Data
03	Sense key (Hardware error in this example)
5200	ASC/ASCQ (Additional Sense Code/Additional Sense Code Qualifier)
20B0	FSC (Fault Symptom Code)
058A	Relative LPOS
02	SCSI ID

SCSI bus error: Example 1

```
LABEL: SCSI_ERR10
IDENTIFIER: 0BA49C99
Date/Time: Wed Oct 17 09:55:32
Sequence Number: 16140
Machine Id: 00003ABF4C00
Node Id: ofgtsm
Class: H
Type: TEMP
Resource Name: scsi3
Resource Class: adapter
Resource Type: sym896
Location: 40-59
VPD:
Product Specific.( ).......DUAL CHANNEL PCI TO ULTRA2 SCSI
ADAPTER
Part Number.................03N3606
EC Level....................F71335
Manufacture ID..............A16592
Serial Number...............0749
Description
SCSI BUS ERROR
Probable Causes
CABLE
CABLE TERMINATOR
DEVICE
ADAPTER
Failure Causes
CABLE LOOSE OR DEFECTIVE
DEVICE
ADAPTER
Recommended Actions
PERFORM PROBLEM DETERMINATION PROCEDURES
CHECK CABLE AND ITS CONNECTIONS
Detail Data
SENSE DATA
0001 0017 0000 0000 0000 0091 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 4304 0000 0000 0000 0000 2000 0003 0203 6760 9808 0000 F7FB E1B8
0000 0015 000B 0210 0678 C800 0000 8200 8277 1B20 00A2 ED00 0000 0002 FFFF FFFF
00FF 0000 111F F000 F3DF F110
```

Figure A-3. Example of error suggesting SCSI bus problem, which takes down entire bus

SCSI bus error: Example 2

```
LABEL: TAPE_ERR4
IDENTIFIER: 5537AC5F
Date/Time: Wed Oct 17 09:00:41
Sequence Number: 16101
Machine Id: 00003ABF4C00
Node Id: ofgtsm
Class: H
Type: PERM
Resource Name: smc0
Resource Class: tape
Resource Type: 3576
Location: 40-58-00-0,1
VPD:
Manufacturer................IBM
Machine Type and Model......ULT3576-TL
Serial Number...............IBM7810698
Device Specific.(FW)........x.xx
Description
TAPE DRIVE FAILURE
Probable Causes
ADAPTER
TAPE DRIVE
Failure Causes
ADAPTER
TAPE DRIVE
Recommended Actions
PERFORM PROBLEM DETERMINATION PROCEDURES
Detail Data
SENSE DATA
0600 0000 1200 0000 FF00 0000 0000 0000 0200 0800 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
```

Figure A-4. SCSI problem points to library control path as possible cause

Summary report

```
1 2 34 5 6
FFE2F73A 1012150900 U H rmt5 UNDETERMINED ERROR
0BA49C99 1012150800 T H scsi8 SCSI BUS ERROR 7
C60BB505 1012141500 P S SOFTWARE PROGRAM ABNORM TERMINATED
C42F11D4 1012105200 U S VSC:DE SOFTWARE ERROR
C42F11D4 1012105000 U S VSC:DE SOFTWARE ERROR
FFFA352B 1012104900 U S MS:CS SOFTWARE ERROR
FFFA352B 1012104900 U S MS:CS SOFTWARE ERROR
5537AC5F 1012091700 P H rmt9 TAPE DRIVE FAILURE
5537AC5F 1012091700 P H rmt9 TAPE DRIVE FAILURE
5537AC5F 1012091700 P H rmt9 TAPE DRIVE FAILURE
5537AC5F 1012091600 P H rmt8 TAPE DRIVE FAILURE
5537AC5F 1012091600 P H rmt8 TAPE DRIVE FAILURE
5537AC5F 1012091600 P H rmt8 TAPE DRIVE FAILURE
C60BB505 1012082000 P S SOFTWARE PROGRAM ABNORM TERMINATED
C42F11D4 1011183600 U S VSC:DE SOFTWARE ERROR
C42F11D4 1011183300 U S VSC:DE SOFTWARE ERROR
C42F11D4 1011181800 U S VSC:DE SOFTWARE ERROR
C42F11D4 1011174700 U S VSC:DE SOFTWARE ERROR
FFFA352B 1011172900 U S MS:CS SOFTWARE ERROR
FFFA352B 1011172900 U S MS:CS SOFTWARE ERROR
C42F11D4 1011155300 U S VSC:DE SOFTWARE ERROR
C42F11D4 1011153900 U S VSC:DE SOFTWARE ERROR
C42F11D4 1011153800 U S VSC:DE SOFTWARE ERROR
C42F11D4 1011150900 U S VSC:DE SOFTWARE ERROR
```

Figure A-5. AIX ERRPT commands: Error log example

NUMBER	DESCRIPTION
1	Error ID
2	Timestamp
3	Error Type
4	Error Class
5	Resource Name
6	Error Description
7	How SCSI Bus Error will Display in Log

ERROR CLASS	DESCRIPTION
H	Hardware
S	Software
O	Informational

ERROR TYPE	DESCRIPTION
PEND	The availability loss of a device or component is imminent.
PERF	The performance of a device or component has degraded to an unacceptable level.
PERM	A hardware or software condition that could not be recovered from.
TEMP	A hardware condition that was recovered from after several unsuccessful attempts.
UNKN	The severity of the condition could not be determined.

A69M0170

Retrieving from an AS/400 system with RISC processor

IBM device drivers for the AS/400 system log error information when an error occurs on a tape drive or library.

The error information includes the following data:

1. Device VPD
2. SCSI command parameters
3. SCSI sense data (if available)

To gain access to the AS/400 problem logs and error logs, sign on at any available workstation with the QSRV logon and its security password (QSRV). After you sign on, the correct access authorizations is granted and the AS/400 MAIN MENU displays.

1. Type STRSST (Start System Service Tools) command on the command entry line on the **AS/400** main menu, and press **[Enter]**.
2. On the "System Service Tool (SST)" screen, select **Start a service tool**, and press **[Enter]**.
3. On the "Start a Service Tool" screen, select **Product activity log**, and press **[Enter]**.
4. On the "Product activity log" screen, select **Analyze log**, and press **[Enter]**.
5. On the "Select Subsystem Data" screen, select **Magnetic media**, enter the From and To time period for searching the error log, and press **[Enter]**.
6. On the "Select Analysis Report Options" screen, select the following, and press **[Enter]**.
   a. Report type. 1
   b. Optional entries to include
      1) Informational . . . . . YES
      2) Statistic . . . . . NO
   c. Reference code selection
      1) Option 1
      2) Reference codes. . . . . *ALL
   d. Device selection
      1) Option 1
      2) Device type or resource names . . *ALL
7. On the "Log Analysis Report" screen, enter a **5** on an error line that has a resource type of 3583 (library) or 3580 (drive), and press **[Enter]**.
8. On the "Display Detail Report for Resource" screen, press:
   - F4=Additional information.

     Pressing F4 displays the machine type and serial number of the device. It also displays SCSI sense data, if available.
   - F6=Hexadecimal report.

     Pressing F6 displays the device hexadecimal data (for support use).
   - F9=Address Information.

     Pressing F9 displays the SCSI address information.

AS/400 product activity log

```
Product Activity Log Page . . . : 1
ROMLPAR1 08/26/05 10:28:40
Invocation . . . . . : Product Activity Log
Title . . . . . : Log ID Report
System type . . . . . : 9406
System model . . . . . : 825
System release . . . . : V5R3M0
System name . . . . . : ROMLPAR1
System serial
number . . . . . : 10-F321B
Log ID . . . . . : 09020145
Include hexadecimal
data . . . . . : Y Y=YES
N=NO
Product Activity Log Page . . . : 2
ROMLPAR1 08/26/05 10:28:40
Detail Report for Resource
Serial Resource
Name Type Model Number Name
TAPMLB19 3580 001 00-1004538
Log ID . . . . . : 09020145 Sequence . . . . . : 211510
Date . . . . . : 04/21/05 Time . . . . . : 10:40:11
Reference code . . . . . : 9350 Secondary code . . . : 00000000
Table ID . . . . . : 63A00001 IPL source/state . . : B / 3
Class . . . . . : Permanent
System ref code . . . . . : 63A09350
Tape unit detected a read or write error on tape medium
Physical location:
Frame ID . . . . . :
Card position . . . . . :
Device position . . . . :
Logical address:
PCI bus: Library:
System bus . . . . . : 36 I/O adapter . . . . . : 2
System board . . . . . : 0 I/O bus . . . . . : 1
System card . . . . . : 32 Library: 20
Controller . . . . . : 4
Device . . . . . : 0
SENSE DATA FOLLOWS. . . . :
DATA OFFSET 0 1 2 3 4 5 6 7 8 9 A B C D E F
00000000 71000300 0000001C 00000000 53000600
00000010 31190601 00020000 00000000 00000000
00000020 00000301
00000000 0000 C5D3F0F5 00000188 00E00180 8983EBC2 4B9D8001 00033A36 20E00902 01450000 *EL05...h....ic.B.....................*
00000000 0040 F3F8F2F8 F4F4F6F3 C1F00002 00240000 00200000 00050001 00140004 00000002 *382844 63A0.....................*
00000000 0060 00000000 00000000 00000000 40404040 40404040 40400000 00000000 00000000 *.............  ..........*
00000000 0080 00000000 00000000 00000000 00000000 00000000 00000000 00000000 0000E3C1 *.............................TA*
00000000 00A0 D7D4D3C2 F1F94040 00000000 00000000 00000000 00000000 40404040 40404040 *PMLB19 ................ *
00000000 00C0 40404040 40404040 40404040 40404040 40404040 40404040 40404040 40404040 * *
00000000 00E0 F6F3C1F0 F0F0F0F1 0000E2D3 C9C3C9D6 4040E5F5 D9F3D4F0 40400000 00000000 *63A00001..SLICIO V5R3M0 ......*
00000000 0100 01030000 00000000 00000141 00000000 00000000 01950000 00000000 00000197 *.....................n.........p*
00000000 0120 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 *..............................*
00000000 0140 E3C1D7F2 F7404040 40404040 40404040 40404040 40404040 40404040 00070001 *TAP27 ....*
00000000 0160 00000000 10200003 00000000 00000000 00000000 00000000 0009001E 00000188 *..............................h*
00000000 0180 F8807800 28440001 00002600 21410400 63A00001 93500100 45381202 05D80000 *8...................l&.......Q..*
00000000 01A0 00000000 00004624 00000000 00000000 00040000 00003580 0001A170 02903435 *..............................*
Product Activity Log Page . . . : 3
ROMLPAR1 08/26/05 10:28:40
00000000 01C0 36310040 00007100 03000000 001C0000 00005300 06003119 06010002 00000000 *... ..........................*
00000000 01E0 00000000 00000000 03010000 00000000 00000000 00000000 00000000 00000000 *..............................*
00000000 0200 00000000 0000D9C5 D8400000 D9E200C 02000000 0000E2C3 E2C91202 00180000 *......REQ ..RS........SCSI......*
00000000 0220 00000000 0000C5D9 D940C3C8 C3D20444 8502D9E2 0000E2C3 E2C91202 00180300 *......ERR CHCK..e.RS..SCSI......*
00000000 0240 00008000 0000E2D5 E2C47100 03000000 001C0000 0000C5D9 D7C11202 05D80000 *......SNSD............ERPA...Q..*
00000000 0260 00171202 05D8D9C5 E2D70000 00171202 05D8D9E2 00000000 D4C5C4C9 C10000C3 *.....QRESP.......QRS....MEDIA..C*
00000000 0280 D7D7F1F2 F5C500D4 E3C1D7C3 D3D500C3 D7D7F6F4 F0F000E4 C6C9F0F0 F8F7F1C3 *PP125E.MTAPCLN.CPP6400.UFI00871C*
00000000 02A0 D7D7F1F8 F5C600D5 00000000 00000000 00000000 00000000 00000000 00000000 *PP185F.N........................*
00000000 02C0 00000000 00000000 00000000 00000000 00000000 00000000 C3D7D7F6 F3F0C3D5 *........................CPP630CN*
00000000 02E0 F6F3C1F0 F9F3F5F0 F0F0F0F0 F0F0F0F0 F0F0F0F0 F0F1F9F7 F8F0F0F7 0000E8D5 *63A0935000000000000001978007..YN*
00000000 0300 00000000 00000000 40404040 40404040 40404040 40404040 40404040 40404040 *........ *
* * * * * E N D O F C O M P U T E R P R I N T O U T * * * * *
```

Retrieving from an HP-UX system

The HP-UX system provides information when an error occurs on a tape drive or library in `syslog /var/adm/syslog.log`. When you locate the error information, refer to the troubleshooting information in this manual.

Retrieving from a Sun system

The Sun system provides information when an error occurs on a tape drive or library in `system-errolog /var/adm/messages`. When you locate the error information, refer to the troubleshooting information in this manual.

The two service aid programs are provided with the IBM SCSI tape device driver for SunOS:

- Tape service program

  A tape service program that is called **tapesrvc.c** is provided and contains the following service aids:

  – Query device serial number

  – Format tape cartridge

  – Force device error dump

– Save device error dump
– Download device code

The tape service program is started with the **/opt/stddutil/tapesrvc** command.

Note: You must have root authority to run the tape service program.

The program is menu-driven. Use discretion when this program is run because it opens the device in diagnostic mode.

- Sample program

  A sample program that is called **tapetest.c** is provided, which gives a demonstration of the device driver interface usage.

  The sample program is started with the **/opt/stddutil/tapetest** command. The program is useful for verifying that the device driver and the device are functional. The program is menu-driven.

Appendix B. TapeAlert flags supported by the drive

This appendix is intended to provide additional information to the reader about the tape drive. All error code and diagnostic information contained in this chapter are accessed from the Operator Panel of the library. The drive portion of the Operator Panel display contains any drive error codes. Therefore there is no need to open the library to access the buttons on the drive as described in this chapter. See the** Setup and Operator Guide **for a complete description of the Operator Panel functions and displays.

TapeAlert is a standard that defines status conditions and problems that are experienced by devices such as tape drives, autoloaders, and libraries. The standard enables a server to read TapeAlert messages (called *flags*) from a tape drive with the SCSI bus. The server reads the flags from Log Sense Page 0x2E.

This library is compatible with TapeAlert technology, which provides error and diagnostic information about the drives and the library to the server. Because library and drive firmware can change periodically, the SNMP interface in the library does not require code changes if devices add extra TapeAlerts that are not supported today. However, should this action occur, the MIB is written to minimize impact to the SNMP monitoring station. At the time of this writing, the TapeAlert flags in this appendix correctly represent TapeAlerts that is sent. The MIB file must not be taken to mean that all traps that are defined in the MIB are sent by the library or that they will be sent in the future.

This appendix lists TapeAlert flags that are supported by the Ultrium tape drives.

Table B-1. TapeAlert flags supported by the Ultrium tape drive

Flag Number	Flag	SNMP Trap	Description	Action Required
3	Hard error	No	Set for any unrecoverable read, write, or positioning error. (This flag is set with flags 4, 5, or 6.)	See the Action Required column for Flag Number 4, 5, or 6 in this table.
4	Media	No	Set for any unrecoverable read, write, or positioning error that is because of a faulty tape cartridge.	Replace the tape cartridge.
5	Read failure	No	Set for any unrecoverable read error where isolation is uncertain and failure might be because of a faulty tape cartridge or to faulty drive hardware.	If Flag 4 is also set, the cartridge is defective. Replace the tape cartridge.
6	Write failure	No	Set for any unrecoverable write or positioning error where isolation is uncertain and failure might be because of a faulty tape cartridge or to faulty drive hardware.	If Flag Number 9 is also set, make sure that the write-protect switch is set so that data can be written to the tape (see “Write-protect switch” on page 9-3). If Flag Number 4 is also set, the cartridge is defective. Replace the tape cartridge.

Table B-1. TapeAlert flags supported by the Ultrium tape drive (continued)

Flag Number	Flag	SNMP Trap	Description	Action Required
7	Media life	No	Set when the tape cartridge reaches its end of life (EOL).	1. Copy the data to another tape cartridge. 2. Discard the old (EOL) cartridge.
8	Not data grade	No	Set when the cartridge is not data-grade. Any data that you write to the tape is at risk.	Replace the tape with a data-grade tape.
9	Write protect	No	Set when the tape drive detects that the tape cartridge is write-protected.	Ensure that the cartridge 's write-protect switch is set so that the tape drive can write data to the tape (see "Write-protect switch" on page 9-3).
10	No removal	No	Set when the tape drive receives an UNLOAD command after the server prevented the tape cartridge from being removed.	Refer to the documentation for your server 's operating system.
11	Cleaning media	No	Set when you load a cleaning cartridge into the drive.	No action that is required.
12	Unsupported format	No	Set when you load an unsupported cartridge type into the drive or when the cartridge format was corrupted.	Use a supported tape cartridge.
14	Unrecoverable snapped tape	No	Set when the operation failed because the tape in the drive snapped.	Do not attempt to extract the old tape cartridge. Contact IBM technical support.
15	Cartridge memory chip failure	No	Set when a cartridge memory (CM) failure is detected on the loaded tape cartridge.	Replace the tape cartridge.
16	Forced eject	No	Set when you manually unload the tape cartridge while the drive was reading or writing.	No action that is required.
17	Media that are loaded is Read-only format	No	Set when a cartridge marked as read-only is loaded into the drive. The flag is cleared when the cartridge is ejected.	No action that is required.
18	Tape directory that is corrupted in the cartridge memory	No	Set when the drive detects that the tape directory in the cartridge memory was corrupted.	Re-read all data from the tape to rebuild the tape directory.
19	Nearing media life	No	Set when the tape cartridge is nearing its specified end of life. The flag is cleared when the cartridge is removed from the drive.	1. Copy the data to another tape cartridge. 2. Replace the tape cartridge.
20	Clean now	No	Set when the tape drive detects that it needs cleaning.	Clean the tape drive.

Table B-1. TapeAlert flags supported by the Ultrium tape drive (continued)

Flag Number	Flag	SNMP Trap	Description	Action Required
21	Clean periodic	No	Set when the drive detects that it needs routine cleaning.	Clean the tape drive as soon as possible. The drive can continue to operate, but you must clean the drive soon.
22	Expired clean	No	Set when the tape drive detects a cleaning cartridge that is expired.	Replace the cleaning cartridge.
23	Invalid cleaning tape	No	Set when the drive expects a cleaning cartridge and the loaded cartridge is not a cleaning cartridge.	Use a valid cleaning cartridge.
30	Hardware A	No	Set when a hardware failure occurs that requires that you reset the tape drive to recover.	See “Resetting a drive” on page 8-30. If resetting the drive does not recover the error, contact IBM technical support.
31	Hardware B	No	Set when the tape drive fails its internal Power-On Self Tests.	Note the error code on the single-character display, then contact IBM technical support. .
32	Interface	No	Set when the tape drive detects a problem with the host interface.	Contact IBM technical support.
33	Eject media	No	Set when a failure occurs that requires you to unload the cartridge from the drive.	Unload the tape cartridge, then reinsert it and restart the operation.
34	Download fail	No	Set when an FMR image is unsuccessfully downloaded to the tape drive through the host interface.	Ensure that it is the correct FMR image. Download the FMR image again.
36	Drive temperature	No	Set when the drive 's temperature sensor indicates that the drive 's temperature is exceeding the recommended temperature of the library.	Contact IBM technical support.
37	Drive voltage	No	Set when the drive detects that the externally supplied voltages are either approaching the specified voltage limits or are outside the voltage limits.	Contact IBM technical support.
38	Predictive failure of drive hardware	No	Set when a hardware failure of the tape drive is predicted.	Contact IBM technical support.
39	Diagnostics required	No	Set when the drive detects a failure that requires diagnostic tests for isolation.	Contact IBM technical support.
51	Tape directory invalid at unload	No	Set when the tape directory on the tape cartridge that was previously unloaded is corrupted. The file-search performance is degraded.	Use your backup software to rebuild the tape directory by reading all the data.
52	Tape system area write failure	No	Set when the tape cartridge that was previously unloaded cannot write its system area successfully.	Copy the data to another tape cartridge, then discard the old cartridge.

Table B-1. TapeAlert flags supported by the Ultrium tape drive (continued)

Flag Number	Flag	SNMP Trap	Description	Action Required
53	Tape system area read failure	No	Set when the tape system area cannot be read successfully at load time.	Copy the data to another tape cartridge, then discard the old cartridge.
55	Loading Failure	No	When a tape is loaded into a drive, a hardware malfunction can prevent the tape from being loaded into the drive, or the tape can actually get stuck in the drive.	Possible Causes: 1. A drive hardware error that prevents the tape from being loaded 2. A damaged tape that cannot be loaded in the drive Take this action if the tape cartridge does not load in the drive: 1. Remove the tape cartridge and inspect it for damage. If damaged, discard it. 2. Try another cartridge in that tape drive. If it still fails, or if the cartridge is stuck in the drive, replace the drive sled. Take this action if the tape is stuck in the drive: 1. Attempt to unload the tape from the drive with the host backup application that is using the drive, or the remote or local UI. 2. If the cartridge does not unload, contact IBM technical support for assistance.

Table B-1. TapeAlert flags supported by the Ultrium tape drive (continued)

Flag Number	Flag	SNMP Trap	Description	Action Required
56	Unload Failure	No	When a tape cartridge attempts an unload, a drive hardware malfunction can prevent the tape from being ejected. The tape can actually be stuck in the drive.	Possible Causes: 1. A drive hardware error that prevents the tape from being unloaded 2. A damaged tape that cannot be unloaded from the drive Take this action if the tape does not unload from the drive: 1. Reset the drive. See "Resetting a drive" on page 8-30 2. If resetting the drive does not recover the error, try to manually remove the tape cartridge from the drive and inspect it for damage. If damaged, discard it. 3. If the cartridge does not unload, contact your next level of support. Take this action if the tape is stuck in the drive: 1. Attempt to unload the tape from the drive with the host backup application that is using the drive, or with the remote or local UI. 2. If the cartridge does not unload, contact IBM technical support for assistance.
59	WORM Medium - integrity check failed	No	Set when the drive determines that the data on tape is suspect from a WORM point of view.	1. Copy the data to another WORM tape cartridge. 2. Discard the old WORM cartridge.
60	WORM Medium - Overwrite attempted	No	Set when the drive rejects a write operations because the rules for allowing WORM writes are not met. Data can be appended only to WORM media. Overwrites to WORM media are not allowed.	Append the information on a WORM tape cartridge, or write the data to a non-WORM cartridge.

Appendix C. Sense data

When a drive encounters an error, it makes sense data available. You can use IBM device drivers to examine the sense data and determine errors. Instructions for downloading, installing, and properly configuring the IBM device drivers are available in the *IBM Ultrium Device Drivers Installation and User 's Guide*. The IBM device drivers can conflict with some commercial software applications unless properly configured. To avoid conflicts on Windows operating systems, refer to your device driver 's procedures for setting the driver to manual startup mode. For applications that use Open Systems device drivers that are provided by IBM (for example, AIX, Linux, Sun Solaris, HP-UX, Windows 2003, Windows 2000, and Windows 2008), the *Ultrium Device Drivers Installation and User 's Guide* contains information about how to obtain sense data after an error occurred.

If your application uses other device drivers, see the appropriate documentation for those drivers to obtain the sense data.

Raw sense data (as returned from the drive) is documented in the *IBM LTO Ultrium Tape Drive SCSI Reference*.

In addition to device drivers, other methods exist for obtaining sense data and error information. The sections that follow describe alternatives for gathering such information from the IBM AS/400, eServer iSeries, RS/6000®, and eServer pSeries servers.

Library sense data

The following table lists the Additional Sense Codes (ASC) and Additional Sense Code Qualifiers (ASCQ) associated with the reported Sense Keys.

Sense Key values are shown in Table C-1.

Table C-1. Sense Key values

Sense Key	Description
0h	No Sense. No specific sense key information to report.
2h	Not Ready. The library is not ready to perform motion commands.
4h	Hardware Error. A hardware error was detected and operator intervention may be required.
5h	Illegal Request. The CDB or supplied parameter data contains an unsupported or illegal parameter.
6h	Unit Attention. The library operating status changed. Additional processing may be required.
Bh	Aborted Command. The library aborted the command.

A sense key of 00h (no sense) has no ASC/ASCQ associated with it. A few ASC/ASCQs can be associated with more than one sense key. The sense keys that can give a particular ASC/ASCQ are indicated within the Sense Key column.

Table C-2. ASC, ASCQ, and Library Sense Keys

ASC	ASCQ	Sense Key	Description
00h	00h	00h	No Additional Sense Code.
04h	00h	0Bh	LU Communication - SCSI Command Communication Failure
	00h	02h	The library is not ready due to an unknown cause.
	01h		The library is becoming ready.
	03h		The library is not ready and a manual intervention is required.
	83h		The library is not ready due to aisle power being disabled.
	8Dh		The library is not ready because it is offline.
	12h		Logical unit not ready, offline
08h	00h	0Bh	LU Communication - Failure
	01h		LU Communication - Timeout
	80h		LU Communication - SCSI failure
	82h		LU Communication - SCSI command execution or queuing failure
	83h		LU Communication - SCSI command failed
	84h		LU Communication - SCSI time-out
	85h		LU Communication - SCSI autosense failed
	86h		LU Communication - SCSI aborted
	87h		LU Communication - SCSI abort failed
	88h		LU Communication - SCSI status failed
	B0h		LU Communication - FC data underrun
	B1h		LU Communication - FC DMA error
	B2h		LU Communication - FC reset
	B3h		LU Communication - FC data overrun
	B4h		LU Communication - FC queue full
	B5h		LU Communication - Port unavailable
	B6h		LU Communication - Port logged out
	B7h		LU Communication - Port configuration changed
15h	01h	04h	A mechanical positioning error occurred.
1Ah	00h	05h	Parameter list length error
1Bh	00h	0Bh	Synchronous data transfer error
20h	00h	05h	Illegal opcode in CDB.
21h	01h		Invalid element address in CDB.
24h	00h		Invalid field in CDB.
25h	00h		Illegal LUN.
26h	00h		Invalid field in Parameter List.
	04h		Invalid release of persistent reservation

Table C-2. ASC, ASCQ, and Library Sense Keys (continued)

ASC	ASCQ	Sense Key	Description
28h	00h	06h	Not Ready to Ready change, door(s) opened and closed.
	01h		I/O station opened and closed.
29h	00h		Power on, SCSI bus reset, or Bus device reset occurred.
	01h		Power on occurred
	03h		Device reset occurred
	04h		Internal reset occurred
2Ah	01h		Mode parameters have been changed.
	03h		Reservations preempted
	04h		Reservations released
	05h		Registrations preempted
2Ch	00h	05h	Command sequence error
30h	00h		Incompatible media installed.
39h	00h		Saving parameters not supported
3Bh	0Dh	04h, 05h	The destination element is full.
	0Eh		The source element is empty.
	12h	05h	Media magazine not installed
	1Ah		Data transfer device removed
	A0h		Media type does not match destination media type
3Eh	00h	02h	Logical Unit has not self-configured yet
3Fh	01h	06h	New firmware loaded
	03h	06h	Inquiry data changed
	0Fh	04h	Echo buffer overwritten
40h	80h	04h	Component failure.
43h	00h	0Bh	Message error
44h	00h	04h, 0Bh	Firmware detected an internal logic failure.
45h	00h	0Bh	Select or reselected failure
47h	00h	0Bh	SCSI parity error
48h	00h	0Bh	Initiator detected error message received
49h	00h	0Bh	Invalid message error
4Ah	00h	0Bh	Command phase error
4Bh	00h	0Bh	Data phase error
4Eh	00h	0Bh	Overlapped commands attempted
53h	00h	04h	A drive did not load or unload a tape.
	01h	04h,05h	A drive did not unload a cartridge.
	02h	05h	Medium removal prevented.
	81h		I/O station door is open.
	82h	04h	Cannot lock the I/O station.
	83h		Cannot unlock the I/O station.

Table C-2. ASC, ASCQ, and Library Sense Keys (continued)

ASC	ASCQ	Sense Key	Description
83h	00h	04h	Label too short or too long.
	02h	05h	Barcode label questionable
	03h		Cell status and bar code label questionable.
	04h		Data transfer element not installed.
	05h		Data transfer element is varied off and not accessible for library operations.
	06h		Element is contained within an offline tower or I/O station and is not accessible for library operations.

Drive sense data

LTO Ultrium drives contain hardware that completes user data write encryption and read decryption, protecting all user data that is written to the medium from unauthorized use, provided it is integrated into a secure system design.

Table C-3. LTO tape drive sense data

Byte	Bit Address or Name							
	7	6	5	4	3	2	1	0
0	Address valid When set to 1, the info byte field contains a valid logical block address.	Error Code						
1	Segment Number (0)							
2	Filemark	EOM (end of medium)	ILI (Incorrect length indicator)	Reserved	Sense Key Description 0 - No sense 1 - Recovered error 2 - Not ready 3 - Media error 4 - Hardware error 5 - Illegal request 6 - Unit attention 7 - Data protect 8 - Blank Check 9 - Reserved A - Reserved B - Aborted command C - Reserved D - Volume overflow E - Reserved F - Reserved			
3	Information byte (most significant byte)							
4	Information byte							
5	Information byte							

Table C-3. LTO tape drive sense data (continued)

Byte	Bit Address or Name							
	7	**6**	**5**	**4**	**3**	**2**	**1**	**0**
6	Information byte (least significant byte)							
7	Additional Sense Length							
8-11	Command specific information							
12-13	Additional Sense Code (ASC) Additional Sense Code Qualifier (ASCQ) **Byte 12 Byte 13** **ASC ASCQ** 00 00 - No additional sense - The flags in the sense data indicate the reason for the command failure 00 01 - Filemark detected - A Read or Space command terminated early because of an FM The FM flag is set. 00 02 - EOM - A Write or Write File Marks command failed because the physical end of tape was encountered, or a Read or Space command encountered EOM The EOM flag is set 00 04 - BOM - A space command ended at Beginning of Tape The EOM bit is also set 00 05 - EOD - Read or Space command terminated early because End of Data was encountered 04 00 - Cause not reportable - A cartridge is present in the drive, but it is in the process of being unloaded 04 01 - Becoming Ready - A media access command was received during a front panel initiated load or an immediate reported load command 04 02 - Initializing Command Required - A cartridge is present in the drive, but is not logically loaded. A Load command is required 04 03 - Manual Intervention Required - A cartridge is present in the drive but could not be loaded or unloaded without manual intervention 0C 00 - Write Error - A Write operation failed. This is probably because of bad media, but can be hardware related 11 00 - Unrecovered Read Error - A Read operation failed. This is probably due to bad media, but can be hardware-related 11 12 - Auxiliary memory read error. The drive reported that it is unable to read the Auxiliary Memory in a WORM cartridge. 14 00 - Recorded Entity Not Found - A space or Locate command failed because a format violation prevented the target from being found. 14 03 - End Of Data not found - A Read type operation failed because a format violation related to a missing EOD data set 14 10 - Not Ready - Auxiliary memory not accessible. The drive is not able to become ready because it is unable to access the Auxiliary Memory in a WORM cartridge. 1A 00 - Parameter list length error - The amount of parameter data sent is incorrect 20 00 - Invalid Command Operation Code - The Operation Code in the command was not a valid Operation Code 24 00 - Invalid field in CDB - An invalid field has been detected in a Command Descriptor Block 25 00 - LUN not supported - The command was addressed to a non-existent logical unit number 26 00 - Invalid Field in Parameter List - An invalid field has been detected in the data sent during the data phase 27 00 - Write Protect - A Write type operation has been requested on a cartridge which has been write protected 28 00 - Not Ready to Ready Transition - A cartridge has been loaded successfully into the drive and is now ready to be accessed 29 00 - Reset - The drive has powered on, received a reset signal or a bus device reset signal since the initiator last accessed it 2A 01 - Mode Parameters Changed - The Mode parameters for the drive are changed by an initiator other than the one issuing the command							

Table C-3. LTO tape drive sense data (continued)

Byte	Bit Address or Name							
	7	6	5	4	3	2	1	0
12-13	Additional Sense Code (ASC) - Additional Sense Code Qualifier (ASCQ) (Continued) **Byte 12 Byte 13** **ASC ASCQ** 30 00 - Incompatible Media Installed - A write type operation could not be executed because it is not supported on the cartridge type that is loaded. 30 01 - Unknown Format - An operation could not be carried out because the cartridge in the drive is of a format not supported by the drive 30 02 - Incompatible Format - An operation could not be completed because the Logical Format is not correct 30 03 - Cleaning Cartridge Installed - An operation could not be carried out because the cartridge in the drive is a cleaning cartridge 30 07 - Cleaning Failure - A cleaning operation was attempted, but could not be completed for some reason 30 0C - Data Protect - WORM overwrite attempted. The drive rejected a write operation because it resulted in an overwrite. Overwrite is not allowed on WORM media. 30 0D - Medium Error - WORM integrity check. The drive rejected a Read or Write operation because the cartridge is a suspicious WORM cartridge. 31 00 - Media format corrupted - Data could not be read because the format on tape is not valid, but is a known format. A failure occurred attempting to write the FID 37 00 - Rounded parameter - A Mode Select command parameter was rounded because the drive cannot store it with the accuracy of the command 3A 00 - Media Not Present - A media access command was received when there is no cartridge loaded 3B 00 - Sequential Positioning Error - A command has failed and left the logical position at an unexpected location 3D 00 - Invalid bits in identify Message - An illegal Identify Message was received at the drive at the start of a command 3E 00 - Logical Unit was not Self-Configured - The drive was powered on and did not complete its self test sequence and cannot process commands 3F 01 - Code Download - The firmware in the drive was changed by a Write Buffer command 40 xx - Diagnostic failure - A diagnostic test failed. The xx (ASCQ) is a vendor-specific code that indicates the failing component. 43 00 - Message Error - A message could not be sent or received because of excessive transmission errors 44 00 - Internal target failure - A hardware failure has been detected in the drive that has caused the command to fail 45 00 - Select/Reset Failure - An attempt to reselect an initiator in order to complete the command has failed 4B 00 - Data Phase Error - A command could not be completed because too many parity errors occurred during the Data phase 4E 00 - Overlapped Commands - An initiator selected the drive even though it already had a command outstanding in the drive 50 00 - Write Append Error - A write type command failed because the point at which to append data was unreadable 51 00 - Erase failure - An Erase command failed to erase the required area on the media							

Table C-3. LTO tape drive sense data (continued)

Byte	Bit Address or Name							
	7	**6**	**5**	**4**	**3**	**2**	**1**	**0**
12-13	Additional Sense Code (ASC) - Additional Sense Code Qualifier (ASCQ) (Continued) **Byte 12 Byte 13** **ASC ASCQ** 52 00 - Cartridge fault - A command was not be completed because of a fault in the tape cartridge 53 00 - Media Load/Eject Failed - (Sense Key 03) An attempt to load or eject the cartridge failed because of a problem with the cartridge. 53 00 - Media Load/Eject Failed - (Sense Key 04) An attempt to load or eject the cartridge failed because of a problem with the drive 53 02 - Media Removal Prevented - An Unload command failed to eject the cartridge because media removal was prevented 5D 00 - Failure Prediction Threshold - Failure Prediction thresholds were exceeded indicating that a failure can occur soon 5D FF - Failure Prediction False - A Mode Select command was used to test for Failure Prediction system. 82 82 - Drive requires cleaning - The drive detected that a cleaning operation is required to maintain good operation 82 83 - Bad Code Detected - The data that is transferred to the drive during a firmware upgrade is corrupted or incompatible with drive hardware							

Table C-3. LTO tape drive sense data (continued)

Byte	Bit Address or Name							
	7	**6**	**5**	**4**	**3**	**2**	**1**	**0**
12-13	Additional Sense Code (ASC) - Additional Sense Code Qualifier (ASCQ) (Continued) **Byte 12 Byte 13** **ASC ASCQ** **Sense Key 0 (No Sense)** EE 13 - Encryption - Key Translate EF 13 - Encryption - Key Translate EKM **Sense Key 3 (Medium Error)** 30 02 - Encryption - Encryption feature is not enabled so format/processing is not supported EE 60 - Encryption - Proxy Command Error EE D0 - Encryption - Data Read Decryption Failure EE D1 - Encryption - Data Read after Write Decryption Failure EE E0 - Encryption - Key Translation Failure EE E1 - Encryption - Key Translation Ambiguous EE F0 - Encryption - Decryption Fenced (Read) EE F1 - Encryption - Encryption Fenced (Write) **Sense Key 4 (Hardware Error)** EE 0E - Encryption - Key Service Timeout EE 0F - Encryption - Key Service Failure 40 00 - Encryption - Failure Hardware, POST, or Module Failure **Sense Key 5 (Illegal Request)** EE 00 - Encryption - Key Service Not Enabled EE 01 - Encryption - Key Service Not Configured EE 02 - Encryption - Key Service Not Available EE 10 - Encryption - Key Required EE 20 - Encryption - Key Count Exceeded EE 21 - Encryption - Key Alias Exceeded EE 22 - Encryption - Key Reserved EE 23 - Encryption - Key Conflict EE 24 - Encryption - Key Method Change EE 25 - Encryption - Key Format Not Supported EE 26 - Encryption - Unauthorized Request - dAK EE 27 - Encryption - Unauthorized Request - dSK EE 28 - Encryption - Unauthorized Request - eAK EE 29 - Encryption - Authentication Failure EE 2A - Encryption - Invalid RDKi EE 2B - Encryption - Key Incorrect EE 2C - Encryption - Key Wrapping Failure EE 2D - Encryption - Sequencing Failure EE 2E - Encryption - Unsupported Type EE 2F - Encryption - New Key Encrypted Write Pending EE 30 - Encryption - Prohibited Request EE 31 - Encryption - Key Unknown EE 42 - Encryption - EKM Challenge Pending EE E2 - Encryption - Key Translation Disallowed EE FF - Encryption - Security Prohibited Function EF 01 - Encryption - Key Service Not Configured 26 11 - Encryption - Incomplete Key - Associate Data Set 26 12 - Encryption (T10) - Vendor Specific Reference Key Not Found 55 08 - Encryption (T10) - Maximum Number of Supplemental Keys Exceeded							

Table C-3. LTO tape drive sense data (continued)

Byte	Bit Address or Name							
	7	**6**	**5**	**4**	**3**	**2**	**1**	**0**
12-13	**Sense Key 6 (Unit Attention)** EE 12 - Encryption - Key Change Detected EE 18 - Encryption - Changed (Read) EE 19 - Encryption - Changed (Write) EE 40 - Encryption - EKM Identifier Changed EE 41 - Encryption - EKM Challenge Changed EE 50 - Encryption - Initiator Identifier Changed EE 51 - Encryption - Initiator Response Changed 2A 11 - Encryption - Data Encryption Parameters Changed by Another I_T Nexus 2A 12 - Encryption - Data Encryption Parameters Changed by Vendor Specific Event **Sense Key 7 (Data Protect)** EF 10 - Encryption - Key Required EF 11 - Encryption - Key Generation EF 13 - Encryption - Key Translate EF 1A - Encryption - Key Optional EF C0 - Encryption - No Operation 26 10 - Encryption - Data Decryption Key Fail Limit 2A 13 - Encryption - Data Encryption Key Instance Counter Has Changed 74 00 - Security Error 74 01 - Encryption - Unable to Decrypt Data 74 02 - Encryption - Unencrypted Data Encountered While Decrypting 74 03 - Encryption - Incorrect Data Encryption Key 74 04 - Encryption - Cryptographic Integrity Validation Failed 74 05 - Encryption - Error Decrypting Data							
14	FRU code							
15	SKSV	C/D	Reserved		BPV When set to 1, the bit pointer is valid.	Bit pointer		
16 -17	SKSV = 0: First Error Fault Symptom Code (FSC). SKSV = 1: Field Pointer							
18-19	First Error Flag Data							
20	Reserved (0)							
21					CLN	Reserved	Reserved	VolValid
22-28	Volume Label							
29	Current Wrap							
30-33	Relative LPOS							
34	SCSI Address							
35	Frame number				Drive number			

The descriptions serve only as an overview of sense reporting in the tape drive. This tape drive conforms to all sense field reporting as specified in the SCSI standards.

Note:

1. The **Error Code** field (Byte 0) is set to 70h to indicate a current error, that is one associated with the most recently received command. It is set to 71h to indicate a deferred error that is not associated with the current command.
2. The segment number (Byte 1) is zero since the Copy, Compare, and Copy and Verify commands are not supported.
3. The File Mark flag (Byte 2, bit 7) is set if a Space, Read, or Verify command did not complete because a file mark was read.
4. The End of Media (EOM) flag (Byte 2, bit 6) is set if a Write or Write File Marks command that is completed in the early warning area. Spacing into BOM also causes this flag to be set. It is also set on an attempt to read or space past EOD, or if an attempt is made to space into Beginning of Media.
5. The Illegal Length Indicator (ILI) flag (Byte 2, bit 5) is set if a Read or Verify ended because a block was read from tape that did not have the block length that is requested in the command.
6. The Information Bytes (Bytes 3-5) are only valid if the Valid flag is set. This occurs only for current errors and not for deferred errors.
7. The **Field Replaceable Unit** field (Byte 14) is set to either zero or to a non-zero, vendor-specific code that indicates which part of the drive is suspected of causing the failure.
8. The Clean (CLN) flag (Byte 21, bit 3) is set if the drive needs cleaning and clear otherwise.
9. The Volume Label Fields Valid (VolValid) bit (Byte 21, bit 0) is set if the Volume Label being reported is valid.
10. The **Volume Label** field (Bytes 22-28) reports the volume label if a cartridge is loaded in the drive and Volume Label Fields Valid is set.
11. The **Current Wrap** field (Byte 29) reports the physical wrap of the tape. The least significant bit reflects the current physical direction. A 0 means that the current direction is away from the physical beginning of the tape. A 1 means that the current direction is towards the physical beginning of the tape.
12. Relative LPOS fields (Bytes 30-33) report the current physical position on the tape.
13. **SCSI Address** field (Byte 34) reports the SCSI Bus Address for the drive. Values returned range from 00h to 0Fh.
14. This field (Byte 35) contains the frame and drive number, passed across the RS-422 serial interface.

Appendix D. SNMP status MIB variables and traps

The three tables in this appendix provide a quick reference for the status MIB variables, status, and audit logging traps.

Table D-1. Status MIB variables

Event	Object ID*	Description
Drive Online/Offline Status	...11.3.1.10	Indicates whether the drive is online or offline. If the drive is offline, use the Operator Panel or Web User Interface to confirm that the drive is varied ON. Also check library power.
Physical Library Online/Offline Status	...14.1	Indicates whether the library is online or offline. Use the Operator Panel or Web User Interface to confirm that the library is online and not being configured.
Robotic Readiness	...14.30.2	Indicates the library robotics ready status. Verify that the module doors are closed and that the robotics are online.
Library Main Door	...14.2	Indicates the library main door status.
I/O Station Door Status	...14.3	Indicates the library I/O station door status.
Logical Library Online/Offline Status	...13.2.1.8	Indicates whether a specific logical library is online or offline. You can use the Operator Panel or Web UI to confirm the logical library is online and not being configured.
* Because the front portion of the MIB variable object ID (OID), 1.3.6.1.4.1.3764.1.10.10, is the same for all variables defined in the MIBs, it is omitted in the OID column of this table. For example, the actual OID of the Drive Online/Offline Status variable is 1.3.6.1.4.1.3764.1.10.10.11.3.1.10.		

Table D-2. Status traps

Event	Trap ID	Description
Starting	1	Indicates that the tape library started running.
Shutting down	2	Indicates that the library is in the process of being shut down.
Restarting	3	Indicates that the library was restarted. This does not imply anything about whether the configuration changed or not (unlike the standard coldStart or warmStart traps).
Startup Sequence Completed	101	Indicates that the library startup sequence completed.
Shutdown Sequence Completed	102	Indicates that the library shutdown sequence completed.
Change in Online State	103	Indicates that the online state of the physical library changed.
Physical Library Door Status Change	104	Indicates whether the physical library door was opened, closed, locked, or unlocked.
I/O Door Status Change	105	Indicates that an I/O station door was opened, closed, locked, or unlocked.
Robotics Ready	106	Indicates the library robotics system has transitioned from "not ready" to "ready". Traps 106 and 107 can occur as part of a startup or shutdown procedure. If they occur at another time, a library door might be open.
Robotics Not Ready	107	Indicates the library robotics system has transitioned from "ready" to "not ready". Traps 106 and 107 can occur as part of a startup or shutdown procedure. If they occur at another time, a library door might be open.

Table D-2. Status traps (continued)

Event	Trap ID	Description
Logical Library State Change	108	Indicates whether a logical library was taken online or offline.
RAS Status Change: Connectivity	109	Indicates that the status of the connectivity subsystem (which includes the I/O management unit and other components) changed. This can indicate a change to "good" status, so refer to the return value to determine what action you should take. If the return value indicates that a problem exists, use the Operator Panel or Web UI to determine how to resolve the issue.
RAS Status Change: Control	110	Indicates that the status of the control subsystem (which includes system firmware, the operator panel, and the Library Control Blade) changed. If the return value indicates that a problem exists, use the Operator Panel or Web UI to determine how to resolve the issue.
RAS Status Change: Cooling	111	Indicates that the status of the cooling subsystem changed. If the return value indicates that a problem exists, use the Operator Panel or Web UI to determine how to resolve the issue.
RAS Status Change: Drives	112	Indicates that the status of the drives and/or media changed. If the return value indicates that a problem exists, use the Operator Panel or Web UI to determine how to resolve the issue.
RAS Status Change: Media	113	Indicates that the status of the media changed. If the return value indicates that a problem exists, use the Operator Panel or Web UI to determine how to resolve the issue.
RAS Status Change: Power	114	Indicates that the status of the power subsystem changed. If the return value indicates that a problem exists, use the Operator Panel or Web UI to determine how to resolve the issue.
RAS Status Change: Robotics	115	Indicates that the status of the robotics subsystem changed. If the return value indicates that a problem exists, use the Operator Panel or Web UI to determine how to resolve the issue.
Operator Intervention Required	116	An error occurred, resulting in an Operator Intervention message. Use the Operator Panel or Web UI to determine how to resolve the issue.
Drive Online State Change	117	Indicates that a tape drive was taken online or offline.
Drive Communication Failure	121	The library set TapeAlert 1, indicating a drive communication failure.
Library Hardware Failure	122	The library set TapeAlert 2, indicating a library hardware failure.
Non-mechanical Hardware Failure	124	The library set TapeAlert 4, indicating a non-mechanical hardware failure.
Cartridge Pick Problem	133	The library set TapeAlert 13, indicating a problem when picking a tape cartridge.
Cartridge Placement Problem	134	The library set TapeAlert 14, indicating a problem when placing a tape cartridge.
Drive Load Problem	135	The library set TapeAlert 15, indicating a problem when loading a tape drive.

Table D-2. Status traps (continued)

Event	Trap ID	Description
Library main Access Door Open	136	The library set TapeAlert 16, indicating an open library access door.
Mailbox Mechanical Problem	137	The library set TapeAlert 17, indicating a mailbox station mechanical problem.
Excessive Scan Retries	143	The library set TapeAlert 23, indicating that excessive scan retries occurred.
Barcode Label Unreadable	152	The library set TapeAlert 32, indicating that a tape cartridge barcode label could not be read.
The library issues a trap whenever the aggregate state of one of the Reliability, Availability, and Serviceability (RAS) status groups changes. Listening for these traps (rather than querying for them) is the preferred method of monitoring the health of the library.		

To enable audit logging traps from the Web UI: **Manage Library** > **Settings** > **SNMP Configuration** and select the checkbox **Enable Audit Logging**.

Table D-3. Audit logging traps

Event	Trap ID	Description
User Logged In	440	A user successfully logged into the library from the Web UI.
User Login Failed	441	A user attempted to log into the library, from the Web UI, and was unsuccessful.
User Logged Out	442	A user logged out of the library from the Web UI.
Library Settings Changed	443	A library configuration setting was changed from the Web UI.
Logical Library Settings Changed	444	A logical library configuration setting was changed from the Web UI.
Drive Settings Changed	445	A tape drive configuration setting was changed from the Web UI.
Media Settings Changed	446	A cartridge was modified from the Web UI.
Firmware Update	447	A library or drive code load was initiated from the Web UI.
Drive Reboot	451	A drive was power cycled from the Web UI.
Admin Password Changed	453	The admin password was changed from the Web UI.

Appendix E. Library configuration form

Make a copy of this form, and fill it out as you are installing and configuring your library. Update the form each time that changes are made to the library. The information on this form is important. You can also save your libraries configuration data from the Web User Interface. See "Saving/restoring system configuration" on page 8-15. Having the information on this form is helpful if a call to IBM service is necessary. Store this form in a secure location.

Library information

Machine type	**3576**
Serial No. for Model L5*x*	
Serial No. for Model E9*x*	
Serial No. for Model E9*x*	
Serial No. for Model E9*x*	
Serial No. for Model E9*x*	
IP address	
Subnet Mask address	
Gateway address	
Advanced Reporting License Key	
Path Failover License Key	
Capacity Expansion License Key	
Transparent LTO Encryption License Key	

Drive information

SCSI drives

	SCSI Drives					
Drive Address	**Serial No.**	**Drive Type**	**SCSI ID**	**Location Coordinate**	**Control Path Drive**	**Host**

	SCSI Drives					

Fibre channel drives

	Fibre Channel Drives						
Drive Address	**Serial No.**	**Loop ID**	**AL-PA**	**Worldwide Node Name**	**Location Coordinate**	**Control Path Drive Y/N**	**Host**

SAS drives

	SAS Drives				
Drive Address	**Serial No.**	**Worldwide Name**	**Location Coordinate**	**Control Path Drive Y/N**	**Host**

	SAS Drives				

Firmware information

Type of Firmware	Current Firmware Level				
Library					
Drive ___					
Drive ___					
Drive ___					
Drive ___					
Drive ___					
Drive ___					
Drive ___					
Drive ___					
Drive ___					
Drive ___					
Drive ___					
Drive ___					
Drive ___					
Drive ___					
Drive ___					
Drive ___					
Drive ___					
Drive ___					
Drive ___					

Users account information

The Administrator password is listed in the table below. Add additional Administrator and User names and passwords that are created.

User name	Password
Administrator	**secure**

Appendix F. Accessibility

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use the HTML version of the customer documentation successfully.

Features

The major accessibility features for the HTML version of this guide:

- You can use screen-reader software and a digital speech synthesizer to hear what is displayed on the screen. The following screen readers are tested: WebKing and Window-Eyes.
- You can operate all features with the keyboard instead of the mouse.

Navigating by keyboard

You can use keys or key combinations to complete operations and initiate many menu actions that can also be done through mouse actions. You can navigate the HTML version of the help system from the keyboard with the following key combinations:

- To traverse to the next link, button, or topic, press **Tab** inside a frame (page).
- To move to the previous topic, press ^ or Shift+Tab.
- To scroll all the way up or down, press **Home** or **End**.
- To print the current page or active frame, press Ctrl+P.
- To select, press **Enter**.

Accessing the publications

You can view the publications for this library in Adobe Portable Document Format (PDF) with the Adobe Acrobat Reader. The PDFs are provided at the following website:

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

Appendix G. Logical SCSI element addressing

The library uses standard industry conventions to logically number every storage slot, I/O station slot, and tape drive in the library. Host software is designed to understand this addressing system, and generally there are no problems that relate to tape cartridge slots. However, hosts sometimes have problems that relate to tape drives, particularly when tape drives, library control modules, or library expansion modules are added or removed, or empty tape drive slots exist. This section explains how the library logically addresses tape drives and slots, so that you can avoid common problems with host software.

Tape drive logical SCSI element addressing

Tape drive logical element addresses are assigned by logical library. The numbering is sequential within a logical library and starts over with each logical library. The addresses start with the lowest library module in a logical library. The top tape drive in the module and logical library is always number 256. The tape drive beneath that is 257, and so on, until all tape drives in that module/logical library are accounted for. Numbering continues with the top tape drive in the next module up. Empty tape drive slots are skipped (they are not given an element address).

Host software might have problems recognizing tape drives when tape drives, control modules, or expansion modules are added, removed, or replaced; or when logical libraries are added, deleted, or modified, because existing logical element addresses can change. Therefore, after any of these types of modifications are made, you must refresh the configuration of any backup application that manages the library to reflect new tape drive positions. In addition, you might need to reboot the host server or rescan the bus to detect the changes.

See Figure G-1 on page G-2 for a simple example of element addressing in a 14U library with a single logical library, six tape drives installed and no empty tape drive slots. Multiple logical libraries can create complexity. If you need help with the element addressing in your library, contact IBM Technical Support.

Cartridge slot logical SCSI element addressing

Tape cartridge slots are assigned logical element addresses by logical library. The numbering is sequential within a logical library and starts over with each logical library. Numbering begins at the upper left slot (as you look at the library from the front) in the lowest module in the library and moves sequentially down the leftmost column. The upper left slot of every logical library is always number 4096, the slot beneath that is 4097, and so on. When the numbering reaches the bottom of the column, it continues to the top slot in the next column to the right (in the same module and partition) and moves down that column. When all of the slots in the lowest module that belong to a logical library are accounted for, numbering continues to the upper left slot in the next module above (in the same partition). The numbering can get tricky when logical libraries span modules and do not use all of the slots in a module.

I/O station slots are numbered differently from partitions. Numbering begins at the top I/O station slot in the uppermost module that contains I/O station slots, and continues sequentially downward. This top slot has element address 16. The slot beneath that is 17, and so on.

Cleaning slots belong to the System partition and are not reported to the host. Cleaning slots are skipped (they are not given a logical element address), so adding or removing a cleaning slot renumbers all of the slots in a logical library.

Generally, host software easily recognizes logical slot element addresses, even when they change. The next time that the host issues a READ ELEMENT STATUS command, it will process the new number and recalculate all of the slot addresses.

See Figure G-1 for a simple example of element addressing in a 14U library with a single logical library.

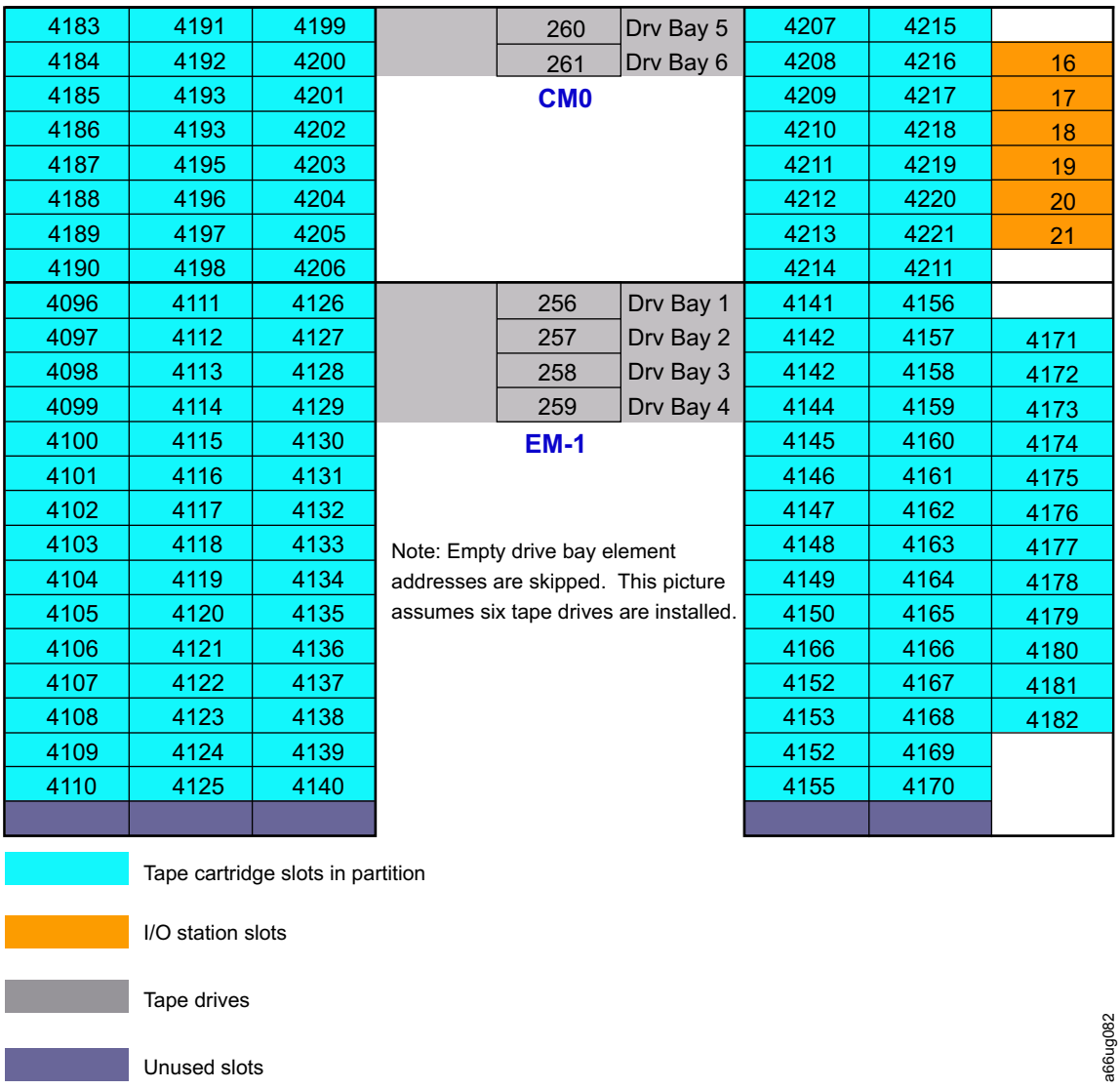


Figure G-1. Logical element addressing, 14U, one partition, six tape drives installed

Notices

The information provided by this media supports the products and services described with consideration for the conditions described herein.

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 to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
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 information 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.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been

estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both.

- AIX
- Enterprise Storage Server
- ESCON
- FICON
- i5/OS
- iSeries
- IBM
- pSeries
- S/390
- System Storage
- TotalStorage
- z/OS
- zSeries

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol ((R) or (TM)), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

ITIL is a registered trademark, and a registered community trademark of The Minister for the Cabinet Office, and is registered in the U.S. Patent and Trademark Office.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. 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.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.

Electronic emission notices

This section contains the electronic emission notices or statements for the United States and other regions.

Federal Communications Commission statement

This explains the Federal Communications Commission's (FCC) statement.

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, might 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. IBM is not responsible for any radio or television interference caused 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 might not cause harmful interference, and (2) this device must accept any interference received, including interference that might cause undesired operation.

Industry Canada compliance statement

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conform à la norme NMB-003 du Canada.

European Union electromagnetic compatibility directive

This product is in conformity with the protection requirements of European Union (EU) Council Directive 2004/108/EC 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 non-recommended modification of the product, including the fitting of non-IBM option cards.

Attention: This is an EN 55022 Class A product. In a domestic environment this product might cause radio interference in which case the user might be required to take adequate measures.

Responsible Manufacturer:

International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
914-499-1900

European community contact:

IBM Deutschland GmbH
Technical Regulations, Department M372
IBM-Allee 1, 71139 Ehningen, Germany
Tele: +49 7032 15 2941
e-mail: lugi@de.ibm.com

Australia and New Zealand Class A statement

Attention: This is a Class A product. In a domestic environment this product might cause radio interference in which case the user might be required to take adequate measures.

Germany electromagnetic compatibility directive

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der IBM gesteckt/eingebaut werden.

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden:

"Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Mabnahmen zu ergreifen und dafür aufzukommen."

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem "Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)." Dies ist die Umsetzung der EU-Richtlinie 2004/108/EG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2004/108/EG) für Geräte der Klasse A

Dieses Gerät ist berechtigt, in übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:

International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:

IBM Deutschland GmbH
Technical Regulations, Abteilung M372
IBM-Allee 1, 71139 Ehningen, Germany
Tele: +49 7032 15 2941
e-mail: lugi@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

People's Republic of China Class A electronic emission statement

中华人民共和国“A类”警告声明

声 明
此为A级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。

Taiwan Class A compliance 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。 taiemi

Taiwan contact information

This topic contains the product service contact information for Taiwan.

IBM Taiwan Product Service Contact Information:
IBM Taiwan Corporation
3F, No 7, Song Ren Rd., Taipei Taiwan
Tel: 0800-016-888

台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

f2c00790

Japan Voluntary Control Council for Interference (VCCI) Class A statement

この装置は、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。 VCCI-A

Japan Electronics and Information Technology Industries Association (JEITA) statement (less than or equal to 20 A per phase)

高調波ガイドライン適合品

jjieta1

Japan Electronics and Information Technology Industries Association (JEITA) statement (greater than 20 A per phase)

高調波ガイドライン準用品

jjieta2

Korean Communications Commission (KCC) Class A statement

이 기기는 업무용(A급)으로 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.

Russia Electromagnetic Interference (EMI) Class A statement

ВНИМАНИЕ! Настоящее изделие относится к классу А. В жилых помещениях оно может создавать радиопомехи, для снижения которых необходимы дополнительные меры

rusemi

Glossary

This glossary defines the special terms, abbreviations, and acronyms that are used in this publication. If you do not find the term you are looking for, refer to the index or to the *Dictionary of Computing*, 1994.

Numbers

2:1 compression
The relationship between the quantity of data that can be stored with compression as compared to the quantity of data that can be stored without compression. In 2:1 compression, twice as much data can be stored with compression as can be stored without compression.

A

A Ampere.

ac Alternating current.

access method
A technique for moving data between main storage and input or output devices.

adapter card
A circuit board that adds function to a computer.

ADI Automation Drive Interface.

adj Adjustment.

AIX Advanced Interactive Executive. IBM's implementation of the UNIX operating system. The RS/6000 system, among others, uses AIX as it's operating system.

alphanumeric
Pertaining to a character set that contains letters, numerals, and usually other characters, such as punctuation marks.

alter To change.

ambient temperature
The temperature of air or other media in a designated area, particularly the area surrounding equipment.

ampere (A)
A unit of measure for electric current that is equivalent to a flow of one coulomb per second, or to the current produced by one volt applied across a resistance of one ohm.

ANSI American National Standards Institute.

archive
To collect and store files in a designated place.

ASCII American National Standard Code for Information Interchange. A 7 bit coded character set (8 bits including parity check) that consists of control characters and graphic characters.

assigning a device
The establishing of the relationship of a device to a running task, process, job, or program.

assignment
The naming of a specific device to perform a function.

asynchronous
Pertaining to two or more processes that do not depend upon the occurrence of specific events such as common timing signals.

attention (notice)
A word for calling attention to the possibility of danger to a program, device, or system, or to data. Contrast with *caution* and *danger*.

ATTN Attention.

B

backup
To make additional copies of documents or software for safekeeping.

bar code
A code representing characters by sets of parallel bars of varying thickness and separation which are read optically by transverse scanning.

bar code label
Paper bearing a bar code and having an adhesive backing. The bar code label must be affixed to a tape cartridge to enable the library to identify the cartridge and its volume serial number.

bar code reader
A laser device specialized for scanning and reading bar codes and converting them into either the ASCII or EBCDIC digital character code.

bezel Decorative and safety cover.

bicolored
Having two colors.

bit Either of the digits 0 or 1 when used in the binary numbering system.

BM or bill of materials
A list of specific types and amounts of direct materials expected to be used to produce a given job or quantity of output.

BRMS Backup Recovery and Media Services.

browser
A client program that initiates requests to a Web server and displays the information that the server returns.

buffer
A routine or storage used to compensate for a difference in rate of flow of data or time of occurrence of events, when transferring data from one device to another.

bus A facility for transferring data between several devices located between two end points, only one device being able to transmit at a given moment.

byte A string consisting of a certain number of bits (usually 8) that are treated as a unit and represent a character. A fundamental data unit.

C

capacity
The amount of data that can be contained on storage media and expressed in bytes of data.

cartridge manual rewind tool
A device that can be fitted into the reel of a cartridge and used to rewind tape into or out of the cartridge.

CM Cartridge Memory.

cartridge storage slot
Individual slot located within a magazine that is used to house tape cartridges.

caution (notice)
A word to call attention to possible personal harm to people. Contrast with *attention* and *danger*.

CE Customer engineer; field engineer; service representative.

centimeter (cm)
One one-hundredth of a meter (0.01 m). Approximately 0.39 inch.

channel command
An instruction that directs a data channel, control unit, or device to perform an operation or set of operations.

char Character.

CHK Check.

cleaning cartridge
A tape cartridge that is used to clean the heads of a tape drive. Contrast with *data cartridge*.

command
A control signal that initiates an action or the start of a sequence of actions.

compact disc (CD)
A disc, usually 4.75 inches in diameter, from which data is read optically by means of a laser.

compression
The process of eliminating gaps, empty fields, redundancies, and unnecessary data to shorten the length of records or blocks.

concurrent
Refers to diagnostic procedures that can be run on one control unit while the rest of the subsystem remains available for customer applications.

contingent connection
A connection between a channel path and a drive caused when a unit check occurs during an I/O operation.

controller
A device that provides the interface between a system and one or more tape drives.

COD Capacity On Demand.

CP Circuit protector.

CPF Control Path Failover.

CRU Customer Replaceable Unit.

CSA Canadian Standards Association.

ctrl Control.

CU Control unit.

D

danger (notice)
A word to call attention to possible lethal harm to people. Contrast with *attention* and *caution*.

data Any representations such as characters or analog quantities to which meaning is or might be assigned.

data buffer
The storage buffer in the control unit. This buffer is used to increase the data transfer rate between the control unit and the channel.

data cartridge
A tape cartridge dedicated to storing data. Contrast with *cleaning cartridge*.

data check
A synchronous or asynchronous indication of a condition caused by invalid data or incorrect positioning of data.

dc Direct current.

degauss
To make a magnetic tape nonmagnetic by means of electrical coils carrying currents that neutralize the magnetism of the tape.

degausser
A device that makes magnetic tape nonmagnetic.

degradation
A decrease in quality of output or throughput or an increase in machine error rate.

degraded
Decreased in quality of output or throughput or increased machine error rate.

deserialize
To change from serial-by-bit to parallel-by-byte.

detented
A part being held in position with a catch or lever.

device Any hardware component or peripheral, such as a tape drive or tape library, that can receive and send data.

device driver
A file that contains the code needed to use an attached device.

DIAG
Diagnostic section of maintenance information manual.

differential
See *High Voltage Differential (HVD)*.

direct access storage
A storage device in which the access time is independent of the location of the data.

DNS Directory Name System. This allows the library to recognize text-based addresses instead of numeric IP addresses.

download
To transfer programs or data from a computer to a connected device, typically a personal computer.

To transfer data from a computer to a connected device, such as a workstation or microcomputer.

DPF Data Path Failover.

DRAM
Dynamic random-access memory.

drive, magnetic tape
A mechanism for moving magnetic tape and controlling its movement.

DRV Drive.

DSE Data security erase.

DSP Digital signal processor.

E

EBCDIC
Extended binary-coded decimal interchange code.

EC Edge connector. Engineering change.

ECC Error correction code.

EEB Ethernet Expansion Blade

EEPROM
Electrically erasable programmable read-only memory.

EIA Electronics Industries Association.

EIA unit
A unit of measure, established by the Electronic Industries Association, equal to 44.45 millimeters (1.75 inches).

eject To remove or force out from within.

EKM Encryption Key Manager.

electronic mail
Correspondence in the form of messages transmitted between user terminals over a computer network.

e-mail See *electronic mail*.

EPO Emergency power off.

EPROM
Erasable programmable read only memory.

EQC Equipment check.

equipment check
An asynchronous indication of a malfunction.

Error log
A dataset or file in a product or system where error information is stored for later access.

ESD Electrostatic discharge.

F

fault symptom code (FSC)
A hexadecimal code generated by the drive or the control unit microcode in response to a detected subsystem error.

FC Feature code.

FCC Federal communications commission.

FE Field engineer, customer engineer, or service representative.

fiducial
A target used for teaching a physical location to a robot.

field replaceable unit (FRU)
An assembly that is replaced in its entirety when any one of its components fails.

file A named set of records stored or processed as a unit. Also referred to as a dataset.

file protection
The processes and procedures established in an information system that are designed to inhibit unauthorized access to, contamination of, or deletion of a file.

file transfer protocol (FTP)
In the Internet suite of protocols, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

firmware
Proprietary code that is usually delivered as microcode as part of an operating system. Firmware is more efficient than software loaded from an alterable medium and more adaptable to change than pure hardware circuitry. An example of firmware is the Basic Input/Output System (BIOS) in read-only memory (ROM) on a PC motherboard.

FLASH EEPROM
An electrically erasable programmable read-only memory (EEPROM) that can be updated.

FMR Field microcode replacement.

format
The arrangement or layout of data on a data medium.

formatter
Part of a magnetic tape subsystem that performs data conversion, speed matching, encoding, first level error recovery, and interfaces to one or more tape drives.

FP File protect.

frayed Damaged as if by an abrasive substance.

FRU Field replaceable unit.

FSC Fault symptom code.

FSI Fault symptom index.

functional microcode
Microcode that is resident in the machine during normal customer operation.

G

g Gram.

GB gigabyte.

GBIC Gigabit Interface Converter.

Gbi gigabit

gigabit (Gbit)
1 000 000 000 bits.

gigabyte (GB)
1 000 000 000 bytes.

Gigabit Interface Converter (GBIC)
Converts copper interface to optic interface.

gnd Ground.

H

HBA Host Bus Adapter.

hertz (Hz)
Unit of frequency. One hertz equals one cycle per second.

hex Hexadecimal.

High Voltage Differential (HVD)
A logic signaling system that enables data communication between a supported host and the library. HVD signaling uses a paired plus and minus signal level to reduce the effects of noise on the SCSI bus. Any noise injected into the signal is present in both a plus and minus state, and is thereby canceled. Synonymous with *differential*.

HVD SCSI Bus High Voltage Differential

Hz Hertz (cycles per second).

I

ID Identifier.

identifier (ID)
(1) In programming languages, a lexical unit that names a language object; for example, the names of variables, arrays, records, labels, or procedures. An identifier usually consists of a letter optionally followed by letters, digits, or other characters. (2) One or more characters used to identify or name data element and possibly to indicate certain properties of that data element. (3) A sequence of bits or characters that identifies a program, device, or system to another program, device, or system.

IEC International Electrotechnical Commission.

IML Initial microprogram load.

initial microprogram load (IML)
The action of loading a microprogram from an external storage to writable control storage.

initiator
The component that executes a command. The initiator can be the host system or the tape control unit.

INST Installation.

interface
A shared boundary. An interface might be a hardware component to link two devices or it might be a portion of storage or registers accessed by two or more computer programs.

interposer
The part used to convert a 68-pin connector to a 50-pin D-shell connector.

intervention required
Manual action is needed.

INTRO
Introduction.

I/O Input/output.

IOP Input/output processor.

IPL Initial program load.

ISV Independent Software Vendor.

ITST Idle-time self-test.

K

Kerberos
Kerberos Authentication is a standard (RFC 1510) third-party authentication protocol that provides end-to-end security for distributed computing environments.

kilogram (kg)
One thousand grams (approximately 2.2 pounds).

km kilometer. 1000 Meters, Approximately 5/8 mile.

L

LAN Local area network. A computer network within a limited area.

LCB Library Control Blade

LCD See *liquid crystal display*.

LDAP Lightweight Directory Access Protocol. This allows the library to use login and password information stored on a server to grant access to the library functionality.

LDAPS
Secure LDAP over SSL.

LDI Library Drive Interface.

LED Light-emitting diode.

Linear Tape-Open (LTO)
A type of tape storage technology developed by the IBM Corporation, Hewlett-Packard, and Quantum. LTO technology is an “open format” technology, which means that its users will have multiple sources of product and media. The “open” nature of LTO technology enables

compatibility between different vendors' offerings by ensuring that vendors comply with verification standards. The LTO technology is implemented in two formats: the Accelis format focuses on fast access; the Ultrium format focuses on high capacity. The Ultrium format is the preferred format when capacity (rather than fast access) is the key storage consideration. An Ultrium cartridge has a compressed data capacity of up to 6250 GB (2.5:1 compression) and a native data capacity of up to 2500 GB.

liquid crystal display (LCD)
A low-power display technology used in computers and other I/O devices.

loadable
Having the ability to be loaded.

LME Library Managed Encryption.

LTO cartridge memory (LTO-CM)
Within each LTO Ultrium data cartridge, an embedded electronics and interface module that can store and retrieve a cartridge's historical usage and other information.

LUN Logical Unit Number.

LVD SCSI Bus Low Voltage Differential

M

magnetic tape
A tape with a magnetical surface layer on which data can be stored by magnetic recording.

MAP Maintenance analysis procedure.

mask A pattern of characters that controls the retention or elimination of portions of another pattern of characters. To use a pattern of characters to control the retention or elimination of portions of another pattern of characters.

master file
A file used as an authority in a given job and that is relatively permanent, even though its contents may change. Synonymous with main file.

MB Mega Byte (usually expressed as data rate in MB/s or MB/second).

media capacity
The amount of data that can be contained on a storage medium, expressed in bytes of data.

media-type identifier
Pertaining to the bar code on the bar code label of the IBM Ultrium Tape Cartridge, a 2-character code, L1, that represents information about the cartridge. L identifies the cartridge as one that can be read by devices which incorporate LTO technology; 1 indicates that it is the first generation of its type.

mega One million of.

meter In the Metric System, the basic unit of length; equal to approximately 39.37 inches.

micro One millionth of.

microcode
(1) One or more micro instructions. (2) A code, representing the instructions of an instruction set, implemented in a part of storage that is

not program-addressable. (3) To design, write, and test one or more micro instructions. (4) See also *microprogram*.

microdiagnostic routine
A program that runs under the control of a supervisor, usually to identify field replaceable units.

microdiagnostic utility
A program that is run by the customer engineer to test the machine.

microinstruction
A basic or elementary machine instruction.

microprogram
A group of microinstructions that when executed performs a preplanned function.

The term microprogram represents a dynamic arrangement or selection of one or more groups of microinstructions for execution to perform a particular function. The term microcode represents microinstructions used in a product as an alternative to hard-wired circuitry to implement certain functions of a processor or other system component.

MIM Media information message.

mm Millimeter.

modifier
That which changes the meaning.

mount a device
To assign an I/O device with a request to the operator.

MP Microprocessor.

ms Millisecond.

MSG Message.

multipath
Pertaining to using more than one path.

N

N/A Not applicable.

NEMA
National Electrical Manufacturers Association.

node In a network, a point at which one or more functional units connect channels or data circuits.

NTP Network Time Protocol. This allows the library to set its internal date and time based on the date and time of a sever.

NVS Nonvolatile storage. A storage device whose contents are not lost when power is cut off.

O

oersted
The unit of magnetic field strength in the unrationalized centimeter-gram-second (cgs) electromagnetic system. The oersted is the magnetic field strength in the interior of an elongated, uniformly wound

solenoid that is excited with a linear current density in its winding of one abampere per 4π centimeters of axial length.

offline
Pertaining to the operation of a functional unit without the continual control of a computer. Contrast with *online*.

online Pertaining to the operation of a functional unit that is under the continual control of a computer. Contrast with *offline*.

OPER Operation.

ov Over voltage.

overrun
Loss of data because a receiving device is unable to accept data at the rate it is transmitted.

overtightening
To tighten too much.

P

parameter
A variable that is given a constant value for a specified application and that may denote the application.

PF Path Failover.

p bit Parity bit.

PC Parity check.

PCC Power control compartment.

PDF Portable Document Format.

PE Parity error. Product engineer.

pick Pertaining to the library, to remove, by means of a robotic device, a tape cartridge from a storage slot or drive.

picker A robotic mechanism located inside the library that moves cartridges between the cartridge storage slots and the drive.

PM Preventive maintenance.

POR Power-on reset.

port A physical connection for communication between the 3590 and the host processor. The 3590 has two SCSI 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 (via 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.

PROM
Programmable read only memory.

PS Power supply.

PWR Power.

R

rack A unit that houses the components of a storage subsystem, such as the library.

rackmount kit
A packaged collection of articles used to install the rack mounted version of the library.

RAM Random access memory.

Random access memory
A storage device into which data is entered and from which data is retrieved in a nonsequential manner.

RAS Reliability, availability, and serviceability.

record A collection of related data or words, treated as a unit.

recording density
The number of bits in a single linear track measured per unit of length of the recording medium.

recoverable error
An error condition that allows continued execution of a program.

ref Reference.

reg Register.

reinventory
To inventory again.

retension
The process or function of tightening the tape onto the cartridge, if it is sensed that the tape has a loose wrap on the cartridge.

RID tag
Repair identification tag.

robot Picker.

robotics
Picker assembly.

RPQ Request for price quotation.

R/W Read/write.

S

s Seconds of time.

SAC Service Action Code. Code developed to indicate possible FRU or FRU's to replace to repair the hardware.

SAN Storage Area Network.

SAS Serial Attached SCSI. A computer bus technology and serial communication protocol for direct attached storage devices. SAS is a replacement for parallel SCSI with higher speeds, but still using SCSI commands.

scratch cartridge
A data cartridge that contains no useful data, but can be written to with new data.

SCD Single Character Display.

SCSI Small computer system interface.

segment
A part.

sel Select.

serialize
To change from parallel-by-byte to serial-by-bit.

serializer
A device that converts a space distribution of simultaneous states representing data into a corresponding time sequence of states.

servo, servos
An adjective for use in qualifying some part or aspect of a servomechanism.

servomechanism
A feedback control system in which at least one of the system signals represents mechanical motion.

Small Computer Systems Interface (SCSI)
A standard used by computer manufacturers for attaching peripheral devices (such as tape drives, hard disks, CD-ROM players, printers, and scanners) to computers (servers). Pronounced "scuzzy". Variations of the SCSI interface provide for faster data transmission rates than standard serial and parallel ports (up to 320 megabytes per second). The variations include:

- Fast/Wide SCSI: Uses a 16-bit bus, and supports data rates of up to 20 MBps.
- SCSI-1: Uses an 8-bit bus, and supports data rates of 4 MBps.
- SCSI-2: Same as SCSI-1, but uses a 50-pin connector instead of a 25-pin connector, and supports multiple devices.
- Ultra SCSI: Uses an 8- or 16-bit bus, and supports data rates of 20 or 40 MBps.
- Ultra2 SCSI: Uses an 8- or 16-bit bus and supports data rates of 40 or 80 MBps.
- Ultra3 SCSI: Uses a 16-bit bus and supports data rates of 80 or 160 MBps.
- Ultra160 SCSI: Uses a 16-bit bus and supports data rates of 80 or 160 MBps.
- Ultra320 SCSI: Uses a 16-bit bus and supports data rates of 320 MBps.

SMI-S See *Storage Management Initiative Specification (SMI-S)*.

SMTP Simple Mail Transfer Protocol. SMTP is a standard for e-mail transmissions across the internet.

SNMP
Simple Network Management Protocol. SNMP is used by network management systems to monitor network-attached devices for conditions that warrant administrative attention.

SMW Servo Manufacturer's Word.

SNS Sense.

special feature
A feature that can be ordered to enhance the capability, storage capacity, or performance of a product, but is not essential for its basic work.

SR Service representative, see also *CE*.

SRAM
Static random access memory.

SS Status store.

SSP Serial SCSI Protocol.

ST Store.

standard feature
The significant design elements of a product that are included as part of the fundamental product.

START
Start maintenance.

StartTLS
Secure LDAP communication using TLS.

Storage Management Initiative Specification (SMI-S)
A storage standard developed and maintained by the Storage Networking Industry Association (SNIA). It has also been ratified as an ISO standard. The main objective of SMI-S is to enable broad interoperable management of heterogeneous storage vendor systems.

subsystem
A secondary or subordinate system, usually capable of operating independently of, or asynchronously with, a controlling system.

SUPP Support.

sync Synchronous, synchronize. Occurring with a regular or predictable time relationship.

T

tachometer, tach
A device that emits pulses that are used to measure/check speed or distance.

tape cartridge
A container holding magnetic tape that can be processed without separating it from the container.

tape void
An area in the tape in which no signal can be detected.

TCP/IP
Transmission Control Protocol/Internet Protocol.

TCU Tape control unit.

TH Thermal.

thread/load operation
A procedure that places tape along the tape path.

TM Tapemark.

U

UART Universal asynchronous receiver/transmitter.

UL Underwriter's Laboratories.

unload
Prepare the tape cartridge for removal from the drive.

utilities
Utility programs.

utility programs
A computer program in general support of the processes of a computer; for instance, a diagnostic program.

uv Under voltage.

V

VOLSER
Volume serial number.

volume
A certain portion of data, together with its data carrier, that can be handled conveniently as a unit.

VPD Vital product data. The information contained within the tape drive that requires nonvolatile storage used by functional areas of the drive, and information required for manufacturing, RAS, and engineering.

W

word A character string that is convenient for some purpose to consider as an entity.

WORM
Write Once Read Many.

Write Write command.

WT world trade.

WWCID
World Wide Cartridge Identifier.

WWN World Wide Name.

WWNN
World Wide Node Name.

WWPN
World Wide Port Name.

X

XR External register.

XRA External register address register.

Index

Numerics

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

Readers' Comments — We'd Like to Hear from You

IBM System Storage TS3310 Tape Library
Setup and Operator Guide
Machine Type 3576

Publication No. GA32-0477-15

We appreciate your comments about this publication. Please comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this book. The comments you send should pertain to only the information in this manual or product and the way in which the information is presented.

For technical questions and information about products and prices, please contact your IBM branch office, your IBM business partner, or your authorized remarketer.

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. IBM or any other organizations will only use the personal information that you supply to contact you about the issues that you state on this form.

Comments:

Thank you for your support.

Send your comments to the address on the reverse side of this form.

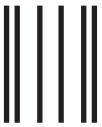
If you would like a response from IBM, please fill in the following information:

Name	Address
Company or Organization	
Phone No.	Email address

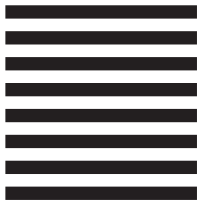
Readers' Comments — We'd Like to Hear from You
GA32-0477-15

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
Information Development
Department GZW
9000 South Rita Road
Tucson, Arizona U.S.A. 85775-4401

Fold and Tape | **Please do not staple** | Fold and Tape

Cut or Fold
Along Line

Printed in USA

GA32-0477-15

Spine information:

IBM System Storage TS3310 Tape Library

TS3310 Tape Library Setup and Operator Guide

Machine Type 3576