StorageTek T10000 Tape Drive

Operator's Guide

Part Number: E20714-02
May 2011

Submit comments about this document to STP_FEEDBACK_US@ORACLE.COM.

StorageTek T10000 Tape Drive Operator's Guide

E20714-02

Oracle welcomes your comments and suggestions for improving this book. Contact us at STP_FEEDBACK_US@ORACLE.COM. Please include the title, part number, issue date, and revision.

Table of Contents

List of Figures

List of Tables

Preface

This book is for users and operators of Oracle's StorageTek T10000 tape drives. It also provides information about the various cartridges and their labels.

The term T10000 is used in this publication to generically reflect all drive models. The specific model suffix is used whenever model differentiation is appropriate.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/support/contact.html or visit http://www.oracle.com/accessibility/support.html if you are hearing impaired.

What's New

Added the Controlling Contaminants appendix.

Added information about the tape drive cleaning threshold.

Updated the document template.

1

Introduction

Oracle's StorageTek T10000 tape drive family provides a range of small, modular, high-performance units designed for high-capacity data storage. The tape drive is either rack mounted or used in various StorageTek libraries (FIGURE 1-1). There are currently three models in the T10000 drive family: T10000A, T10000B, and T10000C.

FIGURE 1-1 T10000 Tape Drive Configurations

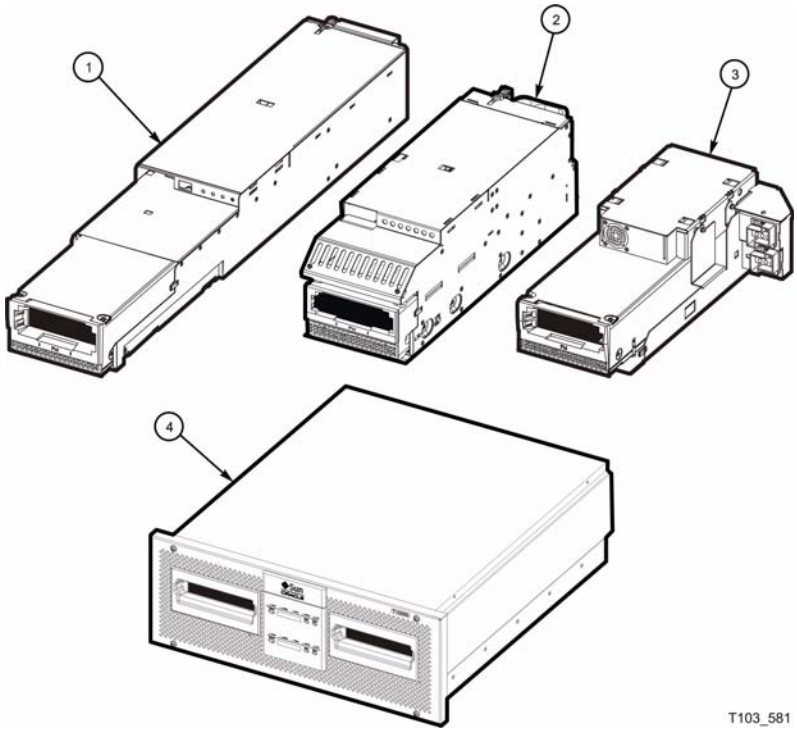


Illustration call-outs (4):
1. SL8500 configuration
2. SL3000 configuration
3. L180/L700e/L1400M configuration (T10000A and T10000B only)
4. Rack mount configuration

The following libraries support certain models of the T10000 tape drive family:

- SL3000
- SL8500
- L180/L700e/L1400M (T10000A and T10000B only)
- 9310 (T10000A only)

Tape Drive Description

The drive uses a unique, single-reel cartridge. The file reel is located inside the cartridge while the machine reel resides inside the tape drive. The drive uses a technology called *partial response, maximum likelihood* (PRML) to provide a high-density data format. PRML enables recording and storing an uncompressed capacity of up to:

- 500 gigabytes (GB) with the T10000A tape drive
- 1 terabyte (TB) with the T10000B tape drive
- 5 terabytes (TB) with the T10000C tape drive and T10000C media

A T10000A drive can read and reclaim a tape cartridge written by a T10000A drive.

A T10000B drive can:

- Read and reclaim a tape cartridge written by a T10000A drive
- Write, read, and reclaim a tape cartridge written by a T10000B drive

A T10000C drive can:

- Read tape cartridges written by either a T10000A or T10000B drive
- Write, read, and reclaim a tape cartridge written by a T10000C drive

The tape drive uses fiber optic host connections to provide a high data-transfer rate.

> **Note –** See Appendix E, "Specifications"and Appendix F, "Controlling Contaminants" for additional specifications and requirements.

Tape Drive Rear Panel

The rear panel has a recessed push-button switch, two multi-color LED indicators, and five connectors. The recessed switch is used by service representatives to toggle the drive in/out of the service mode. The drive status LED is on all drives while the encryption status LED is only on encryption-capable drives.

- FIGURE 1-2 on page 17 shows the locations of those items on a T10000B tape drive.
- FIGURE 1-3 on page 18 shows the locations of those items on a T10000C tape drive.

Note – See TABLE 1-1 on page 19 for drive status LED states. See "Encryption Status LED" on page 20 for encryption status LED states.

FIGURE 1-2 T10000B Tape Drive Rear Panel

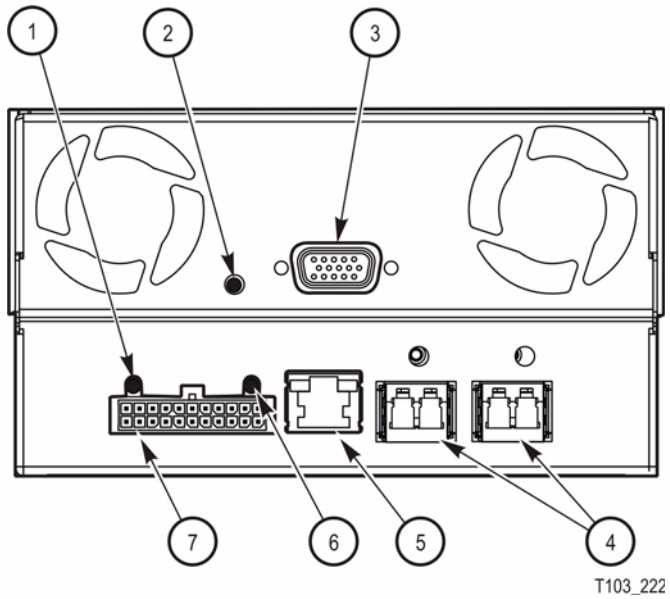


Illustration call-outs (7):
1. Drive status LED indicator
2. Recessed switch (service representative use only)
3. Tape transport interface (TTI) connector (library use)
4. Interface ports
5. Maintenance port (Ethernet)
6. Encryption status LED
7. Power supply connector

FIGURE 1-3 T10000C Tape Drive Rear Panel

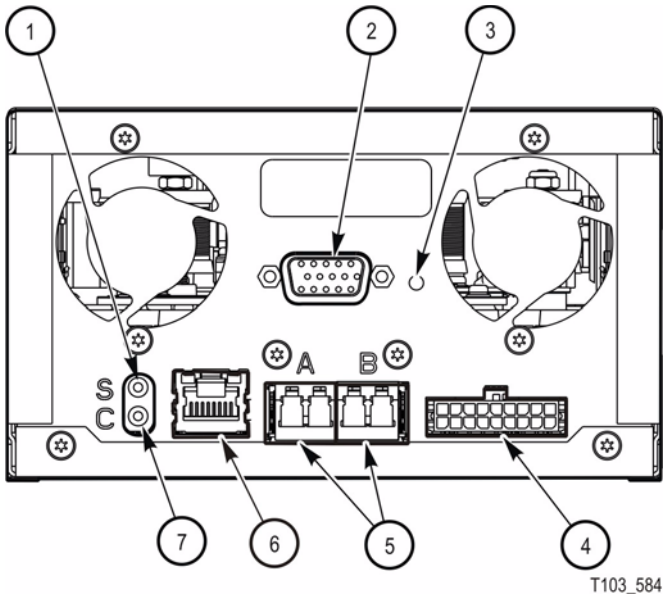


Illustration call-outs (7):
1. Encryption status LED
2. Tape transport interface (TTI) connector (library use)
3. Recessed switch (service representative use only)
4. Power supply connector
5. Interface ports
6. Maintenance port (Ethernet)
7. Drive status LED indicator

Drive Status LED

The drive status LED on the rear panel (see FIGURE 1-2 on page 17 or FIGURE 1-3) indicates the general status of the drive. The normal sequence of the drive status LED during the drive power-on IPL: slow-flashing red, slow-flashing amber, steady or slow-flashing green.

> **Note –** The slow flash rate is one cycle per second, and the fast flash rate is two cycles per second. Some indications alternate between two colors at the slow flash rate.

TABLE 1-1 on page 19 interprets the various states of the drive status LED:

TABLE 1-1 Drive Status LED State Descriptions

LED State	Description	Meaning/Action
Off	Drive powered off	Power not applied to the drive. Turn on the power supply. Possible power related failure if it remains off with power supply switch on.
Red	Hardware failure	Processor not functioning. Call for service.
Red (slow flash rate)	IPL started	Booting, no communication with drive until IPL has completed.
Amber (slow flash rate)	Functional code loading	Initializing, no communication with drive until IPL has completed.
Green	IPL complete (dumps *not* present)	Normal operating condition, drive is ready for functional tasks. Communication with drive is possible.
Green (slow flash rate)	IPL complete (dumps are present)	Normal operating condition, drive is ready for functional tasks. Communication with drive is possible.
Amber	Boot Monitor	Engineering maintenance mode. Call for service.
Red/Blue (alternating)	Hardware failure	Power on failure. Call for service.
Red/Green (alternating)	Service mode	Initiated by service representative. While in the service mode, the drive's IP is static 10.0.0.1.
	Dump-again state	If indication is present without service mode active, it could indicate a recurring malfunction is present, call for service.
Red (fast flash rate)	Dump in progress	Do not power off while the drive is performing a dump operation (drive memory could be corrupted). No communication at this time.
Amber (fast flash rate)	Firmware update in progress	Do not disturb the drive until the firmware update is complete. When the update is complete, the LED will change to green fast flashing.
Green (fast flash rate)	Firmware update is complete	Initiate an IPL when the drive is idle, if the IPL did not auto-initiate.

Interface Ports Use

The T10000 tape drive supports connection of both ports, in accordance with ANSI Fibre Channel specifications (ref. *InterNational Committee on Information Technology Standards [INCITS] documents: SCSI Primary Commands -3, Section 5.6,* and *Fibre Channel Protocol -3*). The drive will support two hosts, provided that both hosts honor the "reserve/release" and/or the "persistent reserve/release" specifications.

It is not recommended that a T10000 tape drive be connected to the same host bus port with another tape or a disk subsystem. The stress on the host bus adapter, due to the bandwidth needs, creates unacceptable error recovery issues between both solutions.

Maintenance Port Use

All service calls for tape drives under warranty, maintenance contract, or time-and-materials service require physical access and connection to the rear panel maintenance (Ethernet) port.

In the event that a customer has an Ethernet cable physically connected to the drive requiring service, the service person must disconnect this cable to perform the required service action.

- T10000 non-encryption drives supported by the Service Delivery Platform (SDP) require 100% dedication of the drive's Ethernet port to the SDP site unit.
- T10000 encryption-enabled drives require 100% dedication of the drive's Ethernet port to the Encryption Service Network except during service activities performed by authorized personnel.

Where Encryption and SDP coexist, the Ethernet Port must be concurrently shared by using the Service Network.

> **Note –** Oracle neither supports nor assumes any responsibility for drive functional failures that occur during the unauthorized use of the drive's maintenance port.

Unauthorized use applies to any use of the drive's Ethernet port for other than the following items:

- Encryption 1.x or 2.x environments
- StorageTek Virtual Operator Panel (VOP) customer or service versions
- Service Delivery Platform (SDP)
- Service's Tape Health Check Tool
- StorageTek Diagnostic System (STDS)

With drive code level 1.40.x07, IPv6 addressing is supported on the Ethernet port of T10000A/B drives. The T10000C drive supports IPv6 addressing. An IPv6 address is a 128-bit value written as eight groups of four hexadecimal characters separated by colons (for example, 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

Encryption Status LED

T10000 drives that are encryption capable have a multi-color encryption status LED on the rear panel (see FIGURE 1-2 on page 17 or FIGURE 1-3 on page 18).

If the encryption status LED is green, it indicates that the drive is encryption capable, but not encryption enabled. In this state, the drive functions only in a non-encryption "Safe" mode and can neither read nor write encrypted tape cartridges. However, the drive can function normally for non-encryption tasks.

After the drive is encryption enabled, the LED turns red to indicate that the drive is "Armed" and functional in the encryption mode. In this state, the drive can read and write encrypted tape cartridges. The drive can also read non-encrypted tape cartridges, but *cannot* write to non-encrypted tape cartridges.

The states of the encryption status LED are:

> **Note –** Slow flash rate is 1 cycle per second.

LED state: Off

The drive does not have encryption hardware.

LED state: Green

Encryption capable, but not enabled.

KMS 1.X: Not encrypting

KMS 2.x: Not licensed

Normal-unencrypted drive write/read cartridge operations.

LED state: Green (slow flashing)

Mode: Reset

Encryption previously enabled, but requires keys. Drive is capable of read-only, unencrypted cartridge operations.

> **Note –** Drive is no longer capable of unencrypted write operation after encryption has been enabled.

LED state: Red

Mode: Armed, idle

Encryption enabled/active. Ready to encrypt.

LED state: Red (slow flashing)

Mode: Armed, active

Encryption read/write cartridge operation in progress.

LED state: Amber

KMS 1.X: Requires media key.

KMS 2.x:

- Enrolled, cartridge not loaded.
- Enrolled, cartridge loaded but waiting for KMS key.

LED state: Amber (slow flashing)

Requires device key (KMS 1.x only).

LED state: Cycling

> **Note –** The LED continuously cycles through several colors at the slow flash rate.

Mode: Zeroed

Media, device, and enabling keys missing. The drive is unusable, and must be returned to manufacturing.

Refer to Crypto Key Management documentation for additional information:

Encryption Options

Encryption-capable T10000 tape drives support data-at-rest encryption and have a second status LED on the rear panel (see FIGURE 1-2 on page 17 [T10000A/B] or FIGURE 1-3 on page 18 [T10000C]).

Federal Information Processing Standards compliance:

- FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*
  - Level 1 — The basic level with production-grade requirements.
  - Level 2 — Adds requirements for physical tamper evidence and role-based authentication.
- With drive code level 1.40.x07 and Key Management System (KMS) 2.1, the T10000A drive complies with FIPS Level 1.
- With drive code level 1.40.x07 and Key Management System (KMS) 2.1, T10000B drive complies with FIPS Level 2.
- The T10000C is designed to comply with FIPS Level 1.

Key Management Solutions

The StorageTek Crypto Key Management Station (KMS 1.x), StorageTek Crypto Key Management System (KMS 2.x), and Oracle Key Management (OKM 2.3) provide device-based encryption solutions. The tape drive is shipped from the factory encryption-capable, but not encryption-enabled. You must explicitly enable the drive for encryption.

> **Note –** A tape drive that has *not* been enabled for encryption can neither read nor append to any encrypted tape cartridge. It can, however, overwrite an encrypted tape from the beginning of tape (BOT).

What an Encryption-Enabled T10000 Tape Drive *CAN* Do:

- Write to a tape cartridge in encrypted mode ONLY, using its assigned write key
- Read an encrypted tape cartridge, if it has the proper read key
- Read non-encrypted tape cartridges—not capable of writing to or appending to the cartridge
- Format or reclaim tape cartridges

What an Encryption-Enabled T10000 Tape Drive *CANNOT* Do:

- Append non-encrypted data to an encrypted tape cartridge
- Write a non-encrypted tape cartridge

Oracle/StorageTek Encryption Resources

For additional information on the encryption capabilities and features of the T10000 Tape Drive, see:

- OKM 2.3
  - *Oracle Key Manager, Administration Guide*
  - *Oracle Key Manager, Systems Assurance Guide*
- KMS 2.x
  - *Crypto Key Management System, Administration Guide*
  - *Crypto Key Management System, Systems Assurance Guide*
- KMS 1.x
  - *Crypto Key Management Station, User's Guide*
  - *Crypto Key Management Station, Configuration and Startup Guide*
  - *Crypto Key Management Station and Data-at-Rest Encryption, Technical Brief*

For further information on the encryption option, see your sales representative.

Data Path Key Management

The data path key management (DPKM) subsystem is the third installment of encryption for StorageTek tape drives. DPKM uses the SCSI 4 commands `Security Protocol In` and `Security Protocol Out` to implement host-based key management on StorageTek encrypting tape drives. Encryption keys are delivered to the tape drive over the Fibre Channel interface (non-FIPS compliant). DPKM provides the ability to toggle the encryption state on/off on a per cartridge basis which allows the user to have a mix of encrypted/non-encrypted files on each tape cartridge. DPKM support is available with drive code level 1.41.x10 or higher on T10000A/B tape drives or with the initial code release for the T10000C. You use the Virtual Operator Panel to enable or disable the DPKM capability of the tape drive.

Interface with the Tape Drive

The T10000 tape drive does not have a built-in physical operator panel; therefore, your communication with library-attached drives is normally through the Virtual Operator Panel (VOP) application.

Virtual Operator Panel

The VOP application window (FIGURE 1-4 on page 24) provides a graphical user interface (GUI) to the connected drive. The GUI has a menu bar, a section that provides several drive status indicators and two drive message windows (primary and secondary), and the bottom portion of the GUI contains the VOP text message pane. Additional information is available in the *Virtual Operator's Panel Customer User's Guide*.

> **Note –** When you use VOP with a T10000C drive, an additional indicator is present that shows the drive hibernate status.

Download VOP 1.0.16, and higher, from the following URL:

http://edelivery.oracle.com/

Select Oracle StorageTek Products and Generic Platform.

FIGURE 1-4 VOP Application Window for a T10000B Drive

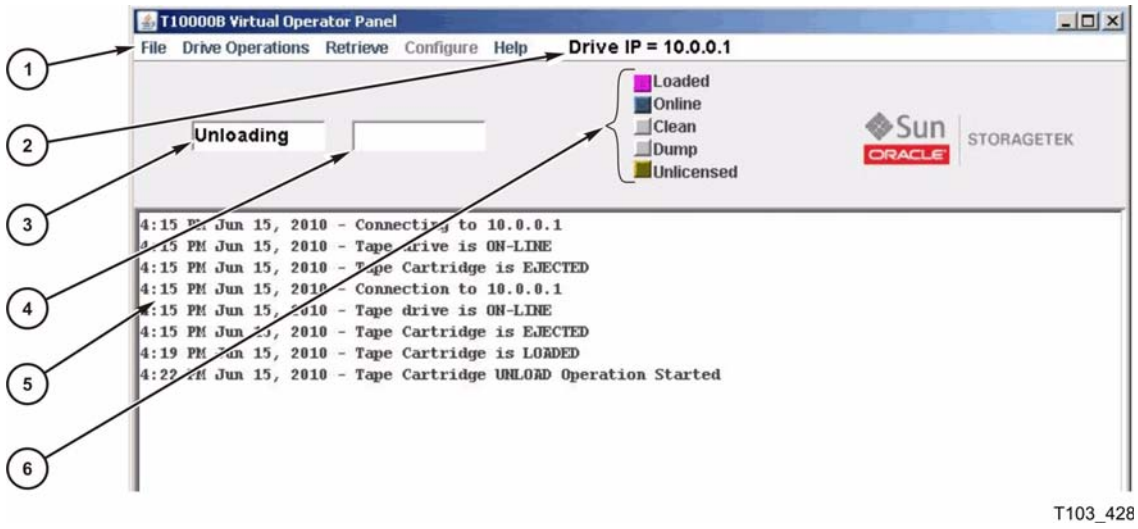


Illustration call-outs (6):
1. Menu bar
2. Drive IP/name
3. Primary drive message window
4. Secondary drive message window
5. VOP text message pane
6. Drive status indicators

Library Drives

Manual drive operations, such as configuration settings and utilities, can be directed by VOP through the drive's rear panel Ethernet maintenance port.

Rack Mount Drives

Rack mounted drive operation is normally accomplished through the drive tray chassis operator panel (see "Operator Panel Controls/Indicators" on page 34). However, you can also operate it with VOP and a connection to the Ethernet port on the rear panel of the drive tray chassis.

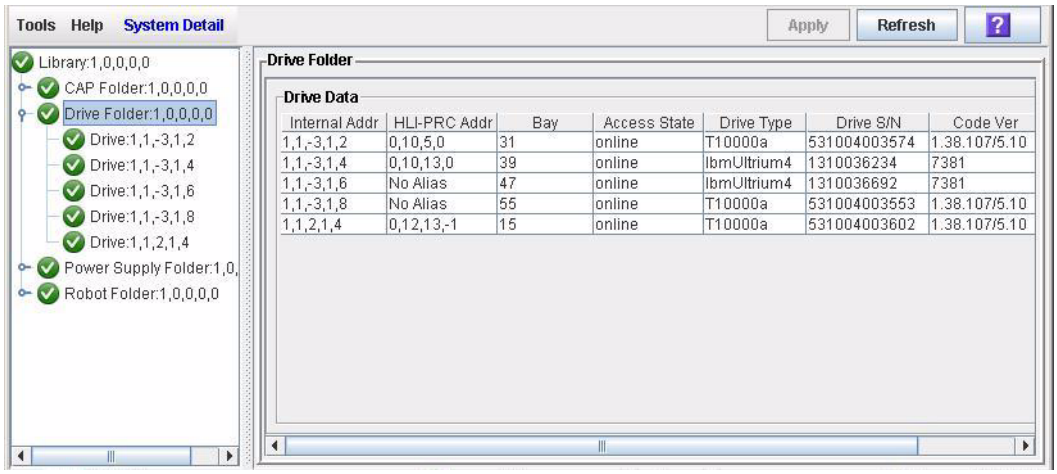
Secure Configuration

The VOP is designed to operate on a service network configured as a private LAN. VOP, tape drives, the Crypto Key Management Station (if drives are encrypted), and Ethernet switches are potential components of the private LAN. The private LAN best practice recommendation ensures security from unauthorized access. See the *StorageTek Crypto Key Management System, Systems Assurance Guide* for details regarding the service network private LAN.

StorageTek Library Console

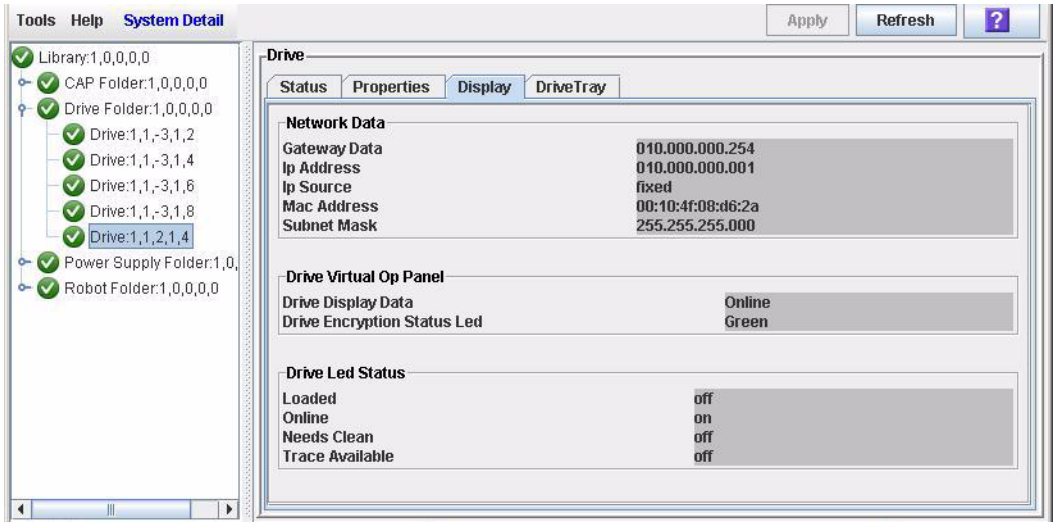
The SL3000 and SL8500 libraries have a GUI called the StorageTek Library Console (SLC) that presents basic drive information. The system detail drive folder, shown in the following figure, contains a list of installed drives and data about each drive (such as the drive access state, the drive type, the drive serial number, and the version of drive code).

FIGURE 1-5 StorageTek Library Console



When you select a specific drive, additional unique data is available for that drive such as the drive status, drive properties, drive display, and drive tray information (see FIGURE 1-6).

FIGURE 1-6 Drive Display - StorageTek Library Console



Note – The SLC drive folder information changes frequently, and the actual data displayed might differ from the example. Click the question mark button on the GUI for additional information.

T10000 Cartridges

The T10000 supports five types of cartridges:

- StorageTek T10000 T1 cartridge (T10000A/B drive):
  - Data: *500* gigabytes T10000A or *1* terabyte T10000B
  - Data, sport: *120* gigabytes T10000A or *240* gigabytes T10000B
  - VolSafe, capacity: *500* gigabytes T10000A or *1* terabyte T10000B
  - VolSafe, sport: *120* gigabytes T10000A or *240* gigabytes T10000B
  - Cleaning cartridge: 50 uses (CT or CL cartridge)
- StorageTek T10000 T2 cartridge (T10000C tape drive):
  - Data, standard: *5* terabytes
  - Data, sport: *1* terabyte
  - VolSafe, capacity: *5* terabytes
  - VolSafe, sport: *1* terabyte
  - Cleaning cartridge: 50 uses (CC or CL cartridge)

Note – The T10000 does not accept a data cartridge for any other type of tape drive.

FIGURE 1-7 identifies key areas of the StorageTek T10000 tape cartridge.

FIGURE 1-7 T10000 Cartridge

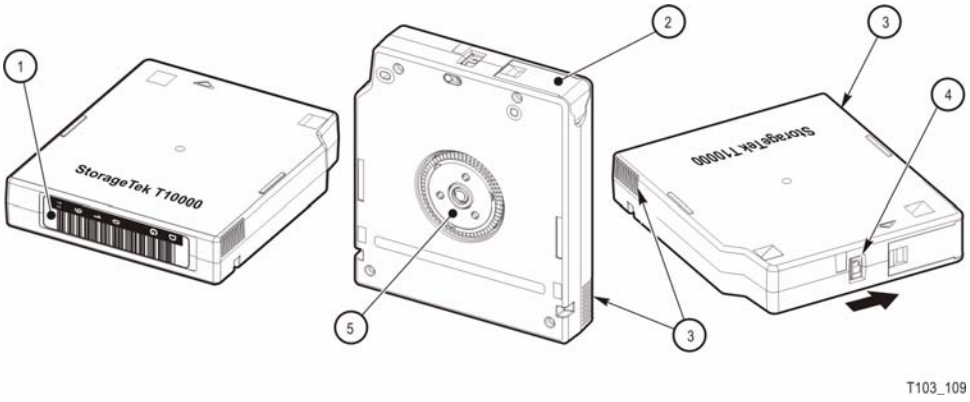


Illustration call-outs (5)
1. Volume label
2. Leader access door
3. Finger grips
4. File protect switch
5. Hub

Standard Data Cartridge

Standard cartridges are the common read/write data cartridges. You can identify a standard cartridge by the *black* access door (see FIGURE 1-7 on page 26).

- Each *standard* data cartridge has a native capacity of:
  - StorageTek T10000 T1: 500 GB (T10000A) or 1 TB (T10000B)
  - StorageTek T10000 T2: 5 TB (T10000C)
- The StorageTek T10000 T1 data cartridge is under warranty for 15,000 mounts. The StorageTek T10000 T2 data cartridge is under warranty for 25,000 mounts. The tape drive issues a warning message to the host when that number is exceeded.

  Note – A mount is defined as the tape drive threading the tape onto the take-up reel and moving to the load point.

Diagnostic Cartridges

The Diagnostic cartridge is a special-use version of the standard data cartridge with a special label. The diagnostic cartridge is typically used by a service representative and most libraries store one or more diagnostic cartridges. (See "Diagnostic Cartridge Labels" on page 92.)

Sport Data Cartridges

Sport cartridges are a smaller version of the standard data cartridges. You can identify a sport cartridge by the *red* access door (see FIGURE 1-7 on page 26).

- Each *sport* data cartridge has a native capacity of:
  - StorageTek T10000 T1: 120 GB (T10000A) or 240 GB (T10000B)
  - StorageTek T10000 T2: 1 TB (T10000C)
- The StorageTek T10000 T1 cartridge is under warranty for 15,000 mounts. The StorageTek T10000 T2 cartridge is under warranty for 25,000 mounts. The tape drive issues a warning message when that number is exceeded.

VolSafe Data Cartridges

VolSafe data cartridges are write-once data cartridges. They cannot be erased without destroying the tape itself. The tape drive writes data on the tape and appends data to the cartridge on free space until the cartridge is full. The tape drives may read these cartridges multiple times. These cartridges are commonly used for information that must be stored for legal reasons and not altered. There are two versions of the VolSafe cartridge:

- VolSafe cartridge—you can identify this cartridge by a yellow leader access door (see FIGURE 1-7 on page 26). This cartridge has the same capacity as the standard data cartridge.
- Sport VolSafe cartridge—you can identify this cartridge by a yellow leader access door and red file protect switch (see FIGURE 1-7 on page 26). This cartridge has the same capacity as the sport data cartridge.

Cleaning Cartridges

As the name implies, you would use a cleaning cartridge to clean a drive's read/write head up to 50 times. An attempt to use a cleaning cartridge beyond that number results in the tape drive rejecting the cleaning cartridge and posting an error message to the host. You can identify a cleaning cartridge by a white leader access door (see FIGURE 1-7 on page 26). There are several versions of the cleaning cartridge:

- T10000A/B cleaning cartridge
- Cleaning cartridge for the T10000C only
- Cleaning cartridge capable of cleaning all three T10000 drive models

> **Note –** It is recommended that you clean the T10000B tape drive every ten full file operations due to its higher linear density and capacity as compared to the T10000A tape drive. This is three times more frequent than with the T10000A tape drive.

Media Information Region

The T10000 tape drives use information recorded on each tape cartridge to reduce access times and manage the useful life of the cartridge. This information is recorded in the cartridge's radio frequency identification (RFID) chip and at the beginning of tape in an area known as the media information region (MIR). The information stored in the RFID is a proper subset of the information stored in the MIR. The media information falls into two categories: statistical counters and data pointers.

Statistical Counters

Statistical counters reflect use of the cartridge and includes read/write activity, error activity, cumulative mounts, and other information about its use.

Data pointers

The data pointer information is a directory (map) used to locate the customer (logical) data on the physical tape media. Because customer data is compressed and written in drive controlled blocks on the tape, a map is needed to efficiently locate the data after it is written. This map provides an index between customer data and the physical block on the tape media. After data is written the drive accesses this map to optimize access to the customer data.

To locate/space to customer data, the logical object that identifies the block is translated to the physical location on the tape media, and the drive determines the quickest method to read the block. If the block is some physical distance from the current location, a calculation results in a high-speed locate to the block location and is followed by a normal speed read.

The existence of the media information is usually transparent to the customer unless it has a problem. This can occur if the information update fails during a dismount. The impact of invalid media information occurs in several areas. Because it enables high speed positioning, invalid media information forces all operations to a slow

speed mode. This has no impact on a sequential read from the beginning of the tape. However, any operation using locate defaults to a sequential slow speed read to the requested block, which can result in longer processing time.

> **Note –** Invalid media information might be suspected if you observe poor performance on a specific tape cartridge.

The following sections describe how media information is processed and some potential implications of problems with the information.

Normal Processing

Every time a tape cartridge is loaded, the media information is read from the tape media and saved in drive-resident memory. After being loaded in drive memory, a read-invalid state is written in the tape-resident RFID. The tape-resident media information is marked open, read-invalid because it does not reflect results of activity in the current mount session. All subsequent media information accesses during the current mount session are saved in the drive-resident information. If no writes are performed to the cartridge, the RFID remains in the read-invalid state meaning the MIR directory information is still completely valid. After a write takes place, the RFID is marked write-invalid meaning the MIR directory information on tape is invalid.

The T10000 drives use the drive-resident copy of the information to access customer data pointers for read-only functions. Statistical counters are continuously updated in the memory-resident information with any drive activity.

When the cartridge is unloaded as part of the unload routine, the drive-resident information is written to the cartridge's RFID and the tape-resident MIR with the closed state indication set.

Cross-Density Cartridge Processing

Whenever a data cartridge is loaded that was written in a data density format that is different from the one used when the drive writes, model-specific MIR processing occurs. In an environment with mixed T10000 drive models, a mandatory firmware update provides the capability for the lower-density drive to read the RFID of a higher-density drive.

For a standard data cartridge or Sport cartridge written by a T10000A drive, the:

- RFID can be read or updated by a T10000A, B, or C drive
- MIR can be read by a T10000A, B, or C drive
- MIR cannot be updated by a T10000B or C drive
- T10000A, B, or C drive counters can be updated after appropriate firmware updates are installed
- Cartridge can be reclaimed by a T10000A or B drive

For a standard data cartridge or Sport cartridge written by a T10000B drive, the:

- RFID can be:
  - Read by a T10000A, B, or C drive
  - Updated by a T10000B or C drive

- MIR can be read by a T10000B or C drive
- MIR cannot be updated by a T10000A or C drive
- T10000B or C drive counters can be updated after appropriate firmware updates are installed
- Cartridge can be reclaimed by a T10000A or B drive

> **Note –** When the T10000A/B drive identifies the data cartridge as an unreadable-density data format, it displays 3215 on the Virtual Operator Panel (VOP) or the physical operator panel of the rack mount drive.

For a standard data cartridge or Sport cartridge written by a T10000C drive, the:

- RFID can be:
  - Read by a T10000A, B, or C drive
  - Updated by a T10000C drive
- MIR can be read by a T10000C drive
- MIR cannot be updated by a T10000A or B drive
- T10000C drive counters can be updated after appropriate firmware updates are installed
- Cartridge can be reclaimed by a T10000C drive

Invalid Media Information Conditions

There are four media invalid conditions for the T10000 drives:

- **Cartridge's RFID is unreadable**. The drive refuses to mount the cartridge (FSC of 403B). Return the cartridge to engineering to recover the customer data.
- **Cartridge's RFID can be partially read.** The drive mounts the cartridge as read-only.
- **RFID and MIR are out-of-sync.** None of the block information, coarse-grained in the RFID or fine-grained in the MIR, can be trusted. The cartridge is usable but the drive must rebuild the block information as it sequentially reads all of the data up to the desired customer data.

  > **Note –** This scenario can cause the drive to spend an hour or more rebuilding the block information, potentially causing the application running on the host to time-out.

- **MIR is corrupted or unreadable.** The fine-grained block location information on the cartridge cannot be used; the tape can be used with the coarse-grained block information on the RFID but with lower performance.

  The drive posts a 4031/4032 informational FSC whenever it loads a cartridge with an *invalid* MIR. When a tape cartridge has an invalid media information, some action is required to correct it. Invalid media information can be corrected in several ways:

  - Run the media correction utility through the VOP (see "To Rebuild the MIR (VOP)" on page 49).

- The drive recovers the media information as it processes host commands, but very slowly.

Tape Drive Features

StorageTek Data Integrity Validation

StorageTek Data Integrity Validation (DIV) ensures that a checksum, provided by an application or file system, is validated by the StorageTek T10000 for each record sent to the drive. The user-generated checksum is stored with each record on tape and can be checked on any future read or verify operation (without the added overhead of sending data to the host). The *StorageTek T10000 Tape Drive Fibre Channel Reference Manual* describes how to use this feature.

StorageTek Maximum Capacity

Maximum Capacity allows the use of tape capacity that is normally reserved to ensure tape-to-tape copy operations succeed. This can increase the capacity by five to ten percent. The *StorageTek T10000 Tape Drive Fibre Channel Reference Manual* describes how to use this feature.

StorageTek File Sync Accelerator

The StorageTek File Sync Accelerator (FSA) allows applications to reduce or eliminate back hitches that are normally caused by writing a tape mark or other sync operations. This feature can be disabled from the Virtual Operator Panel.

StorageTek Tape Application Accelerator

The StorageTek Tape Application Accelerator (TAA) avoids back hitches by converting tape marks to buffered tape marks and syncs to NO-OPs. The feature is enabled with Virtual Operator Panel, but is only available with FICON.

> **Note –** This feature must only be used in environments that handle deferred errors. When this feature is enabled, sending a tape mark does not ensure the data has successfully been written to the tape. A deferred error may be reported when buffered date is written to tape after the command has completed. In a FICON *only* environment, duplex write operations should use this feature.

StorageTek Search Accelerator

The StorageTek Search Accelerator (SSA) allows FICON applications to search for a string up to 1024 bytes in length. This feature can be used to enhance Mainframe HSM Audit performance in FICON environments.

StorageTek MIR Assisted Search

The StorageTek T10000C tape drive supports access to the Media Information Region (MIR) of the cartridge. This command is implemented using a `SCSI Read Buffer` command similar to the StorageTek T10000B tape drive. MIR data provides location information for tape records and can be used by an application to order which records are read first from tape. The T10000 MAS N677 engineering document describes this feature.

StorageTek In-Drive Reclaim Accelerator

The StorageTek In-Drive Reclaim Accelerator (IDR) allows applications to reclaim space on the tape without rewriting the entire tape. The application must save and manage a partition map to get the full benefit of this feature. The StorageTek Virtual Storage Manager (VSM) supports this feature with the StorageTek T10000B and T10000C drives. For more detailed information about this feature, contact your local sales representative to obtain a copy of the *ALP User's Guide*.

StorageTek Tape Tiering Accelerator

The StorageTek T10000C has the ability to partition tape. These partitions can be organized by an application to control where file sets are located on tape. Data sets located near the beginning of tape will have faster access characteristics than data written near the end-of-tape (EOT).

- Applications now have the ability to manage the location of data on the tape.
- StorageTek Tape Tiering Accelerator (TTA) allows partitions to be read only.
- TTA allows up to 480 logical volumes on a cartridge.

For more detailed information about this feature, contact your local sales representative to obtain a copy of the *ALP User's Guide*.

2

Rack Mount Controls and Indicators

This chapter provides information about the indicators and switches located on the rack mount drive.

Front Panel

The T10000 Tape Drive rack mount configuration chassis contains one or two drives. The chassis front panel (FIGURE 2-1) provides manual loading/unloading of tape cartridges into each drive through separate cartridge loading slots. The front panel also has a dual operator panel mounted between the cartridge loading slots. The upper portion is for drive A (left), and the lower portion is for drive B (right).

FIGURE 2-1 Rack Mount Chassis Front Panel

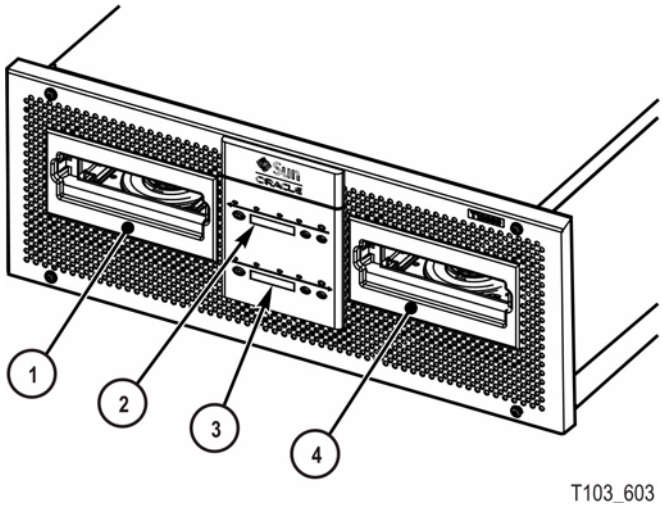


Illustration call-outs (4):
1. Cartridge loading slot drive A
2. Operator panel drive A
3. Operator panel drive B
4. Cartridge loading slot drive B

Load/Unload Slot

The load/unload slots only accept T10000 tape cartridges. All other cartridge types will not load into the T10000 tape drive. After you have inserted a tape cartridge, the loader mechanism lowers the cartridge onto the hub motor, and threads the tape (see "To Load a Cartridge" on page 40). See "To Unload a Cartridge" on page 42 to unload and remove a tape cartridge.

Operator Panel Controls/Indicators

The rack mount chassis dual-operator panel (FIGURE 2-2) provides independent control and indications for the two rack mount T10000 tape drives. Each section contains four push-button micro-switches, four LEDs, and a ten-character display window. TABLE 2-1 describes the controls, and TABLE 2-2 on page 35 describes the LED indicators.

FIGURE 2-2 Operator Panel

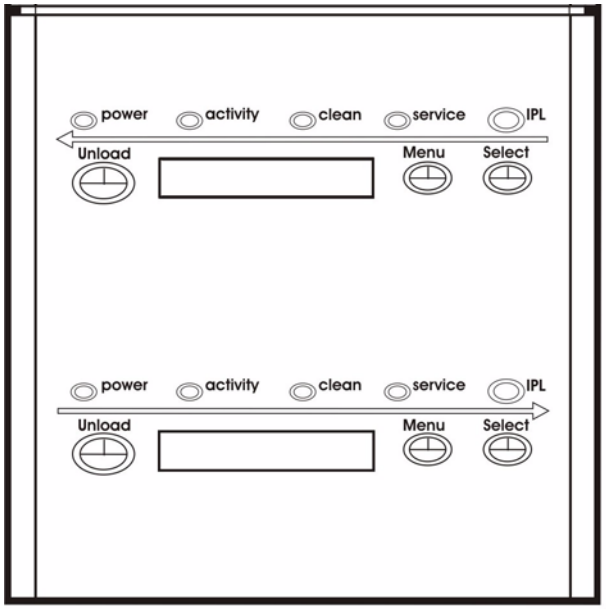


TABLE 2-1 is a two column table that lists the four operator panel push button micro-switches and describes their use.

TABLE 2-1 Operator Panel Controls

Push Button	Use
Unload	Initiates a cartridge rewind and unload operation.
Menu	Steps through a menu sequence or answers **No** to a display window option.
Select	Answers **Yes** to an option appearing in the display window or toggles/increments a variable during a menu sequence.
IPL (recessed)	Initiates an IPL.

TABLE 2-2 lists the front-panel indicator states and recommended action. The table lists the four indicators (power, activity, clean, and service), the state of the indicator, the meaning of the indication, and any recommended action.

TABLE 2-2 Operator-panel Indicators

Power (green)	Activity (green)	Clean (amber)	Service (red)	Meaning	Recommended Action
Off	Off	Off	Off	The drive is not powered.	Power on the drive.
Flashing	Off	Off	Off	Power on, IPL in progress.	Wait for the IPL to complete.
Flashing steadily	Off	Off	Off	Power on IPL sequence failed.	Power cycle the drive. If the problem persists, contact authorized service personnel.
On	Off	Off	Off	Power on, IPL complete but cartridge not loaded.	Load a cartridge as required.
On	On	Off	Off	Power on, cartridge loaded (tape not moving).	Ready for read/write commands from the host software application.
On	Flashing	Off	Off	Power on, cartridge loaded (tape moving).	None, locating or read/write operation in progress.
On	On/Off	On	Off	The drive tape path needs cleaning (see "T10000 Tape Drive Cleaning" on page 43).	Insert a cleaning cartridge.
On	Flashing	Flashing	Off	Cleaning cartridge loaded and moving.	Wait for the cleaning operation to complete.
On	On/Off	Off	Flashing	An error has occurred and dump data is saved.	Read the display message. See TABLE D-1 on page 97 for more information about the message.
On	Off	Off	On (steady)	A drive hardware error has occurred.	Initiate an IPL. If the problem persists, contact authorized service personnel.

Operator Panel Display Window

The window displays alpha/numeric messages relative to drive operation:

- Drive status
- Menu selections and configuration choices
- Error messages and fault symptom codes
- Host-generated messages

The display window is formed by a horizontal row of ten LED array segments. Each segment is an array of 35 dots—five wide and seven high. Each array can form an uppercase or lowercase alpha character, a numeral, or a special character (such as an asterisk [*]).

Multiple messages or a message greater than ten characters are displayed by the window, alternating between required character groups.

Note – Appendix D, "Messages and Translated Messages" lists messages that could appear in the display window.

Rear Panel

FIGURE 2-3 shows the rear of the rack mount chassis. One AC power connector and one AC switch supplies AC power to both drive power supplies, which are mounted internally, between the drives.

FIGURE 2-3 Rack Mount Chassis Rear Panel

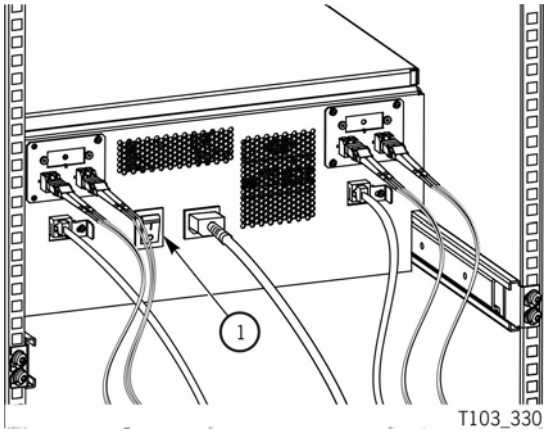


Illustration call-out:

1. AC power switch

Note – The drive status LED and encryption status LED, for encryption-capable drives, are visible through the drive cooling grids.

3

Operator Tasks

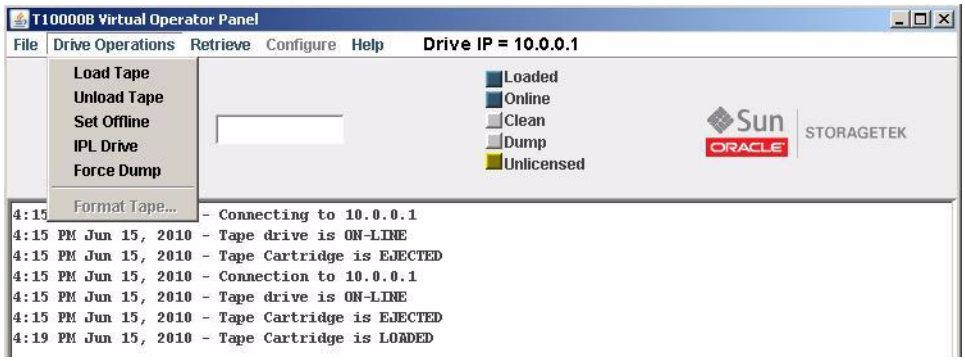
This chapter discusses operator tasks primarily for rack-mounted T10000 tape drives. Many tasks are performed by using the physical operator panel switches (see "Operator Panel Controls/Indicators" on page 34) while some involve using the drive menu system (see "Menu System" on page 55).

You can choose to use the Virtual Operator Panel (VOP) instead of using the physical operator panel. Many of the drive and cartridge tasks are performed by using the Drive Operations menu (see FIGURE 3-1).

> **Note –** The T10000C tape drive has additional commands available in the Drive Operations menu (VOP release 1.0.17). Consult the *Virtual Operator Panel User's Guide* for information regarding the additional commands.

To use the VOP, you connect a computing platform which has VOP installed to the Ethernet port on the drive tray, use the File menu to connect to the drive, and enter the IP address of the drive.

FIGURE 3-1 Virtual Operator Panel Drive Operations Menu (T10000B Tape Drive)



For operator tasks relating to drives within a library, consult library operator guides. The scope of tasks documented depends on the functionality of the particular library. Library information might describe only drive cleaning or provide a broad range of tasks (using the drive operator panel, cleaning a drive, and manually mounting or dismounting a cartridge).

Basic Tasks

The basic tasks include:

- Power-on Rack Mount Drives
- Power-off Rack Mount Drives
- "Write-Protect/Write-Enable a Cartridge" on page 39
- Load a cartridge on page 40
- Unload a cartridge on page 42
- Clean the drive on page 43
- "Initial Program Load (IPL)" on page 44

▼ Power-on Rack Mount Drives

To apply power to the rack mount tray:

1. **Make sure the rack mount tray is connected to an AC power outlet or power strip.**
2. **Make sure that all interface cables are fully seated.**
3. **Set the power switch on the rear panel to on (|) [see FIGURE 2-3 on page 36].**

Both drives power-on and start performing an initial program load (IPL).

> **Note –** The power indicator flashes while the IPL is in progress. It is the left most operator panel LED, see FIGURE 2-2 on page 34. Various messages relative to the IPL sequence appear in the operator panel display window. These messages do not require operator action.

The drive successfully completes an IPL when:

- The drive power indicator is steady.
- An asterisk (*) appears in the operator panel display window.

▼ Power-off Rack Mount Drives

> **Note –** The drive tray switch removes power from both tape drives in a dual-drive tray.

To remove power from the rack mount tray:

1. **Make sure there is not a job or application running on the host that is using the tape drive(s). If there is, stop that job or application.**
2. **Make sure a cartridge is not loaded in the tape drive(s).**
3. **Set the power switch located on the rack mount tray rear panel to off (O).**

   (See FIGURE 2-3 on page 36.)

Cartridge Procedures

▼ Write-Protect/Write-Enable a Cartridge

1. **Locate the write-protect switch beside the cartridge door.**
2. **Move the write-protect switch to the desired setting.**

The symbols (see FIGURE 3-2) indicate the following status:

Locked–(lock image shown closed) Write-protected. The switch is to the right (toward the cartridge door) when the cartridge is positioned with the hub down and the label edge away from you.

> **Note –** The tape drive can only read data from the data cartridge. Write operation attempts will fail.

Unlocked–(lock image shown open) Write-enabled (unprotected). The switch is to the left (away from the cartridge door).

The tape drive can read data from or write data to the data cartridge.

FIGURE 3-2 Data Cartridge Write Protect/Enable Switch

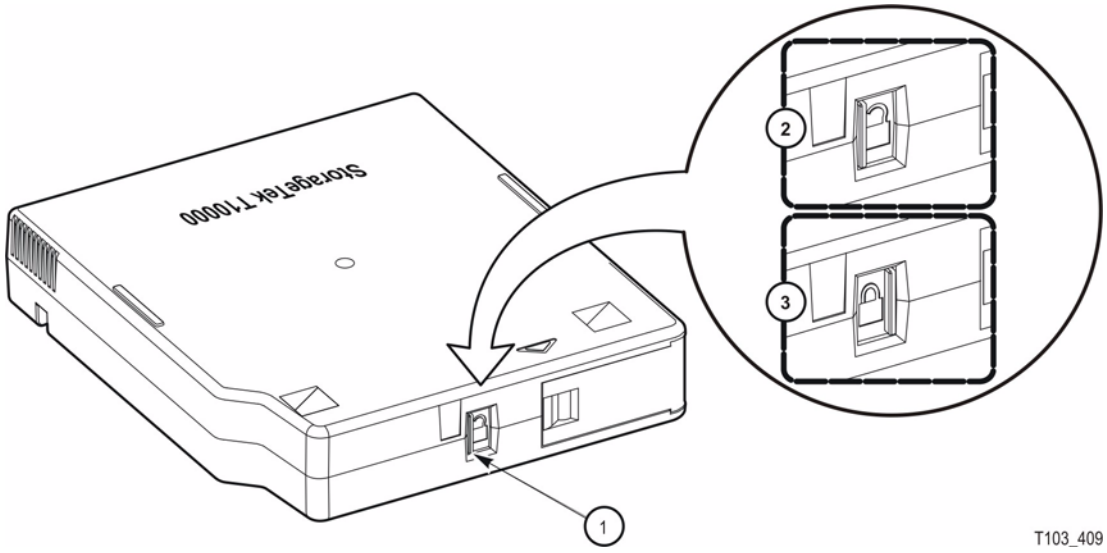


Illustration call-outs (3):
1. File protect switch
2. Unlocked position
3. Locked position

Cartridge Handling Precautions

Caution – *Tape data corruption:* Be certain that a data cartridge never comes close to strong electrical fields or any form of magnet or magnetic field.

Magnetic fields are present near disk drives and electric motors (the larger the electric motor, the stronger the magnetic field surrounding it in most cases). Items containing buzzers of any form produce alternating current electrical fields strong enough to partly erase a magnetic tape.

Caution – *Tape media damage:* You must keep cartridges dry.

Never store cartridges on a floor where moisture might be present or near air conditioners or air handlers. Air conditioners might leak water as a function of cooling the air, and air handlers might be adding moisture to the air as a function of controlling the environment in a computer room.

Caution – *Cartridge damage:* Avoid dropping or handling cartridges roughly.

There is a hub locking mechanism within the T10000 data cartridge, but it has limitations on just how much braking it provides. Rough handling of a data cartridge could cause the locking mechanism or brake to slip, resulting in a loose tape. Loose tapes are easily damaged by a tape drive.

To Identify a Defective Cartridge

- **Look for cartridge problems before you load a cartridge into a drive or library.**
  - Cracked or broken case (including the access door)
  - Dirty case
  - Missing, broken, or cracked leader

    Note – In most cases, your service representative can fix broken leaders.
  - Damaged write-protect switch
  - Liquid in the data cartridge case
  - Loose label
  - Other obvious damage

Also see "Dropped Cartridges" on page 89.

Manually Load or Unload Cartridges

Manual loading or unloading is commonly done on rack mounted drives. For a library failure, you might have to manually load or unload a data cartridge.

▼ To Load a Cartridge

Note – A T10000 tape drive accepts T10000 cartridges only.

To load a cartridge into a T10000 tape drive, do the following:

1. **Look into the drive load/unload slot to make sure there are no obstructions.**
2. **Make sure the cartridge write-protect switch is in the proper position.**

   Note – For any cartridge on which data is to be written, set the write-protect switch to the unlocked position (see FIGURE 3-2 on page 39).

3. **Hold the cartridge by the finger grips (FIGURE 1-7 on page 26) with the hub side down, and carefully insert the cartridge into the tape drive loading slot.**
4. **Push the cartridge all the way into the slot**

   Push on the label edge of the cartridge because there is not enough room for your fingers (finger grip recessions do not exist on the bezel of a library drive). You must overcome some resistance to fully seat the cartridge. When the cartridge is fully seated, the data cartridge is lowered onto the file reel motor hub assembly.

   Note – When manually loading a library-attached drive, make sure the library hold-off signal to the drive is disabled. Otherwise, the drive will not accept a manual load.

   Note – A T10000C drive automatically hibernates to save power after a period of inactivity. When hibernating, the drive cannot detect the presence of a cartridge. The library monitors whether a drive is hibernating and commands the drive to wake up whenever a mount is forthcoming.
   Hibernation poses a problem when a user opens the library door and attempts to manually mount a cartridge. With certain library code levels (for example SL8500 FRS_6.02 and SL3000 FRS_2.81), hibernating drives remain in the hibernation state and will neither detect nor load a cartridge that is manually inserted. To force the drive out of hibernation, you can either power cycle the drive or use VOP 1.0.17. The drive remains awake until after a mount/dismount sequence, but resumes it's auto-hibernation behavior after the cartridge has been extracted.

5. **Observe that for rack mounted tape drives, when a cartridge is loaded, the operator panel display window indicates one of the following:**

   Ready A when the tape is ready and is a VolSafe cartridge

   Ready F when the tape is ready and file protected

   Ready H when a higher density, non-VolSafe cartridge is ready and *not* file-protected in a lower density tape drive

   Ready L when a lower density, non-VolSafe cartridge is ready and *not* file-protected in a higher density tape drive

   Ready U when the tape is ready and *not* file protected

   Note – If a cartridge fails to load, remove it, open the cartridge access door, and see if the leader is either missing entirely or cracked near the opening at the end.

▼ To Unload a Cartridge

Use the following procedure to remove a cartridge from the drive.

1. **Make sure the tape drive is not in use.**

   This is done by checking the following:

   a. There are no active jobs, applications, or programs using this drive.

   b. The rack mount operator panel activity indicator is steady and *not* flashing.

   c. The display window (VOP or operator panel) does not indicate any activity relative to tape movement (such as reading, writing, or locating).

      Caution – *Possible data loss:* Do not push the Unload button while a data cartridge is in use.

2. **Unload the tape drive.**

   Rack mounted tape drive:

   - **Press the operator panel Unload button and wait for the drive to raise the cartridge to the unload position.**

     The display should show an asterisk (*) when the operation is complete.

     Note – If the drive is offline, the asterisk will alternate with `Offline`.

   VOP unload:

   - **Choose Unload Tape from the Drive Operations menu or use the SHIFT + U shortcut keys.**

     Caution – *Tape damage:* Any resistance to removing the cartridge, beyond the usual friction between the cartridge case and the drive, might indicate that the leader is not fully rewound. If you believe the leader is not fully rewound, use the operator panel (rack-mount drives only), VOP, or library software (if it supports that function) to attempt another load operation followed by another unload operation. Should that fail to correct the situation, contact your service representative about a possible stuck cartridge.
     DO NOT forcibly remove a cartridge.

3. **Remove the cartridge.**

     Note – A T10000 tape drive does not eject the cartridge from the tape drive as is commonly done by other cartridge tape drives.

   Rack mount drives:

   - **Use the finger grips on the cartridge (see FIGURE 1-7 on page 26) and carefully withdraw the cartridge from the drive slot.**

   Library-attached drives:

   - **Grasp the top and bottom of the cartridge with your finger tips and carefully withdraw the cartridge from the drive slot.**

T10000 Tape Drive Cleaning

Caution – *Equipment damage:* Do not wet-clean the tape drive. Do not clean the tape drive unless the Clean indicator lights.

After the tape drive transports a predetermined length of tape or records a predetermined number of errors, the Clean indicator lights. The tape-to-head contact values are:

- T10000A tape drive = 1,000,000 meters
- T10000B tape drive = 300,000 meters
- T10000C tape drive = 10,000,000 meters

▼ To Clean the T10000 Tape Drive

Note – You can use the cleaning cartridge approximately 50 times before discarding it. (See "Cleaning Cartridges" on page 28.)

1. **Make sure the tape drive is not in use.**

   Note – If there is a tape loaded in the tape drive, make sure the application or job that was using that tape drive is no longer running before proceeding to Step 2.

2. **Unload any data cartridge in the tape drive. See "To Unload a Cartridge" on page 42 if a data cartridge is loaded in the tape drive.**

3. **Insert a cleaning cartridge in the tape drive.**

   When loaded, the activity light flashes. The activity and clean indicators turn off when cleaning is completed, and the tape drive unloads the cleaning cartridge.

   Note – If the tape drive immediately ejects the cleaning cartridge and the message `Exp ClCart` appears in the tape drive's front panel display screen (a similar message is displayed on the VOP if that program is being used to monitor the tape drive) to indicate the cleaning cartridge has been used to its maximum number of cleaning cycles. Discard the worn cleaning cartridge and insert a new cleaning cartridge into the tape drive.

   TIP – If the message `CHK xxxx` appears in the tape drive's front panel, where xxxx is the FSC, a cleaning cartridge failure occurred. Try the procedure again with a different cleaning cartridge. If the problem persists, contact your service representative.

   Caution – *Tape damage*: Any resistance to removing the tape cleaning cartridge, beyond the usual friction between the tape cleaning cartridge case and the tape drive, probably indicates that the leader is not fully rewound.
   If you believe the clean tape leader is not fully rewound, attempt another load operation by pushing the tape back into the tape drive and then use the tape drive's front panel **Unload** button to attempt another unload operation. Should that fail to correct the situation, contact your service representative about a possible stuck tape cleaning cartridge.
   Do not forcibly remove a tape cleaning cartridge.

4. **Remove the cleaning cartridge from the tape drive.**

This completes the cleaning process and the tape drive is ready to resume normal operations.

Initial Program Load (IPL)

One of the recommended actions listed in Appendix D, "Messages and Translated Messages" is to perform a forced IPL.

When the IPL starts, the following things happen:

- The drive power indicator flashes.
- Various IPL sequence messages appear in the operator panel display window. These messages require no action on your part.

After the drive successfully completes an IPL:

- The drive power indicator is steady.
- An asterisk (*) appears in the operator panel display window.

> **Note –** If there is a dump present, the operator panel display window alternates between the asterisk and the dump message. The dump present indication will stop when you load a tape cartridge.

You can IPL the drive with a physical switch on the operator panel or with a menu command in the VOP.

▼ To IPL the Drive from the Operator Panel

> **Note –** The rack mount drive must be powered-on.

1. **Make sure there is not a job or application running on the host that is using this tape drive. If there is, stop that job or application.**
2. **Make sure a data cartridge is *not* loaded.**
3. **Press the operator panel IPL button (see FIGURE 2-2 on page 34).**

▼ To IPL the Drive Using VOP

To IPL the drive using the VOP program (see FIGURE 1-4 on page 24):

1. **Make sure there is not a job or application running on the host that is using this tape drive. If there is, stop that job or application.**
2. **Make sure a data cartridge is *not* loaded.**
3. **Make sure the drive is `offline` (click the Online button, if the drive is not offline).**

   The Online button turns grey to indicate that the drive is offline.

   > **Note –** You can set the drive offline by selecting the Set Offline command from the Drive Operations menu.

4. **Choose `IPL` from the Drive Operations menu to start the `IPL` process.**

Menu System Tasks

You can perform the following tasks from the menu system:

- Place the drive online
- View the drive configuration settings
- Place the drive offline
- Rebuild the MIR
- Change the drive configuration settings

▼ To Place the Drive Online (Operator Panel)

> **Note –** In a multi-host open systems setting, if there is a switch unit and it has a port blocked to this tape drive, unblock that port before proceeding.

To change the tape drive state from offline to online:

1. **Press the operator panel** Menu **button until** `Offline` **appears in the display window.**

   > **Note –** If you are within a submenu, press the Menu button until `Exit XXX ?` appears in the display window and press the Select button to enter the main menu.

2. **Press the operator panel** Select **button to toggle the drive state.**

   `Online` appears in the display window, indicating the drive state is now online.

3. **Press the** Menu **button until** `Exit Menu?` **appears in the display window.**
4. **Press the** Select **button to exit the menu system.**
5. **Bring the tape drive back online to the host by using one of the following methods:**

   - **Enterprise:** Set the tape drive online for all host paths to the tape drive by using one of the following Vary commands:

     ```
     MVS: V <address> online

     VM: Vary on, <address>
     ```

   - **Open Systems:** if there is a switch unit installed and the port to this tape drive is blocked, unblock that port.

▼ To Place the Drive Online (VOP)

> **Note –** In a multi-host open systems setting, if there is a switch unit and it has a port blocked to this tape drive, unblock that port before proceeding.

On the VOP screen, there are two methods to place the drive offline:

Use the menu bar:

1. **Open the Drive Operations menu (click Drive Operations in the menu bar or use the ALT + D shortcut keys).**
2. **Choose the Set Online command or use the** SHIFT + O **shortcut keys.**

   The second drive status indicator/button changes to blue when the tape drive is online.

Use the status indicator:

If the tape drive is offline, the **button** next to the word `Online` is grey.

- **Click the button to change the state to *Online*.**

  The button color changes to blue when the tape drive is online.

▼ To View the Configuration (Operator Panel)

> **Note –** See Chapter 4, "Menu System" for compete information and guidelines.

1. **Press the operator panel** Menu **button to enter the menu system:**
   - If `Online` appears in the tape drive's front panel display, go to Step 2.
   - If `Offline` appears, press the Select button to toggle the drive state (see "To Place the Drive Online (Operator Panel)" on page 45).

     > **Note –** It is important that you view configuration settings in the online state, because you cannot accidently change settings in this drive state. To change settings, you must first set the drive to the offline state (see "To Place the Drive Offline (Operator Panel)" on page 47).
2. **Press the** Menu **button until** `View CFG ?` **appears in the window display**
3. **Press the operator panel** Select **button (Yes) to enter view configuration submenus.**

   The first configuration setting appears in the operator panel display window.
4. **Press either the** Menu **or the** Select **button to step through the configuration settings.**

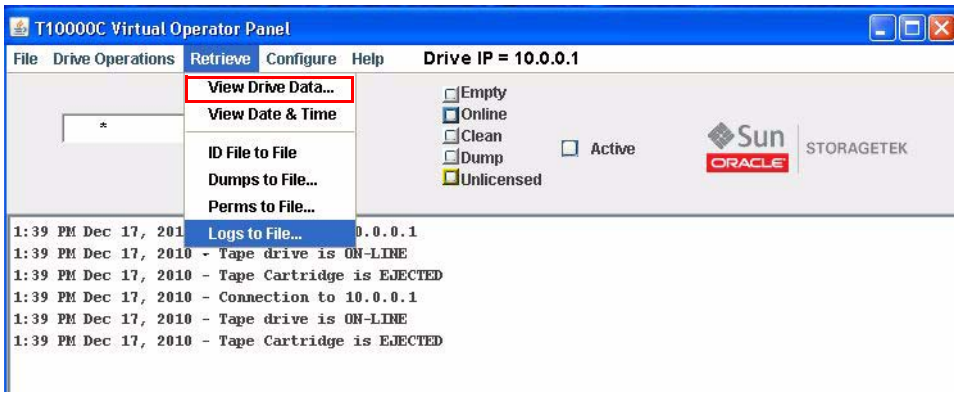
   > **Note –** In the drive online state, the Select button has the same function as the Menu button, except when answering a displayed question.
5. **Press either the** Menu **or** Select **button until** `Exit CFG ?` **appears in the display window.**
6. **Press the** Select **button (Yes) to exit the configuration submenus, or press the** Menu **button (No) to repeat the view configuration sequence.**
7. **Press the** Menu **button until** `Exit Menu?` **appears in the display window.**
8. **Press either the** Select **button (Yes) to exit the menu system or the** Menu **button (No) to return to the online/offline selection menu.**

▼ To View the Configuration (VOP)

Note – The drive must be in the online state.

1. **Choose Retrieve from the menu bar or use the ALT + R shortcut keys to open the menu.**
2. **Choose View Drive Data or use the SHIFT + V shortcut keys to access the View Current Drive Settings property sheet.**

FIGURE 3-3 VOP Retrieve Menu Commands



A new window appears that contains several property sheets (tabs), such as: Encrypt, Fibre, Keyid, Manufacturing, Missing, Network, Rfid, and Version.

Note – See the *Virtual Operator Panel Customer User's Guide* for complete VOP information and instructions.

▼ To Place the Drive Offline (Operator Panel)

1. **Stop all I/O activity from the host.**

   In mainframe environments, set the tape drive offline for all host paths to the tape drive by using one of the following Vary commands:

   - **MVS:** V <address> offline
   - **VM:** Vary off, <address>

   In open systems environments, do one of the following:

   - Stop the job that is using the tape drive
   - In a multi-host setting, stop any job that is using the tape drive and then, if there is a switch unit in use, block the port in that switch to the tape drive.

2. **Press the operator panel** Menu **button.**

   `Online` appears in the display window, indicating the current state of the drive.

3. **Press the operator panel** Select **button to toggle the drive state.**

   `Offline` appears in the display window, indicating a successful transition to the offline state.

4. **Press the** Menu **button until** `Exit Menu?` **appears in the display window.**
5. **Press the** Select **button to exit the menu system.**

> **Note –** If you select Exit Menu?, the display alternates between Offline and the normal message after a cartridge is loaded as a reminder that the drive is still in the offline state.

▼ To Place the Tape Drive Offline (VOP)

1. **Cease all I/O activity from the host.**

   In mainframe environments, set the tape drive offline for all host paths to the tape drive by using one of the following Vary commands:

   - **MVS:** V <address> offline
   - **VM:** Vary off, <address>

   In open systems environments, do one of the following:

   - Stop the job that is using that tape drive
   - In a multi-host setting, stop any job that is using the tape drive and then, if there is a switch unit in use, block the port in that switch to the tape drive.

2. **Click the VOP Online button.**

   If the tape drive is online, the button is blue. You can click the blue button to change the button to grey, indicating that the tape drive is offline.

> **Note –** You can also set the drive offline from the File drop-down menu by selecting Set Offline from the Drive Operations menu.

Rebuilding an MIR

This section discusses the rebuilding of the MIR. This is an abnormal situation as the tape drive automatically builds and changes the MIR as the tape is used. The rebuild process is only used in the event that the MIR on a tape becomes damaged or corrupted.

> **Note –** Make sure the write protect switch on the data cartridge is set to the *unlocked* position.

▼ To Rebuild the MIR (Operator Panel)

> **Note –** This process rebuilds an MIR from the rack mount drive tray operator panel.

1. **Set the drive to the offline state.**

   (see"To Place the Drive Offline (Operator Panel)" on page 47, if required)

2. **Press the** Menu **button until** `Drv Menu?` **appears in the display window.**
3. **Press the** Select **button (Yes) once.**

   The display window now shows the beginning of drive utilities submenus.

4. **Press the** Menu **button until** `Build MIR` **appears.**

5. **Press the** Select **button to begin the MIR rebuilding process.**

   `Ld Cust Tp` appears in the display window.

   > **Note –** Any loaded cartridge unloads at this time. Remove the cartridge.

6. **Insert a write-enabled cartridge with a defective MIR.**

   (see "To Load a Cartridge" on page 40, if required)

   > **Note –** Rebuilding an MIR could take 90 minutes (T10000A formatted cartridge) or longer for a full data cartridge. When the rebuild is complete, the cartridge unloads.

   > **Caution –** *Tape damage:* Any resistance to removing the cartridge, beyond the usual friction between the data cartridge case and the tape drive, probably indicates that the leader is not fully rewound. If you believe the leader is not fully rewound, attempt another load operation by pushing the cartridge back into the tape drive. If it loads properly, use the tape operator panel Unload button to attempt an unload operation. Should that fail to correct the situation, contact your service representative about a possible stuck cartridge. **Do not forcibly remove a cartridge.**

7. **Remove the cartridge from the drive load/unload slot.**

   If there are other cartridges for MIR rebuilding, repeat Step 6 and Step 7 for each cartridge. When all cartridges with defective MIRs have been rebuilt, continue with Step 8.

8. **Press the** Menu **button once.**

   `Exit Drv?` appears in the display window.

9. **Press the** Select **button (Yes) to exit the drive utilities submenus, or press the** Menu **button (No) to repeat the utilities submenu sequence.**

10. **Return the drive to an online state**

    (see "To Place the Drive Online (Operator Panel)" on page 45, if required)

▼ To Rebuild the MIR (VOP)

> **Note –** This can be a lengthy process, especially on a fully written cartridge.

1. **Make sure the tape drive is in the offline state.**

   If the display shows Online, click Drive Operations and choose Set Offline. This sets the tape drive to the `Offline` state.

2. **Choose Format Tape from the Drive Operations menu, and choose Rebuild MIR in the dialog box.**

   > **Note –** You can abort this function before you load a cartridge by clicking the **Abort** button in the Format Tape dialog box.

3. **Follow the on-screen prompts and directions.**

Note – After a successful MIR rebuild, the cartridge automatically unloads.

If more than one tape has a defective MIR, load the next cartridge into the tape drive when the VOP screen displays the prompt to load a customer cartridge. This process continues until all defective MIRs have been rebuilt.

If an MIR rebuild fails:

- The message part of the VOP screen contains a failed message and an FSC.
- The tape drive does *not* automatically eject the cartridge.
- Attempt another rebuild of the MIR before declaring that the MIR part of the tape in that cartridge is defective. Click **Drive Operations** and choose **Unload Tape** and after the cartridge unloads, gently push it back into the tape drive until it lowers onto the hub assembly to reload it.

  Caution – *Tape damage*: Any resistance to removing the data cartridge, beyond the usual friction between the data cartridge case and the tape drive, might indicate that the leader is not fully rewound. If you believe the leader is not fully rewound:
  1. Attempt another load operation (click **Drive Operations** and choose **Load**).
  2. Follow with another unload operation (click **Drive Operations** and choose **Unload**).
  If a load and unload operation fails to correct the situation, contact a service representative about a possible stuck data cartridge. **Do not forcibly remove a data cartridge.**

  Attempt another build of the data cartridge before deciding that the data cartridge is defective. To do this:

  1. Click **Drive Operations** and choose **Unload**.
  2. After the data cartridge unloads, gently push it back into the tape drive until it lowers onto the hub assembly to reload it.

4. **After you have repaired all cartridges with defective MIRs, click the Done button on the format selection submenu.**
5. **Click Drive Operations and choose Set Online.**

This completes the rebuild of the MIR on one or more cartridges. The tape drive is now back online and ready for normal operations.

Change the Drive Configuration

You can change drive configuration parameter values using the drive menu system or the Configure menu of VOP. Note that some configuration parameters must be changed with VOP as there is not an equivalent menu item.

Note – The drive must be offline to change most configuration parameter values and typically requires an IPL to invoke a change.

Data Path Key Management Procedures

You must use VOP to perform the data path key management (DPKM) procedures.

▼ To View Current Drive Settings - Encrypt Tab (DPKM)

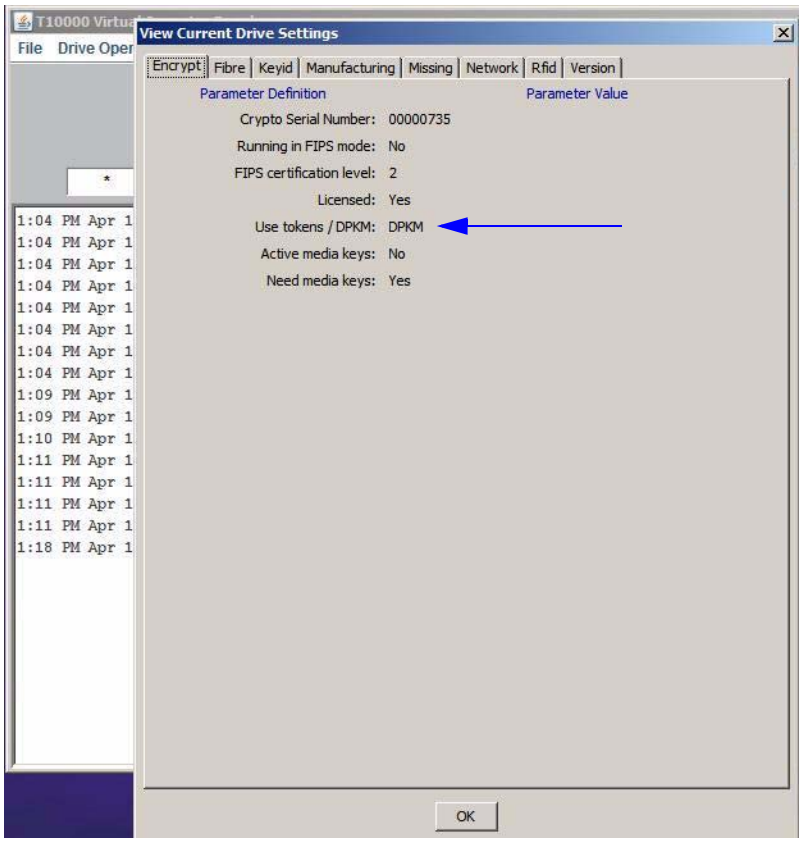
To view the current drive encryption settings:

1. **Choose View Drive Data from the Retrieve menu, and click the Encrypt tab.**

   Note – The Use tokens/DPKM parameter value is DPKM as identified by the arrow in the figure below.

2. **Click the OK button to return to the main VOP window.**

FIGURE 3-4 VOP Drive Data Encrypt Tab



▼ To Turn DPKM On

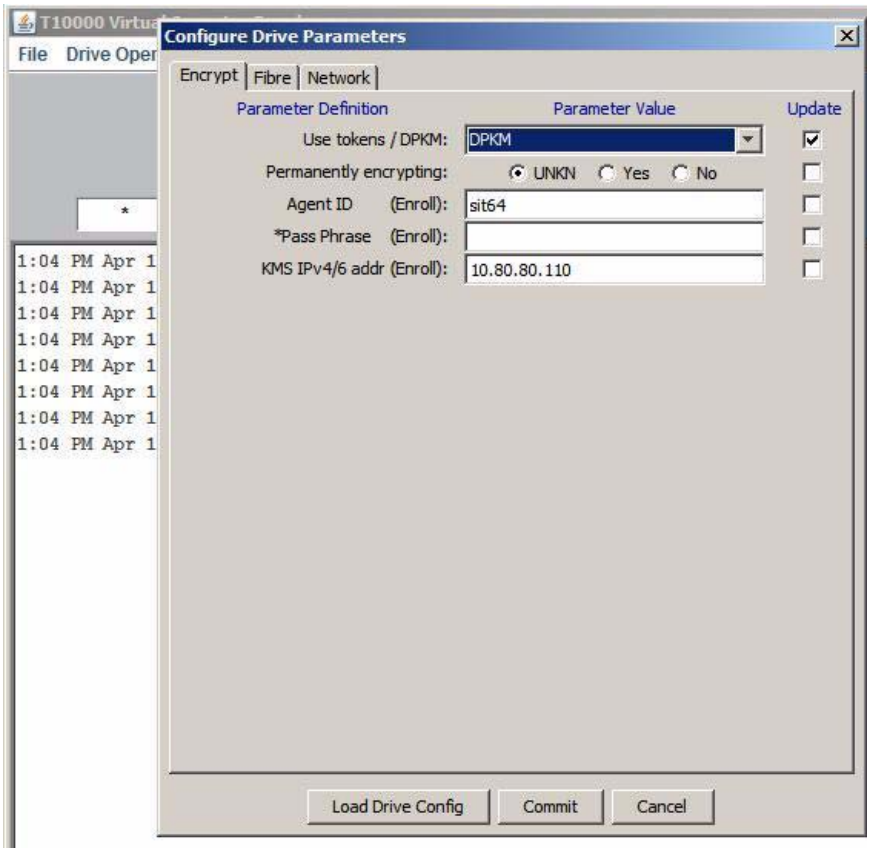
1. **Set the drive offline.**
2. **Choose Drive Data from the Configure menu.**
3. **Select the Encrypt tab from the Configure Drive Parameters property sheet.**
4. **Select the DPKM value for the *Use tokens/DPKM* parameter.**

   Note – A check mark appears in the Update box adjacent to the parameter.

5. **Click the** Commit **button at the bottom of the window.**

   Note – The drive performs an initial program load (IPL).

FIGURE 3-5 Turn DPKM On



▼ To Turn DPKM Off

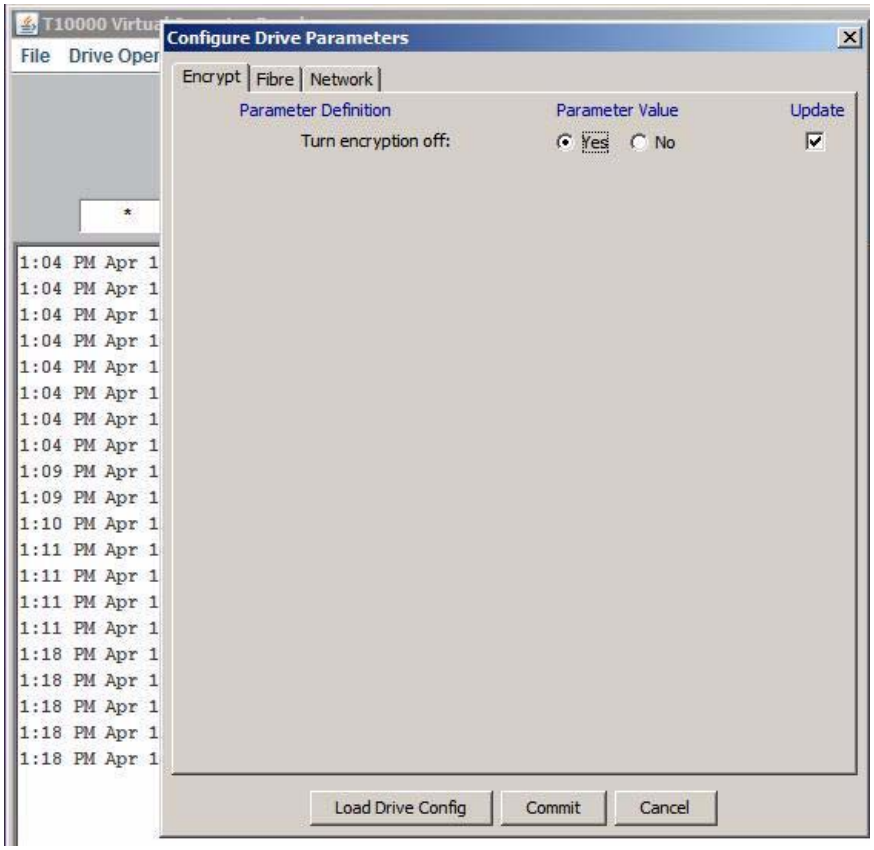
1. **Set the drive offline.**
2. **Choose Drive Data from the Configure menu.**
3. **Select the Encrypt tab from the Configure Drive Parameters property sheet.**
4. **Click the *Yes* option for the** Turn encryption off **parameter.**

   Note – A check mark appears in the Update box adjacent to the parameter.

5. **Click the** Commit **button at the bottom of the window.**

   Note – The drive performs an initial program load (IPL).

FIGURE 3-6 Turn DPKM Off



4

Menu System

This chapter provides information for using the T10000 menu system with the virtual operator panel (VOP) application or the physical operator panel of a rack mount drive. VOP provides a graphical user interface (GUI) representation of the drive menu system.

> **Note –** See the *Virtual Operator's Panel Operator's Guide* for information regarding VOP and guidelines for operation.

Menu System Overview

The T10000 tape drive menu system provides the operator and service representative a means to determine the drive configuration settings and access the drive utilities. The rack mount drive chassis has a physical operator panel on the front panel (see FIGURE 2-2 on page 34) that enables direct access to the menu system, as an alternative to using VOP. On library-attached drives, the primary means of connection is through the drive's Ethernet maintenance port and the use of the virtual operator panel (VOP) application.

> **Note –** Service representatives can also use the PC-based StorageTek Diagnostic System (STDS) application to navigate through the T10000 tape drive menu system. Use version 1.55 (or higher) with a T10000A or version 1.57 (or higher) with Oracle's StorageTek T10000B tape drive.

The menu system information is provided in the following order:

1. "Menu Structure Overview" on page 56
2. "Menu Operations" on page 57
3. "View/Change Configuration Settings" on page 60
4. "View/Change TCP/IP Settings" on page 75
5. "Drive Operations Menu" on page 81.

The information describes the menu system as seen through the physical operator panel and the STDS application.

> **Note –** Although the VOP GUI representation is visually very different from the operator panel view, the information is still quite useful for VOP.

Menu Structure Overview

The T10000 main menu system is very similar to the T9x40 menu system.

When you press the Menu switch on the operator panel, the first menu provides selection of Online (default) or Offline menus. Press the Select switch to toggle between online mode and offline mode as desired, then press the Menu switch to advance to the next menu.

View/Change Configuration menus display drive configuration settings (view only) when online, or allow drive configuration changes when offline. Press Menu to advance the display to the next menu. Press Select to enter submenus.

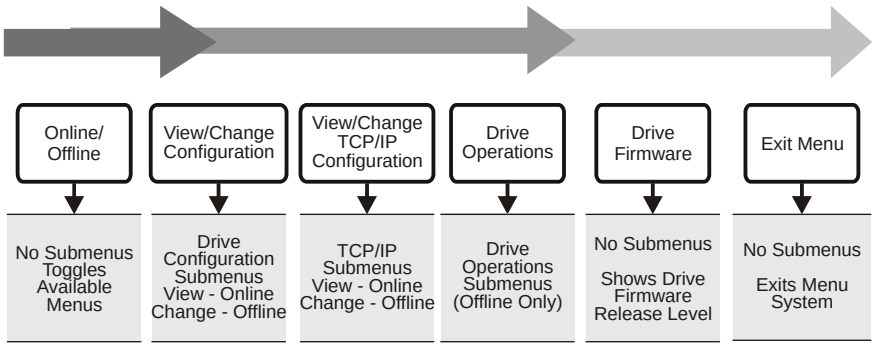
View/Change TCP Configuration menus display the drive Transmission Control Protocol /Internet Protocol (TCP/IP) configuration settings (view only) when online, or allow TCP/IP configuration changes when offline. Press Menu to advances the display to the next menu. Press Select to enter submenus.

Drive Operations menus (offline only) provide drive utilities. Press Menu to advances the display to the next menu. Press Select to enter submenus.

The Drive Firmware menu displays (view only) the current drive firmware release level.

The Exit Menu allows you the choice to loop-back to the Online/Offline selection menu by pressing Menu (No), or to exit the menu system by pressing Select (Yes).

FIGURE 4-1 Main Menu System



Menu Operations

Menu operations for online (View) mode and offline (Change) mode are very similar. Online menus only provide viewing of current settings and/or status. Offline menus allow option selections and/or change to various settings. In both menu systems, press Menu to advance, or to answer No; press Select to scroll options, or to answer Yes.

Online Menu Operation

When the drive is Online, the menus below are available. Press Menu to advance to the View Configuration menu.

Note – At each main menu you have two choices:

- Press Menu (No) to bypass, and advance to the next menu.
- Press Select (Yes) to enter the submenus.

The View Configuration submenus allow you to view current drive configuration settings. See TABLE 4-1 on page 63 for additional information.

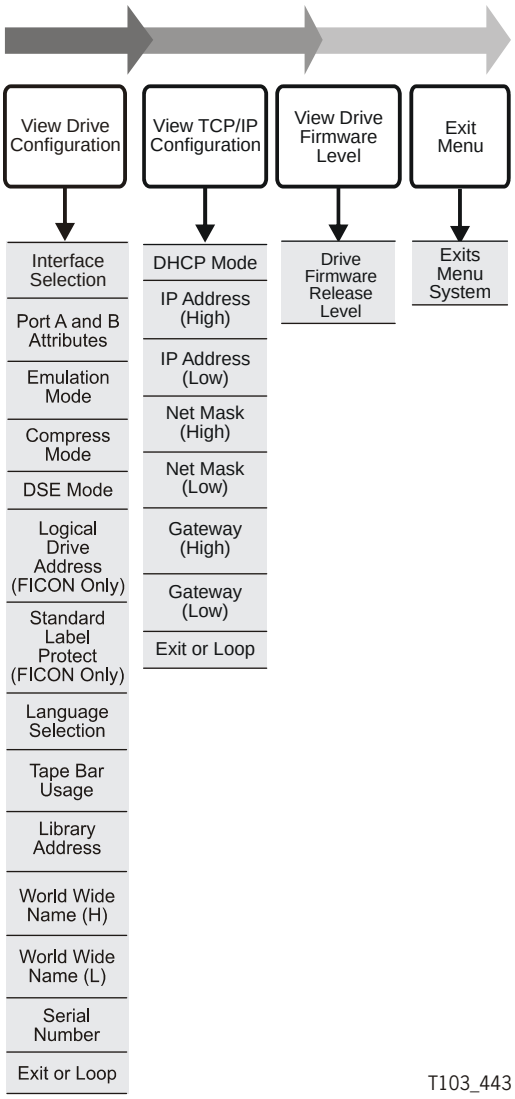
The View TCP Configuration submenus allow you to view current TCP/IP settings. (See TABLE 4-2 on page 76 for additional information.)

The view-only Drive Firmware Level menu displays the drive's current firmware release level in `Rx.yy.zzzc` format, where:

- `x` = major revision level,
- `y` = minor revision level,
- `z` = integration number,
- `c` = channel interface type: for FC.

The Exit Menu option allows you the choice to either return to the Online/Offline selection menu by pressing Menu (No) or to exit the menu system by pressing Select (Yes).

FIGURE 4-2 Online Menus



Offline Menu Operation

When the drive is offline, the menus shown below are active. Press Menu (one or more times) to advance to the Change Configuration menu.

Note – At each main menu you have two choices:

- Press Menu (No) to bypass, and advance to the next menu.
- Press Select (Yes) to enter the submenus.

The Change Configuration submenus allow you to change drive configuration settings. See TABLE 4-1 on page 63 for additional information.

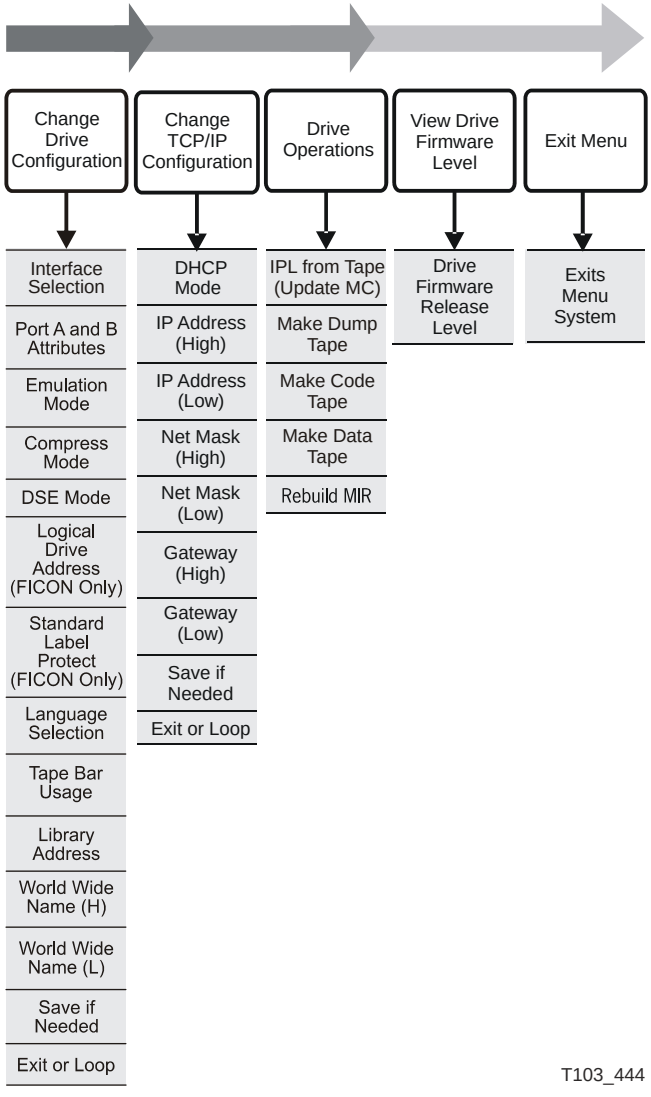
The Change TCP Configuration submenus allow you to enable/disable Dynamic Host Control Protocol (DHCP), set a static IP address, set a static Network Mask (NM), and/or set a static net Gateway. See TABLE 4-2 on page 76 for additional information.

The Drive Operations submenus allow you to perform various drive utilities. See TABLE 4-3 on page 82 for additional information.

The view-only Drive Firmware Level Menu displays the current drive firmware release level, same as the Online Main Menu Operation.

The Exit Menu allows you the choice to either loop-back to the Online/Offline selection menu by pressing Menu (No) or to exit the menu system by pressing Select (Yes).

FIGURE 4-3 Offline Menus



Note – If you exit the menu system with the drive offline, the Operator Panel alternately flashes `Offline` (if a data cartridge has been loaded at least once) as a reminder that drive status is still offline. This reminder flashes until the drive is either placed back online or powered-off.

View/Change Configuration Settings

You can view (only) current configuration settings when the drive is online; or, you can view or change configuration settings when the drive is offline. Use the menu trees for quick reference road maps, or the drive configuration table (TABLE 4-1 on page 63) for more detailed instructions.

Explanation of the Trees

Press Menu to advance the menu display, to set a menu option after selection, or to answer *No* to a menu choice question.

Press Select to toggle/increment menu options, or to answer *Yes* to a menu choice question.

Note – When no option, selection, or choice is presented, such as during view-only menus, pressing Select has the same result as pressing Menu.

To enter variable characters or digits, press Select to start the change mode. (The left-most segment of the ten-character display begins to flash.)

Note – Each additional press of the Select switch increments the value one step.

When the desired value appears, press Menu to set the value and advance the flashing display to the next variable character/digit.

After you have set the last variable character/digit, either press Menu to accept the displayed entry and advance to the next menu or press Select to restart the change mode.

Online Configuration Menu Tree

Use the online view configuration menu tree as a brief guide. See TABLE 4-1 on page 63 for details. If you want to change any settings, you must place the drive offline.

Online/Offline Press Select to toggle, then press Menu to set.

View CFG ? (View Configuration) Press Select to enter, press Menu to bypass.

Intf FCP/FICON (displays active interface)

View PrtA? (view current port attributes)

A= . . . . . . (24-bit address identifier, when logged on to an interface system)
B= . . . . . . (when viewing port B)

SFP module parameters (i.e. **4G MM0150m**)

Hard PA . (Physical Address) Y/N

PA=xx,ddd (PA=hex, decimal index) (only when Hard PA is yes)

Soft PA . . HI/LO (only when Hard PA is no)

Rate . . . . (Auto/fixed rate - 4Gb, 2Gb, 1Gb) (interface speed negotiation)

MaxSz . . . . (2112/2048) (maximum data frame size)

H= . . . . . . (first half, 64-bit port node world-wide-name)

L= . . . . . . (second half, 64-bit port node world-wide-name)

WWN Custom (only when custom or dynamic WWN is set)

View PrtB? (current port B attributes) (same sub-menus as port A)

Emulation Mode: (displays current emulation, based on the active interface)

FCP: **Emul STD/*** (standard/*/*/3592/*)
(*=special modes, used only when directed by Engineering/Tech Support)

FICON: **Emul VSM/3592** (selected to match site requirements)

Cmprss . . . (Yes/Off/No) (compression mode)

Full DSE . (Y/N) (data security erase mode)

Drv Adr xy (2-character hexadecimal logical drive address) (FICON only)

SL Prot . (Y/N) (standard label protection mode)

English/Espanol/Francais/Italiano/Deutsch (current language)

Tape Bar . (Y/N) (tape completion indication)

Lib Adr xy (2-character hexadecimal library address)

H= . . . . . . (first half, 64-bit drive node world-wide-name)

L= . . . . . . (second half, 64-bit drive node world-wide-name)

WWN Custom (only when custom/dynamic WWN is set)

S/N= . . . . . . (drive serial number) (last six-characters of drive DMOD)

Exit CFG ? (exit view configuration)

View TCP ? (see "View/Change TCP/IP Settings" on page 75)

Rx.yy.zzza (current drive firmware release level)

Exit Menu ?

Offline Configuration Menu Tree

Use the menu tree for brief guidelines. See TABLE 4-1 on page 63 for details.

Note – Make sure the host has varied the drive offline before setting the drive offline.

Online/Offline
Press Select to toggle, then press Menu to set.

Chng CFG ? (Change Configuration)
Press Select to enter, press Menu to bypass.

Intf FCP/FICON (active interface displayed,
alternate selection initiates a drive IPL to activate alternate interface)

Cfg Port A ? (change port A attributes)

SFP module parameters (i.e. **4G MM0150m**) [display only, no change]

Hard PA . (Y/N)

PA=xx,ddd (Hard PA Y only) (change decimal index, PA hex auto-changes)

Soft PA .. HI/LO (Hard PA N only)

Rate .... (Auto/fixed rate - 4Gb, 2Gb, 1Gb) [interface speed negotiation]

MaxSz .... (2112/2048) (maximum data frame size)

H= ..... (first half, 64-bit port node world-wide-name)

L= ..... (second half, 64-bit port node world-wide-name)

WWN Custom (only when custom or dynamic WWN is set or changed,
Select toggles to Normal, which recalls factory preset WWN)

Cfg Port B ? (change port B attributes) (same sub-menus as port A)

Emulation Mode: (displays current emulation)

FCP: **Emul STD/3592/*** (standard/*/*/3592/*)
(*=special modes, select only when directed by company technical support)
FICON: **Emul VSM/3592** (select to match site requirements)

Cmprss ... (Yes/Off/No) (compression mode)

Full DSE . (Y/N) (data security erase mode)

Drv Adr xy (2-character hexadecimal logical drive address) (FICON only)

SL Prot . (Y/N) (standard label protection mode)

Language ? (scrolls through options, beginning with current) (English/Espanol/Francais/Italiano/Deutsch)

Tape Bar . (Y/N) (tape completion indication)

Lib Adr xy (2-character hexadecimal library address)

H= . . . . . . (first half, 64-bit drive node world-wide-name)

L= . . . . . . (second half, 64-bit drive node world-wide-name)

WWN Custom (only when custom/dynamic WWN is set or changed, **Select** toggles to Normal, which recalls factory preset WWN)

S/N= . . . . . . ((display only)) (last six-characters of drive DMOD)

Save/IPL ? (if there are pending changes)

Exit CFG ? (no, restarts change configuration mode)

Chng TCP ? (see "View/Change TCP/IP Settings" on page 75)

Drv Menu ? (see "Drive Operations Menu" on page 81)

Rx.yy.zzza (current drive firmware release level) (display only)

Exit Menu ?

TABLE 4-1 provides drive configuration setting details and guidelines for changing selected settings when the drive is offline.

TABLE 4-1 Drive Configuration Settings

Options	Notes	Procedure
Online/Offline Menu		
`Online`/ `Offline`	Defaults to Online at power-on. You must select Offline to change a configuration setting. `OffLn Pend` might appear while waiting for a system response or diagnostics completion.	1. **Press** Menu **repeatedly until** `Online` **or** `Offline` **appears, if required.** 2. **Press** Select **to change modes.** 3. **Press** Menu **to advance to the next menu.**
View/Change Configuration Menu		
`View CFG ?` **(**`online`**)** `Chng CFG ?` **(**`offline`**)**	If bypassed, the display advances to the View/Change TCP/IP Configuration Menu. This is the entry point to the configuration submenus.	• **Do one of the following:** • **Press Menu (No) to bypass.** • **Press Select (Yes) to enter submenus.**

TABLE 4-1 Drive Configuration Settings (Continued)

Options	Notes	Procedure
Interface Select Submenu		

`Intf FCP`
 	
`Intf FICON`
	Defaults to the last saved selection.
	
	Enables the drive interface to run FCP protocol.
	
	Enables the drive interface to run FICON protocol
	
	In the online (View) mode, only the current interface selection appears. You must switch to the offline (Change) mode to toggle the selection.
		• **Do one of the following:**
		• **Press Menu to bypass.**
		• **Press Select (offline) to toggle; then, press Menu to set, and initiate an IPL to load the alternate firmware modules.**

Note – Manufacturing ships drive FRUs with the `Intf FCP` option selected. When a defective drive in a FICON interface is replaced, the selection must be changed to `Intf FICON`. After IPL is complete, the menu system displays appropriate FICON related items. Do not select Intf FICON with code level 1.38.207.		
Port A Attributes Menu		
`View PrtA ?` **(**`online`**)** `Cfg PrtA ?` (`offline`)	View/configure port attributes as defined in the following submenus.	• **Do one of the following:** • **Press Menu (No) to bypass.** • **Press Select (Yes) to enter submenus.**
Port A/B 24-Bit Address Identifier Submenu		

`A=xxyyzzan`
`B=xxyyzzan`
`(online only)`
 	
`A=........`
`B=........`
appears when the port is not logged onto an interface
	24-bit (6 hexidecimal characters) port identifier at interface log on, plus connection type and speed.
	
	xx = domain (00 priv. loop or p-t-p)
	yy = area (00 in priv. loop or p-t-p)
	zz = 00 - EF (per connection type)
	a = connection type:
	f: fabric
	n: point-to-point
	0: public loop
	v: private loop
	n = connection speed: 1, 2, or 4 (Gb)
		Press Menu or Select to advance to the next submenu.

TABLE 4-1 Drive Configuration Settings (Continued)

Options	Notes	Procedure
Port A/B SFP Module Parameter Submenu		
`nG MM0nnnm` **or** `nG SMnn.nk`	Shows the Small Form-factor Pluggable (SFP) module information. Appears when an SFP module is present and readable: *n*G = max. Gigabit speed (2 - 4) MM - Multimode, (short wave) SM - Single Mode, (long wave) *nnn*m = maximum distance, meters (m) (short wave) *nn.n*k = maximum distance, kilometers (k) (long wave) **Note –** Display is information only, and appears in both online and offline menus.	Press Menu or Select to advance to the next submenu.
`?G ??`	Appears when an SFP module is present but unreadable.	
`No SFP`	Appears when an SFP module is not present in the port.	
Port A/B Hard Physical Addressing Submenu		
`Hard PA N` `Hard PA Y`	Defaults to the last saved selection. Disables hard physical address (PA), and causes the drive to seek a soft PA assignment at loop initialization. Enables a hard PA, manually set by the Hard Physical Address Submenu. If the preset hard PA is not available at loop initialization, the drive then seeks a soft PA.	• **Do one of the following:** • **Press Menu (No) to bypass.** • **Press Select (Yes) to enter submenus.**
Note – Manufacturing ships drives with the `Hard PA N` option selected.		

TABLE 4-1 Drive Configuration Settings (Continued)

Options	Notes	Procedure
Port A/B Hard Physical Address Submenu		
`PA=xx,ddd`	Defaults to the last saved selection. *xx* (hex) is the Arbitrated Loop Physical Address (AL_PA). **ddd** is the decimal index into the ALPA table. Appears only with `Hard PA Y` As you manually change the decimal index digits (valid indexes are 125 [highest priority] through 000 [lowest priority]), the PA hex display automatically changes. **Note –** The SL3000 and SL8500 libraries do not support AL_PA addressing.	**1. Do one of the following:** • **Press Menu to bypass.** • **Press Select to start the change mode.** **2. Press Select to increment the digit until the desired value appears, then press Menu to set.** **3. Repeat step 1 for each digit.** **4. Press Menu to advance to the next submenu; or, press Select to restart the change mode.**
Port A/B Soft Physical Addressing Submenu		
`Soft PA HI`	Defaults to the last saved selection. The drive seeks a soft PA in an ascending order at loop initialization.	• **Do one of the following:** • **Press Menu to bypass.** • **Press Select to toggle; then, press Menu to set and advance to the next submenu.**
`Soft PA LO`	The drive seeks a soft PA in a descending order at loop initialization. Appears only with `Hard PA N`.	
Note – Manufacturing ships drives with `Soft PA LO` option selected. The Solaris default FCP-driver behavior requires `Soft PA LO`.		
Interface Speed Rate Submenu		
`Rate Auto`	Selects interface speed rate.	• **Do one of the following:** • **Press Menu to bypass.** • **Press Select until desired option appears; then, press Menu to set and advance to the next submenu.**
`Rate 4Gb`	Speed determined by network.	
`Rate 2Gb`	Speed rate fixed at 4 Gb	
`Rate 1Gb`	Speed rate fixed at 2 Gb Speed rate fixed at 1 Gb **Note –** When fixed speed rate is selected, the drive only operates at the selected rate. If the network is fixed at a different rate, the drive does not log on.	
Note – Manufacturing ships drives with the `Rate Auto` option selected. T10000A drives operating in AS400 environments with code level 1.37.114 should support 4Gb transfer rates. If the user encounters problems when writing highly compressible data, the service representative should refer to Field Action Bulletin (FAB) 200869.		

TABLE 4-1 Drive Configuration Settings (Continued)

Options	Notes	Procedure
Port A/B Maximum Data Frame Size Submenu		

`MaxSz 2112`
`MaxSz 2048`
	Selects maximum frame size.	• **Do one of the following:**
		  • **Press Menu to bypass.**
		  • **Press Select to toggle; then, press Menu to set and advance to the next submenu.**

Note – Manufacturing ships drives with the `MaxSz 2112` option selected.		
Port A/B World Wide Name (WWN) Submenu		
Note – You can create or edit a "Custom" WWN as required for special circumstances. When Custom WWNs are used, Port A, Port B, and Drive Node WWNs should all be changed to designated Custom WWNs to meet special circumstances. Make sure the Custom WWN is registered in the Host interface software. Unregistered or duplicate WWNs cause Host interface anomalies. Libraries using the dynamic WWN (dWWN) feature automatically set the drive Custom WWN setting to a library-determined WWN.		

`H=500104F0`	Defaults to the last saved selection.
	Comprises the first half of a unique 64-bit WWN that identifies the specific port node. This first half includes a company identification (characters 2 through 6); and for StorageTek branded devices, the company ID is "00104F". Therefore, you would not typically edit the first half of a WWN.
		1. Do one of the following:
		  a. Press Menu to bypass.
		  a. Press Select to start the change mode.
		2. Press Select to increment the character until the desired value appears, then press Menu.
		3. Repeat step 2 for each character.
		4. Press Menu to advance to the second half of the WWN; or, press Select to restart the change mode.

TABLE 4-1 Drive Configuration Settings (Continued)

Options	Notes	Procedure
L=yyyyyyyy	Defaults to the last saved selection. Comprises the second half of the 64-bit WWN that identifies this specific port node. Typically, only the last character is different than the other port node. Generally, when setting a Custom WWN in a drive, you edit the second half of the WWN to replicate the second half of the WWN which was in use for the removed drive.	**1. Do one of the following:** **a. Press** Menu **to bypass.** **a. Press** Select **to start the change mode.** **2. Press** Select **to increment character until desired value appears, then press** Menu**.** **3. Repeat step 2 for each character.** **4. Press** Menu **to advance to the next submenu; or, press** Select **to restart the change mode.**
Note – Manufacturing generates "Normal" drive node and port A/B WWNs as a set, and stores them in the drive EEPROM. The format is: Drive Node: H=500104F0 (StorageTek brand device), L=yyyyyyyy. Port A: H=500104F0, L=yyyyyyyy (last character, one higher than drive node) Port B: H=500104F0, L=yyyyyyyy (last character, one higher than port A)		
Port A/B Custom/Normal WWN Submenu		
Note – This submenu appears only when the Custom WWN is in use or when one is being created/edited.		
`WWN Custom`	Appears whenever a Custom WWN is in use, or is being created/edited. `WWN Custom` also appears when the drive is using dynamic WWN, set by a library invoking dWWN.	• **Do one of the following:** • **Press Menu to bypass to the next submenu.** • **Press Select to toggle the selection to `WWN Normal`.**
`WWN Normal`	Selection recalls the stored Normal WWN from the drive EEPROM.	• **Do one of the following:** • **Press Menu to recall the stored Normal WWN, and advance to the next submenu.** • **Press Select to toggle the selection to `WWN Custom`.**
Port B Attributes Menu		
`View PrtB ?` **(**`online`**)** `Cfg PrtB ?` (`offline`)	View or change Port B attributes as defined in the preceding port A/B attributes submenus, starting on page 64.	• **Do one of the following:** • **Press Menu to bypass.** • **Press Select to enter the port attributes submenus.**

TABLE 4-1 Drive Configuration Settings (Continued)

Options	Notes	Procedure
Emulation Mode Submenu (FCP)		

`Emul XXXXX`	`Emul STD` is Native.
	`Emul 9840`
	`Emul 9940`
	`Emul 3592`
		• **Do one of the following:**
		• **Press Menu to bypass**
		• **Press Select until desired option appears; then, press Menu to set, and advance to the next submenu.**

Note – Manufacturing ships Fibre Channel (FCP) drives with the `Emul STD` option selected. Use the special emulation modes (`Emul 9840` and `Emul 9940`) only at the direction of company technical support. **Note –** When using VOP to change Emulation mode, you must have VOP version 1.0.9, or higher. Otherwise, the current mode option cannot be changed by VOP.		
Emulation Mode Submenu (FICON)		
`Emul XXXX`	`Emul 3592` `Emul VSM`	• **Do one of the following:** • **Press Menu to bypass** • **Press Select to toggle; then, press Menu to set, and advance to the next submenu.**
Note – Manufacturing ships FICON drives with the `Emul 3592` option selected. Change the selection to `Emul VSM` as needed to match site requirements. **Note –** When using VOP to change the emulation mode, you must have VOP version 1.0.9, or higher. Otherwise, the current mode option cannot be changed by VOP.		
Compress Mode Submenu		
`Cmprss Yes`	Defaults to the last saved selection. When you select `Yes`, data is compressed, by default. Host can request no data compression.	• **Do one of the following:** • **Press Menu to bypass.** • **Press Select until the desired option appears; then, press Menu to set and advance to the next submenu.**
`Cmprss Off`	When you select `Off`, data is not compressed, and a host request has no effect.	
`Cmprss No`	When you select `No`, data is not compressed, by default. Host can request data compression.	
Note – Manufacturing ships drives with the `Compress Yes` option selected.		

TABLE 4-1 Drive Configuration Settings (Continued)

Options	Notes	Procedure
Data Security Erase Mode Submenu		
`Full DSE Y`	Defaults to the last saved selection. Writes a random binary pattern on the media, over-writing existing data from the point of an *erase* command, to the end-of-tape.	• **Do one of the following:** • **Press Menu to bypass.** • **Press Select to toggle; then, press Menu to set and advance to the next submenu.**
`Full DSE N`	Writes data on the media that indicates valid data does not exist beyond the point of an *erase* command.	
Note – Manufacturing ships drives with the `Full DSE Y` option selected.		
Drive Address Submenu (FICON only)		
`Drv Adr xy`	Defaults to the last saved selection. `x` and `y` are hexadecimal characters. Establishes the device (not CU) address for the drive. It should usually remain zero (00). Recheck this address if the link is not operating.	1. **Do one of the following:** • **Press Menu to bypass.** • **Press Select to start the change mode.** 2. **Press Select to increment the x character until the desired value appears, then press Menu.** 3. **Repeat step 2 for the y character.** 4. **Press Menu to advance to the next submenu; or, press Select to restart the change mode.**
Note – Manufacturing ships drives with `Drv Adr 00` selected when the FICON interface is active.		
Standard Label Overwrite Protection Submenu		
`SL Prot Y`	Defaults to the last saved selection. Selects standard label overwrite protection.	• **Do one of the following:** • **Press Menu to bypass.** • **Press Select to toggle; then, press Menu to set and advance to the next submenu.**
`SL Prot N`	Deselects standard label overwrite protection.	

Notes:

1. Manufacturing ships drives with `SL Prot N` selected.
2. Only select "`SL Prot Y`" if label overwrite code is loaded, or if running standard labels and want the drive to display a fatal error (CHK 33EX) when writing a non-80-byte record for VOLSER or HDR1.
3. Customers using NL or NSL tape processing cannot use SL Prot.
4. POST WRCART cannot be run with this feature enabled.
5. Contact Technical Support for any assistance.

TABLE 4-1 Drive Configuration Settings (Continued)

Options	Notes	Procedure
Language Selection Submenu		

`Language ?`	Defaults to the last saved selection.
	
	Selects display language: **English**, **Espanol**, **Francais**, **Italiano**, or **Deutsch**.
	
	In the online (View) mode, only the active language appears.
		• **Do one of the following:**
		  • **Press Menu to bypass.**
		  • **Press Select until desired option appears; then, press Menu to set and advance to the next submenu**.

Note – Manufacturing ships drives with the `English` option selected.		
Tape Bar Submenu		

`Tape Bar Y`	Defaults to the last saved selection. Enables secondary display of current read/write point, relative to the beginning of data mark on the tape.	• **Do one of the following:**
		  • **Press Menu to bypass.**
		  • **Press Select to toggle; then, press Menu to set and advance to the next submenu.**

`Tape Bar N`	Disables the option.	
Note – Manufacturing ships drives with the `Tape Bar N` option selected.		
Library Address Submenu		

`Lib Adr xy`	Defaults to the last saved selection.
	
	For SL8500, SL3000, and L180/L700/ L1400 libraries; use the factory preset `(FF)` with T10000 tape drives.
	
	In 9310 libraries (T10000A only), looking at the back of the drives, the address sequence in the drive cabinet is:
	• Left column from top: **00** through **09**
	• Right column from top: **0A** through **13**.
		1. Do one of the following:
		  • **Press Menu to bypass.**
		  • **Press Select to start the change mode.**
		2. Press Select to increment the x digit until the desired value appears, then press Menu to set.
		3. Repeat step 2 for the y digit.
		4. Press Menu to advance to the next submenu; or, press Select to restart the change mode.

Note – Manufacturing ships drives with `Lib Adr FF` selected.		

TABLE 4-1 Drive Configuration Settings (Continued)

Options	Notes	Procedure
Drive Node WWN Submenu		
Note – You can create/edit a "Custom" WWN as required for special circumstances. When Custom WWNs are used, Drive Node, Port A, and Port B WWNs should all be changed to the designated Custom WWNs to meet special circumstances. Make sure the Custom WWN is registered in the Host interface software. Unregistered or duplicate WWNs cause Host interface anomalies. Libraries using the dynamic WWN (dWWN) feature automatically set the drive Custom WWN setting to a library-determined WWN.		
H=500104F0	Defaults to the last saved selection. Comprises the first half of a unique 64-bit node WWN that identifies this drive node. This first half includes a company identification (characters 2 through 6); and for StorageTek branded devices, the company ID is "00104F". Therefore, you would not typically custom edit the first half of a WWN.	**1. Do one of the following:** • **Press Menu to bypass.** • **Press Select to start the change mode.** **2. Press Select to increment the character until the desired value appears, then press Menu.** **3. Repeat step 2 for each character.** **4. Press Menu to advance to the second half of the WWN; or, press Select to restart the change mode.**
L=yyyyyyyy	Defaults to the last saved selection. Comprises the second half of the 64-bit WWN that identifies this specific node. Typically, only the last character is different than the port nodes. Generally, when setting a Custom WWN in a drive, you edit the second half of the WWN to replicate the second half of the WWN which was in use for the removed drive.	**1. Do one of the following:** • **Press Menu to bypass.** • **Press Select to start the change mode.** **2. Press Select to increment the character until the desired value appears, then press Menu.** **3. Repeat step 2 for each character.** **4. Press Menu to advance to the next submenu; or, press Select to restart the change mode.**
Note – Manufacturing generates the "Normal" drive node and port A/B WWNs as a set and stores them in the drive EEPROM. The format is: Drive Node: H=500104F0 (StorageTek brand device), L=yyyyyyyy. (lowest of set) Port A: H=500104F0, L=yyyyyyyy (last character, one higher than drive node) Port B: H=500104F0, L=yyyyyyyy (last character, one higher than port A node)		

TABLE 4-1 Drive Configuration Settings (Continued)

Options	Notes	Procedure
Drive Node Custom/Normal WWN Submenu		
Note – This submenu only appears if either a Custom WWN is in use or when one is being created/edited.		

`WWN Custom`	Appears when either a Custom WWN is in use or is being created/edited. `WWN Custom` also appears when the drive is using a dynamic WWN set by a library invoking dWWN.	• **Do one of the following:**
		  • **Press Menu to bypass to the next submenu.**
		  • **Press Select to toggle the selection to `WWN Normal`.**

`WWN Normal`	Selection recalls the stored Normal WWN from the drive EEPROM.	• **Do one of the following:**
		  • **Press Menu to recall the stored Normal WWN, and advance to the next submenu.**
		  • **Press Select to toggle the selection to `WWN Custom`.**

Serial Number Menu		
`S/N=zzzzzz` (online only)	Identifies the manufacturing assigned serial number of the drive. **zzzzzz =** the last six characters of the rear panel DMOD label. This data is read from an internal EEPROM for online viewing only.	• **Press Menu or Select to advance to the next submenu.**
Save Configuration Submenu		

`Save/IPL ?` (offline only)	This submenu appears only if changes were made in any submenu.
	`Saving CFG` appears for 2 seconds after you press Select.
	After you save the configuration, the drive performs an IPL.
		• **Do one of the following:**
		  • **Press Menu (No) to cancel changes.**
		  • **Press Select (Yes) to save changes and initiate an IPL.**

Exit Configuration Submenu		

`Exit CFG ?`	This submenu allows you to either repeat the change configuration submenus or exit the configuration submenus.	• **Do one of the following:**
		  • **Press Menu (No) to loop back to the Interface Select Submenu.**
		  • **Press Select (Yes) to exit and advance to the TCP/IP Configuration Menu.**

TABLE 4-1 Drive Configuration Settings (Continued)

Options	Notes	Procedure
TCP/IP Configuration Menu		
`View TCP ? (online)` `Chng TCP ? (offline)`	If bypassed, the display advances to the Firmware Release Level Menu (online) or the Drive Operations Menu (offline). This is the entry point for the TCP/IP submenus. See "View/Change TCP/IP Settings" on page 75.	• **Do one of the following:** • **Press Menu (No) to bypass.** • **Press Select (Yes) to enter TCP/IP configuration submenus.**
Drive Operation Menu		
`Drv Menu ? (offline only)`	If bypassed, the display advances to the Firmware Release Level Menu. This is the entry point to the offline drive operations submenus. See "Drive Operations Menu" on page 81.	• **Do one of the following:** • **Press Menu (No) to bypass.** • **Press Select (Yes) to enter Drive Operations submenus.**
Firmware Release Level Menu		
`Rx.yy.zzza`	This submenu displays the current drive firmware release level.	• **Press Menu or Select and advance to the Exit Main Menu.**
Exit Menu		
`Exit Menu?`	This menu allows you to either stay in the menu system to return the drive to Online or to exit the menu system.	• **Do one of the following:** • **Press Menu (No) to go to the Online/Offline menu.** • **Press Select (Yes) to exit the Menu System.**

Note – If you exit the menu system with the drive Offline, the display flashes `Offline` every few seconds as a reminder that drive is still Offline (if a data cartridge has been loaded at least once).

View/Change TCP/IP Settings

Use following menu tree as a brief guide to view or change the TCP/IP settings. See TABLE 4-2 on page 76 for more detailed guidelines.

> **Note –** Make sure the host has varied the drive offline before setting the drive offline.

Online/Offline
Press Select to toggle, then press Menu to set.

View/Chng CFG ? View (online)/Change (offline) Configuration
Press Menu to bypass.

View/Chng TCP ? (View (online)/Change (offline) Configuration
Press Select to enter, press Menu to bypass.

- **DHCP.** (Y/N) (must be set to "N" to view/change the static settings)
- **IPh aaa . bbb** (IP Address, high) (first half of static IP address)
- **IPl ccc . ddd** (IP Address, low) (second half of static IP address)
- **NMh aaa . bbb** (Net Mask, high) (first half of sub-net mask)
- **NMl ccc . ddd** (Net Mask, low) (second half of sub-net mask)
- **GWh aaa . bbb** (Gateway, high) (first half of gateway address)
- **GWl ccc . ddd** (Gateway, low) (second half of gateway address)
- **Save/IPL ?** (if there are pending changes)
- **Exit TCP ?** (no, cancels changes, and restarts view/change TCP)

Drv Menu ? (offline only) (see "Drive Operations Menu" on page 81)

Rx.yy.zzza (current drive firmware release level) (display only)

Exit Menu ?

TABLE 4-2 provides details of TCP/IP configuration settings, and guidelines for changing selected settings when the drive is offline.

TABLE 4-2 TCP/IP Configuration Settings

Options	Notes	Procedure
TCP/IP Configuration Menu		

`View TCP ? (online)`
`Chng TCP ? (offline)`
	If bypassed, the display advances to the Firmware Release Level menu (online) or the Drive Operations menu (offline).
	This is the entry point for the TCP/IP submenus.
		• **Do one of the following:**
		  • **Press Menu (No) to bypass.**
		  • **Press Select (Yes) to enter the TCP/IP submenus.**

DHCP Submenu		

`DHCP Y/N`	Defaults to the last saved selection.
	With `DHCP Y` selected, a DHCP server (remote to the drive) assigns the dynamic TCP/IP settings.
	With `DHCP N` selected, DHCP is disabled. The drive uses Static TCP/IP settings.
		• **Do one of the following:**
		  • **Press Menu to bypass.**
		  • **Press Select to toggle; then, press Menu to set and advance to the next submenu.**

Notes: 1. `DHCP N` must be active/selected for you to change the static IP, Net Mask, and Gateway. 2. When `DHCP Y` is active/selected, you *cannot* change the static IP, Net Mask, and Gateway. 3. Manufacturing ships all drives with the `DHCP N` option selected.		
IP Address Hi Submenu		

`IPhaaa.bbb`	Defaults to the last saved selection.
	Valid entries are 000-255 for each digit trio.
	If you attempt to enter a value greater than 255 in either trio, all digits flash when the last digit is set.
		1. **Do one of the following:**
		  • **Press Menu to bypass.**
		  • **Press Select to start the change mode.**
		2. **For each digit:**
		  a. **Press Select to increment the flashing digit until the desired value appears.**
		  a. **Press Menu to set.**
		3. **Press Menu to advance to the next submenu; or, press Select to restart the change mode.**
		4. **If all digits flash, press either Select or Menu to clear; then, press Select to restart the change mode.**

Note – Manufacturing ships all drives with the static IP Address Hi set to `010.000`.		

TABLE 4-2 TCP/IP Configuration Settings (Continued)

Options	Notes	Procedure
IP Address Lo Submenu		
`IPlccc.ddd`	Defaults to the last saved selection. Valid entries are 000-255 for each digit trio. If you attempt to enter a value greater than 255 in either trio, all digits flash when the last digit is set.	**1. Do one of the following:** • **Press Menu to bypass.** • **Press Select to start the change mode.** **2. For each digit:** **a. Press Select to increment the flashing digit until the desired value appears.** **a. Press Menu to set.** **3. Press Menu to advance to the next submenu; or, press Select to restart the change mode.** **4. If all digits flash, press either Select or Menu to clear; then, press Select to restart the change more.**
Note – Manufacturing ships all drives with static IP Address Lo set to `000.001`.		
Net Mask Hi Submenu		
`NMhaaa.bbb`	Defaults to the last saved selection. Valid entries are 000-255 for each digit trio. If you attempt to enter a value greater than 255 in either trio, all digits flash when the last digit is set.	**1. Do one of the following:** • **Press Menu to bypass.** • **Press Select to start the change mode.** **2. For each digit:** **a. Press Select to increment the flashing digit until the desired value appears.** **a. Press Menu to set.** **3. Press Menu to advance to the next submenu; or, press Select to restart the change mode.** **4. If all digits flash, press either Select or Menu to clear; then, press Select to restart the change more.**
Note – Manufacturing ships all drives with static Net Mask Hi set to `255.255`.		

TABLE 4-2 TCP/IP Configuration Settings (Continued)

Options	Notes	Procedure
Net Mask Lo Submenu		
NMlccc.ddd	Defaults to the last saved selection. Valid entries are 000-255 for each digit trio. If you attempt to enter a value greater than 255 in either trio, all digits flash when the last digit is set.	**1. Do one of the following:** • **Press Menu to bypass.** • **Press Select to start the change mode.** **2. For each digit:** **a. Press Select to increment the flashing digit until the desired value appears.** **a. Press Menu to set.** **3. Press Menu to advance to the next submenu; or, press Select to restart the change mode.** **4. If all digits flash, press either Select or Menu to clear; then, press Select to restart the change more.**
Note – Manufacturing ships all drives with static Net Mask Lo set to 255.000.		
Gateway Hi Submenu		
GWhaaa.bbb	Defaults to the last saved selection. Valid entries are 000-255 for each digit trio. If you attempt to enter a value greater than 255 in either trio, all digits flash when the last digit is set.	**1. Do one of the following:** • **Press Menu to bypass.** • **Press Select to start the change mode.** **2. For each digit:** **a. Press Select to increment the flashing digit until the desired value appears.** **a. Press Menu to set.** **3. Press Menu to advance to the next submenu; or, press Select to restart the change mode.** **4. If all digits flash, press either Select or Menu to clear; then, press Select to restart the change more.**
Note – Manufacturing ships drives with a static Gateway Hi set to either 0.0. or 255.255		

TABLE 4-2 TCP/IP Configuration Settings (Continued)

Options	Notes	Procedure
Gateway Lo Submenu		
`GWlccc.ddd`	Defaults to the last saved selection. Valid entries are 000-255 for each digit trio. If you attempt to enter a value greater than 255 in either trio, all digits flash when the last digit is set.	**1. Do one of the following:** • **Press Menu to bypass.** • **Press Select to start the change mode.** **2. For each digit:** **a. Press Select to increment the flashing digit until the desired value appears.** **a. Press Menu to set.** **3. Press Menu to advance to the next submenu; or, press Select to restart the change mode.** **4. If all digits flash, press either Select or Menu to clear; then, press Select to restart the change more.**
Note – Manufacturing ships drives with static Gateway Lo set to either `0.0.` or `255.255`		
Save TCP/IP Submenu		
`Save/IPL ?`	This submenu is present if either the DHCP selection or the static TCP/IP settings were changed. `Saving TCP` appears for 2 seconds after you press Select. After saving the TCP configuration, the drive automatically perform an IPL. `Save Fails` appears for RAM problems.	• **Do one of the following:** • **Press Menu (No) to cancel changes.** • **Press Select (Yes) to save changes and initiate an IPL.**
Exit TCP/IP Submenu		
`Exit TCP ?`	This submenu allows you to either repeat the TCP/IP submenus or to exit TCP/IP.	• **Do one of the following:** • **Press Menu (No) to loop back to the DHCP Y/N submenu.** • **Press Select (Yes) to exit and advance to the Firmware Release Level menu (online), or the Drive Operation menu (offline)**

TABLE 4-2 TCP/IP Configuration Settings (Continued)

Options	Notes	Procedure
Drive Operation Menu		

`Drv Menu ? (offline only)`	If bypassed, the display advances to the Firmware Release Level menu. This is the entry point to the offline drive operations submenus.
	
	See "Drive Operations Menu" on page 81.
		• **Do one of the following:**
		  • **Press Menu (No) to bypass.**
		  • **Press Select (Yes) to enter the drive operations submenus.**

Firmware Release Level Submenu		
`Rx.yy.zzza`	This submenu displays current drive firmware release level.	• **Press Menu or Select and advance to the Exit menu.**
Exit Menu		

`Exit Menu?`	This menu allows you to stay in the menu system to return the drive to Online, or to exit the menu system.	• **Do one of the following:**
		  • **Press Menu (No) to go to the Online/Offline menu**
		  • **Press Select (Yes) to exit the menu system.**

Note – If you exit the menu system with the drive offline, the display flashes `Offline` every few seconds as a reminder that the drive is still offline (if a data cartridge has been loaded at least once).

Drive Operations Menu

Use the following menu tree for drive operations. The Drv Menu is only available when the drive is offline. See TABLE 4-3 on page 82 for details.

> **Note –** Make sure the host has varied the drive offline before you set the drive offline.

Online/Offline
Press Select to toggle, then press Menu to set.

Chng CFG ? (Change Configuration)
Press Menu to bypass.

Chng TCP ? (Change Configuration)
Press Menu to bypass.

Drv Menu ? (Drive Operations Menu)

Press Select to enter, press Menu to bypass.

- **IPL FromTP** (uploads drive firmware from code tape cartridge)
  - **Ld IPL TP** (load write-protected cartridge containing drive firmware image)

  Note – After the firmware image is uploaded into the drive PROM, the drive performs an IPL to load/activate the new firmware. The drive is in the online state.
- **MakeDumpTP** (formats tape cartridge to retrieve drive dump logs)
  - **Ld Dump TP** (load write-enabled code/data/dump cartridge)
- **MakeCodeTP** (downloads drive firmware image to tape cartridge)
  - **Ld Code TP** (load write-enabled code/data/dump tape cartridge)
- **MakeDataTP** (reclaims/reformats tape cartridge for data read/write)
  - **Ld Data TP** (load write-enabled code/data/dump tape cartridge)
- **Build MIR** (reclaims/reformats tape cartridge for data read/write)
  - **Ld Cust TP** (load write-enabled data cartridge with invalid MIR)
- **Exit Drv ?** (no, restarts drive operation options)

Rx.yy.zzza (current drive firmware release level) (display only)

Exit Menu ?

TABLE 4-3 provides details for drive operation utilities.

TABLE 4-3 Drive Operations

Options	Notes	Procedure
Drive Operation Menu		

`Drv Menu ? (offline only)`	If bypassed, the display advances to the Firmware Release Level menu.
	This is the entry point to the Drive Operations submenus.
		• **Do one of the following:**
		  • **Press Menu (No) to bypass.**
		  • **Press Select (Yes) to enter the submenus.**

Code Update Submenu		

`IPL FromTP`	IPL From Tape, updates the drive firmware from a code tape that you insert in the drive.
	A normal data cartridge, if present, unloads when this function is activated.
	If `CHK xxxx` appears, try a different code tape.
		1. Do one of the following:
		  • **Press Menu to bypass.**
		  • **Press Select to activate.**
		2. When `Ld IPL Tp` appears, insert the code tape (write-protected data cartridge that contains the desired firmware release level image).
		Note – After the update completes, the drive unloads the code tape and initiates an IPL.
		3. Remove the unloaded code tape.

Make Dump Tape Submenu		

`MakeDumpTp`	Make Dump Tape specially formats and identifies a data cartridge as a *dump tape*; but, it does not collect dump logs. Data cartridges used to collect dump logs must first be formatted this way to accept dump logs.
	A normal data cartridge, if present, ejects when this function is activated.
	If Make Dump Tape fails and `CHK xxxx` appears, try a different data cartridge.
		1. Do one of the following:
		  • **Press Menu to bypass.**
		  • **Press Select to activate.**
		2. When `Ld Dump Tp` appears, insert a write-enabled data cartridge.
		3. After the formatted dump tape unloads, remove the cartridge.
		4. Insert another write-enabled data cartridge, or press Menu to exit the dump tape submenu.

TABLE 4-3 Drive Operations (Continued)

Options	Notes	Procedure
Make Code Tape Submenu		
Note – Only drives with all images loaded into the EEPROM can make code tapes.		
`MakeCodeTp`	Make Code Tape copies the firmware image from the drive EEPROM to a data cartridge. You can use this *code tape* to update firmware in other drives using the Code Update submenu. A normal data cartridge, if present, ejects when this function is activated. If Make Code Tape fails and `CHK xxxx` appears, try a different cartridge. If the problem persists, consult your service representative. **Note –** This operation might not work on encryption-enabled tape drives.	**Note –** Make sure the drive is properly prepared to create code tapes. If required, exit the Drive Operations menu and update the drive to a full code of the desired firmware release level. **1. Do one of the following:** • **Press Menu to bypass.** • **Press Select to activate.** **2. When `Ld Code Tp` appears, insert a write-enabled data cartridge.** **3. After the new code tape unloads, remove the cartridge and write protect it (set the switch to the locked position).** **4. Insert another write-enabled data cartridge, or press Menu to exit the create code tape submenu.**
Make Data Tape Submenu		
`MakeDataTp`	Make Data Tape reformats cartridges so they can be reused as normal *data tapes*. This is sometimes referred to as "reclaiming." A cartridge, if present, unloads when this function is activated. Information in the MIR about old data files on a tape being reformatted is erased. VolSafe data cartridges cannot be reformatted. If inserted, the drive rejects a VolSafe cartridge. If Make Data Tape Fails, and `CHK xxxx` appears, try a different data cartridge.	**1. Do one of the following:** • **Press Menu to bypass.** • **Press Select to activate.** **2. When `Ld Data Tp` appears, insert a write-enabled data cartridge.** **3. After the reformatted data tape unloads, remove the data cartridge.** **4. Insert another write-enabled data cartridge, or press Menu to exit the reclaim tape submenu.**

TABLE 4-3 Drive Operations (Continued)

Options	Notes	Procedure
Build Media Information Region Submenu		
`Build MIR`	T10000 tape drives use information recorded at the beginning of tape of a data cartridge, in an area known as the Media Information Region (MIR), to access and manage data files while the data cartridge is loaded in the drive. Make sure the drive is unloaded before you activate Build MIR. `Rebuild MIR` flashes on the operator panel while the MIR is rebuilding.	**1. Do one of the following:** • **Press Menu to bypass.** • **Press Select to activate.** **2. When `Ld Cust Tp` appears, insert the write-enabled data cartridge with an invalid MIR.** **Note –** After the MIR is rebuilt, the cartridge unloads. **3. Remove the data cartridge.** **4. Insert another write-enabled data cartridge requiring a MIR rebuild; or, press Menu to exit the build MIR submenu.**
Exit Drive Submenu		
`Exit Drv ?`	This submenu allows you to either repeat the drive operations submenus or exit Drive Operations.	• Do one of the following: • **Press Menu (No) to loop back to the Code Update Submenu.** • **Press Select (Yes) to exit Drive Operations and advance to the Firmware Release menu.**
Firmware Release Level Menu		
`Rx.yy.zzza`	This submenu displays the current drive firmware release level.	• **Press Menu or Select and advance to the Exit menu.**
Exit Menu		
`Exit Menu?`	This menu allows you to either stay in the menu system to return the drive to Online or to exit the menu system.	• **Do one of the following:** • **Press Menu (No) to go to the Online/Offline menu.** • **Press Select (Yes) to exit the menu system.**

Note – If you exit the menu system with the drive offline, the display flashes `Offline` every few seconds as a reminder that drive is still `Offline` (if a data cartridge has been loaded at least once).

5

Service Calls and Help

A fault symptom code (FSC) might appear on the Virtual Operator Panel (VOP) screen or the tape drive's front panel display screen of rack mounted tape drives. You might be able to correct the problem, see TABLE D-1 on page 97 or "Potential Operator Recovery Scenarios" on page 101. If you can not correct the problem:

- **Record the FSC information for your service representative.**

Some errors result in the state of the drive status LED on the rear of the tape drive changing color, flashing, or both. See:

- FIGURE 1-2 on page 17 or FIGURE 1-3 on page 18 for the location of the LED
- "Drive Status LED" on page 18 for information about the LED
- TABLE 1-1 on page 19 for the various LED states and colors you may encounter

If you gather as much of the following information as possible before you place a service call, the process is much easier:

- Account name
- Site location number
- Contact name
- Telephone number
- Equipment model number
- Tape drive address
- Tape drive code level
- Tape drive serial number
- Urgency of the problem
- Fault Symptom Code (FSC) from either the tape drive's front panel display screen (rack mount), the VOP window, or as displayed on the host system display screen
- Problem description
- What color and flash rate is exhibited by LED on the rear of the tape drive? (This LED is not visible when the tape drive is installed in some libraries.)
- Is the tape drive in a library? If so, which library?

- If the tape drive was running properly before this incident:
  - What changes has the site made recently?
  - What software application was running at the time of the failure?
  - Were any hardware configuration changes made recently?
  - Were any software configuration or upgrades done recently?
  - Were any additions or deletions to the hardware or software done at the site?
- If the drive was NOT running properly before this incident, what was the last problem?

A

Cartridge Care

StorageTek T10000 tape cartridges require care to ensure proper operation and longevity. This appendix deals with the handling of cartridges, including unpacking and shipping cartridges to another site. For information regarding cartridge labels, particularly those cartridges used inside a library, see "Library Use Cartridge Labels" on page 91.

> **Note –** In this chapter, "data cartridges" refers to all data cartridges: Standard data, Sport data, VolSafe data, and Sport VolSafe data cartridges.

Guidelines for Handling

> **Caution –** *Tape Damage*: Cartridges are easily damaged and you must handle them carefully.

- Do not expose the tape or cartridge to direct sunlight or moisture.
- Do not expose a data cartridge to magnetic fields.
- Maintain clean operating, working, and storage environments.

> **Note –** See Appendix F, "Controlling Contaminants".

▼ To Unpack and Acclimate Cartridges

- **Unpack new data cartridges in the area intended for use, and allow them to acclimate for a period of at least 72 hours.**

▼ To Clean a Cartridge

- **Wipe all dust, dirt, and moisture from the cartridge case with a lint-free cloth.**

Storage Environment

Always store cartridges in an environment within the specified range of temperature and humidity found in "Tape Cartridge Environmental Requirements" on page 109. When you store cartridges, follow these recommendations:

- Do not take data cartridges out of their protective wrapping until you need them.
- Store cartridges in a dirt-free environment that, if possible, duplicates the conditions of the data processing center.
- Before you use a cartridge that has been in storage, acclimate it to the operating environment for at least 72 hours.

▼ To Ship a Cartridge

Use the following guidelines to prepare StorageTek T10000 tape cartridges for shipment:

> **Caution –** *POTENTIAL Cartridge Damage*: Cartridges are easily damaged in shipment if improperly packaged. USE ONLY THE DESIGNATED PACKAGING ASSEMBLIES, AND IN MATCHING QUANTITIES WITH NUMBER OF CARTRIDGES.

1. **Obtain appropriate quantities of designated packaging assemblies:**

   Only the following assemblies are qualified for shipping T10000 cartridges:

   - Single Cartridge - PN 1095329xx, T10000 Cartridge 1-Pack Packaging Assembly
   - Five Cartridges - PN 1095332xx, T10000 Cartridge 5-Pack Packaging Assembly

   > **Note –** Customers must obtain cartridge shipping packages from service representatives.
   >
   > The 5-Pack packaging assembly only protects *exactly* five (5) T10000 tape cartridges. DO NOT attempt to package more than five cartridges by forcing the additional cartridge/s into the package. DO NOT attempt to package less than five cartridges by filling the missing cartridge/s void with any other material. Use the single cartridge 1-Pack packaging assembly when packaging less than five cartridges.

2. **Follow the packaging instructions included in the packaging assembly.**

   Specific packaging instructions are included with each packaging assembly.

   > **Note –** Do not improvise or use older packaging instructions as they might not be applicable to the current packaging assembly.

3. **Attach the appropriate shipping label to the sealed package.**

   Shipping labels will vary relative to prescribed/available shipping services.

Dropped Cartridges

Whenever a cartridge is dropped, there is a potential for damage to the case. Even if the case is visibly undamaged, the cartridge leader might be jarred out of the home position and result in a load failure.

> **Note –** If the drop was greater than 75 centimeters (29.5 inches), use the cartridge only for a one-time data transfer, even if otherwise undamaged, then discarded.
>
> After a full inspection if the cartridge is damaged but fit for loading, transfer data to a serviceable cartridge.

- **Inspect a dropped cartridge thoroughly by looking for damage to the case; and, if necessary, making sure the leader is recovered to the home position.**

▼ To Inspect a Dropped Cartridge

1. **Closely examine the entire case, front and back, for breaks and/or cracks.**

   If cracks and/or breakage is visible, the cartridge must be discarded.

   > **Note –** A dropped cartridge with visible damage that precludes normal loading into a drive, might be a candidate for data recovery. Contact your service representative regarding damaged data cartridge recovery options.

2. **Check all four case screws (1, FIGURE A-1) for security.**

   If a screw post is broken, the screw might be noticeably loose.

FIGURE A-1 Cartridge Inspection Points

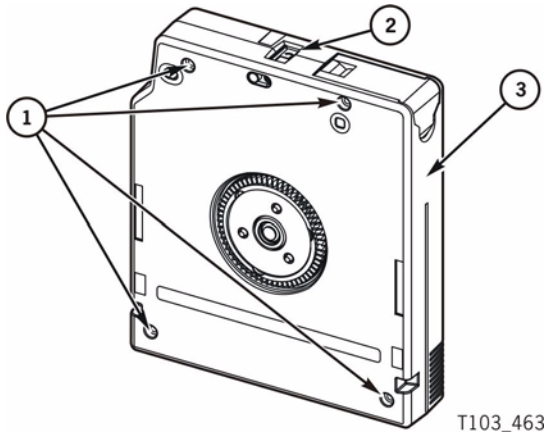


Illustration call-outs (3):
1. Case screw (4x)
2. Write-protect switch
3. Sonic weld area

3. **Attempt to separate the case halves near each screw.**

   If a screw post is broken, the case separates slightly, even if the screw seems tight.

4. **Examine the sonic weld area near the tape access door, (3, FIGURE A-1 on page 89) for integrity.**

   Sonic weld damage might not be easily discernible. If there is any question about the integrity of the sonic weld, consult your service representative. If the sonic weld area has failed, the cartridge must be discarded, even if otherwise visibly undamaged.

5. **Slowly turn the cartridge over and listen for any loose items within the cartridge.**

   Caution – *Any loose items within the cartridge indicate internal damage, and loading of the cartridge could either damage the tape so data can never be retrieved or damage the tape drive.*

6. **Operate the write-protect switch, (2, FIGURE A-1 on page 89) several cycles.**

   The write-protect switch should slide smoothly.

7. **Open/close the tape access door (1, FIGURE A-2) several times, and examine the door for damage.**

   If the door is visibly damaged, and/or does not open/close smoothly, the cartridge must be discarded.

8. **Hold the tape access door open, and determine if the leader (2, FIGURE A-2) is in the home position (securely butted against stops).**

FIGURE A-2 Cartridge Door and Tape Leader

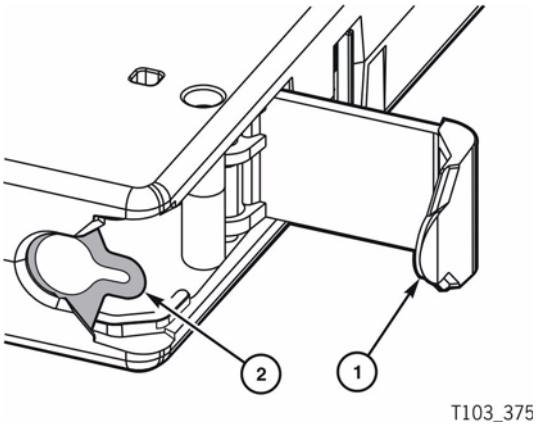


Illustration call-outs (2):
1. Tape access door
2. Leader

Caution – If the leader was jarred out of the home position, it is loose and floppy, or might be fully retracted into the cartridge case. If a load attempt was made with the leader out of the home position, the tape drive fully retracts the leader; it is pulled back into the cartridge and is no longer visible.

Do not attempt to force the leader back into the home position. If the leader is not in the home position, contact your service representative.

B

Data Cartridge Labels

Rack Mount Cartridge Labels

If you are using the data cartridges in a rack mount situation, almost any label across the data cartridge is acceptable, as long as it does not interfere with the operation of the tape drive.

Library Use Cartridge Labels

A cartridge label contains bar codes and visual characters. The visual characters are for operator use and are not used by the library. Moreover, the visual characters do not have to line up with the bar code lines for that character.

If you are using the data cartridges in a library, the labels must conform to a specification for the label size. See the library User's Guide for information regarding the label requirements. It is very important to follow these specifications.

- AIM Uniform Symbology Specification USS-39
- ANSI MH10.8M-1993 ANSI Code 39 Barcode Specification
- ANSI NCITS 314-199X SCSI 3 Medium Changer Commands (SMC)

You must put a label on the data cartridge in the label attachment area as shown by item 1 in FIGURE 1-7 on page 26. You must carefully place the label in the label area with the bar code down (to the hub side of the data cartridge—the hub is showing in the "Bottom View" in the figure).

Standard/Sport Cartridge Labels

Standard data cartridge labels consist of eight characters and the associated bar code.

- The first six characters in the label are the customer volume ID (such as, NGD018). Label characters may consist of A through Z and the numbers 0 through 9. No special characters (& $% @ # and so on) may be used.
- The last two characters are the media identifier:
  - StorageTek T10000 T1 cartridge (used with T10000A/B drive)
    - T1 for the standard T10000A/B data cartridge

  - TS for the T10000A/B sport data cartridge
- StorageTek T10000 T2 cartridge (used with T10000C drive)
  - T2 for the standard T10000C data cartridge
  - TT for the T10000C Sport data cartridge

The color behind the media identifier is usually white for standard cartridges. An example of a label for the T1 cartridge is shown in FIGURE B-1

FIGURE B-1 T10000A/B Standard Eight-character Label

VolSafe/Sport VolSafe Cartridge Labels

VolSafe labels are the same as standard cartridge labels with the exception that the background color of the media ID area is usually yellow.

Diagnostic Cartridge Labels

To be recognized by the library as a diagnostic cartridge, the label on the data cartridge must start with DG and a space (no third character is used). The five remaining label characters are:

- *xxx* can be 000 to 999
- *M*edia identifier (two characters)
  - StorageTek T10000 T1 cartridge (used with T10000A/B drive)
  - StorageTek T10000 T2 cartridge (used with T10000C drive)

An example of a diagnostic cartridge label for a T10000A/B drive is shown in FIGURE B-2.

FIGURE B-2 T10000A/B Diagnostic Cartridge Label

Cleaning Cartridge Labels

The cleaning label characters are:

- CLN are the first three characters
- Fourth through sixth characters can be 000 to 999 (for identification of each individual cleaning cartridge)
- Media identifier (two characters):
  - CT for the T10000A/B cartridge
  - CC for the T10000C cartridge
  - CL for the cleaning cartridge used on the T10000A/B/C drives

An example of a cleaning cartridge label for a T10000A/B drive is shown in FIGURE B-3.

FIGURE B-3 T10000A/B Cleaning Cartridge Label

C

Initial Drive Configuration Settings

Manufacturing presets the drive configuration sector after internal testing and before the tape drive is shipped. These preset, initial settings suffice for most sites. However, specific site requirements might dictate some alternative settings.

TABLE C-1 and "FICON Configuration Differences" on page 96 show drive configuration settings preset at the factory and available options.

TABLE C-1 Drive Configuration Initial Settings

Item	Function	Preset	Option
Hard PA (Port)	Hard Physical Address	N	Yes (Y), No (N)
Soft PA (Port)	Soft Physical Address	LO	HI, LO
Rate (Port)	Data transfer speed	Auto	Auto, 4 Gb, 2 Gb, 1 Gb
MAXSz (Port)	Maximum data frame	2112	2112, 2048
WWN (Port)	Port World-wide Name	Normal (assigned)	Normal, Custom
Emul XXXX (see Note 1)	Emulation Mode	STD	Standard, 9840B, 9940B, 3592 (see Note 2)
Cmprss	Data compression	Y	Yes, Off, No
Full DSE	Data Security Erase	Y	Yes (Y), No (N)
SL Prot	Standard Label Protection	N	Yes (Y), No (N)
Language	Message language (specific messages)	English	English, Spanish, French, Italian, German
Tape Bar	Tape activity display	N	Yes (Y), No (N)
LIB Adr xy	Library Address (hex.)	FF	Two digit he xi decimal
WWN	Drive Node World-wide Name	Normal (assigned)	Normal, Custom

Notes:

1. Fibre Channel interface only, see "FICON Configuration Differences" on page 96.
2. Emulation modes 9840B and 9940B are special modes used only at the direction of technical support.

TABLE C-1 Drive Configuration Initial Settings (Continued)

Item	Function	Preset	Option
TCP/IP	Maintenance Port IP		
DHCP	Dynamic Host Control	N	Yes (Y), No (N)
IP	Static IP Address	010.000.000.001	aaa.bbb.ccc.ddd
NM	Sub Net Mask	255.255.255.000	aaa.bbb.ccc.ddd
GW	Gateway	255.255.255.255	aaa.bbb.ccc.ddd

Notes:

1. Fibre Channel interface only, see "FICON Configuration Differences" on page 96.
2. Emulation modes 9840B and 9940B are special modes used only at the direction of technical support.

FICON Configuration Differences

The FICON interface has the following configuration differences:

- Emulation Mode:

  Preset: VSM

  Options: VSM, 3592

- Drive Address (device)

  Preset: 00

  Option: Two-digit hexadecimal

All other configuration settings are the same as shown in TABLE C-1 on page 95.

Other Configuration Settings

The following registers are set to the conditions shown:

- Network:

  IP address: 10.0.0.1

  Subnet mask: 255.255.255.0

  Gateway: 255.255.255.255

- IP Node Name: T10000-<last 9 digits of Serial Number>
- SNMP Alerts: All turned OFF
- Library Locator: ACS: 0 LSM: 0 Panel: 0 Drive: 0
- SNMP Managers: None Specified
- Drive Statistics: All zeroed
- Permanent Errors: All zeroed, pointers initialized.
- Temporary Errors: All zeroed, pointers initialized.

D

Messages and Translated Messages

This appendix summarizes the T10000 tape drive operator-panel indicator lights and display messages. Where applicable, this appendix recommends operator actions.

Messages

TABLE D-1 lists operator panel display messages, meanings, and recommended actions.

TABLE D-1 Operator Panel Display Messages

Display	Meaning	Recommended Action
* (asterisk)	The tape drive is online but a cartridge tape is not loaded.	Load a cartridge tape as required.
ASIA Diags	IPL diagnostics are running.	None
Bank n Bad	During boot, a section of memory was found bad.	IPL the tape drive. If the problem persists, contact authorized service personnel.
Boot Fail	The IPL failed.	IPL the tape drive again. If the problem persists, contact authorized service personnel.
BT Monitor	A sequence of switches accessed an engineering area.	IPL the tape drive.
CC Diags	IPL diagnostics are running.	None
Chk xxxx, where *xxxx* is an FSC	An operational failure occurred; the tape drive automatically performs an IPL.	Wait for the IPL to complete and retry the operation (see TABLE D-2 on page 101). If the problem persists, contact authorized service personnel.
Cleaning (*Cleaning*)	A cleaning cartridge is in the tape drive and is now cleaning.	None
*c*n*h*n*d*n*s*n (Hardware revision level supported by the firmware in this drive)	The tape drive firmware level is insufficient to control the tape drive hardware.	Contact authorized service personnel.

TABLE D-1 Operator Panel Display Messages (Continued)

Display	Meaning	Recommended Action
CodCrFail1	The tape drive cannot write code onto the data cartridge tape, or the tape drive cannot position the data cartridge tape.	Ensure that the tape is write-enabled, or try another cartridge tape.
CodCrFail2	The tape drive cannot read code from the data cartridge tape.	Retry the operation, or try another cartridge tape. If the problem persists, contact authorized service personnel.
CodeUpDate	The firmware in the tape drive is being updated from the host; the operator panel switches are locked.	None
CodUpFail1	The tape drive cannot read the data cartridge tape, or the tape drive cannot position the data cartridge tape.	Try another cartridge tape.
CodUpFail2	The EEPROM failed.	Contact authorized service personnel.
CodUpFail3	The tape drive cannot read code from the data cartridge tape.	Retry the operation, or try another cartridge tape. If the problem persists, contact authorized service personnel.
CodUpFail4	The data cartridge tape is not a code update cartridge tape.	Try another code update cartridge tape. If the problem persists, contact authorized service personnel.
DatCrFail1	The tape drive cannot create (reformat or reclaim) a cartridge tape.	Ensure that the data cartridge tape is write-enabled, or try to reformat the tape on another drive. If the problem persists, contact authorized service personnel.
DmpCrFail1	The tape drive cannot create (reformat or reclaim) a diagnostic dump tape.	Ensure that the data cartridge tape is write-enabled. If the problem persists, contact authorized service personnel.
DmpCrFail2	The tape drive cannot read the format of the data cartridge tape.	Retry the operation, or try another cartridge tape. If the problem persists, contact authorized service personnel.
DmpWrFail1	The tape drive cannot write diagnostic data onto the data cartridge tape, or the tape drive cannot position the data cartridge tape.	Contact authorized service personnel.

TABLE D-1 Operator Panel Display Messages (Continued)

Display	Meaning	Recommended Action
DmpWrFail2	There is no diagnostic dump data to process.	Contact authorized service personnel.
xxxx:Dmp y	Alternates with * (an asterisk) after completion of IPL, where *xxxx*=the FSC of last dump data collected and *Y*=number of uncollected dumps in non-volatile memory.	Contact authorized service personnel who accesses the diagnostic data and collects it to tape or to the host.
DumpAgain? alternating with Chk *xxxx*, where *xxxx* is an FSC. The Service indicator is flashing.	The tape drive detected the same error within a minute.	IPL the tape drive. If the problem persists, contact authorized service personnel.
DumpToHost	The dump or event log is being transferred to the host; operator panel switches are locked.	None
Exp ClCart	The cleaning cartridge is used up.	Replace the cleaning cartridge.
Fix CfgErr	The checksum does not match after an IPL.	Contact authorized service personnel.
Init *xxxx*. where *xxxx* is an FSC	An initialization error occurred.	Contact authorized service personnel.
IPL Pend	The IPL switch has been pressed.	None
Load CC	The common controller code is loading; IPL is proceeding.	None
Loading	A cartridge tape is loading.	None
Load *xxxx*, where *xxxx* is an FSC	The load or unload operation failed.	If the load failed, insert another cartridge tape. If it loads successfully, suspect the original tape. If another tape fails to load, IPL the tape drive. If the problem persists, contact authorized service personnel.
Load FIBRE	Fibre Channel firmware is loading; IPL is proceeding.	None
Locating	The tape drive is doing a high-speed seek.	None
Memory Err	The IPL failed.	IPL the tape drive again. If the problem persists, contact authorized service personnel.
NTReady F	A write-protected tape is in the process of a manual unload.	None

TABLE D-1 Operator Panel Display Messages (Continued)

Display	Meaning	Recommended Action
`NTReady U`	A write-enabled tape is in the process of a manual unload.	None
`Offline` alternating with *	The tape drive is offline.	None
`Online`	The tape drive is online.	None
`Power Fail`	The power supply failed.	Contact authorized service personnel.
`Reading`	The tape drive is reading data.	None
`Ready A`	The loaded cartridge tape is a VolSafe cartridge.	None
`Ready F`	The loaded cartridge tape is write-protected.	None
`Ready H`	The loaded higher density, non-VolSafe cartridge tape is ready and not file protected in a lower density drive.	Reload with a low-density cartridge or intentionally over-write from BOT. **Note –** High-density data cannot be read by a lower density drive.
`Ready L`	The loaded lower density, non-VolSafe cartridge tape is ready and not file protected in a higher density drive.	Use for read-only jobs or intentionally over-write from BOT. **Note –** Low-density data file can be read, but not revised by a higher density drive.
`Ready U`	The loaded cartridge tape is write-enabled (write-unprotected).	None
`Rewinding`	The tape drive is rewinding.	None
`Save Fails`	The new configuration cannot be saved because the read-access memory (RAM) might be defective.	This message is associated with changing the tape drive configuration, a task for authorized service personnel only.
`SavingDump`	A dump is being saved to non-volatile memory.	None
`Start Init`	Initialization has started.	None
`Trapped`	The IPL process is trapped in a loop.	IPL the tape drive again. If the problem persists, contact authorized service personnel.
`Unloading`	A cartridge tape is unloading.	None

TABLE D-1 Operator Panel Display Messages (Continued)

Display	Meaning	Recommended Action
`UnWr` *xxxx*, where *xxxx* is an FSC	The Unload switch was pressed during a write operation. Some data remains unwritten.	To write the unwritten data, issue the command: `ESCON Swap in VM/MVS` environment Or, Press the Unload switch again; the unwritten data is lost.
`Write Prot`	The tape drive attempted to write to a write-protected cartridge tape.	Change the switch on the data cartridge tape to enable writing.
`Writing`	The tape drive is writing data.	None

Potential Operator Recovery Scenarios

The following table contains Fault Symptom Codes (FSCs) that commonly result from an operator error. The first column in the table lists an operator panel message at the time of the error event. The description column provides insight into the error condition from which you should be able to determine a recovery action.

TABLE D-2 Selected Check Message Meanings

Message	Description
`CHK 6109`	This drive does not contain the key needed to decrypt this tape. The ID of the missing key can be viewed from this drive using the VOP program.
`CHK A33A`	The user requested a motion operation that requires a tape to be installed, however, a tape has not been loaded.
`CHK A34C`	The user requested a write operation that requires a tape to be installed, however, a tape has not been loaded.
`CHK A3FB`	A format override tape write operation failed. The failure may not be serious. Error recovery was not invoked for the failure. Re-attempting the test may resolve this issue.
`CHK A733`	The operator or library inserted a write protected tape into the drive while in a menu selected create tape mode. If the write protect switch on the cartridge is moved to the unlocked position, operation will work.

Translated Messages

TABLE D-3 lists operator panel display messages selected for translation. These messages appear in the language selected by the drive configuration language selection submenu.

Note – See TABLE 4-1 on page 63 for language selection guidelines.

TABLE D-3 Translated Display Messages

English	Espanol	Francais	Italiano	Deutsch
Cleaning	*LIMPIEZA*	*NETTOYAGE	*PULIZIA*	*REINIGEN*
Erasing	*BORRANDO*	EFFACEMENT	*CANCELLA*	*LOESCHEN*
Locating	Localizar	Recherche	Ricerca	Suchen
Loading	Cargando	Chargement	Carico	Laden
NT Ready F	No Listo A	NPret F	No Prnt F	N Bereit F
NT Ready U	No Listo U	NPret U	No Prnt U	N Bereit U
Ready A	Listo A	Pret A	Pronto A	Bereit A
Ready F	Listo F	Pret F	Pronto F	Bereit F
Ready H	Listo H	Pret H	Pronto H	Bereit H
Ready L	Listo L	Pret L	Pronto L	Bereit L
Ready U	Listo U	Pret U	Pronto U	Bereit U
Rewinding	Rebobinar	Rebobinage	Riavvolgi	Spulen
Unloading	Descarga	Dechargemt	Scarico	Entladen

E

Specifications

This appendix lists the physical, power, and performance specifications; and, environmental requirements for the T10000 tape drive and tape cartridge.

Physical Specifications (Drive)

TABLE E-1 lists the physical specifications of Oracle's StorageTek T10000 tape drive.

TABLE E-1 Tape Drive Physical Specifications

Measurement	Specification
Width	14.7 cm (5.77 inches) drive, 48.3 cm (19 inches) rackmount tray
Depth	43.3 cm (17 inches) T10000A/B drive [includes cartridge bezel and D connector]
	42.7 cm (16.8 inches) T10000C drive [includes cartridge bezel and SFP modules]
	64 cm (25 inches) rackmount tray
Height	8.1 cm (3.2 inches), 17.8 cm (7 inches) rackmount tray
Weight (with drive tray)	
SL8500	9.4 kg (20.75 pounds)
SL3000	10.1 kg (22.25 pounds)
L-Series (T10000A/B only)	8.3 kg (18.3 pounds)
9310 (T10000A only)	6.9 kg (15.25 pounds)

Physical Specifications (Tape Cartridge)

T10000 tape cartridge physical specifications:

Height: 2.45 centimeters (0.96 inches)

Width: 10.9 centimeters (4.29 inches)

Length: 12.5 centimeters (4.92 inches)

Media length:

- 917 meters (3,009 feet) [recordable 855 m (2,805 feet)] for the T10000A/B cartridge
- 1,147 meters (3,763 feet) [recordable 1107 m (3,632 feet)] for the T10000C cartridge

Media thickness:

- 6.5 microns (µm) for the T10000A/B cartridge
- 5.2 microns (µm) for the T10000C cartridge

Nominal weights:

- T10000A/B cartridge:
  - Standard data cartridge: 262.5 grams (0.59 pound)
  - Sport data cartridge: 187.0 grams (0.41 pound)
  - Cleaning cartridge: 196.3 grams (0.433 pound)
- T10000C cartridge:
  - Standard data cartridge: 270 grams (0.595 pound)
  - Sport data cartridge: 191 grams (0.42 pound)
  - Cleaning cartridge: 196.3 grams (0.433 pound)

Power Specifications

This section lists power specifications for tape drives.

Rack Mount Tape Drive Power Specifications

TABLE E-2 lists the input power and current requirement for each tape drive power supply in the rack mount assembly under nominal conditions at various input voltages. Nominal conditions occur when the tape drive is moving tape in read/write and rewind modes.

TABLE E-2 Tape Drive Power Supply Input Power

Input Voltage	Power in Watts	Input Current (mA)
60 Hz		
90 V	172.3	1786
100 V	161.4	1612
240 V	161.3	691
254 V	168.2	649
50 Hz		
90 V	166.3	1767
100 V	163.2	1570
240 V	156.4	678
254 V	156.2	633

Note – The tape drive draws the same power from the power supply regardless of the AC input voltage.

For the purposes of figuring the amount of heat generated by a tape drive *and* its associated power supply, use the figure of 172.3 watts, which converts to approximately 588 Btu/hr. Because there are usually two tape drives in a rack mount unit, these figures are doubled for a complete rack mounted pair of tape drives, or 244.6 watts, which converts to 1,176 Btu/hr.

Library-attached Tape Drive Power Specifications

For SL3000 and SL8500 libraries, use the power figure of 100 watts for each tape drive and its associated power supply and use a heat figure of 341.29 Btu/hr.

For other libraries, use the power specifications for a single rack mount tape drive and power supply. In those libraries, there is one AC/DC power supply for each tape drive.

T10000C Power

The T10000C uses approximately 25% less power than the T10000A because of power management including hibernate mode, low power modes, and power reduction during normal operation.

> **Note –** The external interfaces remain active during all power management modes.

Performance Specifications

Capacity and Performance:

- Capacity, native

  T10000A: 500 GB (5×10^{11} bytes)

  T10000B: 1 TB (1×10^{12} bytes)

  T10000C: 5 TB (5×10^{12} bytes)

- Capacity (Sport Cartridge)

  T10000A: 120 GB

  T10000B: 240 GB

  T10000C: 1 TB (1×10^{12} bytes)

- Data buffer size

  T10000A/B: 256 MB

  T10000C: 2 GB

- Tape speeds:
  - Read and Write

    T10000A: 2.0 and 4.95 meters/second

    T10000B:

    T10000B-formatted cartridges: 2.0 and 3.74 meters/second

    T10000A-formatted cartridges: 2.0 and 4.95 meters/second

    T10000C: 5.62 meters/second
  - File search and locates:

    T10000A/B: 8.0 – 12 meters/second (varying speeds)

    T10000C: 10 – 13 meters/second (varying speeds)
  - High speed rewind:

    T10000A/B: 8.0 – 12 meters/second (varying speeds)

    T10000C: 10 – 13 meters/second (varying speeds)

Interfaces:

- Types:

  T10000A: 2 gigabit/4 gigabit Fibre Channel and FICON

  T10000B/C: 4 gigabit Fibre Channel and FICON

- Data rate:

  T10000A/B: 120 megabytes/second

  T10000C: 240 megabytes/second

Access times:

- Tape load and thread to ready

  T10000A/B: 16.5 seconds

  T10000C: 13.1 seconds

- File access, average (includes loading)

  T10000A/B: 62.5 seconds (30.5 seconds for Sport Cartridge)

  T10000C: 73.5 seconds (34 seconds for Sport Cartridge)

- Rewind (maximum):

  T10000A/B: 91 seconds (23 seconds for Sport Cartridge)

  T10000C: 115 seconds (32.5 seconds for Sport Cartridge)

- Unload time: 23 seconds

Reliability:

- Head life: 5 years
- Uncorrected bit error rate: 1×10^{-19}
- Undetected bit error rate: 1×10^{-23}

Environmental Requirements

This section lists the environmental requirements for the T10000 tape drive, and the T10000 tape cartridge.

> **Note –** Industry best practices recommends computer rooms maintain a relative humidity of 40% to 50% for best performance.

Tape Drive Environmental Requirements

Temperature:

- Operating:
  - Optimal: 22°C (72°F)
  - Recommended: 20° – 25°C (68° – 77°F)
  - Ranges: 15.6° to 32.2°C (60° to 90°F) - dry bulb
- Shipping:
  - Optimal: 22°C (72°F)
  - Recommended: 20° – 25°C (68° – 77°F)
  - Ranges: -40° to 60°C (-40° to 140°F)
- Storing:
  - Optimal: 22°C (72°F)
  - Recommended: 20° – 25°C (68° – 77°F)
  - Ranges: 10° to 40°C (50° to 104°F) - dry bulb

Relative Humidity:

- Operating:
  - Optimal: 45%
  - Recommended: 40% – 50%
  - Ranges: 20% to 80%
- Shipping: 10% to 95%
  - Optimal: 45%
  - Recommended: 40% – 50%
  - Ranges: 10% to 95%
- Storing:
  - Optimal: 45%
  - Recommended: 40% – 50%
  - Ranges: 10% to 95%

Wet bulb (non-condensing):

- Operating: 29.2°C (84.5°F)
- Shipping: 35°C (95°F)
- Storing: 35°C (95°F)

Although the tape drive functions over the full list of ranges as specified previously, *optimal reliability* is achieved if the environment is maintained between the optimum and recommended ranges.

Tape Cartridge Environmental Requirements

Note – The acclimation time before use is 72 hours. (See "Guidelines for Handling" on page 87.)

Note – The shipping environment must not exceed the limit of the storage environment, archive or non-archive, for longer than 10 days.

The T10000 tape cartridge environmental requirements follow:

Temperature:

Operating: 10° to 45°C (50° to 113°F)

Storage (up to four weeks): 10° to 32°C (50° to 90°F)

Storage (archival): 15° to 26°C (59° to 79°F)

Shipping: -23° to 49°C (-9° to 120°F)

Relative Humidity, Non-condensing:

Operating: 20% to 80%

Storage (up to four weeks): 5% to 80%

Storage (archival): 15% to 50%

Shipping: 5% to 80%

Wet Bulb Maximum:

Operating: 26°C (79°F)

Storage (nonarchive): 26°C (79°F)

Storage (archival): 26°C (79°F)

Shipping: 26°C (79°F) with no condensation

Airborne Contamination

Tape drives and media are subject to damage from airborne particles. The operating environment must adhere to the requirements listed in Appendix F, "Controlling Contaminants".

F

Controlling Contaminants

Environmental Contaminants

Control over contaminant levels in a computer room is extremely important because tape libraries, tape drives, and tape media are subject to damage from airborne particulates. Most particles smaller than ten microns are not visible to the naked eye under most conditions, but these particles can be the most damaging. As a result, the operating environment must adhere to the following requirements:

- ISO 14644-1 Class 8 Environment
- The total mass of airborne particulates must be less than or equal to 200 micrograms per cubic meter
- Severity level G1 per ANSI/ISA 71.04-1985

Oracle currently requires the ISO 14644-1 standard approved in 1999, but will require any updated standards for ISO 14644-1 as they are approved by the ISO governing body. The ISO 14644-1 standard primarily focuses on the quantity and size of particulates as well as the proper measurement methodology, but does not address the overall mass of the particulates. As a result, the requirement for total mass limitations is also necessary as a computer room or data center could meet the ISO 14644-1 specification, but still damage equipment because of the specific type of particulates in the room. In addition, the ANSI/ISA 71.04-1985 specification addresses gaseous contaminations as some airborne chemicals are more hazardous. All three requirements are consistent with the requirements set by other major tape storage vendors.

Required Air Quality Levels

Particles, gasses and other contaminants may impact the sustained operations of computer hardware. Effects can range from intermittent interference to actual component failures. The computer room must be designed to achieve a high level of cleanliness. Airborne dusts, gasses and vapors must be maintained within defined limits to help minimize their potential impact on the hardware.

Airborne particulate levels must be maintained within the limits of *ISO 14644-1 Class 8 Environment*. This standard defines air quality classes for clean zones based on airborne particulate concentrations. This standard has an order of magnitude less particles than standard air in an office environment. Particles ten microns or smaller are harmful to most data processing hardware because they tend to exist in large

numbers, and can easily circumvent many sensitive components' internal air filtration systems. When computer hardware is exposed to these submicron particles in great numbers they endanger system reliability by posing a threat to moving parts, sensitive contacts and component corrosion.

Excessive concentrations of certain gasses can also accelerate corrosion and cause failure in electronic components. Gaseous contaminants are a particular concern in a computer room both because of the sensitivity of the hardware, and because a proper computer room environment is almost entirely recirculating. Any contaminant threat in the room is compounded by the cyclical nature of the airflow patterns. Levels of exposure that might not be concerning in a well ventilated site repeatedly attack the hardware in a room with recirculating air. The isolation that prevents exposure of the computer room environment to outside influences can also multiply any detrimental influences left unaddressed in the room.

Gasses that are particularly dangerous to electronic components include chlorine compounds, ammonia and its derivatives, oxides of sulfur and petrol hydrocarbons. In the absence of appropriate hardware exposure limits, health exposure limits must be used.

While the following sections will describe some best practices for maintaining an ISO 14644-1 Class 8 Environment in detail, there are some basic precautions that must be adhered to:

- Do not allow food or drink into the area
- Cardboard, wood, or packing materials must not be stored in the data center clean area
- Identify a separate area for unpacking new equipment from crates and boxes
- Do not allow construction or drilling in the data center without first isolating sensitive equipment and any air targeted specifically for the equipment. Construction generates a high level of particulates that exceed ISO 14644-1 Class 8 criteria in a localized area. Dry wall and gypsum are especially damaging to storage equipment.

Contaminant Properties and Sources

Contaminants in the room can take many forms, and can come from numerous sources. Any mechanical process in the room can produce dangerous contaminants or agitate settled contaminants. A particle must meet two basic criteria to be considered a contaminant:

- It must have the physical properties that could potentially cause damage to the hardware
- It must be able to migrate to areas where it can cause the physical damage

The only differences between a potential contaminant and an actual contaminant are time and location. Particulate matter is most likely to migrate to areas where it can do damage if it is airborne. For this reason, airborne particulate concentration is a useful measurement in determining the quality of the computer room environment. Depending on local conditions, particles as big as 1,000 microns can become airborne, but their active life is very short, and they are arrested by most filtration devices.

Submicron particulates are much more dangerous to sensitive computer hardware, because they remain airborne for a much longer period of time, and they are more apt to bypass filters.

Operator Activity

Human movement within the computer space is probably the single greatest source of contamination in an otherwise clean computer room. Normal movement can dislodge tissue fragments, such as dander or hair, or fabric fibers from clothing. The opening and closing of drawers or hardware panels or any metal-on-metal activity can produce metal filings. Simply walking across the floor can agitate settled contamination making it airborne and potentially dangerous.

Hardware Movement

Hardware installation or reconfiguration involves a great deal of subfloor activity, and settled contaminants can very easily be disturbed, forcing them to become airborne in the supply air stream to the room's hardware. This is particularly dangerous if the subfloor deck is unsealed. Unsealed concrete sheds fine dust particles into the airstream, and is susceptible to efflorescence -- mineral salts brought to the surface of the deck through evaporation or hydrostatic pressure.

Outside Air

Inadequately filtered air from outside the controlled environment can introduce innumerable contaminants. Post-filtration contamination in duct work can be dislodged by air flow, and introduced into the hardware environment. This is particularly important in a downward-flow air conditioning system in which the sub-floor void is used as a supply air duct. If the structural deck is contaminated, or if the concrete slab is not sealed, fine particulate matter (such as concrete dust or efflorescence) can be carried directly to the room's hardware.

Stored Items

Storage and handling of unused hardware or supplies can also be a source of contamination. Corrugated cardboard boxes or wooden skids shed fibers when moved or handled. Stored items are not only contamination sources; their handling in the computer room controlled areas can agitate settled contamination already in the room.

Outside Influences

A negatively pressurized environment can allow contaminants from adjoining office areas or the exterior of the building to infiltrate the computer room environment through gaps in the doors or penetrations in the walls. Ammonia and phosphates are often associated with agricultural processes, and numerous chemical agents can be produced in manufacturing areas. If such industries are present in the vicinity of the data center facility, chemical filtration may be necessary. Potential impact from automobile emissions, dusts from local quarries or masonry fabrication facilities or sea mists should also be assessed if relevant.

Cleaning Activity

Inappropriate cleaning practices can also degrade the environment. Many chemicals used in normal or “office” cleaning applications can damage sensitive computer equipment. Potentially hazardous chemicals outlined in the “Cleaning Procedures and Equipment” section should be avoided. Out-gassing from these products or direct contact with hardware components can cause failure. Certain biocide treatments used in building air handlers are also inappropriate for use in computer rooms either because they contain chemicals, that can degrade components, or because they are not designed to be used in the airstream of a re-circulating air system. The use of push mops or inadequately filtered vacuums can also stimulate contamination.

It is essential that steps be taken to prevent air contaminants, such as metal particles, atmospheric dust, solvent vapors, corrosive gasses, soot, airborne fibers or salts from entering or being generated within the computer room environment. In the absence of hardware exposure limits, applicable human exposure limits from OSHA, NIOSH or the ACGIH should be used.

Contaminant Effects

Destructive interactions between airborne particulate and electronic instrumentation can occur in numerous ways. The means of interference depends on the time and location of the critical incident, the physical properties of the contaminant and the environment in which the component is placed.

Physical Interference

Hard particles with a tensile strength at least 10% greater than that of the component material can remove material from the surface of the component by grinding action or embedding. Soft particles will not damage the surface of the component, but can collect in patches that can interfere with proper functioning. If these particles are tacky they can collect other particulate matter. Even very small particles can have an impact if they collect on a tacky surface, or agglomerate as the result of electrostatic charge build-up.

Corrosive Failure

Corrosive failure or contact intermittence due to the intrinsic composition of the particles or due to absorption of water vapor and gaseous contaminants by the particles can also cause failures. The chemical composition of the contaminant can be very important. Salts, for instance, can grow in size by absorbing water vapor from the air (nucleating). If a mineral salts deposit exists in a sensitive location, and the environment is sufficiently moist, it can grow to a size where it can physically interfere with a mechanism, or can cause damage by forming salt solutions.

Shorts

Conductive pathways can arise through the accumulation of particles on circuit boards or other components. Many types of particulate are not inherently conductive, but can absorb significant quantities of water in high-moisture environments. Problems caused by electrically conductive particles can range from intermittent malfunctioning to actual damage to components and operational failures.

Thermal Failure

Premature clogging of filtered devices will cause a restriction in air flow that could induce internal overheating and head crashes. Heavy layers of accumulated dust on hardware components can also form an insulative layer that can lead to heat-related failures.

Room Conditions

All surfaces within the controlled zone of the data center should be maintained at a high level of cleanliness. All surfaces should be periodically cleaned by trained professionals on a regular basis, as outlined in the "Cleaning Procedures and Equipment" section. Particular attention should be paid to the areas beneath the hardware, and the access floor grid. Contaminants near the air intakes of the hardware can more easily be transferred to areas where they can do damage. Particulate accumulations on the access floor grid can be forced airborne when floor tiles are lifted to gain access to the sub-floor.

The subfloor void in a downward-flow air conditioning system acts as the supply air plenum. This area is pressurized by the air conditioners, and the conditioned air is then introduced into the hardware spaces through perforated floor panels. Thus, all air traveling from the air conditioners to the hardware must first pass through the subfloor void. Inappropriate conditions in the supply air plenum can have a dramatic effect on conditions in the hardware areas.

The subfloor void in a data center is often viewed solely as a convenient place to run cables and pipes. It is important to remember that this is also a duct, and that conditions below the false floor must be maintained at a high level of cleanliness. Contaminant sources can include degrading building materials, operator activity or infiltration from outside the controlled zone. Often particulate deposits are formed where cables or other subfloor items form air dams that allow particulate to settle and accumulate. When these items are moved, the particulate is re-introduced into the supply airstream, where it can be carried directly to hardware.

Damaged or inappropriately protected building materials are often sources of subfloor contamination. Unprotected concrete, masonry block, plaster or gypsum wall-board will deteriorate over time, shedding fine particulate into the air. Corrosion on post-filtration air conditioner surfaces or subfloor items can also be a concern. The subfloor void must be thoroughly and appropriately decontaminated on a regular basis to address these contaminants. Only vacuums equipped with High Efficiency Particulate Air (HEPA) filtration should be used in any decontamination procedure. Inadequately filtered vacuums will not arrest fine particles, passing them through the unit at high speeds, and forcing them airborne.

Unsealed concrete, masonry or other similar materials are subject to continued degradation. The sealants and hardeners normally used during construction are often designed to protect the deck against heavy traffic, or to prepare the deck for the application of flooring materials, and are not meant for the interior surfaces of a supply air plenum. While regular decontaminations will help address loose particulate, the surfaces will still be subject to deterioration over time, or as subfloor activity causes wear. Ideally all of the subfloor surfaces will be appropriately sealed at the time of construction. If this is not the case, special precautions will be necessary to address the surfaces in an on-line room.

It is extremely important that only appropriate materials and methodology are used in the encapsulation process. Inappropriate sealants or procedures can actually degrade the conditions they are meant to improve, impacting hardware operations and reliability. The following precautions should be taken when encapsulating the supply air plenum in an on-line room.

- Manually apply the encapsulant. Spray applications are totally inappropriate in an on-line data center. The spraying process forces the sealant airborne in the supply airstream, and is more likely to encapsulate cables to the deck.
- Use a pigmented encapsulant. The pigmentation makes the encapsulant visible in application, ensuring thorough coverage, and helps in identifying areas that are damaged or exposed over time.
- It must have a high flexibility and low porosity in order to effectively cover the irregular textures of the subject area, and to minimize moisture migration and water damage.
- The encapsulant must not out-gas any harmful contaminants. Many encapsulants commonly used in industry are highly ammoniated or contain other chemicals that can be harmful to hardware. It is very unlikely that this out-gassing could cause immediate, catastrophic failure, but these chemicals will often contribute to corrosion of contacts, heads or other components.

Effectively encapsulating a subfloor deck in an on-line computer room is a very sensitive and difficult task, but it can be conducted safely if appropriate procedures and materials are used. Avoid using the ceiling void as an open supply or return for the building air system. This area is typically very dirty and difficult to clean. Often the structural surfaces are coated with fibrous fire-proofing, and the ceiling tiles and insulation are also subject to shedding. Even prior to filtration, this is an unnecessary exposure that can adversely affect environmental conditions in the room. It is also important that the ceiling void does not become pressurized, as this will force dirty air into the computer room. Columns or cable chases with penetrations in both the subfloor and ceiling void can lead to ceiling void pressurization.

Exposure Points

All potential exposure points in the data center should be addressed to minimize potential influences from outside the controlled zone. Positive pressurization of the computer rooms will help limit contaminant infiltration, but it is also important to minimize any breaches in the room perimeter. To ensure the environment is maintained correctly, the following should be considered:

- All doors should fit snugly in their frames.
- Gaskets and sweeps can be used to address any gaps.

- Automatic doors should be avoided in areas where they can be accidentally triggered. An alternate means of control would be to remotely locate a door trigger so that personnel pushing carts can open the doors easily. In highly sensitive areas, or where the data center is exposed to undesirable conditions, it may be advisable to design and install personnel traps. Double sets of doors with a buffer between can help limit direct exposure to outside conditions.
- Seal all penetrations between the data center and adjacent areas.
- Avoid sharing a computer room ceiling or subfloor plenum with loosely controlled adjacent areas.

Filtration

Filtration is an effective means of addressing airborne particulate in a controlled environment. It is important that all air handlers serving the data center are adequately filtered to ensure appropriate conditions are maintained within the room. In-room process cooling is the recommended method of controlling the room environment. The in-room process coolers re-circulate room air. Air from the hardware areas is passed through the units where it is filtered and cooled, and then introduced into the subfloor plenum. The plenum is pressurized, and the conditioned air is forced into the room, through perforated tiles, and then travels back to the air conditioner for reconditioning. The airflow patterns and design associated with a typical computer room air handler have a much higher rate of air change than typical comfort cooling air conditioners so air is filtered much more often than in an office environment. Proper filtration can capture a great deal of particulates. The filters installed in the in-room, re-circulating air conditioners should have a minimum efficiency of 40% (Atmospheric Dust-Spot Efficiency, ASHRAE Standard 52.1). Low-grade pre-filters should be installed to help prolong the life of the more expensive primary filters.

Any air being introduced into the computer room controlled zone, for ventilation or positive pressurization, should first pass through high efficiency filtration. Ideally, air from sources outside the building should be filtered using High Efficiency Particulate Air (HEPA) filtration rated at 99.97% efficiency (DOP Efficiency MILSTD-282) or greater. The expensive high efficiency filters should be protected by multiple layers of pre-filters that are changed on a more frequent basis. Low-grade pre-filters, 20% ASHRAE atmospheric dust-spot efficiency, should be the primary line of defense. The next filter bank should consist of pleated or bag type filters with efficiencies between 60% and 80% ASHRAE atmospheric dust-spot efficiency.

ASHRAE 52-76	**Fractional Efficiencies %**		
Dust spot efficiency %	**3.0 micron**	**1.0 micron**	**0.3 micron**
25-30	80	20	<5
60-65	93	50	20
80-85	99	90	50
90	>99	92	60
DOP 95	--	>99	95

Low efficiency filters are almost totally ineffective at removing sub-micron particulates from the air. It is also important that the filters used are properly sized for the air handlers. Gaps around the filter panels can allow air to bypass the filter as it passes through the air conditioner. Any gaps or openings should be filled using appropriate materials, such as stainless steel panels or custom filter assemblies.

Positive Pressurization and Ventilation

A designed introduction of air from outside the computer room system will be necessary in order to accommodate positive pressurization and ventilation requirements. The data center should be designed to achieve positive pressurization in relation to more loosely controlled surrounding areas. Positive pressurization of the more sensitive areas is an effective means of controlling contaminant infiltration through any minor breaches in the room perimeter. Positive pressure systems are designed to apply outward air forces to doorways and other access points within the data processing center in order to minimize contaminant infiltration of the computer room. Only a minimal amount of air should be introduced into the controlled environment. In data centers with multiple rooms, the most sensitive areas should be the most highly pressurized. It is, however, extremely important that the air being used to positively pressurize the room does not adversely affect the environmental conditions in the room. It is essential that any air introduction from outside the computer room is adequately filtered and conditioned to ensure that it is within acceptable parameters. These parameters can be looser than the goal conditions for the room since the air introduction should be minimal. A precise determination of acceptable limits should be based on the amount of air being introduced and the potential impact on the environment of the data center.

Because a closed-loop, re-circulating air conditioning system is used in most data centers, it will be necessary to introduce a minimal amount of air to meet the ventilation requirements of the room occupants. Data center areas normally have a very low human population density, thus the air required for ventilation will be minimal. In most cases, the air needed to achieve positive pressurization will likely exceed that needed to accommodate the room occupants. Normally, outside air quantities of less than 5% make-up air should be sufficient (ASHRAE Handbook: Applications, Chapter 17). A volume of 15 CFM outside air per occupant or workstation should sufficiently accommodate the ventilation needs of the room.

Cleaning Procedures and Equipment

Even a perfectly designed data center will require continued maintenance. Data centers containing design flaws or compromises may require extensive efforts to maintain conditions within desired limits. Hardware performance is an important factor contributing to the need for a high level of cleanliness in the data center.

Operator awareness is another consideration. Maintaining a fairly high level of cleanliness will raise the level of occupant awareness with respect to special requirements and restrictions while in the data center. Occupants or visitors to the data center will hold the controlled environment in high regard and are more likely to act appropriately. Any environment that is maintained to a fairly high level of cleanliness and is kept in a neat and well organized fashion will also command respect from the room's inhabitants and visitors. When potential clients visit the room they will interpret the overall appearance of the room as a reflection of an

overall commitment to excellence and quality. An effective cleaning schedule must consist of specially designed short-term and long-term actions. These can be summarized as follows:

Frequency	Task
Daily Actions	Rubbish removal
Weekly Actions	Access floor maintenance (vacuum and damp mop)
Quarterly Actions	Hardware decontamination
	Room surface decontamination
Bi-Annual Actions	Subfloor void decontamination
	Air conditioner decontamination (as necessary)

Daily Tasks

This statement of work focuses on the removal of each day's discarded trash and rubbish from the room. In addition, daily floor vacuuming may be required in Print Rooms or rooms with a considerable amount of operator activity.

Weekly Tasks

This statement of work focuses on the maintenance of the access floor system. During the week, the access floor becomes soiled with dust accumulations and blemishes. The entire access floor should be vacuumed and damp mopped. All vacuums used in the data center, for any purpose, should be equipped with High Efficiency Particulate Air (HEPA) filtration. Inadequately filtered equipment cannot arrest smaller particles, but rather simply agitates them, degrading the environment they were meant to improve. It is also important that mop-heads and dust wipes are of appropriate non-shedding designs.

Cleaning solutions used within the data center must not pose a threat to the hardware. Solutions that could potentially damage hardware include products that are:

- Ammoniated
- Chlorine-based
- Phosphate-based
- Bleach enriched
- Petro-chemical based
- Floor strippers or re-conditioners.

It is also important that the recommended concentrations are used, as even an appropriate agent in an inappropriate concentration can be potentially damaging. The solution should be maintained in good condition throughout the project, and excessive applications should be avoided.

Quarterly Tasks

The quarterly statement of work involves a much more detailed and comprehensive decontamination schedule and should only be conducted by experienced computer room contamination-control professionals. These actions should be performed three to four times per year, based on the levels of activity and contamination present. All room surfaces should be thoroughly decontaminated including cupboards, ledges, racks, shelves and support equipment. High ledges and light fixtures and generally accessible areas should be treated or vacuumed as appropriate. Vertical surfaces including windows, glass partitions, doors, etc. should be thoroughly treated. Special dust cloths that are impregnated with a particle absorbent material are to be used in the surface decontamination process. Do not use generic dust rags or fabric cloths to perform these activities. Do not use any chemicals, waxes or solvents during these activities.

Settled contamination should be removed from all exterior hardware surfaces including horizontal and vertical surfaces. The unit's air inlet and outlet grilles should be treated as well. Do not wipe the unit's control surfaces as these areas can be decontaminated by the use of lightly compressed air. Special care should also be taken when cleaning keyboards and life-safety controls. Specially treated dust wipes should be used to treat all hardware surfaces. Monitors should be treated with optical cleansers and static-free cloths. No Electro-Static Discharge (ESD) dissipative chemicals should be used on the computer hardware, since these agents are caustic and harmful to most sensitive hardware. The computer hardware is sufficiently designed to permit electrostatic dissipation thus no further treatments are required. After all of the hardware and room surfaces have been thoroughly decontaminated, the access floor should be HEPA vacuumed and damp mopped as detailed in the Weekly Actions.

Bi-Annual Tasks

The subfloor void should be decontaminated every 18 months to 24 months based on the conditions of the plenum surfaces and the degree of contaminant accumulation. Over the course of the year, the subfloor void undergoes a considerable amount of activity that creates new contamination accumulations. Although the weekly above floor cleaning activities will greatly reduce the subfloor dust accumulations, a certain amount of surface dirt will migrate into the subfloor void. It is important to maintain the subfloor to a high degree of cleanliness since this area acts as the hardware's supply air plenum. It is best to perform the subfloor decontamination treatment in a short time frame to reduce cross contamination. The personnel performing this operation should be fully trained to assess cable connectivity and priority. Each exposed area of the subfloor void should be individually inspected and assessed for possible cable handling and movement. All twist-in and plug-in connections should be checked and fully engaged before cable movement. All subfloor activities must be conducted with proper consideration for air distribution and floor loading. In an effort to maintain access floor integrity and proper psychrometric conditions, the number of floor tiles removed from the floor system should be carefully managed. In most cases, each work crew should have no more than 24 square feet (six tiles) of open access flooring at any one time. The access floor's supporting grid system should also be thoroughly decontaminated, first by vacuuming the loose debris and then by damp-sponging the accumulated residue. Rubber gaskets, if present, as the metal framework that makes up the grid system should be removed from the grid

work and cleaned with a damp sponge as well. Any unusual conditions, such as damaged floor suspension, floor tiles, cables and surfaces, within the floor void should be noted and reported.

Activity and Processes

Isolation of the data center is an integral factor in maintaining appropriate conditions. All unnecessary activity should be avoided in the data center, and access should be limited to necessary personnel only. Periodic activity, such as tours, should be limited, and traffic should be restricted to away from the hardware so as to avoid accidental contact. All personnel working in the room, including temporary employees and janitorial personnel, should be trained in the most basic sensitivities of the hardware so as to avoid unnecessary exposure. The controlled areas of the data center should be thoroughly isolated from contaminant producing activities. Ideally, print rooms, check sorting rooms, command centers or other areas with high levels of mechanical or human activity should have no direct exposure to the data center. Paths to and from these areas should not necessitate traffic through the main data center areas.

G

Third-Party Software Licenses

T10000C_THIRDPARTYLICENSEREADME.txt

DO NOT TRANSLATE OR LOCALIZE.

==========

- TABLE OF CONTENTS -

==========

==========

I. COMPONENTS

==========

The following software (or certain identified files distributed with the software) may be included in this product. Unless otherwise specified, the software identified in this file is licensed under the licenses described below.

The disclaimers and copyright notices provided are based on information made available to Oracle by the third party licensors listed.

==========

AES and Combined Encryption/Authentication Modes

==========

This code implements the CCM combined encryption a
Use of any of this software is governed by the terms of the license below:
Copyright (c) 2003, Dr Brian Gladman, Worcester, UK. All rights reserved.

LICENSE TERMS

The free distribution and use of this software in both source and binary form is allowed (with or without changes) provided that:

1. distributions of this source code include the above copyright notice, this list of conditions and the following disclaimer;

2. distributions in binary form include the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other associated materials;

3. the copyright holder's name is not used to endorse products built using this software without specific written permission.

ALTERNATIVELY, provided that this notice is retained in full, this product may be distributed under the terms of the GNU General Public License (GPL), in which case the provisions of the GPL apply INSTEAD OF those given above.

DISCLAIMER

This software is provided 'as is' with no explicit or implied warranties in respect of its properties, including, but not limited to, correctness

and/or fitness for purpose.

Issue Date: 26/08/2003

==========

gsoap Public License v1.3

==========

"Part of the software embedded in this product is gSOAP software.

Portions created by gSOAP are Copyright (C) 2001-2009 Robert A. van Engelen, Genivia inc. All Rights Reserved.

THE SOFTWARE IN THIS PRODUCT WAS IN PART PROVIDED BY GENIVIA INC AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE."

You are receiving a copy of the gSOAP program. The terms of the Oracle license do NOT apply to the gSOAP program; it is licensed under the following license, separately from the Oracle programs you receive.

gSOAP Public License

Version 1.3b

The gSOAP public license is derived from the Mozilla Public License (MPL1.1). The sections that were deleted from the original MPL1.1 text are 1.0.1, 2.1.(c),(d), 2.2.(c),(d), 8.2.(b), 10, and 11. Section 3.8 was added. The modified sections are 2.1.(b), 2.2.(b), 3.2 (simplified), 3.5 (deleted the last sentence), and 3.6 (simplified).

This license applies to the gSOAP software package, with the exception of the soapcpp2 and wsdl2h source code located in gsoap/src and gsoap/wsdl, all code generated by soapcpp2 and wsdl2h, the UDDI source code gsoap/uddi2, and the

Web server sample source code samples/webserver. To use any of these software tools and components commercially, a commercial license is required and can be obtained from www.genivia.com.

1 DEFINITIONS.

1.0.1.

1.1. “Contributor”

means each entity that creates or contributes to the creation of Modifications.

1.2. “Contributor Version”

means the combination of the Original Code, prior Modifications used by a Contributor, and the Modifications made by that particular Contributor.

1.3. “Covered Code”

means the Original Code, or Modifications or the combination of the Original Code, and Modifications, in each case including portions thereof.

1.4. “Electronic Distribution Mechanism”

means a mechanism generally accepted in the software development community for the electronic transfer of data.

1.5. “Executable”

means Covered Code in any form other than Source Code.

1.6. “Initial Developer”

means the individual or entity identified as the Initial Developer in the Source Code notice required by Exhibit A.

1.7. “Larger Work”

means a work which combines Covered Code or portions thereof with code not governed by the terms of this License.

1.8. “License”

means this document.

1.8.1. “Licensable”

means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently acquired, any and all of the rights conveyed herein.

1.9. “Modifications”

means any addition to or deletion from the substance or structure of either the Original Code or any previous Modifications. When Covered Code is released as a series of files, a Modification is:

A.

Any addition to or deletion from the contents of a file containing Original Code or previous Modifications.

B.

Any new file that contains any part of the Original Code, or previous Modifications.

1.10. “Original Code”

means Source Code of computer software code which is described in the Source Code notice required by Exhibit A as Original Code, and which, at the time of its release under this License is not already Covered Code governed by this License.

1.10.1. “Patent Claims”

means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent Licensable by grantor.

1.11. “Source Code”

means the preferred form of the Covered Code for making modifications to it, including all modules it contains, plus any associated interface definition files, scripts used to control compilation and installation of an Executable, or source code differential comparisons against either the Original Code or another well known, available Covered Code of the Contributor’s choice. The Source Code can be in a compressed or archival form, provided the appropriate decompression or de-archiving software is widely available for no charge.

1.12. “You” (or “Your”)

means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License or a future version of this License issued under Section 6.1. For legal entities, “You” includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, “control” means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2 SOURCE CODE LICENSE.

2.1. The Initial Developer Grant.

The Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license, subject to third party intellectual property claims:

(a)

under intellectual property rights (other than patent or trademark) Licensable by Initial Developer to use, reproduce, modify, display, perform, sublicense and distribute the Original Code (or portions thereof) with or without Modifications, and/or as part of a Larger Work; and

(b)

under patents now or hereafter owned or controlled by Initial Developer, to make, have made, use and sell (“offer to sell and import”) the Original Code, Modifications, or portions thereof, but solely to the extent that any such patent is reasonably necessary to enable You to utilize, alone or in combination with other software, the Original Code, Modifications, or any combination or portions thereof.

(c)

(d)

2.2. Contributor Grant.

Subject to third party intellectual property claims, each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license

(a)

under intellectual property rights (other than patent or trademark) Licensable by Contributor, to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof) either on an unmodified basis, with other Modifications, as Covered Code and/or as part of a Larger Work; and

(b)

under patents now or hereafter owned or controlled by Contributor, to make, have made, use and sell ("offer to sell and import") the Contributor Version (or portions thereof), but solely to the extent that any such patent is reasonably necessary to enable You to utilize, alone or in combination with other software, the Contributor Version (or portions thereof).

(c)

(d)

3 DISTRIBUTION OBLIGATIONS.

3.1. Application of License.

The Modifications which You create or to which You contribute are governed by the terms of this License, including without limitation Section 2.2. The Source Code version of Covered Code may be distributed only under the terms of this License or a future version of this License released under Section 6.1, and You must include a copy of this License with every copy of the Source Code You distribute. You may not offer or impose any terms on any Source Code version that alters or restricts the applicable version of this License or the recipients' rights hereunder. However, You may include an additional document offering the additional rights described in Section 3.5.

3.2. Availability of Source Code.

Any Modification created by You will be provided to the Initial Developer in Source Code form and are subject to the terms of the License.

3.3. Description of Modifications.

You must cause all Covered Code to which You contribute to contain a file documenting the changes You made to create that Covered Code and the date of any change. You must include a prominent statement that the Modification is derived, directly or indirectly, from Original Code provided by the Initial Developer and including the name of the Initial Developer in (a) the Source Code, and (b) in any notice in an Executable version or related documentation in which You describe the origin or ownership of the Covered Code.

3.4. Intellectual Property Matters.

(a) Third Party Claims.

If Contributor has knowledge that a license under a third party's intellectual property rights is required to exercise the rights granted by such Contributor under Sections 2.1 or 2.2, Contributor must include a text file with the Source Code distribution titled "LEGAL" which describes the claim and the party making the claim in sufficient detail that a recipient will know whom to contact. If Contributor obtains such knowledge after the Modification is made available as described in Section 3.2, Contributor shall promptly modify the LEGAL file in all copies Contributor makes available thereafter and shall take other steps (such as notifying appropriate mailing lists or newsgroups) reasonably calculated to inform those who received the Covered Code that new knowledge has been obtained.

(b) Contributor APIs.

If Contributor's Modifications include an application programming interface and Contributor has knowledge of patent licenses which are reasonably necessary to implement that API, Contributor must also include this information in the LEGAL file.

(c) Representations.

Contributor represents that, except as disclosed pursuant to Section 3.4(a) above, Contributor believes that Contributor's Modifications are Contributor's original creation(s) and/or Contributor has sufficient rights to grant the rights conveyed by this License.

3.5. Required Notices.

You must duplicate the notice in Exhibit A in each file of the Source Code. If it is not possible to put such notice in a particular Source Code file due to its structure, then You must include such notice in a location (such as a relevant directory) where a user would be likely to look for such a notice. If You created one or more Modification(s) You may add your name as a Contributor to the notice described in Exhibit A. You must also duplicate this License in any documentation for the Source Code where You describe recipients' rights or ownership rights relating to Covered Code. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Code. However, You may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor.

3.6. Distribution of Executable Versions.

You may distribute Covered Code in Executable form only if the requirements of Section 3.1-3.5 have been met for that Covered Code. You may distribute the Executable version of Covered Code or ownership rights under a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable version does not attempt to limit or alter the recipient's rights in the Source Code version from the rights set forth in this License. If You distribute the Executable version under a different license You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or any Contributor. If you distribute executable versions containing Covered Code as part of a product, you must reproduce the notice in Exhibit B in the documentation and/or other materials provided with the product.

3.7. Larger Works.

You may create a Larger Work by combining Covered Code with other code not governed by the terms of this License and distribute the Larger Work as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Code.

3.8. Restrictions.

You may not remove any product identification, copyright, proprietary notices or labels from gSOAP.

4 INABILITY TO COMPLY DUE TO STATUTE OR REGULATION.

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Code due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be included in the LEGAL file described in Section 3.4 and must be included with all distributions of the Source Code. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5 APPLICATION OF THIS LICENSE.

This License applies to code to which the Initial Developer has attached the notice in Exhibit A and to related Covered Code.

6 VERSIONS OF THE LICENSE.

6.1. New Versions.

Grantor may publish revised and/or new versions of the License from time to time. Each version will be given a distinguishing version number.

6.2. Effect of New Versions.

Once Covered Code has been published under a particular version of the License, You may always continue to use it under the terms of that version. You may also choose to use such Covered Code under the terms of any subsequent version of the License.

6.3. Derivative Works.

If You create or use a modified version of this License (which you may only do in order to apply it to code which is not already Covered Code governed by this License), You must (a) rename Your license so that the phrase "gSOAP" or any confusingly similar phrase do not appear in your license (except to note that your license differs from this License) and (b) otherwise make it clear that Your version of the license contains terms which differ from the gSOAP Public License. (Filling in the name of the Initial Developer, Original Code or Contributor in the notice described in Exhibit A shall not of themselves be deemed to be modifications of this License.)

7 DISCLAIMER OF WARRANTY.

COVERED CODE IS PROVIDED UNDER THIS LICENSE ON AN "AS IS" BASIS, WITHOUT WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, OF FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS, AND ANY WARRANTY THAT MAY ARISE BY REASON OF TRADE USAGE, CUSTOM, OR COURSE OF DEALING. WITHOUT LIMITING THE FOREGOING, YOU ACKNOWLEDGE THAT THE SOFTWARE IS PROVIDED "AS IS" AND THAT THE AUTHORS DO NOT WARRANT THE SOFTWARE WILL RUN UNINTERRUPTED OR ERROR FREE. LIMITED LIABILITY THE ENTIRE RISK AS TO RESULTS AND PERFORMANCE OF THE SOFTWARE IS ASSUMED BY YOU. UNDER NO CIRCUMSTANCES WILL THE AUTHORS BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES OF ANY KIND OR NATURE WHATSOEVER, WHETHER BASED ON CONTRACT, WARRANTY, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, ARISING OUT OF OR IN ANY WAY RELATED TO THE SOFTWARE, EVEN IF THE AUTHORS HAVE BEEN ADVISED ON THE POSSIBILITY OF SUCH DAMAGE OR IF SUCH DAMAGE COULD HAVE BEEN REASONABLY FORESEEN, AND NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY EXCLUSIVE REMEDY PROVIDED. SUCH LIMITATION ON DAMAGES INCLUDES, BUT IS NOT LIMITED TO, DAMAGES

FOR LOSS OF GOODWILL, LOST PROFITS, LOSS OF DATA OR SOFTWARE, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION OR IMPAIRMENT OF OTHER GOODS. IN NO EVENT WILL THE AUTHORS BE LIABLE FOR THE COSTS OF PROCUREMENT OF SUBSTITUTE SOFTWARE OR SERVICES. YOU ACKNOWLEDGE THAT THIS SOFTWARE IS NOT DESIGNED FOR USE IN ON-LINE EQUIPMENT IN HAZARDOUS ENVIRONMENTS SUCH AS OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR CONTROL, OR LIFE-CRITICAL APPLICATIONS. THE AUTHORS EXPRESSLY DISCLAIM ANY LIABILITY RESULTING FROM USE OF THE SOFTWARE IN ANY SUCH ON-LINE EQUIPMENT IN HAZARDOUS ENVIRONMENTS AND ACCEPTS NO LIABILITY IN RESPECT OF ANY ACTIONS OR CLAIMS BASED ON THE USE OF THE SOFTWARE IN ANY SUCH ON-LINE EQUIPMENT IN HAZARDOUS ENVIRONMENTS BY YOU. FOR PURPOSES OF THIS PARAGRAPH, THE TERM "LIFE-CRITICAL APPLICATION" MEANS AN APPLICATION IN WHICH THE FUNCTIONING OR MALFUNCTIONING OF THE SOFTWARE MAY RESULT DIRECTLY OR INDIRECTLY IN PHYSICAL INJURY OR LOSS OF HUMAN LIFE. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS LICENSE. NO USE OF ANY COVERED CODE IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER.

8 TERMINATION.

8.1.

This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. All sublicenses to the Covered Code which are properly granted shall survive any termination of this License. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

8.2.

8.3.

If You assert a patent infringement claim against Participant alleging that such Participant's Contributor Version directly or indirectly infringes any patent where such claim is resolved (such as by license or settlement) prior to the initiation of patent infringement litigation, then the reasonable value of the licenses granted by such Participant under Sections 2.1 or 2.2 shall be taken into account in determining the amount or value of any payment or license.

8.4.

In the event of termination under Sections 8.1 or 8.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or any distributor hereunder prior to termination shall survive termination.

9 LIMITATION OF LIABILITY.

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL YOU, THE INITIAL DEVELOPER, ANY OTHER CONTRIBUTOR, OR ANY DISTRIBUTOR OF COVERED CODE, OR ANY SUPPLIER OF ANY OF SUCH PARTIES, BE LIABLE TO ANY PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF SUCH PARTY SHALL HAVE

BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY RESULTING FROM SUCH PARTY'S NEGLIGENCE TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS EXCLUSION AND LIMITATION MAY NOT APPLY TO YOU.

10 U.S. GOVERNMENT END USERS.

11 MISCELLANEOUS.

12 RESPONSIBILITY FOR CLAIMS.

As between Initial Developer and the Contributors, each party is responsible for claims and damages arising, directly or indirectly, out of its utilization of rights under this License and You agree to work with Initial Developer and Contributors to distribute such responsibility on an equitable basis. Nothing herein is intended or shall be deemed to constitute any admission of liability.

EXHIBIT A.

"The contents of this file are subject to the gSOAP Public License Version 1.3 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.cs.fsu.edu/ engelen/soaplicense.html

Software distributed under the License is distributed on an "AS IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the License.

The Original Code of the gSOAP Software is: stdsoap.h, stdsoap2.h, stdsoap.c, stdsoap2.c, stdsoap.cpp, stdsoap2.cpp, soapcpp2.h, soapcpp2.c, soapcpp2_lex.l, soapcpp2_yacc.y, error2.h, error2.c, symbol2.c, init2.c, soapdoc2.html, and soapdoc2.pdf, httpget.h, httpget.c, stl.h, stldeque.h, stllist.h, stlvector.h, stlset.h.

The Initial Developer of the Original Code is Robert A. van Engelen. Portions created by Robert A. van Engelen are Copyright (C) 2001-2004 Robert A. van Engelen, Genivia inc. All Rights Reserved.

Contributor(s):

"_____."

[Note: The text of this Exhibit A may differ slightly form the text of the notices in the Source Code files of the Original code. You should use the text of this Exhibit A rather than the text found in the Original Code Source Code for Your Modifications.]

EXHIBIT B.

"Part of the software embedded in this product is gSOAP software.

Portions created by gSOAP are Copyright (C) 2001-2009 Robert A. van Engelen, Genivia inc. All Rights Reserved.

THE SOFTWARE IN THIS PRODUCT WAS IN PART PROVIDED BY GENIVIA INC AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,

SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE."

Contributors:

Oracle America, Inc., for additions marked *ORACLE CHANGE*, * SUN Change * or * SUN CHANGE *

March 4 2008:

- customization of the SSL accept timeout
- work around for SSL_Sleep reporting closed connection
- Function ssl_auth_init was static, but is now exported for external override
- redirection of gSoap debug logs when debug builds enabled
- added SSL_CTX_set_cipher_list call to restrict the cipher suite to RSA-2048/AES

  TLS_RSA_WITH_AES_256_CBC_SHA is defined in RFC 3268

  also see http://www.openssl.org/docs/apps/ciphers.html
- Added SSL_OP_NO_SSLv3 to force use of TLS
- bug fix: added call to close socket handle in various places noted in the code,

  since the caller overwrites soap->socket with the return value
- added support for the Metaware ARM7/9 compiler and the Treck Ethernet SSL stack
- conditionally made tcp_init non-static to allow access from other functions
- conditionally added structure member sessionId to SOAP structure for Treck access.
- conditionally modified logging to use buffers rather than files.
- conditionally made certain functions defined as WITH_LEAN

    available even if LEAN is not true
- conditionally removed time calls that Metaware does not support

Wind River Systems, Inc., for the following additions (marked WR[...]):

- vxWorks compatible
- Support for IPv6.

This software is released under one of the following three licenses:
GPL, the gSOAP public license, or Genivia's license for commercial use.

---

gSOAP public license.

The contents of this file are subject to the gSOAP Public License
Version 1.3
(the "License"); you may not use this file except in compliance with the
License. You may obtain a copy of the License at
http://www.cs.fsu.edu/~engelen/soaplicense.html
Software distributed under the License is distributed on an "AS IS" basis,
WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License
for the specific language governing rights and limitations under the
License.

The Initial Developer of the Original Code is Robert A. van Engelen.
Copyright (C) 2000-2004, Robert van Engelen, Genivia, Inc., All Rights
Reserved.

GPL license.

This program is free software; you can redistribute it and/or modify it under
the terms of the GNU General Public License as published by the Free Software
Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY

WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A
PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc.,
59 Temple Place, Suite 330,
Boston, MA 02111-1307 USA

Author contact information:
engelen@genivia.com / engelen@acm.org

A commercial use license is available from Genivia, Inc.,
contact@genivia.com
---
*/

==========
II. APPENDIX
==========

Written Offer for Source Code

For binaries that you receive from Oracle on physical media that are licensed under any version of the GNU General Public License (GPL) or the GNU LGPL, you can receive a complete machine-readable copy of the source code by sending a written request to:

Oracle America, Inc.
Attn: Associate General Counsel,
Development and Engineering Legal
500 Oracle Parkway, 7th Floor

Redwood Shores, CA 94065

Your request should include (i) the name of the covered binary, (ii) the version number of the Oracle product containing the covered binary, (iii) your name, (iv) your company name (if applicable) and (v) your return mailing and email address (if available).

We may charge you a nominal fee to cover the cost of the media and distribution.

Your request must be sent within three (3) years of the date you received the GPL or LGPL covered code.

For your convenience, some or all of the source code may also be found at:

http://www.sun.com/opensourcecode

Glossary

This glossary defines terms and abbreviations in this publication.

Some of the definitions are taken from other glossaries. The letters in the parentheses that follow some definitions indicate the source of the definition:

(A) *The American National Standard Dictionary for Information Systems*, ANSI X3.172-1990, copyright 1990 by the American National Standards Institute (ANSI).

(E) The ANSI/Electronic Industries Association (EIA) Standard-440-A, *Fiber Optic Terminology*.

(I) The *Information Technology Vocabulary*, developed by Subcommittee 1, Joint Technical Committee 1, of the International Organization for Standardization and International Electro-technical Commission (ISO/IEC/JTC1/SC1).

(IBM) *The IBM Dictionary of Computing*, copyright 1994 by IBM.

(T) Draft international standards committee drafts, and working papers being developed by the ISO/IEC/JTC1/SC1.

A

accessory rack
An area of the drive and electronics module that is used for SL8500 library electronic and power equipment and for other standard 19-inch rack-mount electronic equipment. Up to four racks are permitted in the electronics/drive assembly. Rack-mount equipment must be on the approved equipment list.

adapter
Any hardware that joins different connector types.

address
A character or group of characters that identifies a register, a particular part of storage, or some other data source or destination. (A).

alphanumeric
A character or group of characters that identifies a register, a particular part of storage, or some other data source or destination. (A).

arbitrated loop
A Fibre Channel interconnect topology in which all parts are connected in a common loop. Before transmitting data, devices must participate in arbitration to gain control of the loop.

arbitrated loop physical address (AL_PA)
A one-byte value that identifies a port in an arbitrated loop topology.

arbitration
Any process by which a user of shared resources negotiates with other users for the right to use the resource. A port connected to a shared bus must win arbitration before it transmits data on the bus.

C

cartridge
A storage device that consists of magnetic tape on a supply reel in a protective housing.

cascading
The process of connecting two or more Fibre Channel switches together to increase the number of ports or to extend distances.

channel
A functional unit, controlled by the processor (or host), that handles the transfer of data between processor storage and local peripheral equipment. (IBM)

cleaning cartridge
A data cartridge that contains special material to clean the tape path in a transport or drive.

compress
To save space by eliminating gaps, empty fields, redundancy, or unnecessary data to shorten the length of records or files. (IBM)

condition
One of a set of specified values that a data item can assume. (IBM)

conditioning time
The amount of time to prepare a tape cartridge for use in a T10000 Tape Drive.

configuration
The manner in which the hardware and software of an information processing system is organized and interconnected. (T)

connector
An electrical or optical part that joins two or more other parts.

coupler
Fiber-optic hardware that joins optical fiber connectors of the same type.

D

data path key management (DPKM)
The use of the SCSI 4 commands `Security Protocol In` and `Security Protocol Out` to implement host-based key management encryption on StorageTek tape drives.

data rate
The speed of a data transfer process, usually expressed in bits per second or bytes per second. (IBM)

data security erase (DSE)
A random binary pattern over-writing existing data from the point of an Erase command to the end-of-tape.

data tape
A data cartridge formatted for use as a regular data tape for the system in which it is used.

data tracks
The regions of recorded tape containing user data formed as discreet longitudinal "tracks" (similar to railroad tracks).

diagnostics
Pertaining to the detection and isolation of errors in programs and faults in equipment.

DPKM
See data path key management.

drive
A drive controls the movement of the tape and records or reads the data on the tape as desired by the customer.

DSE
See data security erase.

dump
To copy the contents of all or part of storage to collect error information.

dynamic host configuration protocol (DHCP)
A network protocol that enables a server to automatically assign an IP address to devices on a network. DHCP assigns a number dynamically from a defined range of numbers for a given network.

dynamic world wide name (dWWN)
A feature that applies dynamic names to network devices rather than fixed names. When a dWWN-named device is replaced, it is assigned the same WWN as the one it replaced, preventing re-configuration of the network.

E

emulation
The use of programming techniques and special machine features to permit a computing system to execute programs written for another system. (IBM)

encryption
The translation of data into a secret code. Encryption is one of the most effective ways to achieve data security. To read an encrypted file, you must have access to a special key or password that enables you to decipher it.

end of block (EOB)
A code that marks the end of a block of data. (IBM)

end of file (EOF)
A coded character recorded on a data medium to indicate the end of the medium. (IBM)

end-of-file label
1. An internal label indicating the end of a file and possible containing data for file control. (T)
2. Synonymous with trailer label.

end-of-tape marker (EOT)
A marker on a magnetic tape to indicate the end of the permissible recording area. (IBM)

environmental requirement
Any of the physical conditions required for the protection and proper operation of a functional unit; the requirement is usually specified as a nominal value and a tolerance range. For a device, there may be more than one set of environmental requirements; for example, one set for transport, another for storage, and another for operation. (T) (A)

EOT
End of tape.

erase
To remove data from a data medium, leaving the medium available for recording new data. (I) (A)

error
A discrepancy between a computed, observed, or measured value or condition and the true, specified, or theoretically correct value or condition. (I) (A)

ESD
Electrostatic Discharge.

F

F_Port
A port in a fabric to which an N_Port or NL_Port attaches.

fabric
The Fibre Channel topology similar to a telephone switch in that the initiator of a call to the receiving port simply provides the receiver with the port address, and the fabric routes the transmission to the correct port. A fabric differs from a point-to-point or arbitrated loop topology in that it provides for interconnections between ports without having a point-to-point connection. The fabric also serves as a media-type converter.

fault symptom code (FSC)
A four-character hexadecimal code generated in response to an error to help isolate failures within the device. Some FSCs are for information purposes only.

FC
See Fibre Channel.

fiber optics
The branch of optical technology concerned with the transmission of radiant power through fibers made of transparent materials such as glass, fused silica, and plastic. (E)

fiber-optic cable
A cable made of ultra-thin glass or silica fibers which can transmit data using pulses of laser light. Fiber-optic cables have several advantages over copper cables: they have much less signal loss; they allow information to be transmitted at higher speeds and over longer distances; they are not affected by external electrical noise; and they are better for transmissions which require security.

fiber-optic connector
One of several types of devices used to join pairs of optical fibers together.

Fibre Channel
The National Committee for Information Technology Standards standard that defines an ultrahigh-speed, content-independent, multilevel data transmission interface that supports multiple protocols simultaneously. Fibre Channel supports connectivity to millions of devices over copper and/or fiber-optic physical media and provides the best characteristics of both networks and channels over diverse topologies.

fibre connection (FICON)
An ESA/390 and zSeries computer peripheral interface. The I/O interface uses ESA/390 and zSeries FICON protocols (FC-FS and FC-SB-2) over a Fibre Channel serial interface that configures units attached to a FICON-supported Fibre Channel communications fabric.

FICON channel
A channel having a Fibre Channel connection (FICON) channel-to-control-unit I/O interface that uses optical cables as a transmission medium. May operate in either FC or FCV mode.

file-protect
To prevent the erasure or overwriting of data stored on data cartridges. *See also* write-protect switch.

firmware
An ordered set of instructions and data stored in a way that is functionally independent of main storage; for example, microprograms stored in a ROM. (T) *See also* microcode.

FL_Port
A special type of fabric port that an arbitrated loop uses to connect N_Ports and NL_Ports into a fabric, thus making a public loop.

FRU
Field replaceable unit.

FSC
Fault symptom code.

full duplex
A communication protocol that allows signals to be transmitted and received simultaneously.

G

gateway
A 32-bit, or 4-byte, number in dotted decimal format (typically written as four numbers separated by periods, such as 107.4.1.3 or 84.2.1.111) that is applied to an IP Address to identify router interface.

Gb
Gigabit, equal to 10^9 bits.

Gbps
Gigabits per second.

gigabyte (GB)
One billion (10^9) bytes. When referring to disk and tape capacity, one GB equals 1,000,000,000 bytes.
When referring to memory capacity, one GB equals 1,073,741,824 in decimal notation or 2^{30} bytes.

gripper
The portion of the hand assembly that grasps the cartridge.

H

hand assembly
A part of the library robot whose function is to grasp cartridges and move them between storage slots and drives. A camera on the hand assembly reads cartridge volume labels.

hardware
All or part of the physical components of an information processing system, such as computers or peripheral devices. (T) (A)

host
The primary computer on a network with which other computers interact.

host bus adapter (HBA)
A circuit installed in a multi-platform host or device that interfaces between the device and the bus.

host interface
An interface between a network and host computer. (T)

hub
A Fibre Channel Arbitrated Loop switching device that allows multiple servers and targets, such as storage systems, to connect at a central point. A single hub configuration appears as a single loop.

I

indicator
A device that provides a visual or other indication of the existence of a defined state. (T)

initial program load (IPL)
A process that activates a machine reset and loads system programs to prepare a computer system for operation. Processors having diagnostic programs activate these programs at initial program load execution. Devices running firmware usually reload the functional firmware from a diskette or disk drive at initial program load execution.

initialization
The operations required for setting a device to a starting state, before the use of a data medium, or before implementation of a process. (T)

interface
Hardware, software, or both, that links systems, programs, or devices. (IBM)

internet protocol (IP)
A protocol used to route data from its source to its destination in an Internet environment. (IBM)

internet protocol v4 (IPv4) address
A four-byte value that identifies a device and makes it accessible through a network. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be from 0 to 255. For example, 129.80.145.23 could be an IP address.

internet protocol v6 (IPv6) address
The next generation internet protocol. It provides a much larger address space than IPv4. This is based upon the definition of a 128-bit address - IPv4 used a 32-bit address. The IPv6 address format is eight fields of four hexadecimal characters separated by colons (for example, 2001:0db8:85a3:0000:0000:8a2e:037 0:7334)

IP
See internet protocol.

IPL
See initial program load.

L

LC connector
A standard connector for 2-Gbps or 4-Gbps Fibre Channel data transfer. This type of connector is used on fiber-optic cables.

library
A robotic system that stores, moves, mounts, and dismounts data cartridges that are used in data read or write operations.

link
A physical connection (electrical or optical) between two nodes of a network.

logical path
A relationship between a channel and control unit that designates the physical path to be used for device-level communication between each entity, defined by a link address assigned to each entity.

M

magnetic tape
A tape with a magnetizable layer on which data can be stored. (T)

magnetic tape drive
A mechanism for moving magnetic tape and controlling its movement.

MB
Megabytes or 1,000,000 bytes for disk or tape storage but 1,048,576 (2^{20}) bytes of memory capacity.

menu
A list of options displayed to the user by a data processing system, from which the user can select an action to be initiated. (T)

microcode
A code, representing the instructions of an instruction set, that is implemented in a part of storage that is not program-addressable. (IBM)

multi mode
A graded-index or step-index optical fiber that allows more than one bound mode to propagate. (E) Contrast with single mode.

multimode fiber
An optical fiber designed to carry multiple signals, distinguished by frequency or phase, at the same time.

N

net mask
A 32-bit, or 4-byte number, in dotted decimal format (typically written as four numbers separated by periods, such as 255.255.0.0 or 255.255.255.0) that is applied to an IP address to identify the network and node address of a host or router interface. (*Synonymous* with subnet mask.)

network
An arrangement of nodes and branches that connects data processing devices to one another through software and hardware links to facilitate information interchange.

NL_Port
A port attached to a node for use in the point-to-point arbitrated loop and fabric topologies of Fibre Channel. The NL_Port is configured as a private and/or a public loop.

node
A device that contains a minimum of one N_Port and/or NL_Port.

N_Port
A port that connects a node to a fabric or to another node.

nexus
A connection that exists between an initiator, a target, and a logical unit. This is where one initiator port talks to one target port, addressing one LUN and together they execute a task.

O

offline
Neither controlled by, nor communicating with, a computer. (IBM)

online
Pertaining to the operation of a functional unit when under the direct control of the computer. (T)

operator control panel
A functional unit that contains switches used to control all or part of a computer and possibly the indicators giving information about its functioning. (T)

P

performance
One of two major factors on which the total productivity of a system depends. Performance is largely determined by a combination of throughput, response time, and availability. (IBM)

point-to-point
A topology in which exactly two ports communicate. In Fibre Channel, the two ports are N_Ports.

port
A specific communications end point within a host. A port is identified by a port number. (IBM) (2) In Fibre Channel, an access point in a device where a link attaches.

private loop
A Fibre Channel arbitrated loop with no fabric attachment.

Private NL_Port
An NL_Port that does not attempt a Fabric Login.

protocol
A set of semantic and syntactic rules that determines the behavior of functional units in achieving communication. (I)

public loop
A Fibre Channel arbitrated loop with an attachment to a fabric.

Public NL_Port
An NL_Port that attempts a Fabric Login.

R

read/write head
The data sensing and recording unit of a tape drive. (IBM)

reclaim
The act of overwriting a legacy data cartridge by a newer generation drive. For example, a cartridge written by a T10000A drive can be overwritten (reclaimed) by a T10000B drive while a cartridge written by a T10000B drive can be reclaimed by a T10000A drive.

release
A distribution of a new product or new function and fixes for an existing product. (IBM)

rewind
To move tape from the take-up hub to the supply hub. (IBM)

R/W
Read/write

S

SC connector
A standard connector for 1-Gbps Fibre Channel data transfer. This type of connector is used on fiber-optic cable.

serial transmission
A transmission in which bits are sent in a stream in a single fiber.

single mode fiber
Optical fiber in which only the lowest-order bound mode can propagate at the wavelength of interest. (E)

small form-factor pluggable (SFP)
Technology with a 2-gigabit or 4-gigabit transfer speed over smaller connectors, cables, and transceivers for larger bandwidth capability.

StorageTek Diagnostic System (STDS)
A tool that enables a service engineer to connect to the maintenance port of StorageTek products to perform maintenance functions.

submenu
A menu related to and reached from a main menu. (IBM)

subsystem
A system that is part of some larger system.

switch
In Fibre Channel technology, a device that connects Fibre Channel devices together in a fabric.

system
A combination of functionally interrelated interacting mechanical and electrical elements designed to work as a coherent entity.

T

tape
See magnetic tape.

tape cartridge
A container holding magnetic tape that can be processed without separating the tape from the container.

tape drive
A device for moving magnetic tape and controlling its movement. (T)

TB
See terabyte.

TCP/IP
Transmission Control Protocol/Internet Protocol.

terabyte (TB)
A unit of measure equal to one trillion (10^{12}) bytes of disk or tape storage capacity. When referring to memory capacity, one TB equals 1,099,511,627,776 in decimal notation or 2^{40} bytes.

transmission control protocol/internet protocol (TCP/IP)
A set of communication protocols that support peer-to-peer connectivity functions for both local and wide area networks. (IBM)

V

vary offline
To change the status of a device from online to offline. When a device is offline, no data set may be opened on that device. (IBM)

vary online
To restore a device to a state where it is available for use by the system. (IBM)

virtual operator panel (VOP)
A software application that allows a user to monitor and perform some operations on one or more tape drives remotely.

VolSafe
VolSafe (volume safe) is a special feature that provides write once, read many (WORM) technology to VolSafe-designated tape cartridges. VolSafe permits new data to only append the tape media, while it prevents erasure or overwrite of previously written data.

volume serial number (VOLSER)
An alphanumeric label that the host software uses to identify a volume. It attaches to the spine of a cartridge and is both human- and machine-readable.

VOP
See virtual operator panel.

W

world wide name (WWN)
A 64-bit integer that identifies a Fibre Channel port.

World Wide Node Name (WWNN)
A 64-bit network address that identifies the company (in IEEE format) with a vendor specific identifier.

World Wide Port Name (WWPN)
A 64-bit network address that identifies the port name.

wrap
A single pass of tape from either BOT to EOT or EOT to BOT with the heads in a fixed transverse location.

write-enabled
A setting on a data cartridge that allows data to be written on the tape.

write once read many (WORM)
A storage classification for media that can be written only once but read many times.

write operation
An output operation that sends a processed record to an output device or output file. (IBM)

write-enabled
A setting on a cartridge tape that allows data to be written on the tape.

write-protected
A setting on data cartridges that prevents data from being written on the tape. Reading data is still possible.

Index

Symbols

A

B

C

D

E

F

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

X