Hewlett Packard Enterprise

HPE StoreEver LTO-8 Ultrium Tape Drives

Technical Reference Manual Volume 2 Software Integration Guide

Abstract

This guide is intended to provide a bridge between existing documentation about HPE Ultrium tape drives (SCSI specification, data sheets, etc.) and the practical work needed to support HPE Ultrium in software applications.

Part Number: BC023-60007b
Published: September 2020
Edition: 3

© Copyright 2017, 2018, 2020 Hewlett Packard Enterprise Development LP

Notices

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Acknowledgments

Intel®, Itanium®, Optane™, Pentium®, Xeon®, Intel Inside®, and the Intel Inside logo are trademarks of Intel Corporation in the U.S. and other countries.

Microsoft® and Windows® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Java® and Oracle® are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

All third-party marks are property of their respective owners.



Contents

Introduction 7
- Hewlett Packard Enterprise Ultrium products 7

Inquiry strings and product recognition 9
- To determine drive technology family 9
- To determine interface type 9
- To determine Ultrium format 10
  - Return data 10
- To determine the drive Serial Number 12
- To determine the drive World Wide Node Name and World Wide Port Name 12
- To Identify a WORM-compatible tape drive through host interface 12
- To determine support for SCSI commands 13

SCSI commands supported 14

New features in LTO-8 drives 18

New features in LTO-7 drives 20
- Append-only mode 20
- Alternative CRC algorithm for Logical Block Protection 21

Manageability, diagnosability and supportability (MDS) 22
- Set/Report time stamp 22
- Device statistics log page 22
- Tape diagnostics log page 25

WORM 28

Partitioning 33
- General operation 34
  - Load / Unload 34
  - Modifying partitions 34
  - Switching between partitions 34
  - Determining current partition 34
  - Determining partition configuration 34
  - Erasing media 34
  - Encryption parameters 34
- SCSI behavior specific to partitioning 34
  - `LOCATE(10)` and `LOCATE(16)` commands 35
  - `READ POSITION` command 35
  - `SET CAPACITY` command 35

READ ATTRIBUTE / WRITE ATTRIBUTE 35
FORMAT MEDIUM command 35
Device Configuration mode page 36
Medium Partition mode page 36
Volume Statistics log page 38

Cartridge Memory (LTO-CM) & Medium Auxiliary Memory (MAM) 39
Desired application software support 39

Media format and cartridge type 40
Identifying cartridge type via MAM read attribute 41
Identifying cartridge type through Mode Sense Mode Parameter Header 41

Data compression control 42
Desired application software support 42

TapeAlert 43

Load / Unload 47
Desired application software support 47

SCSI log pages 49

Recommended timeout values 50
Using timeout descriptors 51

Performance optimization 53
Recommended minimum transfer sizes 53
Maximum block size 54
Media type identification 54
Using cartridge memory instead of tape headers 54

Operating system drivers 55
Microsoft Windows 55
UNIX 55

Encryption 56
Standards and references 56
Minimum requirements 56
Key management comments 56

End-to-end logical block protection 57

Websites 58

Support and other resources 59
- Accessing Hewlett Packard Enterprise Support 59
- Accessing updates 59
- Remote support 60
- Warranty information 60
- Regulatory information 60
- Documentation feedback 61

Related information 62

Diagnostic features 63
- Set Capacity command 63
- Drive (DTD) status log page 63

Encryption 67
- Caveats 67
- Tape drive encryption overview 67
- How encryption works 68
- Minimum requirements for an application supporting an encrypting tape drive 70
- Related standards 71
  - Ultrium format agreement 71
  - T10 standards - SSC-5 and SPC-4 71
- SCSI commands 71
  - `SECURITY PROTOCOL IN` command and pages 71
  - `SECURITY PROTOCOL OUT` command and pages 85
- Encryption sense codes and qualifiers 90
- Encryption information in Cartridge Memory 93
- Usage recommendations 93
  - Detecting encryption capability 93
  - Enabling encryption 93
  - Disabling encryption 93
  - Persistent reservation 93
- Tape copying 93
  - Tagging externally encrypted data 94
  - Tagging data to disallow raw reads 94
  - Keyless copy recommendations 94
- Key management 95
- Frequently asked questions 96

Logical block protection 97
- Standards and references 97
- Minimum requirements 97
- General operation overview 97
  - Set-up 97
  - Backup 98
  - Restore / Verify 98

Backup with E2E-LPB disabled....98
Restore / Verify with E2E-LPB disabled....98
Specific SCSI behavioral changes....98
WRITE(6)....98
READ(6)....99
READ BLOCK LIMITS....99
INQUIRY....99
Control data protection mode page....99
Sense data....100
E2E-LBP CRC algorithm....100
Error handling and deferred errors....100
Key considerations....100
Background to deferred error handling....101
Data transfer performance and Server CPU loading considerations....101
Summary....101
Experimental findings for data transfer performance and server CPU loading....102
Measured CPU loading due to E2E-LBP processing....103
Bottlenecking is principally in the Host E2E Software Algorithm....105
Experimental configurations for E2E-LBP data transfer performance and server CPU loading....106
References for E2E-LBP data transfer performance and server CPU loading....108



Introduction

This release of the *HPE Ultrium LTO-8 Technical Reference Manual Volume 2: Software Integration Guide* includes details of the eighth-generation HPE Ultrium format tape drives. It has been simplified to remove information which related only to earlier generations; refer to the previous version of this document for specific details relevant up to LTO-7.

Hewlett Packard Enterprise Ultrium products

The following table shows the range of Hewlett Packard Enterprise Ultrium products including code names, capacities and interfaces.

Table 1: Hewlett Packard Enterprise Ultrium product range

Year release	Product name	Native capacity	Transfer rate (native)	Form factor	Host interface
2000	Ultrium230	100 GB	15 MB/s	5 1/4 in full-height	SCSI Ultra2
	Ultrium215	100 GB	7.5 MB/s	5 1/4 in half-height	SCSI Ultra2
2002	Ultrium460	200 GB	30 MB/s	5 1/4 in full-height	SCSI Ultra160
	n/a	200 GB	30 MB/s	5 1/4 in full-height	2 Gb/s Fibre Channel
2004	Ultrium960	400 GB	80 MB/s	5 1/4 in full-height	SCSI Ultra320
2005	n/a	400 GB	80 MB/s	5 1/4 in full-height	2 Gb/s Fibre Channel
	Ultrium448	200 GB	24 MB/s	5 1/4 in half-height	SCSI Ultra160
	Ultrium232	100 GB	16 MB/s	5 1/4 in half-height	SCSI Ultra160
2006	n/a	400 GB	80 MB/s	5 1/4 in full-height	4 Gb/s Fibre Channel
	Ultrium448 SAS	200 GB	24 MB/s	5 1/4 in half-height	Serial Attached SCSI (SAS1.1)

Table Continued

Year release	Product name	Native capacity	Transfer rate (native)	Form factor	Host interface
	Ultrium920, Ultrium920 SAS	400 GB	60 MB/s	5 1/4 in half-height	SCSI Ultra320, Serial Attached SCSI (SAS1.1)
2007	Ultrium1840	800 GB	120 MB/s	5 1/4 in full-height	4 Gb/s Fibre Channel, SCSI Ultra320, Serial Attached SCSI (SAS1.1)
2008	Ultrium 1760	800 GB	80 MB/s	5 1/4 in half-height	4 Gb/s Fibre Channel, SCSI Ultra320, Serial Attached SCSI (SAS1.1)
2010	Ultrium 3280	1.5 TB	140 MB/s	5 1/4 in full-height	8 Gb/s Fibre Channel, Serial Attached SCSI (SAS2.0)
	Ultrium 3000	1.5 TB	140 MB/s	5 1/4 in half-height	8 Gb/s Fibre Channel, Serial Attached SCSI (SAS2.0)
2012	Ultrium 6650	2.5 TB	160 MB/s	5 1/4 in full-height	8 Gb/s Fibre Channel, Serial Attached SCSI (SAS2.0)
	Ultrium 6250	2.5 TB	160 MB/s	5 1/4 in half-height	8 Gb/s Fibre Channel, Serial Attached SCSI (SAS2.0)
2015	Ultrium 15750	6 TB	300 MB/s	5 1/4 in full-height	8 Gb/s Fibre Channel
	Ultrium 15000	6 TB	300 MB/s	5 1/4 in half-height	8 Gb/s Fibre Channel, Serial Attached SCSI (SAS2.0)
2018	Ultrium 30750	12 TB	300 MB/s	5 1/4 in half-height	8 Gb/s Fibre Channel, Serial Attached SCSI (SAS2.0)

Inquiry strings and product recognition

The following table shows the inquiry identification data for eighth generation LTO drives.

Table 2: Standards inquiry data

Standard inquiry page data	SAS+FC
Vendor ID (bytes 8-15)	"HPE "
Product ID (bytes 16-23)	"Ultrium "
Product ID (bytes 24-31)	"8-SCSI "
Product Revision Level (bytes 32-35)	YMDV

Vendor ID (bytes 8-15)

"HPE " The previous Hewlett Packard Ultrium products used to be "HP "

NOTE: There are five blank spaces following HPE.

Product ID (bytes 16-23)

“Ultrium ” - the ID is the same for all Hewlett Packard Enterprise Ultrium products, regardless of model or generation

Product ID (bytes 24-31)

Byte 24: Ultrium (LTO) identifier: “8” for LTO-8

Byte 25: “-” hyphen separator (ASCII 2Dh)

Byte 26-29: “SCSI” for all interfaces (Fibre Channel, SAS)

Product Revision Level (32-35)

Byte 32: (Y) ASCII character representing the year of the firmware build, for example, **A** represents 2010, **H** represents 2017

Byte 33: (M) ASCII character representing the month of the firmware build (1-9, A-C) for example, **1** represents January, **B** represents November

Byte 34: (D) ASCII character representing the day of the firmware build (1-9, A-V) for example, **1** represents 1st, **J** represents 19th

Byte 35: (V) ASCII character representing the build version (1-9, a-z, A-Z) for example, **1** represents the first build, **a** represents the tenth build

To determine drive technology family

Examine the first eight bytes of the Product ID field and check for the string "Ultrium ".

To determine interface type

Examine byte 38 of the standard Inquiry data. This contains two vendor-unique fields as shown in the following table.

Table 3: Interface information

	7	6	5	4	3	2	1	0
Byte 38	Protocol identifier 0h = Fibre Channel (FCP-4) 6h = SAS (SAS-2) 7h = ADT (ADT-2)				Maximum speed supported SAS: 0h = unknown 8h = 1.5Gbps 9h = 3Gbps Ah = 6Gbps		Fibre channel: 0h = 1Gbps 1h = 2Gbps 2h = 4Gbps 3h = 8Gbps 4h = 10Gbps	

To determine this information using standardized methods, read the protocol identifier from the Device Identification VPD page (83h), and the negotiated speed from the Primary Port Status log parameter reported in the DT Device Status log page (11h).

To determine Ultrium format

Send a `SCSI REPORT DENSITY SUPPORT` command as shown in the following table and examine the returned data.

Table 4: `REPORT DENSITY SUPPORT` CDB

	7	6	5	4	3	2	1	0
0	Operation Code (44h)							
1	Reserved (0)							`MEDIA`
2	Reserved (0)							
…								
6								
7	(MSB)			Allocation Length				
8								(LSB)
9	Control							

Return data

If the `MEDIA` bit is set, the returned data describes the currently loaded media in a single density support descriptor, as shown in the following table. If the `MEDIA` bit is clear, then the data includes descriptors for all supported media types,

and the fields in bytes 4-55 are repeated for each descriptor. The default cartridge type for this device is indicated by the descriptor which has the DEFLT bit set. The WRTOK bit indicates whether media of this descriptor type can be written by the device. In every case, the secondary density code is identical to the primary density code because every given generation of the LTO format has its own unique density.

Table 5: Report density support return data

	7	6	5	4	3	2	1	0
01	Available Density Descriptor Length (0036h)							
23	Reserved (0)							
4	Primary Density Code							
5	Secondary Density Code							
6	WRTOK	DUP (0)	DEFLT	Reserved (0)				DLV (0)
78	Descriptor Length (0 – not valid, indicated by DLV=0)							
9…11	Bits per mm							
1213	Media Width							
1415	Tracks							
16……19	Capacity (MB)							
20……27	Assigning Organization (LTO-CVE)							
28……35	Density Name							
36……55	Density Description							

For an LTO-8 product, three descriptors will be returned (assuming the media bit was set to 0):

Primary Density Code	5Ch	Density Code for Ultrium LTO-7
Density Name	U-732	Ultrium generation 7, 32 tracks
Description	Ultrium 7/32T	
DEFLT	No	LTO-7 media can be written in LTO-8 drives
WRTOK	Yes	

Primary Density Code Density Name Description	5Dh U-832M Ultrium 8/32T Type M	Density Code for LTO-7 cartridge initialized as Type M media Ultrium generation 8, 32 tracks
DEFLT	No	LTO-7 Type M media can be written in LTO-8 drives
WRTOK	Yes	

Primary Density Code Density Name Description	5Eh U-832 Ultrium 8/32T	Density Code for Ultrium LTO-8 Type A Ultrium generation 8, 32 tracks
DEFLT	Yes	This is the native format of an LTO-8 drive
WRTOK	Yes	LTO-8 media can be written in LTO-8 drives

NOTE: No descriptor will be returned for LTO-1 through LTO-6 since these types of media are not compatible.

See **Media format and cartridge type** for more information on which cartridge types are compatible with various generations of drive.

To determine the drive Serial Number

Examine Inquiry VPD Page 80h (Unit Serial Number Page) bytes 4 to 13.

To determine the drive World Wide Node Name and World Wide Port Name

Examine Inquiry VPD Page 83h (Device Identification Page). Note that the list and order of descriptors contained in this page is not fixed, so the application must parse the headers to identify each descriptor rather than relying on fixed offsets.

To Identify a WORM-compatible tape drive through host interface

Examine the vendor-unique field at byte 40 in the standard Inquiry data (see the following table).

Table 6: Identifying WORM-capable drive in Inquiry data

	7	6	5	4	3	2	1	0
Byte 40				WORM version				WORM

WORM: Indicates whether the drive supports WORM media

0 = drive does not support WORM media

1 = drive supports WORM media (always true for LTO-7 and LTO-8 drives)

WORM version: Indicates the supported WORM version

00h = first WORM version

01-7Fh = reserved for future use

Alternatively WORM support can be verified by reading the Inquiry VPD page B0h as defined in SSC-5. See **WORM** for more information on using WORM media.

To determine support for SCSI commands

The LTO-8 drive supports the T10-defined `REPORT SUPPORTED OPCODES` command. This command can be used to find which commands are available, and also to obtain recommended timeout values. See **Using timeout descriptors** for more information.

SCSI commands supported

The following table summarizes the SCSI commands supported by LTO-8 drives. A few commands from earlier generations have been discontinued. The `REPORT SUPPORTED OPCODES` command can be used to get the list of commands supported by the drive (see **Using timeout descriptors**).

Table 7: Supported SCSI commands

Command	OpCode [SA / SA Qualifier]	LTO-8
`ALLOW OVERWRITE (16)`	82h	yes
`ERASE (6)`	19h	yes
`FORMAT MEDIUM (6)`	04h	yes
`INQUIRY (6)`	12h	yes
`LOAD/UNLOAD (6)`	1Bh	yes
`LOCATE (10)`	2Bh	yes
`LOCATE (16)`	92h	yes
`LOG SELECT (10)`	4Ch	yes
`LOG SENSE (10)`	4Dh	yes
`MODE SELECT (6)`	15h	yes
`MODE SELECT (10)`	55h	yes
`MODE SENSE (6)`	1Ah	yes
`MODE SENSE (10)`	5Ah	yes
`PERSISTENT RESERVE IN (10) [Read Keys]`	5Eh [00h]	yes
`PERSISTENT RESERVE IN (10) [Read Reservation]`	5Eh [01h]	yes
`PERSISTENT RESERVE IN (10) [Report Capabilities]`	5Eh [02h]	yes
`PERSISTENT RESERVE IN (10) [Read Full Status]`	5Eh [03h]	yes

Table Continued

Command	OpCode [SA / SA Qualifier]	LTO-8
PERSISTENT RESERVE OUT (10) [Register]	5Fh [00h]	yes
PERSISTENT RESERVE OUT (10) [Reserve]	5Fh [01h]	yes
PERSISTENT RESERVE OUT (10) [Release]	5Fh [02h]	yes
PERSISTENT RESERVE OUT (10) [Clear]	5Fh [03h]	yes
PERSISTENT RESERVE OUT (10) [Preempt]	5Fh [04h]	yes
PERSISTENT RESERVE OUT (10) [Preempt and Report]	5Fh [05h]	yes
PERSISTENT RESERVE OUT (10) [Register & Ignore Existing Key]	5Fh [06h]	yes
PERSISTENT RESERVE OUT (10) [Register and Move]	5Fh [07h]	yes
PREVENT / ALLOW MEDIUM REMOVAL (6)	1Eh	yes
READ (6)	08h	yes
READ ATTRIBUTE (16) [Attribute Values]	8Ch [00h]	yes
READ ATTRIBUTE (16) [Attribute List]	8Ch [01h]	yes
READ ATTRIBUTE (16) [Logical Volume List]	8Ch [02h]	yes
READ ATTRIBUTE (16) [Partition List]	8Ch [03h]	yes
READ ATTRIBUTE (16) [Supported Attributes]	8Ch [05h]	yes
READ BLOCK LIMITS (6)	05h	yes
READ BUFFER (10)	3Ch	yes
READ DYNAMIC RUNTIME ATTRIBUTE (12)	A3h [1Eh]	yes
READ LOGGED-IN HOST TABLE (12)	A3h [1Fh/01h]	yes
READ POSITION (10) [Short Form]	34h [00h]	yes

Table Continued



Command	OpCode [SA / SA Qualifier]	LTO-8
READ POSITION (10) [Long Form]	34h [06h]	yes
READ POSITION (10) [Extended Form]	34h [08h]	yes
RECEIVE DIAGNOSTIC RESULTS (6)	1Ch	yes
RELEASE UNIT (6)	17h	yes
RELEASE UNIT (10)	57h	yes
REPORT DENSITY SUPPORT (10)	44h	yes
REPORT LUNS (12)	A0h	yes
REPORT SUPPORTED OPERATION CODES (12)	A3h [0Ch]	yes
REPORT SUPPORTED TASK MANAGEMENT FUNCTIONS (12)	A3h [0Dh]	yes
REPORT TIMESTAMP (12)	A3h [0Fh]	yes
REQUEST SENSE (6)	03h	yes
RESERVE UNIT (6)	16h	yes
RESERVE UNIT (10)	56h	yes
REWIND (6)	01h	yes
SECURITY PROTOCOL IN (12)	A2h	yes
SECURITY PROTOCOL OUT (12)	B5h	yes
SEND DIAGNOSTIC (6)	1Dh	yes
SET CAPACITY (6)	0Bh	yes
SET TIMESTAMP (12)	A4h [0Fh]	yes
SPACE (6)	11h	yes
SPACE (16)	91h	yes

Table Continued



Command	OpCode [SA / SA Qualifier]	LTO-8
TEST UNIT READY (6)	00h	yes
VERIFY (6)	13h	yes
WRITE (6)	0Ah	yes
WRITE ATTRIBUTE (16)	8Dh	yes
WRITE BUFFER (10)	3Bh	yes
WRITE DYNAMIC RUNTIME ATTRIBUTE (12)	A4h [1Eh]	yes
WRITE FILEMARKS (6)	10h	yes

New features in LTO-8 drives

Encrypt only mode

HPE LTO-8 drives have support for Encrypt only mode as defined in the T10 draft SSC-5 and ADC-4 standards. An overview of operation is provided here; for full details refer to section 4.2.29.13 of ssc5r04.

Encrypt only mode is intended to ensure that all data written to tape is encrypted. This mode of operation is determined by the value of two new bits whose values are reported in the Device Configuration Extension mode page (mode page 10h subpage 01h). The first of these bits, ACWRE (Automation Configured Writes Require Encryption) can only be configured over the automation interface by writing to the Configure Encryption Policy page (see ADC4). ACWRE is always set to '0' on power-up and cannot be altered by a Mode Select command on the host interface. The second bit, WRE (Writes Require Encryption), is configurable over the host interface using a standard Mode Select command. The values of the WRE and ACWRE bits determine Encrypt only operation as shown in the following table.

Table 8: Encrypt only functionality as determined by the WRE and ACWRE bits

WRE bit	ACWRE bit	Description
0	0	Normal mode.
0	1	Encrypt only mode - the drive is configured to require encryption for writing to partitions.
1	0	
1	1	

When the drive is in Encrypt only mode, then write commands sent to the drive will fail with CHECK CONDITION status with the sense key set to DATA PROTECT and the additional sense code set to ENCRYPTION PARAMETERS NOT USEABLE if one or more logical blocks in the active partition is not encrypted.

LTO-7 Type M media for LTO-8 drives

This feature provides the LTO-8 drive with the capability to write 9 TB on an LTO-7 cartridge instead of 6 TB as specified by the LTO-7 format. Such a cartridge is referred to as LTO-7 cartridge initialized as Type M media. When used in automation, LTO-7 cartridges initialized as Type M media use barcode labels whose last two characters are 'M8'. A normal LTO-8 cartridge is referred to as LTO-8 Type A, has a capacity of 12 TB, and is indicated with an automation barcode label whose last two characters end in 'L8'. This extra capacity is achieved through the use of a different track layout which is defined in the cartridge memory upon initialization. A normal 6TB LTO-7 cartridge is indicated with an automation barcode label ending in 'L7'.

The use of LTO-7 Type M media for LTO-8 drives allows an LTO-8 drive to write 50% more tracks than on normal LTO-7 cartridges. Although the data is written at the same linear density as LTO-7, because the LTO-8 drive has narrower read heads, it is able to read the resulting narrower tracks, whereas the read heads in an LTO-7 drive are too wide to read them.

Only new, unused LTO-7 cartridges may be initialized as LTO-7 Type M media and once initialized, cannot be changed back to a normal 6TB LTO-7 cartridge. In addition, an LTO-7 Type M cartridge can only be written and read in an LTO-8 drive; LTO-7 drives are not capable of reading LTO-7 cartridges initialized as Type M media.

An LTO-7 Type M cartridge is initialized the first time it is loaded into a LTO-8 drive. When this occurs the drive performs an initialization which configures tables in the cartridge memory with the correct track definition. These tables are different for LTO-7 format and LTO-7 Type M formats, so the drive must be set up to choose the correct format. LTO-7 Type M cartridges must be initialized in a library that supports the format and this is determined by the number on the cartridge barcode label. As stated above, if the barcode ends in 'M8' it will be initialized as LTO-7 Type M media, otherwise it will be initialized as a normal LTO-7 cartridge. To avoid the confusion of labels not matching the cartridge format, LTO-7 Type M media can only be initialized in libraries or autoloaders. However if an 'M8' barcode is inadvertently placed on a cartridge which has already been initialized as a normal LTO-7 cartridge, then it will remain an LTO-7 cartridge.

An LTO-7 cartridge initialized as Type M media also has a unique density code (0x5D) in the cartridge memory. LTO-7 Type M media can only be used with ISV software that supports it and this software should use the density code to properly handle media operations. Since initialization is controlled by the drive and library, the software need only recognize the density code to be able handle LTO-7 Type M media.

Although standalone LTO-8 drives cannot initialize LTO-7 Type M cartridges, they are fully compatible and able to read and write any LTO-7 Type M cartridges which have been previously initialized in a library.

LTO-7 cartridges initialized as Type M media support normal LTO features including encryption, data compression, partitions and LTFS. LTO-7 Type M media is only available as Read/Write cartridges, not as WORM.

New features in LTO-7 drives

Append-only mode

LTO-7 introduced support for Append-only mode as defined in the T10 draft SSC4 standard. An overview of operation is provided here; for full details refer to section 4.2.13 of ssc4r03.

The default behavior of the drive is unchanged, and may be referred to as **Overwrite-allowed** mode. When a `WRITE` command is received, the drive processes it as normal and writes data at the current logical position. This process is subject to any applicable constraints such as WORM media. Any previous data after that logical position will be overwritten.

The drive may also be configured into **Append-only** mode. In this case, write operations are only allowed when the current logical position is one of the following:

- Beginning of the partition (BOP) with nothing written to tape; or
- BOP (Beginning of the partition) with only filemarks before EOD; or
- Between BOP and EOD with only filemarks between this position and EOD; or
- EOD

Write operations will complete normally in these cases. In all other cases, where data is overwritten, the `WRITE` command will fail with `CHECK CONDITION` status, with the sense key set to `DATA PROTECT` and the additional sense code set to `OPERATOR SELECTED WRITE PROTECT`. TapeAlert flag 09h will also be set.

The desired mode of operation may be selected through the Device Configuration Extension mode page (mode page 10h subpage 01h). In particular, the `WRITE MODE` field can be set to one of the values shown in the following table.

Table 9: WRITE MODE values

Value	Description
0h	Overwrite-allowed mode
1h	Append-only mode
2h to Fh	Reserved

NOTE: Once the `WRITE MODE` is set to Append-only, it cannot be changed to Overwrite-allowed until there the drive is empty.

When the drive is in **Append-only** mode, an application may explicitly allow overwriting at a nonappend point by using an `ALLOW OVERWRITE` command. The CDB for this command includes both partition number and logical object identifier. These values must match the current logical position. If the values do not match, the command will fail with `CHECK CONDITION` status with the sense key set to `ILLEGAL REQUEST` and the additional sense code set to `SEQUENTIAL POSITIONING ERROR`. Again, the T10 draft standard ssc4r03 contains more information on the `ALLOW OVERWRITE` command.

Alternative CRC algorithm for Logical Block Protection

The Reed-Solomon CRC is supported by LTO-6, LTO-7, and LTO-8 drives. LTO-7 and LTO-8 drives also support the CRC32C (Castagnoli) polynomial. On some systems, CRC32C may be considerably faster than the Reed-Solomon polynomial. For more information on optimizing the CRC, see **https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/**.

Manageability, diagnosability and supportability (MDS)

All generations of Hewlett Packard Enterprise Ultrium drives monitor processes and events within the tape drive during operation and make decisions based on the information, for example by turning on the Cleaning LED, or Media Error LED. In addition, a considerable amount of data is collected and stored within the drive in volatile and non-volatile storage. This data may be extracted from the drive through all interface ports by software applications, library controllers, or management software.

Management software applications may, for example, be querying the drive to identify the device and which library it is located within and to find out the health of the drive. Backup or archive software applications may interrogate the drive prior to starting a backup or archive session to determine whether the drive is healthy and to check the status of Tape Alert flags for errors that may identify that the drive needs cleaning, for example.

In the event of a failure of the backup or archive operation, the drive may be interrogated and the returned data analyzed to discover whether the problem was with the cartridge, drive, or a problem with the host interface communications.

The information within the drive is also used by Support personnel to determine the health of the drive and to decide whether the drive needs replacing, and also during the repair process to quickly and accurately identify the failing component.

Set/Report time stamp

The LTO-8 drive maintains an internal timer of elapsed time from power-on. An application client can use the `SET TIMESTAMP` and `REPORT TIMESTAMP` commands as defined in SPC-4 to set or read the world time in the drive.

NOTE: The drive also has a separate timer for use in a library environment, and the two timers are maintained separately.

Device statistics log page

This standard log page provides information about the utilization of the tape device. More detail can be found in the T10 draft standard SSC-5; the supported log parameters include those shown in the table below. Most of the log parameters are `counters`, and are formatted as shown in *Log parameter counter value* table. For the `medium type` descriptor, the first four bytes are a header as for the `counters` descriptor; the header is followed by six descriptors (one per supported density code / medium type combination) in the format shown in the *Log parameter medium descriptor* table. For the `string data` descriptor, the same format four-byte header is followed by an ASCII string value.

NOTE: Several parameters in this log page are designed to measure activity over a particular time period (the “Duty Cycle”), and an application may control this period by using a `LOG SELECT` command to reset the Duty Cycle Sample Time parameter. For example, the log page can be read after unloading a cartridge, and then the period reset using LOG SELECT. The values reported in the log page on subsequent `LOG SENSE` commands will cover the time since the last unload.

Table 10: Device statistics log page parameters

Parameter code	Description	Length (bytes)	Type
0000h	Lifetime volume loads	4	Counter
0001h	Lifetime cleaning operations	4	Counter
0002h	Lifetime power on hours	4	Counter
0003h	Lifetime media motion (i.e head) hours	4	Counter
0004h	Lifetime metres of tape processed	4	Counter
0005h	Lifetime medium motion (head) hours when incompatible volume was last loaded	4	Counter
0006h	Lifetime power on hours when the last temperature condition occurred (TapeAlert code 24h)	4	Counter
0007h	Lifetime power on hours when the last power consumption condition occurred (TapeAlert code 1Ch)	4	Counter
0008h	Medium motion (head) hours since last successful cleaning operation	4	Counter
0009h	Medium motion (head) hours since 2nd to last successful cleaning operation	4	Counter
000Ah	Medium motion (head) hours since 3rd to last successful cleaning operation	4	Counter

Table Continued

Parameter code	Description	Length (bytes)	Type
000Bh	Lifetime power on hours when the last operator initiated forced reset and/or emergency eject occurred	4	Counter
000Ch	Lifetime power cycles	4	Counter
000Dh	Volume loads since last parameter reset	4	Counter
000Eh	Hard write errors	4	Counter
000Fh	Hard read errors	4	Counter
0010h	Duty cycle sample time (milliseconds since last reset)	6	Counter
0011h	Read duty cycle (% of duty cycle spent processing read-type commands)	1	Counter
0012h	Write duty cycle (% of duty cycle spent processing write-type commands)	1	Counter
0013h	Activity duty cycle (% of duty cycle spent processing commands that move the medium)	1	Counter
0014h	Volume not present duty cycle (% of duty cycle when there is no volume present)	1	Counter
0015h	Ready duty cycle (% of duty cycle in the Ready state)	1	Counter
0040h	Drive manufacturer's serial number	As Inquiry page B1h	String
0041h	Drive serial number	As Inquiry page 80h	String
0080h	Medium removal prevented	1	Counter

Table Continued



Parameter code	Description	Length (bytes)	Type
0081h	Max recommended mechanism temperature exceeded	1	Counter
1000h	Medium motion (head) hours for each medium type	48	Medium

Table 11: Log parameter counter value

	7	6	5	4	3	2	1	0
0	Parameter code							
1								
2	Log flags (03h)							
3	Parameter length							
4..n	Counter value							

Table 12: Log parameter medium descriptor

	7	6	5	4	3	2	1	0
0	Reserved (0000h)							
1								
2	Density code							
3	Medium type							
4..7	Medium motion hours							

Tape diagnostics log page

This log page provides a mechanism for the drive to record a list of error events, with the most recent error event presented first. The format of each Tape Diagnostic Data log parameter is summarized in the following table. More details can be found in the T10 draft standard SSC-5.

Table 13: Log parameter - tape diagnostic data

	7	6	5	4	3	2	1	0
0	Parameter code							
1								
2	Log flags (03h)							
3	Parameter length (44h)							
4..5	Reserved (0)							
6	Density code							
7	Medium type							
8..11	Lifetime medium motion hours							
12	Reserved (0)							
13	Reserved		Reserved (0)			Sense key		
14	Additional sense code							
15	Additional sense code qualifier							
16..19	Vendor-specific code qualifier							
20..23	Product revision level							
24..27	Hours since last clean							
28	SCSI command opcode							
29		Reserved (0)				Service action		
30..31	Reserved (0)							
32..63	Medium identifier							
64			Reserved (0)				Timestamp Origin	

Table Continued

	7	6	5	4	3	2	1	0
65	Reserved (0)							
66..71	Timestamp							

Distinctive appearance

Ultrium WORM data cartridges are distinctive in appearance compared with other Ultrium cartridge types. The shell is two-tone in color with the lower half gray and the other half the same as for RW media.

Write protection tab

Ultrium WORM data cartridges have a write protect tab. The tab behaves as the tab on a Read/Write (RW) cartridge. When in the write enabled setting, appended writes will be allowed, when in the write-protect setting, writes will not be allowed. When in the write-protect setting, writes will terminate with check condition status, with sense data of 07/2700h (Data Protect/ Write Protected). Tape Alert flag 09h (Write Protect) is also set.

The WP bit in the Mode Parameter header will not reflect the write-protect status at the logical position on tape. It will reflect the status of the write-protect switch on the cartridge.

Unique Cartridge Type

So that the drive can recognize a WORM cartridge, a WORM cartridge has a unique Cartridge Type value stored within the cartridge memory. For automation configurations with auto-eject disabled, the cartridge will not be physically ejected from the drive. The cartridge will be located within the drive and held at the “ready eject” position.

Error Usage Page

For WORM cartridges, a new version of the Error Usage Page will be implemented. This version will replace the Wrap Number fields with an Error Code field. This field will contain the ASCQ value reported to the host when the associated error was detected.

Drive keeps a record of the EOPD value

The EOPD (End of Protected Data) value is a logical position on tape that is automatically calculated based on the End of Data (EOD) value. This value is read from the Cartridge Memory (CM) when the cartridge is loaded into the drive. The EOD value is an “intrinsic” code that is stored, protected, and updated after each write session in the CM of each WORM cartridge. The EOPD indicates that data between BOM (Beginning of Media) and this position cannot be over-written. The EOPD value is held within the drive memory. This values updates automatically and continuously as each block (typically 64k or 128k bytes) of data is written to the tape. The EOPD value indicates a logical position immediately after the last block of data written to tape.

When the cartridge is unloaded, the EOD value in the CM is updated to reflect the end of successfully written data. The EOPD value stored within the drive is cleared. Any future writes to the cartridge will occur after the location of the EOD, which also is the beginning location for the EOPD during the next write operation.

Only appended writes are accepted

When a WORM cartridge is present in a drive, the drive will only accept write commands (Records, File Marks) if the current logical position is at or beyond the position identified by the EOPD value. If a write command is attempted when the logical position is before EOPD, then the drive will return Check Condition status with sense 07/300Ch (Data Protect / WORM medium - Overwrite attempted). The drive will also set Tape Alert flags 3Ch (WORM medium - Overwrite attempted) and 09h (Write Protect).

See **Figure 1: Media label overview** for the special case of overwriting a media label.

Erase commands are rejected

When the drive contains a WORM cartridge, erase commands (short or long) are only executed when the logical position is at EOPD. The drive will not overwrite or erase any user data on tape; attempting to do so will result in CHECK CONDITION status with sense 07/300Ch (DATA PROTECT / WORM MEDIA – OVERWRITE ATTEMPTED), and the drive will set Tape Alert flags 3Ch (WORM medium - Overwrite attempted) and 09h (Write Protect).

`SET CAPACITY` command

The SET CAPACITY command will only be accepted and executed if the WORM cartridge has never been written too or initialized. If a SET CAPACITY command is received by the drive when the cartridge has been initialized, then the command will be terminated with Check Condition status and sense 07/300Ch (Data Protect / WORM Media – Overwrite Attempted). The drive will set Tape Alert flags 3Ch (WORM medium - Overwrite attempted) and 09h (Write protect).

Allow rewriting of media label if no user data is written to tape

This feature enables compatibility with software applications that rewrite the media label on a piece of media with no user data. The media label contains software application-related information such as a unique identification code and does not contain user data.

Writing will be allowed when the current logical position is at BOT, but there are only:

- Filemarks between this position and EOD.
- One or two sequential Records followed by any number of Filemarks, but no further Records, between this position and EOD.

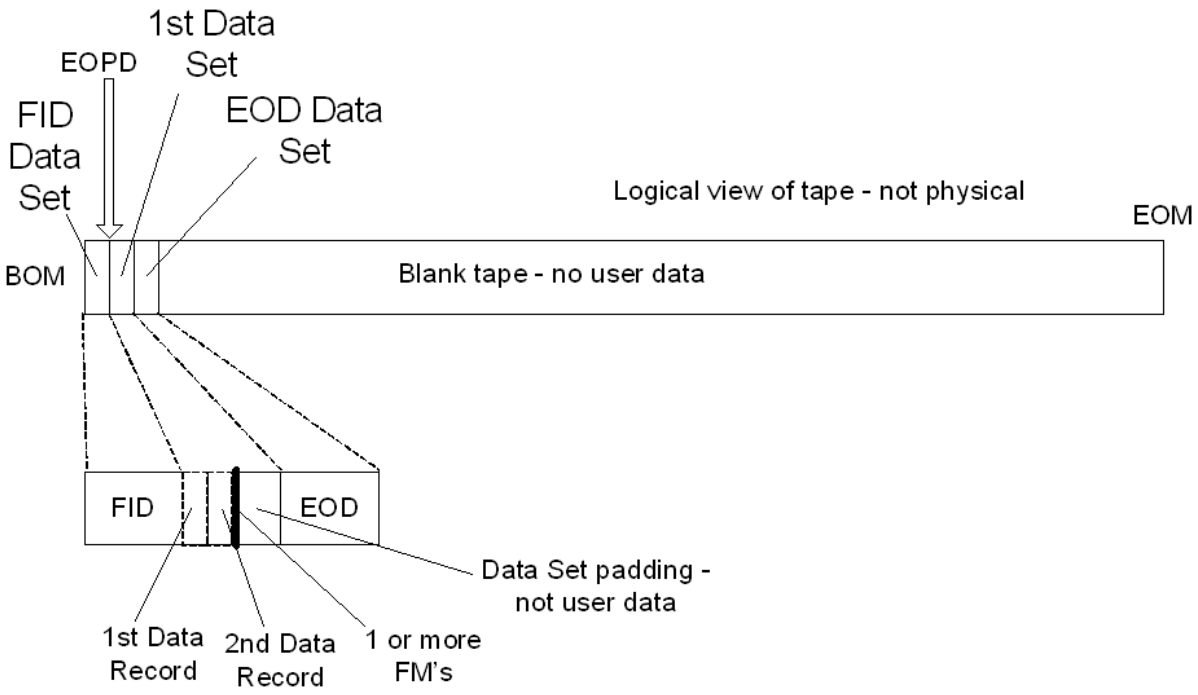

Figure 1: Media label overview

Allow overwrite of last FM(s) before EOD Data Set

It is common for software applications at the end of a backup or archive session to write two Filemarks (FMs) to tape immediately before the EOD Data Set is written. The FMs do not contain user data but are logical markers used by the application to enable the application to locate the tape in preparation for subsequent writing or reading operations. At the start of an appending archive or backup session, it is common for the application to locate the tape to a logical position immediately preceding the second FM. The second FM is over-written during the data appending session.

Writes are allowed when:

- The current logical position is at EOD. This position means that the drive must have read the EOD from tape before attempting to overwrite it.
- There are only Filemarks between the current logical position, and EOD, and that there is at least one Filemark immediately before the current logical position.

CM-Tape integrity checks

A drive that supports WORM cartridges will check that the anti-tampering measures have not been violated before and during media access operations. If a violation is detected, then the cartridge will be treated as Read-only, and Tape Alert flag 3Bh (WORM medium - integrity check failed) will be set. For example, the content of the CM does not match the content of the tape.

HPE recommends that the ISV software check for the presence of TapeAlert flag 3Bh after a tape load, and periodically during operation. If set, alert the operator and log the incident for audit purposes.

To control whether the drive returns data in cases where the drive has detected an inconsistency in the integrity checks, a WTRE field is added to the Device Configuration mode page (10h). This field allows an initiator to control behavior of device when reading WORM media when WORM integrity is in doubt.

Table 14: Device configuration mode page

	7	6	5	4	3	2	1	0
0	PS	SPF	PAGE CODE (10h)					
1	PAGE LENGTH (0Eh)							
2	Rsvd	Obsolete	CAF	ACTIVE FORMAT				
3	ACTIVE PARTITION							
4	WRITE OBJECT BUFFER FULL RATIO							
5	READ OBJECT BUFFER EMPTY RATION							
6	(MSB)	WRITE DELAY TIME						
7								(LSB)
8	OBR	LOIS	Obsolete	AVC	SOCF		ROBO	REW
9	Obsolete							
10		EOD DEFINED		EEG	SEW	SWP	BAML	BAM
11	(MSB)	OBJECT BUFFER SIZE AT EARLY WARNING						
12								
13								(LSB)
14	SELECT DATA COMPRESSION ALGORITHM							
15		WTRE	OR	REWIND ON RESET		ASOCWP	PERSWP	PRMWP

The WORM Tamper Read Enable (WTRE) field controls the behavior of the device when reading WORM media, as described in the following table.

Table 15: WORM tamper read enable control

WTRE	Behavior
00b	As for 10b
01b	Data is returned on a Read operation from WORM media regardless of whether tampering has been detected on the WORM cartridge. Set this bit **in extremis** where data recovery overrides concerns about WORM integrity.
10b	If no tampering has been detected, then data is returned as normal. If tampering is detected, then data is not returned in response to a `Read` command at or after the position of tamper. The status is check condition with sense 03/300Dh (Medium Error/WORM Medium – Integrity check) and TapeAlert flag 3Bh (WORM medium - Integrity check failed) will be set. In addition, the Error Code field in the Error Usage Page in Cartridge Memory will be filled with the ASC/Q 300Dh.
11b	Reserved

WTRE has no effect on reads of normal (non-WORM) media.

Any attempt to write, overwrite, or append to the cartridge will be terminated with Check Condition status, with sense 07/300Dh (Data Protect / WORM medium – Integrity check failed). The drive will set Tape Alert flags 3Bh (WORM medium - Integrity check failed) and 09h (Write protect).

Behavior when no EOD value is present or EOD value is inconsistent

This behavior could occur, due to CM corruption, or deliberate, malicious alteration of the EOD value in the CM. This behavior can also occur from an interruption of the drive power supply while writing data.

If a WORM cartridge contains data, but no EOD value or an EOD value within the CM that is inconsistent with the EOD position on tape, then the drive will treat the cartridge as Read-Only. The TapeAlert flags 09h (Write Protected) and 04h (Media) is set.

The drive will behave as an RW cartridge with no EOD Data Set. Except that any attempt to overwrite data will be terminated with Check Condition status and with sense 07/300Ch (Data Protect/WORM medium – Overwrite attempted). The drive will set Tape Alert flags 3Ch (WORM medium - Overwrite attempted) and 09h (Write Protect).

Identify illegal writes to WORM media or media inconsistency

The following sense codes and TapeAlert flags are supported by the drive:

Additional Sense code/Additional Sense code Qualifier:

300Ch (WORM medium - Overwrite attempted)

300Dh (WORM Medium – Integrity Check)

TapeAlert flags:

3Bh (WORM medium - Integrity check failed)

3Ch (WORM medium - Overwrite attempted)

Unique media identifier

For added security, it is recommended that ISV applications read and track cartridge manufacturer and serial number values read from the CM using the `READ ATTRIBUTE` command.

- Attribute ID 0x0400: Cartridge manufacturer ID
- Attribute ID 0x0401: Cartridge serial number

It is recommended that both values are read and concatenated to ensure the uniqueness of the number.

Automation – cartridge barcode

Ultrium barcode support is required for WORM media to distinguish WORM media from normal RW media or Cleaning cartridges by the application software and the tape library.

It is recommended that the following barcode formats are used for Ultrium media:

123456L1	Ultrium generation 1
123456L2	Ultrium generation 2
123456L3	Ultrium generation 3
123456L4	Ultrium generation 4
123456L5	Ultrium generation 5
123456L6	Ultrium generation 6
123456L7	Ultrium generation 7
123456M8	Ultrium generation 7 Type M
123456L8	Ultrium generation 8
123456LT	Ultrium generation 3 – WORM
123456LU	Ultrium generation 4 – WORM
123456LV	Ultrium generation 5 – WORM
123456LW	Ultrium generation 6 – WORM
123456LX	Ultrium generation 7 – WORM
123456LY	Ultrium generation 8 – WORM

Cartridge and data shelf-life

Ultrium cartridges are specified as having an archive life of 30 years.

Partitioning

Ultrium products from generation 5 onwards are capable of formatting media into partitions, which can then be written and read independently. This provides a mechanism for maintaining an index which can be updated without affecting the main data partition. The maximum number of partitions supported is shown in the following table:

Table 16: Number of supported partitions

Drive	Media							
	LTO-1	LTO-2	LTO-3	LTO-4	LTO-5	LTO-6	LTO-7	LTO-8 and LTO-7 Type M
LTO-1	1	n/a	n/a	n/a	n/a	n/a	n/a	n/a
LTO-2	1	1	n/a	n/a	n/a	n/a	n/a	n/a
LTO-3	1	1	1	n/a	n/a	n/a	n/a	n/a
LTO-4	n/a	1	1	1	n/a	n/a	n/a	n/a
LTO-5	n/a	n/a	1	1	2	n/a	n/a	n/a
LTO-6	n/a	n/a	n/a	1	2	4	n/a	n/a
LTO-7	n/a	n/a	n/a	n/a	2	4	4	4
LTO-8	n/a	n/a	n/a	n/a	n/a	n/a	4	4

Partition numbering

If the medium has only one partition (default), it is designated Partition 0. If a second partition is created, it is designated Partition 1. Partition 0 remains the default partition, and at load time logical position is always set to BOP of Partition 0 (BOP0).

Partition layout

The LTO format specification defines how partitions are laid out on tape. The medium is partitioned longitudinally, that is, along the whole length of the tape. There is a small loss of capacity for each additional partition created, because a “guard band” is required between the partitions; this leaves a small gap between adjacent wraps from different partitions to prevent interference between the partitions.

WORM media

Partitioning is not supported on WORM media, which will only ever have exactly one partition (Partition 0).



General operation

IMPORTANT:

Hewlett Packard Enterprise recommends that a reservation should be established prior to modifying the partition layout or changing between partitions. Failure to do so may result in unexpected behavior and possible data loss.

Load / Unload

Partition-capable drives recognize and load a partitioned cartridge, positioning to the logical beginning of partition (BOP) in partition 0. The same applies if a drive powers up with a partitioned cartridge present.

Modifying partitions

Two separate SCSI commands are needed to modify the partition layout on tape. First a `MODE SELECT` command is executed to configure the desired partition layout (number of partitions, desired size etc.) using the Medium Partition mode page. Secondly a `FORMAT MEDIUM` command is executed to actually change the tape contents. Sending the first without the second will not modify the tape.

Switching between partitions

The only way to change partitions is to use the `LOCATE(10)` or `LOCATE(16)` commands; see **LOCATE(10) and LOCATE(16) commands**. The older method of the change active partition (CAP) bit in the Device Configuration mode page is obsolete and is not supported.

Determining current partition

The `READ POSITION` command will indicate the active partition along with the logical position. Alternatively the Device Configuration mode page will also report the current active partition.

Determining partition configuration

Reading the Medium Partition mode page returns information on the number of additional partitions and the size of all partitions on the medium.

Erasing media

The `ERASE` command will only operate on the current partition. To erase partitioned media fully it will be necessary to execute `ERASE` in each partition in turn, using `LOCATE` to switch partitions.

For situations where it is also desired to remove all additional partitions (returning a partitioned cartridge to a single partition), a `SET CAPACITY` command may be used with the proportion value set to FFFFh. Another alternative is to use the `FORMAT MEDIUM` command with the format field set to 0. Both commands will result in the loss of all user data in all partitions.

Encryption parameters

The drive will retain a single set of encryption parameters for use across all partitions; switching between partitions will not affect the encryption parameters in use.

SCSI behavior specific to partitioning

LOCATE(10) and LOCATE(16) commands

The CHANGE PARTITION (CP) bit provides a method to change partitions. If CP is set to 1 for media that is not partitioned, and the PARTITION field is not set to 0 (the default partition), then the command will be terminated with CHECK CONDITION status, the sense key set to ILLEGAL REQUEST, and additional sense code set to INVALID FIELD IN CDB.

If CP is set to 0 then the PARTITION field will be ignored; if CP is set to 1 then the PARTITION field must indicate a valid partition.

READ POSITION command

All three supported formats of position data (Short, Long, Extended) support the partition number field and return the PARTITION NUMBER for the current logical position.

SET CAPACITY command

The SET CAPACITY command will return the tape to a single partition of the size specified. If the SET CAPACITY command is used to limit the apparent size of the tape, then the capacity available to future partitions will also be limited until another SET CAPACITY command is executed to restore the original size. New partitions may then be created up to the full capacity of the tape.

As specified in SSC-5, if execution of SET CAPACITY results in a change in partitioning, a Unit Attention condition will be established for all other initiators with the additional sense code set to MODE PARAMETERS CHANGED.

READ ATTRIBUTE / WRITE ATTRIBUTE

The PARTITION NUMBER field must be valid for the current medium. If a value is provided which is not valid for the current medium then the command will be terminated with CHECK CONDITION status, the sense key set to ILLEGAL REQUEST, and the additional sense code set to INVALID FIELD IN CDB.

The Partition List service action of READ ATTRIBUTE reports the number of partitions on the current medium.

FORMAT MEDIUM command

This command is supported in accordance with SSC-5. It is accepted only when the logical position is BOP in Partition 0. In all other cases the command will be terminated with CHECK CONDITION status, the sense key set to ILLEGAL REQUEST, and the additional sense code set to POSITION PAST BEGINNING OF MEDIUM.

If a FORMAT MEDIUM command is sent while WORM media is loaded, the command will be terminated with CHECK CONDITION status, the sense key set to DATA PROTECT, and the additional sense code set to WORM MEDIUM – OVERWRITE ATTEMPTED.

The IMMED bit is supported, and progress indication may be used during execution of an immediate mode FORMAT MEDIUM command to determine progress through the operation.

The VERIFY bit is not supported and must be set to 0.

The FORMAT field may take the values 0, 1 and 2 with their meaning as shown in the following table:

Table 17: Format options

Code	Description	Effect
0h	Use default format	Format medium as a single partition. All data on the physical volume is lost.
1h	Partition volume	Format medium according to the parameters in the Medium Partition mode page. All data on the physical volume may be lost.
2h	Default format then partition	Equivalent to formatting with code 0h followed by formatting with code 1h.
3–7h	Reserved	ILLEGAL REQUEST
8–Fh	Vendor-specific (not used)	ILLEGAL REQUEST

There is no format data to be transferred and so the TRANSFER LENGTH field must be 0.

Device Configuration mode page

The ACTIVE PARTITION field will reflect the partition wherein lies the current logical position.

Medium Partition mode page

The Medium Partition mode page (11h) is supported in accordance with SSC-5. Refer to the standards document for the description of fields not otherwise mentioned.

Executing MODE SELECT when incompatible media is loaded will result in CHECK CONDITION status with the sense key set to ILLEGAL REQUEST and the additional sense code set to INVALID FIELD IN PARAMETER LIST.

On MODE SELECT, the POFM (Partition On Format) bit must be set to 1 since partition configuration is only supported through the FORMAT MEDIUM command. If the POFM bit is set to 0, then the command will be terminated with CHECK CONDITION status, the sense key set to ILLEGAL REQUEST, and the additional sense code set to INVALID FIELD IN PARAMETER LIST.

There are three methods for specifying the partition sizes, using the FDP, SDP, or IDP bits (which are all mutually exclusive). The resultant partition configurations for each method are shown in the following table for LTO-7 or LTO-8 media loaded into an LTO-8 drive.

Table 18: Partition sizes for FDP=1 or SDP=1

FDP	SDP	IDP	ADDITIONAL PARTITIONS DEFINED	Resulting partition 0	Resulting partition 1	Resulting partition 2	Resulting partition 3
1	0	0	Ignored	LTO-7: 5.8 TB LTO-7 Type M: 8.8 TB LTO-8: 11.8 TB	LTO-7: 107 GB LTO-7 Type M: 107 GB LTO-8: 115 GB	0 (nonexistent)	0 (nonexistent)
0	1	0	00h	LTO-7: 6 TB LTO-7 Type M: 9 TB LTO-8: 12 TB	0 (nonexistent)	0 (nonexistent)	0 (nonexistent)
0	1	0	01h	LTO-7: 2.9 TB LTO-7 Type M: 4.4 TB LTO-8: 5.9 TB	LTO-7: 3.0 TB LTO-7 Type M: 4.5 TB LTO-8: 6.0 TB	0 (nonexistent)	0 (nonexistent)
0	1	0	02h	LTO-7: 1.9 TB LTO-7 Type M: 2.9 TB LTO-8: 3.9 TB	LTO-7: 1.9 TB LTO-7 Type M: 2.9 TB LTO-8: 3.9 TB	LTO-7: 1.9 TB LTO-7 Type M: 3.0 TB LTO-8: 3.9 TB	0 (nonexistent)
0	1	0	03h	LTO-7: 1.4 TB LTO-7 Type M: 2.1 TB LTO-8: 2.9 TB	LTO-7: 1.4 TB LTO-7 Type M: 2.1 TB LTO-8: 2.9 TB	LTO-7: 1.4 TB LTO-7 Type M: 2.1 TB LTO-8: 2.9 TB	LTO-7: 1.5 TB LTO-7 Type M: 2.2 TB LTO-8: 3.0 TB

The capacity figures shown in the previous table are nominal only, and assume that the medium capacity has not been reduced using the SET CAPACITY command; otherwise they need to be scaled accordingly.

If these combinations do not give enough control over partition size, the IDP bit can be used to request specific sizes; the drive may round the values provided since the tape format precludes arbitrary sizes.

The recommended method of specifying partitions is as follows:

- To create a single partition, set SDP = 1 and ADDITIONAL PARTITIONS DEFINED = 00.
- To create a minimal second partition, set FDP = 1.
- To create roughly equal-sized partitions, set SDP = 1 and set ADDITIONAL PARTITIONS DEFINED to the desired number of additional partitions.
- To create an arbitrary sized partition, set IDP = 1, set ADDITIONAL PARTITIONS DEFINED to the desired number of additional partitions, and set the desired PARTITION SIZE for whichever partition you wish to create.



For MODE SELECT when the IDP bit is set to 1, if one PARTITION SIZE field is set to FFFFh, the corresponding partition will occupy whatever capacity remains after satisfying the specified size for one or more other partitions.

The specified size will be rounded up to the nearest multiple-of-two wraps, and the MODE SELECT command may return sense data indicating that parameter rounding has occurred (1/3700h, Recovered Error: Rounded Parameter). The drive will round up the parameters as necessary. Partition 0 will always take precedence (be calculated first) with the highest-numbered partition occupying the remaining capacity.

If the IDP bit is set to 1 and neither PARTITION SIZE field is set to FFFFh, then the partition sizes must not exceed the total available capacity. Also specified partitions must take up the whole of the tape capacity; attempting to specify two “small” partitions will result in CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST and the additional sense code set to INVALID FIELD IN PARAMETER LIST because this tape layout is prohibited by the LTO format specification.

The size constraints are dictated by the format, which requires an even number of wraps for a partition. When a volume is partitioned, there is some capacity lost due to the overhead of the two “guard wraps” between partitions.

The CLEAR and ADDP bits must be set to 0 in any Mode Select data; if either bit is set to 1 then the command will be terminated with CHECK CONDITION status, the sense key set to ILLEGAL REQUEST, and the additional sense code set to INVALID FIELD IN PARAMETER LIST.

The PSUM and PARTITION UNITS fields are supported in accordance with SSC-5.

If the medium partition mode parameters are successfully changed using a MODE SELECT command, a MODE SENSE command will report the pending values rather than the values currently in use on the tape. Once a FORMAT MEDIUM command has completed, a MODE SENSE command will then report the values now in use on the tape.

Regardless of which method was used to specify partition sizes (FDP, SDP, or IDP bits), once a FORMAT MEDIUM command has completed, a MODE SENSE command will always report IDP=1. The drive will not retain information on how the partitions were specified.

Volume Statistics log page

The Volume Statistics log page reports values for partition-relevant parameters (0200h - 0203h). Note that all of the values previously reported in the vendor-specific Tape Capacity log page (31h) have been incorporated into the standardized Volume Statistics log page (17h). The Tape Capacity log page has been deprecated and should no longer be used.

Cartridge Memory (LTO-CM) & Medium Auxiliary Memory (MAM)

A contact-less, non-volatile EEPROM memory is embedded in every piece of Ultrium media. The LTO Cartridge Memory (LTO-CM) is designed primarily to speed up drive internal operations such as loading and spacing, but free space in the LTO-CM may be used by application software. About 1KB of cartridge memory is free and available to the host. This may be used to store “Common” information (shared by all software vendors), and “Vendor Unique” information (specific to each ISV). The LTO-CM is accessed using the `WRITE ATTRIBUTE` and `READ ATTRIBUTE` commands defined in SPC-4.

Desired application software support

The T10 standard includes “Common” attributes that all application software may maintain - these include items like ‘Application Name’ and ‘Date Last Written’. Additionally, applications may define vendor-unique attributes for their own value-add. Note that if vendor-unique attributes **are** defined, some additional method should be employed to check the integrity of those attributes since a different application may use the same attribute ID for a different vendor-unique purpose.

The MAM standard provides for the storage and access of information held as a set of pre-defined and user-definable **attributes** which are divided into six main sections as shown in the following table.

Table 19: MAM attributes

Attribute ID range	Attribute type	Written by	Typical use
0000h-03FFh	Device, standard	Tape drive, as required	Remaining capacity; tape alert flags; Load count
0400h-07FFh	Medium, standard	Media manufacturer only	Mfr name, cartridge serial number, media type
0800h-0BFFh	Host, standard	Application client	Software vendor name & version, media label
0C00h-0FFFh	Device, vendor-unique	Tape drive, as desired	Vendor-unique content
1000h-13FFh	Medium, vendor-unique	Media manufacturer	Unique identity information
1400h-17FFh	Host, vendor-unique	Application client	Proprietary content
1800h-FFFFh	Reserved	n/a	n/a

Media format and cartridge type

The following table shows which generations and types of cartridge are compatible with each Ultrium drive generation.

Table 20: Cartridge compatibility matrix

	Drive type							
Cartridge type	Ultrium 1	Ultrium 2	Ultrium 3	Ultrium 4	Ultrium 5	Ultrium 6	Ultrium 7	Ultrium 8
Ultrium 1 (100 GB)	W+R	W+R	R	–	–	–	–	–
Ultrium 2 (200 GB)	–	W+R	W+R	R	–	–	–	–
Ultrium 3 (400 GB)	–	–	W+R	W+R	R	–	–	–
Ultrium 3 WORM	–	–	WORM	WORM	R	–	–	–
Ultrium 4 (800 GB)	–	–	–	W+R	W+R	R	–	–
Ultrium 4 WORM	–	–	–	WORM	WORM	R	–	–
Ultrium 5 (1.5 TB)	–	–	–	–	W+R	W+R	R	–
Ultrium 5 WORM	–	–	–	–	WORM	WORM	R	–
Ultrium 6 (2.5 TB)	–	–	–	–	–	W+R	W+R	–
Ultrium 6 WORM	–	–	–	–	–	WORM	WORM	–
Ultrium 7 (6 TB)	–	–	–	–	–	–	W+R	W+R
Ultrium 7 WORM	–	–	–	–	–	–	WORM	WORM

Table Continued

	Drive type							
Ultrium 7 Type M (9TB)	–	–	–	–	–	–	–	W+R
Ultrium 8 (12 TB)	–	–	–	–	–	–	–	W+R
Ultrium 8 WORM	–	–	–	–	–	–	–	WORM
Universal Cleaning Cartridge[1]	Clean	Clean	Clean	Clean	Clean	Clean	Clean	Clean
Legacy Cleaning Cartridge[2]	Clean	Clean	Clean	–	–	–	–	–

[1] Hewlett Packard Enterprise Universal Cleaning Cartridge (C7978A) has an orange shell and is supported by all LTO drives.

[2] Hewlett Packard Legacy Cleaning Cartridge has (C7979A) a blue shell and is supported by a subset of LTO drives.

Identifying cartridge type via MAM read attribute

A Read-Write, WORM, or Cleaning cartridge may be identified by reading the Medium Type attribute (attribute ID 0408h) in the Media Auxiliary Memory (MAM). The attribute has the following values:

- 00h – Read-Write
- 80h – WORM
- 01h – Cleaning cartridge

Identifying cartridge type through Mode Sense Mode Parameter Header

The medium type (whether Read-Write or WORM) may be identified through the Medium Type field in the Mode Parameter Header. This value will take the form:

- 00h = No cartridge loaded
- *n*8h = Read-Write cartridge, generation *n*
- *n*Ch = WORM cartridge, generation *n*

Thus an LTO-8 Read-Write cartridge would be reported as 88h, and an LTO-7 WORM cartridge as 7Ch.

Data compression control

The data compression hardware in Ultrium drives can detect whether incoming data is already compressed and will not attempt to compress it again. The drive is able to switch dynamically and automatically between the compressing and non-compressing modes, thereby optimizing both compression ratio performance and data rate. As this mode of behavior is embedded in the Ultrium format, there is no need for host application software to switch the drive's data compression on and off and Hewlett Packard Enterprise **strongly** recommends leaving data compression ON (the default).

Desired application software support

Host applications may use the `MODE SENSE` command to read the Data Compression Mode Page (0Fh) and determine the drive's data compression characteristics; the mode page has the following format:

Table 21: Data compression mode page (0Fh)

	7	6	5	4	3	2	1	0
0	Page Code (0Fh)							
1	Page Length (0Eh)							
2	DCE	DCC (1)		Reserved (0)				
3	DDE (1)		RED (00b)	Reserved (0)				
4	(MSB)	Compression Algorithm (000000FFh)						
7								(LSB)
8	(MSB)	Decompression Algorithm (000000FFh)						
11								(LSB)
12	Reserved (0)							
15								

DCE = Data Compression Enable (0=Disabled; 1=Enabled)

DCC = Data Compression Capable (Always set to 1, Read only)

DDE = Data Decompression Enable (Always set to 1, Read only)

RED = Report Exception on Decompression (Always set to 00b)

The Compression and Decompression algorithms will always be reported as 000000FFh (Unregistered algorithm). It is permissible to set them both to 00000001h (Default algorithm) on MODE SELECT, but there is no reason to modify them nor value in doing so.

The `MODE SELECT` command may be used to turn compression on or off. However, only the DCE bit is changeable, so all other parameters must not be altered.

TapeAlert

Ultrium drives support TapeAlert (as defined in the T10 draft SSC-5 standard), in which the drive constantly monitors the condition of the mechanism and media, and presents the results in a form that host software can readily use and users can easily understand.

Implementation of the TapeAlert standard allows for predictive failure reporting. The 'Predictive Failure' flag is a single TapeAlert flag. If the drive sets this flag, then the host should display a message that the drive is 'about to fail and should be replaced'.

The full benefits of the system can only be realized if the host software can provide TapeAlert information to a Management Console (for example using SNMP) rather than basic TapeAlert. The sending of SNMP traps in response to tape drive-initiated TapeAlert flags allows network management consoles to be aware of tape drive and backup status.

The TapeAlert log page is page 2Eh. There are 64 parameters numbered from 1 through 64, with each parameter being one byte in length. A parameter is set to one when the corresponding condition has occurred.

All parameters are cleared when the log is read. The log is also cleared at power-on, on a reset condition, and by a `LOG SELECT` command. Specific flags may be cleared at other times as shown, or when corrective action has removed the condition that caused the flag to be set.

The parameters supported by drives are listed in the following table. Any parameters not shown will always be reported as 0.

Table 22: TapeAlert parameter list

Parameter		Description	Type	Also cleared on:
Dec	**Hex**			
1	0x01	Read warning	Warning	Medium removal
2	0x02	Write warning	Warning	Medium removal
3	0x03	Hard error	Warning	Medium removal
4	0x04	Media	Critical	Medium removal
5	0x05	Read failure	Critical	Medium removal
6	0x06	Write failure	Critical	Medium removal
7	0x07	Media life	Warning	Medium load
8	0x08	Not data grade	Warning	Medium removal
9	0x09	Write protect	Critical	Medium removal
10	0x0A	No removal	Information	Medium removal

Table Continued

Parameter		Description	Type	Also cleared on:
Dec	Hex			
11	0x0B	Cleaning media	Information	Medium removal
12	0x0C	Unsupported format	Information	Medium removal
14	0x0E	Unrecoverable snapped tape	Critical	Medium removal
15	0x0F	Memory in cartridge failure	Warning	Medium removal
16	0x10	Forced eject	Critical	Medium load
17	0x11	Read-only format	Warning	Medium removal
18	0x12	Tape directory corrupted	Warning	Medium removal
19	0x13	Nearing media life	Information	Medium removal
20	0x14	Clean now	Critical	Cleaning cart load
21	0x15	Clean periodic	Warning	Cleaning cart load
22	0x16	Expired cleaning media	Critical	Cleaning cart load
23	0x17	Invalid cleaning cartridge	Critical	Medium removal
25	0x19	Host channel failure	Warning	
26	0x1A	Cooling fan failure	Warning	
27	0x1B	Power supply failure	Warning	
30	0x1E	Hardware A	Critical	
31	0x1F	Hardware B	Critical	
32	0x20	Interface	Warning	
33	0x21	Eject media	Critical	Medium eject or removal

Table Continued



Parameter		Description	Type	Also cleared on:
Dec	Hex			
34	0x22	Download fault	Warning	
36	0x24	Drive temperature	Warning	Returns to compliant range
37	0x25	Drive voltage	Warning	Returns to compliant range
38	0x26	Predictive failure	Critical	
39	0x27	Diagnostics required	Warning	
41	0x29	Loader stray tape	Critical	
42	0x2A	Loader hardware	Warning	
45	0x2D	Loader magazine	Critical	
49	0x31	Diminished native capacity	Information	Medium removal, Medium load, Format as 1 partition
50	0x32	Lost statistics	Warning	Medium removal
51	0x33	Tape directory invalid at unload	Warning	Medium removal, Medium load
52	0x34	Tape system area write failure	Critical	Medium removal, Medium load
53	0x35	Tape system area read failure	Critical	Medium removal
54	0x36	No start of data	Critical	Medium removal
55	0x37	Loading failure	Critical	Medium removal
56	0x39	Unrecoverable unload failure	Critical	Medium removal
57	0x3A	Automation interface failure	Critical	

Table Continued

Parameter		Description	Type	Also cleared on:
Dec	**Hex**			
58	0x3B	Firmware failure	Warning	
59	0x3C	WORM medium - integrity check failed	Warning	Medium removal
60	0x3D	WORM medium - Overwrite attempted	Warning	Medium removal

NOTE: Medium removal means when the medium is fully removed from the drive.

Load / Unload

All Ultrium products support a partial Load operation to allow the CM (cartridge memory) to be accessed via the MAM commands without the drive needing to fully load the cartridge (load, thread the media and read the header).

Desired application software support

For a robotic arm with no integrated CM reader this feature is designed to speed up the inventorying of cartridges. It also allows the robotic controller to obtain additional information about each individual cartridge, such as its usage or format. This feature may also be used by an application to read an “application label” from the Cartridge Memory (CM) in a standalone drive or a drive within a library, without waiting for the tape drive to fully load the cartridge and then having to read the "application label" from the physical tape media.

The drive behavior is outlined in the following table. Note that the autoload field in the Control mode page (0Ah) is not supported; tape libraries can configure autoload mode using the RMC logical unit descriptor in the ADC Device Server Configuration mode page.

Table 23: Partial load drive behavior

		Load bit	Hold bit	Medium access commands[1]	MAM access commands[1]
Unload	Cartridge not removed	0	0	02/0402	Read: Good status Write: 03/0410
	Cartridge fully removed	0	0	02/3A00	Read: Good status Write: 02/3A00
Partial unload	Using HOLD bit	0	1	02/0402	Good status
Load	Cartridge fully removed	1	0	02/3A00[2]	Read: Good status Write: 02/3A00
	From the hold position	1	0	Good status	Good status
Partial load	Using HOLD bit	1	1	02/0402	Good status
Manual eject	Cartridge not removed	N/A	N/A	02/0400 then 02/0402	Read: Good status Write: 03/0410

Table Continued

		Load bit	Hold bit	Medium access commands[1]	MAM access commands[1]
	Cartridge fully removed	N/A	N/A	02/3A00	Read: Good status Write: 02/3A00
Manual load	Normal behavior	N/A	N/A	02/0401 then 06/2800 then Good status	Good status[3]

[1] The Medium Access commands and MAM Access commands columns indicate the outcome of issuing a command in that category. If not Good status then the command will result in Check Condition status, with the sense data containing the indicated sense key and ASC/Q values.

[2] When the tape drive receives a `LOAD` command, the drive may attempt a physical load operation by trying to pull the cartridge carrier tray into the drive. If no tape is sensed in the tray, the tray will be pushed back out. The operation may be retried several times by the drive firmware, before the `LOAD` command fails with Check Condition status and sense data 02/3A00 to indicate “no tape present”. Applications must not continue to issue `LOAD` commands in this situation, because drive damage may eventually occur.

[3] MAM access commands (`READ ATTRIBUTE`, `WRITE ATTRIBUTE`) commands may fail during the first part of the load with sense 03/0410 whilst the MAM is becoming accessible and actually being read; subsequent commands will return Good status (apart from 06/2800 when the load completes).

SCSI log pages

Ultrium drives support at least the following SCSI log pages:

- 00h – List of supported log pages
- 02h – Write Error Counters
- 03h – Read Error Counters
- 06h – Non-Medium Errors
- 0Ch – Sequential Access Device log
- 11h – DTD Status log
- 12h – Tape Alert Response
- 14h – Device Statistics log
- 16h – Tape Diagnostic log
- 17h – Volume Statistics log
- 1Ah – Power Condition Transitions
- 1Bh – Data compression log
- 2Eh – Tape Alert log
- 30h – Tape Usage log (**deprecated in favor of the standard Volume Statistics page**)
- 31h – Tape Capacity log (**deprecated in favor of the standard Volume Statistics page**)
- 32h – Data Compression log (**deprecated in favor of the standard Data Compression page**)
- 33h – Write Errors
- 34h – Read Forward Errors
- 37h – Performance Characteristics
- 38h – Blocks/Bytes Transferred
- 39h – Host Port 0 Interface Errors
- 3Bh – Host Port 1 Interface Errors
- 3Ch – Drive Usage Information
- 3Dh – Subsystem Statistics

Refer to the T10 draft standards SSC-5 and SPC-4 for more details of these pages.

Although some of the legacy vendor-specific pages are still supported, they have largely been replaced by standards-defined pages and their use is now deprecated. Software vendors should move to the standard pages to ensure future ongoing support.

Other pages have been discontinued and are no longer available, so must not be used to report information to the user or to determine / modify application behavior.

Vendor-specific pages may in some cases return different proprietary information from earlier drive generations.



Recommended timeout values

It is almost always preferable for an application to use appropriate timeout values for the various SCSI commands, rather than having commands time out and be aborted by the host. If the command times out then potentially useful diagnostic information will be lost; allowing the tape drive to complete the command (even if there is an error) means it can report useful sense information. This section contains recommended timeout values for each SCSI command. Ultrium generation 5 and later products also support a mechanism to retrieve suitable timeout values, as described in the following table.

SCSI command	Recommended timeout	Typical duration
Load / Unload	14 min (840 sec)	Load - 13 sec Unload - 25 sec
Rewind (full tape length)	11 min (660 sec)	105 sec
Space/Locate	49 min (2,940 sec)	210 sec
Erase (long)	33.74 hrs (121,488 sec)	27.4 hrs
Erase (short)	32 min (1,920 sec)	
Write/Write Filemarks	28 min (1,680 sec)	
Read	39 min (2,340 sec)	
Read/write attribute (MAM)	1 min (60 sec)	1 sec
Other non-tape-motion commands	1 min (60 sec)	20 ms
Security Protocol In (pages other than 0x0021)	1 min (60 sec)	20 ms
Security Protocol Out, Security Protocol In (page 0x0021)	20 min (1,200 sec)	1 sec
Verify	14.8 hrs (53,040 sec)	

The previous table displays the recommended timeout values for LTO-8 products. They are slightly different from previous generations; using the technique described in the following section avoids the need to hard code timeout values.

These values are for a single SCSI command in non-Immediate mode. As most commands (where applicable) will be sent in Immediate mode, status will be received by the host within typically 20ms. In such cases, the timeout indicates when the drive will have completed the operation and be ready for the next tape movement command.

The typical duration values reflect how long the command is normally expected to take, and indicate the margin applied.

Read, Write, and Short Erase values are too position-dependent to give meaningful ‘typical’ values, and only the recommended timeout is listed.

Space/Locate time depends on the current tape position - the “typical” time quoted is a worst-case operation time for two full-length tape traversals with no errors encountered.



The time-outs shown for Security Protocol In/Out commands are very much worst-case. Generally a SECURITY PROTOCOL OUT command will complete quickly (<1s). If the drive has write data in the buffer, then this command will be flushed before the encryption parameters are changed. Similar “flush time” must be allowed if the SECURITY PROTOCOL OUT is queued behind a REWIND or SPACE command.

All of these values are subject to change.

Using timeout descriptors

LTO-8 drives support the command timeout descriptors feature of the REPORT SUPPORTED OPERATION CODES command, which means that applications can interrogate the drive for a list of suitable time-outs rather than using hard-coded values. One example of the benefit of doing this is that a later revision of drive firmware could add further data recovery techniques, which may require longer timeout values. If the application reads the time-outs at startup, then this improvement would be available immediately.

The T10 draft SCSI standard SPC-4 contains details of the REPORT SUPPORTED OPERATION CODES command. The following table provides an overview.

Table 24: REPORT SUPPORTED OPERATION CODES CDB

	7	6	5	4	3	2	1	0
0	OPERATION CODE (A3h)							
1	SERVICE ACTION (0Ch)							
2	RCTD	Reserved (0)					REPORTING OPTIONS	
3	REQUESTED OPCODE							
4..5	REQUESTED SERVICE ACTION							
6..9	ALLOCATION LENGTH							
10	Reserved (0)							
11	CONTROL							

Set the RCTD bit to 1 to request that command timeout descriptors be returned along with one or more requested opcodes support information. Earlier generations of drives (prior to LTO-5) did not support RCTD and will reject the command, in which case the application should fall back to default timeout values. Timeout descriptors are 12 bytes in length and follow each command descriptor returned. The format of each timeout descriptor is as shown in the following table. The field of interest is the recommended command timeout which is expressed in seconds.

Table 25: Command timeout descriptors

	7	6	5	4	3	2	1	0
0..1	DESCRIPTOR LENGTH (000Ah)							
2	RESERVED (0)							
3	COMMAND SPECIFIC (0)							
4..7	NORMAL COMMAND PROCESSING TIMEOUT (00000000h)							
8..11	RECOMMENDED COMMAND TIMEOUT							

Performance optimization

Ultrium drives are capable of sustaining high transfer rate performance as shown in the following table.

Table 26: Transfer rate performance

Generation	Native transfer rate	Transfer rate assuming 2:1 compression	Native rate in performance log page	Recommended minimum transfer size
1	15 MB/s	30 MB/s	96h	64 kB
	7.5 MB/s	15 MB/s	4Bh	
	16 MB/s	32 MB/s	A0h	
2	30 MB/s	60 MB/s	12Ch	
	24 MB/s	48 MB/s	F0h	
3	80 MB/s	160 MB/s	320h	96 kB
	60 MB/s	120 MB/s	258h	
4	120 MB/s	240 MB/s	4B0h	128 kB
	80 MB/s	160 MB/s	320h	
5	140 MB/s	280 MB/s	578h	
6	160 MB/s	400 MB/s[1]	640h	
7	300 MB/s	750 MB/s[1, 2]	N/A[3]	256 kB
8	300 MB/s	750 MB/s[1, 2]	N/A[3]	256 kB

[1] Assumes 2.5:1 compression for generation 6 and up drives, due to the improved compression performance.

[2] Max transfer rate of Ultrium 7 and 8 SAS drives will be limited by the interface bandwidth.

[3] The Performance Log Page is not supported in Ultrium 7 and 8 drives

These transfer rates are only achievable with the correct “native” media type for that drive technology; for example, the Ultrium-8 drive requires Ultrium-8 media to reach the transfer rate shown. Note that the value returned will depend on the media type loaded; an Ultrium-6 drive with an Ultrium-5 cartridge will report the Ultrium-5 transfer rate.

Recommended minimum transfer sizes

In general, larger SCSI transfer sizes for Reads and Writes will result in better performance. When operating in fixed block mode the actual block size used is largely immaterial, but the size of each SCSI transfer (e.g. `WRITE` command) needs to



be maximized. Hewlett Packard Enterprise recommends the minimum transfer sizes listed in the previous table; this will maximize performance by minimizing SCSI command overheads. If the initiator supports transfers larger than these values, then they should be used since that may yield further improvements particularly with compressible data.

Maximum block size

The `READ BLOCK LIMITS` command (05h) indicates that block sizes and variable length transfer sizes are supported for values between 1 byte and 8388608 bytes. Note that other factors may limit maximum transfer sizes depending on the particular operating system and/or host controller. For more information, see **Related information**.

Media type identification

Hewlett Packard Enterprise recommends that the `REPORT DENSITY SUPPORT` command (with the `MEDIA` bit set) be used to identify the type of media loaded in the drive.

Using cartridge memory instead of tape headers

For optimum performance, it is also recommended that the host write application tape identification information to Cartridge Memory as well as (or rather than) to the actual tape. This will allow cartridges to load and unload faster. As the access method to Cartridge Memory data is an open standard, it also permits other software systems to positively identify alien media in shared storage environments. For additional information, see **Cartridge Memory (LTO-CM) & Medium Auxiliary Memory (MAM)**.

Operating system drivers

Microsoft Windows

Hewlett Packard Enterprise has a proprietary tape driver for Microsoft Windows.

UNIX

Hewlett Packard Enterprise provides the *LTO Ultrium Tape Drives Technical Reference Manual Vol 5 - UNIX, Linux, and OpenVMS Configuration Guide LTO-8 drives* to help ISVs implement Ultrium support under these operating systems. It is important to refer to the latest edition of that document for further operating system-specific details.

Encryption

Ultrium tape drives from generation four onwards have had the ability to secure data written to tape using strong encryption (AES-GCM with 256bit keys). The tape drive's functions are fairly straightforward, but to use encryption safely and effectively, users need significant guidance and help from the application which handles the encryption keys. Strong encryption of this sort is not realistically "crackable" and therefore loss of an encryption key means loss of the unencrypted data.

NOTE: Key destruction is an acceptable way of expiring or deleting data.

Standards and references

The encryption and encryption interface is based on the following standards:

- IEEE1619.1 Standard Architecture for Encrypted Variable Block Storage Media
- T10 draft SSC-5 standard (Tape Data Encryption)
- T10 draft SPC-4 standard (`SECURITY PROTOCOL IN` and `SECURITY PROTOCOL OUT` commands)

Minimum requirements

An application which supports the drive encryption features will need as a minimum to:

- Provide suitable advice and warnings to the user on appropriate use of encryption, the importance of secure key storage and other related matters
- Assist the user in generating 256bit keys and storing those keys by an appropriate method (note that this may be within the backup application itself or via interaction with some other key management device or application)
- Support the SCSI commands to interact with the tape drive including reading drive encryption capabilities, setting encryption parameters (including the key) and interpreting sense codes
- Provide some media management tools to allow identification of encrypted data on tape

Key management comments

The key management tools should be suited to the sophistication of the user, the level of security required, and the objectives of encrypting data on tape. Key management within the backup application may suit the volume of users but enterprise security objectives may differ and require external dedicated key management tools.

Standards and guidelines on all aspects of data encryption can be found on the website of the US National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC) at **http://csrc.nist.gov/CryptoToolKit/**.

Full details of how to use the encryption capabilities are given in **Encryption**.

End-to-end logical block protection

Support for End-to-End Logical Block Protection (E2E-LBP) was introduced in Ultrium 6 drives. E2E-LBP provides enhanced data protection for the full 'round trip' between an ISV backup or archive application and the Ultrium tape media. The process involves the ISV application and the tape drive utilizing an additional CRC field added to each transferred SCSI data block. The scope of the scheme covers both variable-block and fixed-block transfer modes. If there is fixed-block mode, each individual SCSI data block within a given WRITE/READ transfer has its own CRC.

E2E-LBP is an option configurable by the ISV to be enabled or disabled at any convenient point in proceedings. Data is stored on the Ultrium media using the same LTO format whether E2E-LBP was applied at any stage. Full backwards compatibility is preserved between any E2E-LBP protected transfers and data stored on any supported Ultrium media.

E2E-LBP utilizes the LTO Reed-Solomon CRC scheme (specified in ECMA-319) - which has always been applied internally by all generations of LTO drives. E2E-LBP extends the CRC scheme to the full external datapath to and from the application, including providing for early pre-emptive detection of CRC errors in the backup phase. A CRC is always calculated by LTO drives and stored along with the data on tape. An application can enable Logical Block Protection mode on reads even if it was not enabled on writes. This means that an application cannot determine whether E2E-LBP was used when the original data was written.

As mentioned in **Alternative CRC algorithm for Logical Block Protection**, LTO-8 drives also support the alternative CRC32C (Castagnoli) polynomial. CRC32C may offer better performance if the application is compiled to take advantage of the hardware support for this algorithm in some newer processors.

For further information on enabling and using E2E-LBP, see **Logical block protection**.

Websites

Hewlett Packard Enterprise Information Library

www.hpe.com/info/enterprise/docs

Single Point of Connectivity Knowledge (SPOCK) Storage compatibility matrix

www.hpe.com/storage/spock

Storage white papers and analyst reports

www.hpe.com/storage/whitepapers

Subscription Service/Support Alerts

www.hpe.com/support/e-updates

Software Depot

www.hpe.com/support/softwaredepot

Serviceguard Solutions for HP-UX

www.hpe.com/info/hpux-serviceguard-docs

For additional websites, see **Support and other resources**.

General documents and standardization websites

General LTO technology information

www.lto.org

T10 Documents (SCSI standards and specifications under development)

www.t10.org

INCITS (published SCSI standards)

www.incits.org

ISO (International Standards Organization)

www.iso.org

Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:

  https://www.hpe.com/info/assistance

- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

  https://www.hpe.com/support/hpesc

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates:

  Hewlett Packard Enterprise Support Center

  https://www.hpe.com/support/hpesc

  Hewlett Packard Enterprise Support Center: Software downloads

  https://www.hpe.com/support/downloads

  My HPE Software Center

  https://www.hpe.com/software/hpesoftwarecenter

- To subscribe to eNewsletters and alerts:

  https://www.hpe.com/support/e-updates

- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:

  https://www.hpe.com/support/AccessToSupportMaterials

IMPORTANT: Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HPE Passport set up with relevant entitlements.

Remote support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

If your product includes additional remote support details, use search to locate that information.

Remote support and Proactive Care information

HPE Get Connected

https://www.hpe.com/services/getconnected

HPE Proactive Care services

https://www.hpe.com/services/proactivecare

HPE Datacenter Care services

https://www.hpe.com/services/datacentercare

HPE Proactive Care service: Supported products list

https://www.hpe.com/services/proactivecaresupportedproducts

HPE Proactive Care advanced service: Supported products list

https://www.hpe.com/services/proactivecareadvancedsupportedproducts

Proactive Care customer information

Proactive Care central

https://www.hpe.com/services/proactivecarecentral

Proactive Care service activation

https://www.hpe.com/services/proactivecarecentralgetstarted

Warranty information

To view the warranty information for your product, see the links provided below:

HPE ProLiant and IA-32 Servers and Options

https://www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise and Cloudline Servers

https://www.hpe.com/support/EnterpriseServers-Warranties

HPE Storage Products

https://www.hpe.com/support/Storage-Warranties

HPE Networking Products

https://www.hpe.com/support/Networking-Warranties

Regulatory information

To view the regulatory information for your product, view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products*, available at the Hewlett Packard Enterprise Support Center:

https://www.hpe.com/support/Safety-Compliance-EnterpriseProducts



Additional regulatory information

Hewlett Packard Enterprise is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements such as REACH (Regulation EC No 1907/2006 of the European Parliament and the Council). A chemical information report for this product can be found at:

https://www.hpe.com/info/reach

For Hewlett Packard Enterprise product environmental and safety information and compliance data, including RoHS and REACH, see:

https://www.hpe.com/info/ecodata

For Hewlett Packard Enterprise environmental information, including company programs, product recycling, and energy efficiency, see:

https://www.hpe.com/info/environment

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (**docsfeedback@hpe.com**). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.

Related information

The following documents and websites provide related information:

- LTO Ultrium Technical Reference Manual Vol 5: Unix, Linux and OpenVMS Configuration Guide
- T10 draft standards: SSC-5, SPC-4, ADC-4
- Documentation: **http://www.hpe.com/support/manuals**
- Intel document on optimizing CRC calculations:

  https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/

Diagnostic features

This section describes some of the diagnostic features that are available in Ultrium drives. See **Manageability, diagnosability and supportability (MDS)**.

Set Capacity command

Problem to be addressed: The ever-greater capacity of the tapes make it harder and more time consuming to test tape spanning with each successive generation of Ultrium drives.

Details: Implements the `SET CAPACITY` SCSI command in such a way that it adjusts the position of the tape turn-around (wrap) point on the tape so that the tape appears logically shorter than it actually is.

The SSC-5 standard includes some guidelines on usage; those most pertinent are:

- The command shall only be accepted at BOP.
- The new capacity is set as a proportion of the total volume capacity, with the value being the numerator to a fraction with a denominator of 65535. So for a 400GB (native) tape, the smallest specifiable capacity would be 400GB/65535 = 6.25MB. Note that use of small values that would result in a tape that is shorter than the legal physical format (around 50m of tape length) will result in a minimum tape length, and no error will be reported to the host.
- A valid `SET CAPACITY` command shall cause all data on the entire physical volume to be lost.

It is allowed and indeed expected that data is not preserved across invocations of this command; effectively becoming unreachable.

NOTE: The `SET CAPACITY` command will only be accepted for a WORM cartridge if it has never been written to previously.

Drive (DTD) status log page

Problem to be addressed: To get a snapshot of the current state of the drive, it is necessary to issue multiple commands including some diagnostics which are not well documented or portable. The information must then be extracted and combined to form a complete picture; and even then there are some things which cannot be determined.

Details: The T10 standards work on ADI (the automation interface) has resulted in a log page (DTD Status log page, 11h) which combines key useful information into 4 bytes. The following table summarizes the fields returned in the “Very High Frequency Data” log parameter (parameter code 0000h); refer to the T10 draft standard ADC-4 for further information.

NOTE: The log page contains other parameters as well, so the page must be parsed carefully to locate the relevant information.

Table 27: DTD status log page (11h) return data

	7	6	5	4	3	2	1	0
0	DS		SPF	Page code (11h)				
1	SUBPAGE CODE (00h)							

Table Continued

	7	6	5	4	3	2	1	0
2	PAGE LENGTH							
3								
4	PARAMETER CODE (0000h)							
5								
6	DU(0)	Obsolete	TSD(0)	ETC(0)	TMC (00b)		FORMAT AND LINKING (11b)	
7	PARAMETER LENGTH (04h)							
8	PAMR	HIU	MACC	CMPR	WRTP	CRQST	CRQRD	DINIT
9	INXTN	Reserved	RAA	MPRSNT	Reserved	MSTD	MTHRD	Mounted
10	Tape motion status							
11	VS	Reserved	TDDEC	EPP	ESR	RRQST	INTFC	TAFC

PAMR

Prevent/Allow Medium Removal

MACC

MAM Accessible

WRTP

Write Protected media

CRQRD

Clean required

INXTN

In transition

MPRSNT

Media present

MTHRD

Media Threaded

VS

Vendor Specific

EPP

Encryption parameters established

RRQST

Recovery requested

TAFC

Tape Alert state Flag Changed

HIU

Host Initiated Unload

CMPR

Compression enabled

CRQST

Clean requested

DINIT

DTD Initialized (these fields now valid)

RAA

Robotic Access Allowed

MSTD

Media seated

MOUNTED

Cartridge loaded and accessible

TDDEC

A new tape diagnostic data log entry created

ESR

Library-managed encryption requesting response

INTFC

Interface changed

The Tape motion status field describes what the drive is doing, as shown in the following table:

Table 28: Tape motion status

Status	Description
00h	No tape motion
01h	Cleaning operation in progress
02h	Tape is being loaded
03h	Tape is being unloaded
04h	Tape in motion

Table Continued

Status	Description
05h	Reading
06h	Writing
07h	Locating
08h	Rewinding
09h	Erasing
0Ah	Formatting
0Bh	Calibrating
0Ch	Other activity
0Dh	Firmware update in progress
0E–7Fh	Reserved
80–FFh	Vendor-unique status

Encryption

From the fourth generation onwards, Ultrium tape format mandates encryption support. Encryption support is defined as the capability to identify encrypted media and to support the relevant commands and sense codes. It does not mandate the ability to encrypt or decrypt data on tape. However, Hewlett Packard Enterprise Ultrium drives (generation four onwards) are fully capable of encrypting data written to tape. The objective of encrypting the data is to provide confidential data on removable tape media. Encryption can be combined with WORM technology to provide a powerful tool to meet compliance legislation and mitigate security risks associated with removable media.

The T10 SSC-5 draft standard defines a protocol for use with the SSC-4 commands `SECURITY PROTOCOL IN` and `SECURITY PROTOCOL OUT`, called “Tape Data Encryption”. This protocol provides the interface for the tape drive encryption features, and this appendix describes the LTO-8 implementation of these commands. Read this document along with SSC-5 and SPC-4 for an understanding of the tape drive interface.

Caveats

Since the tape format mandates encryption awareness, all LTO-4 and later tape drives support sense codes which need to be supported by the backup applications.

Strong encryption such as AES-GCM 256, used in Ultrium tape drives, can cause problems if not used correctly; so any applications supporting this feature need to guide and assist the user to prevent the classic pitfalls such as:

- A lost key = lost data – **no-one** can recover the backup without the key
- An insecurely stored key can give a false sense of security

Tape drive encryption overview

Ultrium tape drives implement AES-GCM 256bit encryption in the data formatting hardware. When encryption is enabled the tape drive compresses then encrypts data as it is written to tape. The diagram below simplistically shows how data is processed with or without encryption/decryption enabled. The result is that data written to tape has the same format whether encrypted or not and in theory can be read back with or without decryption turned on (although in practice this presents some challenges). To simplify diagrams in most cases only encryption is shown, but unless otherwise stated, decryption is simply the reverse process.

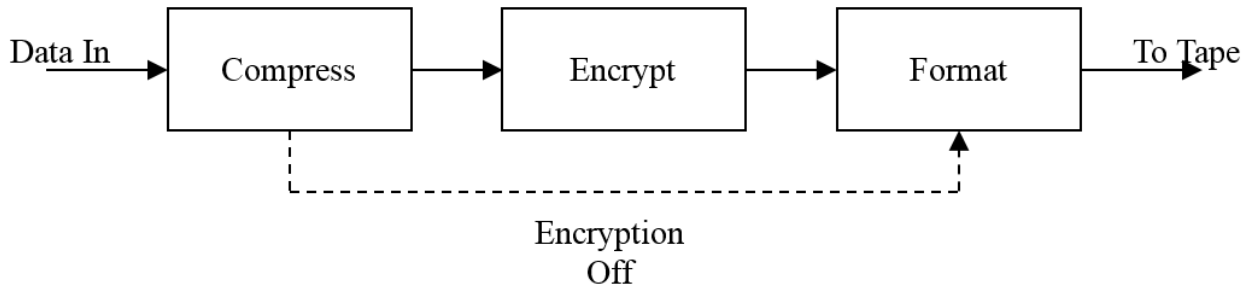

Figure 2: Encryption process

Key points:

- Filemarks are not encrypted
- Encryption does not affect locate or space operations
- Any combination of encrypted and unencrypted blocks are possible

- Different keys can be used for different encrypted blocks
- No performance impact with encryption/decryption turned on

Side effects:

- A single Ultrium format dataset on tape can only contain a single set of data encryption parameters. This means that a change to encryption parameters, e.g. an encryption key change or a switch from encrypted to unencrypted data, results in a flush of the current dataset and the start of a new one. A dataset in the LTO-4 format represents about 1.6MB of (compressed) user data, thus if there are frequent encryption parameter changes then there is likely to be some capacity wastage and some performance loss. However, this is not expected to be significant in normal usage.
- The encryption process adds approximately 74 bytes to each encrypted record. This will have an effect on capacity proportional to the record size and compression ratio of the data. Examples of capacity reductions for encrypted data is shown in the table below:

Table 29: Estimate of capacity reduction due to encryption

Record size	Non-compressible data	2:1 compressible data	3:1 compressible data
2 k	3.6%	7.2%	10.8%
64 k	0.1%	0.2%	0.3%
128 k	0.1%	0.1%	0.2%
256 k	0.03%	0.06%	0.08%

How encryption works

AES-GCM (Advanced Encryption Standard in Galois Counter Mode) is a standard encryption algorithm which uses AES in counter mode and in addition generates a tag for each record which provides a “tamper” check. AES in counter mode encrypts an incrementing counter or IV (initialization vector) with the encryption key and then XORs this with the data in 128bit blocks.

Ctr = Counter (IV)
Key = Encryption Key
E = Encryption hardware block
M = 128 bit data blocks
C = Resulting cyphertext

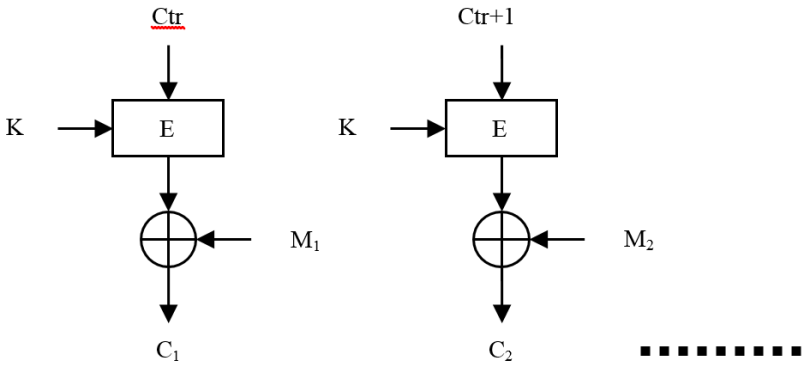

Figure 3: AES-GCM encryption

A “Galois” tag is generated over the record and appended. Failure of authentication of the tag during a decrypt operation indicates that either the encrypted data has been altered in some way, or more likely that the decryption key loaded is not the same as the encryption key.

Note that because the tag is appended to the record, it is possible that (for very large records) buffering issues and latencies will mean that parts of a record could be returned to the host prior to the completion of the authentication process. It is therefore essential that data from a record is not used until the complete record has been received. In the event of an authentication failure, any data from the affected record which has been received should be deleted by the application. This is consistent with the SAM-5 specification which says that the contents of the data-in buffer are to be treated as invalid unless the command completes with GOOD status or CONDITION MET status (see SAM-5, Execute Command procedure call).

GCM mode also defines Additional Authenticated Data (AAD) which in the LTO format is known as A-KAD (Authenticated Key Associated Data). Using these bytes is optional but they could for example be used to contain an encryption key reference. Writing the A-KAD is achieved through the KEY-ASSOCIATED DATA DESCRIPTORS LIST field in the Set Data Encryption page described in **Data encryption status page (0020h)** below.

Note that since the AAD is included in the Galois tag generation, tampering of the AAD fields would result in tag authentication failure. Therefore data such as a key reference kept in this field could in fact be incorrect. This needs to be considered in the design of a highly secure solution. Refer to **Data encryption status page (0020h)** for more detail on Key-Associated Descriptors.

An encrypted record is constructed as shown in **Figure 4: Constructing an encrypted record**.

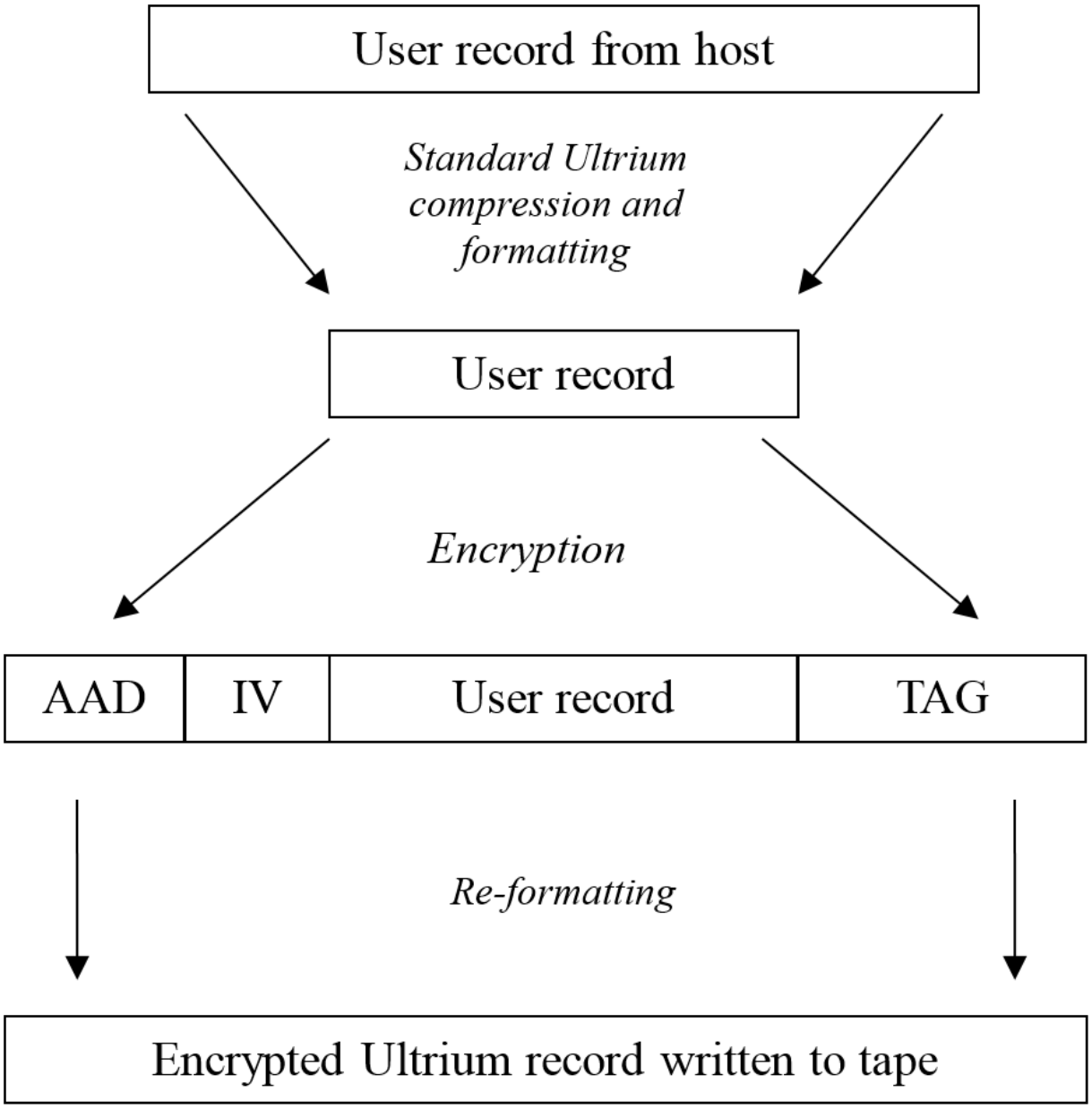

Figure 4: Constructing an encrypted record

Minimum requirements for an application supporting an encrypting tape drive

- Support the encryption command set as defined in T10 draft SSC-5 standard (see **SCSI commands**)
- Recognize and report appropriately the sense codes relating to encryption (see **Encryption sense codes and qualifiers**)
- Generate a secure 256bit data encryption key (see **Encryption sense codes and qualifiers**)
- Basic encrypted media/session management tools

- Manual key change and key management by user
- Appropriate warnings and advice to user on:
  - Key security
  - Key storage
  - Risks of losing key (i.e. won't be able to recover data)

Related standards

Ultrium format agreement

The Ultrium Technology Provider Companies (TPCs) have agreed to the LTO-8 format specification. This standardization ensures interchange of tape cartridges between all Ultrium tape drives.

T10 standards - SSC-5 and SPC-4

The definition of the SCSI command set for encryption commands has been approved and is included in the draft T10 standards SSC-5 and SPC-4; Hewlett Packard Enterprise tape drives implement these standards.

SCSI commands

The `SECURITY PROTOCOL IN` command is used to discover the type of data security features supported by the tape drive, and the current configuration and status. The `SECURITY PROTOCOL OUT` command is used to set data encryption parameters, including the data encryption key.

`SECURITY PROTOCOL IN` command and pages

Table 30: SECURITY PROTOCOL IN CDB

	7	6	5	4	3	2	1	0
0	OPERATION CODE (A2h)							
1	SECURITY PROTOCOL							
2	SECURITY PROTOCOL SPECIFIC							
3								
4	INC_512(0)	Reserved (0)						
5	Reserved (0)							
6…9	ALLOCATION LENGTH							

Table Continued

	7	6	5	4	3	2	1	0
10	Reserved (0)							
11	CONTROL							

Sending this command with the SECURITY PROTOCOL set to 00h and the SECURITY PROTOCOL specific field set to 0000h will report the list of supported security protocols:

Table 31: Supported security protocols

Code	Description
00h	Security protocol information
20h	Tape data encryption protocol

Table 32: Supported SP-In pages for Security Protocol Information (00h)

Code	Description
0000h	Supported security protocol list
0001h	Certificate data
0002h	Security compliance information

The Supported security protocol list will report support for protocols 00h and 20h.

Security Protocol 00h is the Security Protocol Information Security protocol. The Certificate Data page will report a certificate length of 0 if no certificate is installed or if the drive does not support certificates. The Security compliance information will report information relating to the security standards that apply to the drive. Refer to SPC4 for further details.

Security Protocol 20h is the Tape Data Encryption protocol; the following pages (see the following table) are supported, as may be verified by sending a SECURITY PROTOCOL IN command with the SECURITY PROTOCOL field set to 20h and the SECURITY PROTOCOL SPECIFIC field set to 0000h to request the list of supported pages.

Table 33: Supported SP-In pages for Tape Data Encryption Information Protocol (20h)

Code	Description
0000h	Tape Data Encryption In Support page
0001h	Tape Data Encryption Out Support page
0010h	Data Encryption Capabilities page

Table Continued

Code	Description
0011h	Supported Key Formats page
0012h	Data Encryption Management Capabilities page
0020h	Data Encryption Status page
0021h	Next Block Encryption Status page
0030h	Random Number page
0031h	Device Server Public Key page

Tape data encryption out support page (0001h)

The Set Data Encryption page (0010h) is the only supported Encryption Out page (see **Data encryption capabilities page (0010h)**).

Data encryption capabilities page (0010h)

The LTO-8 drive will return data as shown in the following table. The fields from byte 20-43 represent an algorithm descriptor. Multiple descriptors may be returned representing the different capabilities for each supported format (LTO-7, and LTO-8). It is therefore important to locate the correct algorithm index to ensure that you are checking the values relevant to the current cartridge.

Table 34: Data encryption capabilities

	7	6	5	4	3	2	1	0
0	PAGE CODE (0010h)							
1								
2	PAGE LENGTH (0028h)							
3								
4	Reserved (0)					EXTDECC (10b)		CFG_P
5..19	Reserved (0)							
20	ALGORITHM INDEX (LTO-7/LTO-8)							
21	Reserved (0)							
22	DESCRIPTOR LENGTH (0014h)							

Table Continued

	7	6	5	4	3	2	1	0
23								
24	AVFMV	SDK_C (0)	MAC_C (1)	DELB_C (1)	DECRYPT_C (10b)		ENCRYPT_C (10b)	
25	AVFCLP		NONCE_C (11b)		KADF_C (1)	VCELB_C (1)	UKADF (0)	AKADF (0)
26	MAXIMUM UNAUTHENTICATED KEY-ASSOCIATED DATA BYTES (0020h)							
27								
28	MAXIMUM AUTHENTICATED KEY-ASSOCIATED DATA BYTES (003Ch)							
29								
30	ENCRYPTION KEY SIZE (0020h)							
31								
32	DKAD_C (11b)		EEMC_C (10b)		RDMC_C (101b)			EAREM (1)
33	Reserved (0)							
34..35	MSDK_COUNT (0000h)							
36..39	Reserved (0)							
40	SECURITY ALGORITHM CODE (0001 0014h)							
43								

The CFG_P field indicates whether the drive is configured to allow changes to the encryption configuration. If this field contains 01b then encryption parameters may be established or changed. However, a value of 10b means that they may not be changed. The parameters may change most likely because a tape library controller is managing the drive's encryption configuration.

The Data Encryption Algorithm descriptor within the Data Encryption Capabilities page (bytes 20 to 43) contains information about one or more data encryption algorithms supported by Ultrium tape drives.

Descriptor fields

ALGORITHM INDEX	Set to 3 (LTO-7/LTO-8 media): one descriptor for each supported format
AVFMV	Set to 1 if the current cartridge is LTO-7, or LTO-8 (that is, supports encryption)

Table Continued

SDK_C	Set to 0, the drive does not support a supplemental decryption key
MAC_C	Set to 1, since the algorithm includes a message authentication code
DELB_C	Set to 1, indicating that the drive can distinguish encrypted from unencrypted blocks
DECRYPT_C	Set to 10b, the drive is capable of decrypting data in hardware using this algorithm
ENCRYPT_C	Set to 10b, the drive is capable of encrypting data in hardware using this algorithm
AVFCLP	Set to 00b if no tape, 01b if the algorithm is not valid at this position, 10b if it is valid
NONCE_C	Set to 11b, the application client may provide part or all of the nonce value
KADF_C	Set to 1, the drive supports KAD as required by the format
VCELB_C	Set to 1, the drive determines at mount time whether the volume contains encrypted blocks
UKADF	Set to 0, the drive does not enforce a fixed U-KAD length
AKADF	Set to 0, the drive does not enforce a fixed A-KAD length
MAXIMUM UNAUTHENTICATED KEY-ASSOCIATED DATA BYTES	Set to 0020h, indicating that the drive supports up to 32bytes of U-KAD
MAXIMUM AUTHENTICATED KEY-ASSOCIATED DATA BYTES	Set to 003Ch, indicating that the drive supports up to 60 bytes of A-KAD
KEY SIZE	Set to 0020h, the drive accepts (only) 256-bit data encryption keys (32 bytes)
DKAD_C	Set to 11b, the drive is KAD-capable (can accept KAD but not required)
EEMC_C	Set to 10b, the drive will accept write operations in External Encryption mode

Table Continued

RDMC_C	Set to 101b. By default the drive will write data that can be read in Raw Decryption mode. This behavior can be changed through the RDMC field in the Set Data Encryption page. **NOTE:** This is a change from earlier generations of LTO drives. See sections **Set Data Encryption Page (0010h)** and **Tape copying**.
EAREM	Set to 1, the drive always records the encryption mode with each recorded block
MSDK_COUNT	Always 0, the drive does not support supplementary decryption keys
SECURITY ALGORITHM CODE	00010014h – the identifier for the AES-GCM encryption algorithm

Supported key formats page (0011h)

The LTO-8 drive supports two different key formats: plaintext and wrapped. This support is indicated in the Supported Key Formats page as shown in the following table.

Table 35: Supported key formats

	7	6	5	4	3	2	1	0
0	PAGE CODE (0011h)							
1								
2	PAGE LENGTH (0002h)							
3								
4	First supported key format: 00h (plaintext keys)							
5	Second supported key format: 02h keys wrapped with Device server public key							

Data encryption management capabilities page (0012h)

This page reports the capabilities of the drive with regard to the features available for managing encryption. The response is as shown in the following table.

Table 36: Data encryption management capabilities

	7	6	5	4	3	2	1	0
0	PAGE CODE (0012h)							
1								
2	PAGE LENGTH (000Ch)							
3								
4	Reserved (0)							LOCK_C(1)
5	Reserved (0)					CKOD_C(1)	CKOPR_C(1)	CKORL_C(1)
6	Reserved (0)							
7	Reserved (0)					AITN_C(1)	LOCAL_C(1)	PUBLIC_C(1)
8..15	Reserved (0)							

LOCK_C	The LOCK bit is supported
CKOD_C	The Clear Key on Dismount bit is supported
CKORP_C	The Clear Key on Reservation Pre-empt bit is supported
CKORL_C	The Clear Key on Reservation Loss bit is supported
AITN_C	ALL I_T NEXUS scope is supported
LOCAL_C	LOCAL scope is supported
PUBLIC_C	PUBLIC scope is supported

Data encryption status page (0020h)

This page contains information about the current encryption configuration of the drive. The following table shows the fields and details available.

Table 37: Data encryption status

	7	6	5	4	3	2	1	0
0	PAGE CODE (0020h)							
1								
2	PAGE LENGTH (n-3)							
3								
4	Reserved (0)						KEY SCOPE	
5	ENCRYPTION MODE							
6	DECRYPTION MODE							
7	ALGORITHM INDEX							
8..11	KEY INSTANCE COUNTER							
12	Reserved		PARAMETERS CONTROL		VCELB		CEEMS	RDMD
13	ENCRYPTION PARAMETERS KAD FORMAT							
14..15	ASDK_COUNT (0000g)							
16..23	Reserved							
24..n	KEY-ASSOCIATED DATA DESCRIPTORS LIST							

I_T NEXUS SCOPE

Contains the value from the data encryption scope saved for the I_T nexus on which this command was received.

KEY SCOPE

Contains the scope value for the key that the drive will use for a read/write command received on the current I_T nexus.

Possible scope values are shown in the following table (see **Set Data Encryption Page (0010h)** for descriptions).

Table 38: Encryption parameters scope values

Code	Name
0	Public
1	Local
2	All I_T Nexus

The possible combinations of I_T nexus and key scopes are shown in the following table:

Table 39: Combined scope values

I_T nexus scope	Key scope	Comments
Public	Public	There is no key set for this I_T nexus
Public	All I_T Nexus	This I_T nexus will use a key set by another I_T nexus which has a scope of All I_T Nexus
Local	Local	This I_T Nexus is using its own security parameters which are not shared with others
All I_T Nexus	All I_T Nexus	This I_T Nexus is using its own security parameters which are shared with other I_T Nexi whose scopes are Public

ENCRYPTION MODE

The possible values are shown in the following table:

Table 40: Encryption modes

Code	Name	Description
0h	Disable	Data encryption disabled
1h	External	Data being written has been pre-encrypted with an algorithm specified by the ALGORITHM INDEX field
2h	Encrypt	Data written will be encrypted

DECRYPTION MODE

The possible values for this field are:

Table 41: Decryption modes

Code	Name	Description
0h	Disable	Data decryption disabled
1h	Raw	Data decryption is disabled. Data being read will be returned in its encrypted state. If unencrypted, data is encountered an error will be returned
2h	Decrypt	Data decryption enabled
3h	Mixed	Encrypted and unencrypted data will be returned without error as long as the drive has the correct encryption parameters set for the encrypted data

ALGORITHM INDEX

The index value of the algorithm in use (00h for none, 03h for LTO-7 and LTO-8).

KEY INSTANCE COUNTER

The tape drive keeps a counter for each key that it is managing, called the key instance counter. All key instance counters are set to zero when a drive reset occurs. Any other event that sets, clears, or changes a value in a set of data encryption parameters causes the key instance counter for that set parameters to be incremented. The key instance counter is 32 bits long and rolls over to zero when incremented beyond this.

PARAMETERS CONTROL

This specifies information on how the encryption parameters are controlled according to the following table. This specifies information on how the encryption parameters are controlled according to the following table:

Table 42: Encryption parameters control

Code	Description
000b	Encryption parameters control is not reported
001b	Encryption parameters are not exclusively controlled by external data encryption control
010b	Encryption parameters are exclusively controlled by the sequential access device server
011b	Encryption parameters are exclusively controlled by the automation/drive interface (ADI) device server
100b	Encryption parameters are exclusively controlled by a management interface
Other	Reserved



VCELB

Volume Contains Encrypted Logical Blocks. This bit will be set (1) if media is loaded and contains at least one encrypted logical block, and clear (0) if not.

CEEMS

Check External Encryption Mode Status. This reports the value of CEEM in the current encryption parameter set. See **Tape copying** for more information on keyless copy controls.

RDMD

Raw Decryption Mode Disabled. This is set to 1 if the tape drive is configured to write encrypted data that cannot be read in RAW decrypt mode. A value of 0 indicates that data written will be readable in RAW mode. See **Tape copying** for more information on keyless copy controls.

ENCRYPTION PARAMETERS KAD FORMAT

This field contains the value of the KAD Format field set when the initiator set the encryption parameters.

KEY-ASSOCIATED DATA DESCRIPTORS LIST

If both ENCRYPTION MODE and DECRYPTION MODE are set to DISABLE, then the KEY-ASSOCIATED DATA DESCRIPTORS LIST will not be included in this page.

KEY-ASSOCIATED DATA DESCRIPTORS

If present, Key-Associated Data Descriptors use the following format:

Table 43: Key-associated data descriptors

	7	6	5	4	3	2	1	0
0	KEY DESCRIPTOR TYPE							
1	Reserved (0)							AUTHENTICATED
2	KEY DESCRIPTOR LENGTH (n-3)							
3								
4...n	KEY DESCRIPTOR							

KEY DESCRIPTOR TYPE:

Table 44: Key descriptor types

Code	Description
00h	Unauthenticated key-associated data
01h	Authenticated key-associated data
02h	Nonce value
03h	Security Metadata key-associated data

AUTHENTICATED

For SECURITY PROTOCOL OUT pages, this field is reserved and must be set to 0.

For SECURITY PROTOCOL IN pages, the following values are defined:

Table 45: Key descriptor types

Code	Description	When reported
000b	Reserved	Encryption Status page
001b	Not covered by the authentication algorithm	Next Block Encryption Status page, U-KAD
010b	Authentication not attempted	Next Block Encryption Status page, A-KAD(or S-KAD in RAW mode)
Other	Not supported by Ultrium drives	

KEY DESCRIPTOR

Contains the key descriptor data bytes.

Next block encryption status page (0021h)

This page contains information about the next logical block (object) with regard to its encryption status. Details are shown in the following table.

Table 46: Next block encryption status page

	7	6	5	4	3	2	1	0
0	PAGE CODE (0021h)							
1								
2	PAGE LENGTH (n-3)							
3								
4..11	LOGICAL OBJECT NUMBER							
12	COMPRESSION STATUS (0h)				ENCRYPTION STATUS			
13	ALGORITHM INDEX							
14	Reserved (0)						EMES	RDMDS

Table Continued

	7	6	5	4	3	2	1	0
15	NEXT BLOCK KAD FORMAT							
16..n	KEY-ASSOCIATED DATA DESCRIPTORS							

LOGICAL OBJECT NUMBER

The logical block to which this page is referring (records plus filemarks).

COMPRESSION STATUS

This will always be reported as 0h; this field is not supported by Ultrium drives.

ENCRYPTION STATUS

The following codes are supported by Ultrium drives:

Table 47: Logical block encryption status values

Code	Description
0h	The drive is not capable of determining if the next logical object is encrypted
1h	The drive is capable of determining if the next logical object is encrypted but cannot because: • the next logical block has not been read into the buffer • there was an error reading the next logical block • there are no more logical blocks (EOD)
2h	The object referenced by the LOGICAL OBJECT NUMBER is not a logical block
3h	The next logical block is not encrypted
4h	The next logical block is encrypted but not with a supported algorithm
5h	The next logical block is encrypted using an algorithm supported by the tape drive
6h	The next logical block is encrypted using an algorithm supported by the tape drive. However, the tape drive is unable to decrypt the block or does not have the correct key or nonce value to decrypt the block

ALGORITHM INDEX

The index number of the algorithm used to encrypt the block (03h for LTO-7 and LTO-8)

EMES

Encryption Mode External Status: Set to 1 if the next logical block is encrypted and was written in EXTERNAL encrypt mode; otherwise set to 0

RDMDS

Raw Decryption Mode Disabled Status: Set to 1 if the next logical block is encrypted and when written was marked as disabled for RAW decrypt mode; set to 0 otherwise (see **Tape copying**).

KEY-ASSOCIATED DATA DESCRIPTORS

Refer to the description in **Data encryption status page (0020h)**.

Device server key wrapping public key page (0031h)

If the application client desires to send the encryption key wrapped with the device server public key, then it must first read this page to determine the public key to be used in the wrapping. For more information on key format 02h, see **Data encryption capabilities page (0010h)**. The returned data will take the form shown in the following table.

Table 48: Device server key wrapping public key page

	7	6	5	4	3	2	1	0
0	PAGE CODE (0031h)							
1								
2	PAGE LENGTH (522)							
3								
4…7	PUBLIC KEY TYPE (00000000h)							
8…11	PUBLIC KEY FORMAT (00000000h)							
12	PUBLIC KEY LENGTH (00000000h)							
13								
14…525	PUBLIC KEY							

PUBLIC KEY TYPE, PUBLIC KEY FORMAT

Always 00000000h, indicating that the key is of type RSA2048 (length will always be 512)

PUBLIC KEY

Bytes 0-255 contain the modulus **n**, bytes 256-511 contain the public exponent **e**

Refer to T10 draft standard SSC-5 and PKCS#1 V2.1 for further details.

SECURITY PROTOCOL OUT command and pages

Table 49: SECURITY PROTOCOL OUT CDB

	7	6	5	4	3	2	1	0
0	OPERATION CODE (B5h)							
1	SECURITY PROTOCOL (20h)							
2	SECURITY PROTOCOL SPECIFIC (0010h)							
3								
4	INC_512(0)			Reserved (0)				
5	Reserved (0)							
6…9	ALLOCATION LENGTH							
10	Reserved (0)							
11	CONTROL							

SECURITY PROTOCOL

This command must be set to 20h, specifying Tape Data Encryption

SECURITY PROTOCOL SPECIFIC

This command must be set to 0010h, specifying the Set Data Encryption Page

Set Data Encryption Page (0010h)

Encryption is set up and configured by sending this page to the drive. The various fields are shown in the following table:

Table 50: Set Data Encryption page

	7	6	5	4	3	2	1	0
0	PAGE CODE (0010h)							
1								
2	PAGE LENGTH (m-3)							
3								
4	SCOPE				Reserved			LOCK

Table Continued

	7	6	5	4	3	2	1	0
5		CEEM		RDMC	SDK (0)	CKOD	CKORP	CKORL
6	ENCRYPTION MODE							
7	DECRYPTION MODE							
8	ALGORITHM INDEX							
9	KEY FORMAT							
10	KAD FORMAT							
11..17	RESERVED							
18	KEY LENGTH							
19								
20..n	KEY							
n+1..m	KEY-ASSOCIATED DATA DESCRIPTORS LIST							

SCOPE

This determines how the encryption parameters will be applied, as shown in the following table:

Table 51: Set Data encryption scope

Code	Name	Description
0	Public	All fields other than the LOCK bit are ignored. This I_T nexus will use data encryption parameters that have been set by another I_T nexus with a SCOPE of ALL_IT_NEXUS. If no I_T nexus has set encryption parameters with the SCOPE of ALL I_T NEXUS, then the tape drive will use the default data encryption parameters. PUBLIC is the default SCOPE
1	Local	The data encryption parameters are unique to the I_T nexus sending the `SECURITY PROTOCOL OUT` command. The parameters will not be shared with any other I_T nexus.
2	All_IT_Nexus	The data encryption parameters will be shared with all I_T nexuses. In particular, other I_T nexuses with a scope of PUBLIC will use the encryption parameters set by this I_T nexus.

LOCK

If the LOCK bit is set, then the key instance counter and encryption parameters received with the `SECURITY PROTOCOL OUT` command are locked to this I_T nexus until a hard reset occurs or until another Set Data Encryption page from that I_T nexus is processed. If the key instance counter changes, then all subsequent write commands received from that I_T nexus will terminate with check condition status until a hard reset occurs, or until a new Set Data Encryption page is received from that I_T nexus.

CEEM

Check External Encryption Mode – part of the keyless copy controls mechanism. Specifies what checks to perform when reading data; possible values are shown in the following table. See **Tape copying** for more information on keyless copy controls.

Table 52: Check External Encryption Mode

Code	Description
00b	Vendor-specific; for LTO-8 drives this mode has the same meaning as 01b.
01b	Do not check the encryption mode that was used to write the block.

Table Continued

Code	Description
10b	Check the encryption mode that was used to write the block. Report Check Condition (sense key 7h, ASC/Q 7409h) if it was written in EXTERNAL mode.
11b	Check the encryption mode that was used to write the block, report Check Condition (sense key 7h, ASC/Q 7409h) if it was written in ENCRYPT mode.

RDMC

Raw Decryption Mode Control – part of the keyless copy controls mechanism. Specifies if data written to the medium should be marked as allowing RAW decrypt mode reading. Supported values are shown in the following table. See **Tape copying** for more information on keyless copy controls.

Table 53: Raw Decryption Mode Control

Code	Description
00b	The drive will follow its default setting, see RDMC_C in the Encryption Capabilities page. For LTO-8 drives this is the same as specifying 10b.
01b	Reserved.
10b	Mark each logical block as enabled for RAW decrypt mode operations.
11b	Mark each logical block as disabled for RAW decrypt mode operations.

SDK

Must be set to 0; Supplemental Decryption Keys are not supported.

CKOD

Clear Key On Dismount - if this bit is set then the tape drive will set the encryption parameters to default values when the tape is unloaded.

CKORP

Clear Key On Reservation Pre-empt – if this bit is set then the tape drive will set the encryption parameters to default values when a persistent reservation is preempted.

If there is no persistent reservation in effect for this I_T nexus, then the drive will return an error (sense key ILLEGAL REQUEST with additional sense code INVALID FIELD IN PARAMETER DATA).

CKORL

Clear Key On Reservation Loss – if this bit is set then the tape drive will set the encryption parameters to default values on a reservation loss.

If there is no reservation in effect for this I_T nexus, then the drive will return an error (sense key ILLEGAL REQUEST with additional sense code INVALID FIELD IN PARAMETER DATA).

ENCRYPTION MODE

This is described in **Data encryption status page (0020h)**.

DECRYPTION MODE

This is described in **Data encryption status page (0020h)**.

ALGORITHM INDEX

Either the specific algorithm index to use (03h for LTO-7 and LTO-8) or the default index (01h) in which case the drive will automatically select the correct algorithm for the current media.

KEY FORMAT

Must be set to 00h (the KEY field contains the plaintext key), or 02h (the KEY field contains a wrapped key as described in SSC-5).

KAD FORMAT

Identifies the format of any key-associated data stored in the U-KAD and/or A-KAD.

Table 54: KAD format

Value	Description
00h	Unspecified
01h	A binary key name
02h	An ASCII key name
03h-FFh	Reserved

If the KAD format field is set to a non-zero value, then the key name is comprised of:

- The A-KAD, if only an A-KAD descriptor is provided; or
- The U-KAD, if only a U-KAD descriptor is provided; or
- The A-KAD followed by the U-KAD, if both descriptors are provided

KEY LENGTH

Number of bytes in the encryption key.

For KEY FORMAT 00h, the length must be 0020h that is, a 256-bit key.

For KEY FORMAT 02h, the length indicates the total length of the wrapped key field.

KEY

When KEY FORMAT is set to 00h, this is the 256-bit data encryption key.

When KEY FORMAT is set to 02h, this field contains a wrapped key.

KEY-ASSOCIATED DATA DESCRIPTORS LIST

The format of the key-associated data descriptors is described in **Data encryption status page (0020h)**.

Default data encryption parameters

Table 55: Default data encryption parameters

Field	Default value
Scope	Public
Lock	0
Encryption mode	Disable
Decryption mode	Disable

Encryption sense codes and qualifiers

Table 56: Sense data pertaining to encryption

Sense key	ASC	ASCQ	Description	Meaning
07h (Data protect)	74h	00h	Security error	Generic security error indication
07h (Data protect)	74h	01h	Unable to decrypt data	Generic security error indication
07h (Data protect)	74h	02h	Unencrypted data encountered while decrypting	When reading, the drive has encountered an encrypted block but decryption is not enabled
07h (Data protect)	74h	03h	Incorrect data encryption key	Decryption mode is enabled, but the read has found unencrypted data
07h (Data protect)	74h	04h	Cryptographic integrity validation failed	The current key does not match the key used to encrypt the next logical block
07h (Data protect)	74h	09h	Encryption mode mismatch on Read	The next block failed the integrity validation process as the drive attempted to read it

Table Continued

Sense key	ASC	ASCQ	Description	Meaning
07h (Data Protect)	74h	0Ah	Encrypted block not Raw-Read enabled	Decryption mode is set to RAW but the next logical block is marked as disabled for RAW mode reads
07h (Data Protect)	74h	0Dh	Encryption algorithm disabled	The algorithm specified in the Algorithm Index field was disabled by external data encryption control
07h (Data Protect)	74h	21h	Data encryption configuration prevented	External data encryption control has configured the drive not to accept control of encryption parameters from this port
07h (Data Protect)	74h	61h	External data encryption key manager access error	A cryptographic key could not be provided because an unrecoverable error occurred while attempting to access an external key manager
07h (Data Protect)	74h	62h	External data encryption key manager error	A cryptographic key could not be provided because the key manager returned an error
07h (Data Protect)	74h	63h	External data encryption key not found	A cryptographic key could not be provided because the requested key was not found
07h (Data Protect)	74h	64h	External data encryption request not authorized	Requesting a cryptographic key is not authorized

Table Continued



Sense key	ASC	ASCQ	Description	Meaning
07h (Data Protect)	74h	6Eh	External data encryption control timeout	The data encryption period timer expired whilst waiting for an external key manager to provide a key
07h (Data Protect)	74h	6Fh	External data encryption control error	An unspecified error occurred while attempting to retrieve a key
07h (Data Protect)	74h	71h	Logical Unit Access not authorized	An external device is controlling drive encryption and has not allowed the drive to decrypt data for this initiator
07h (Data Protect)	74h	80h	Key-associated data descriptors changed (VENDOR-UNIQUE)	The key-associated data descriptors have changed from those in the last logical block
07h (Data Protect)	26h	10h	Data decryption key fail limit reached	Ten incorrect keys have been tried consecutively in an attempt to read an encrypted block
06h (Unit Attention)	2Ah	11h	Data encryption parameters changed by another I_T nexus	Using shared (public) encryption parameters, which have been changed by a different initiator
06h (Unit Attention)	2Ah	12h	Data encryption parameters changed by vendor specific event	One of CKOD, CKORL or CKORP bits were set in the SP-Out, and the corresponding condition has occurred
07h (Data Protect)	2Ah	13h	Data encryption key instance counter changed	The LOCK bit was specified in SP-Out, and the key instance counter has now changed

Encryption information in Cartridge Memory

Two MAM attributes contain information about the position of encrypted blocks of data on tape. These may be used to determine whether a given cartridge contains any encrypted data.

Attribute **0224h** returns the logical position of the first encrypted logical block in the specified partition. If there is no encrypted logical block in the specified partition then the value FFFF FFFF FFFF FFFFh is returned. If it is not known whether there are any encrypted logical blocks, then the value FFFF FFFF FFFF FFFEh is returned.

Attribute **0225h** returns the logical position of the first unencrypted block in the specified partition which is located after the first encrypted logical block. The value FFFF FFFF FFFF FFFFh is returned if there is no encrypted logical block in the specified partition, or if there is no unencrypted block after the first encrypted block. The value FFFF FFFF FFFF FFFEh is returned if it is not known whether there are any encrypted logical blocks, or whether there are any unencrypted logical blocks after the first encrypted logical block.

As an example, consider the case where attribute 0224h contains the value 3h and attribute 0225h contains all FFh bytes. Taken together, these values indicate that the first three blocks (at logical positions 0, 1 and 2) are not encrypted, the block at logical position 3 is encrypted, and everything from logical position 3 to the end of the specified partition is also encrypted.

Usage recommendations

Detecting encryption capability

Encryption capability should not be predicated on the drive generation or inquiry data. A better solution is to use the `SECURITY PROTOCOL IN` command to read the Data Encryption Capabilities page. Look at the ENCRYPT_C and DECRYPT_C fields to confirm the capabilities of the drive; if the drive is able to control encryption and decryption via the primary port, then both fields will have the value 2.

Enabling encryption

Use the `SECURITY PROTOCOL OUT` command, recommended SCOPE is LOCAL (separate encryption parameters per initiator), Encryption Mode ENCRYPT, Decryption Mode DECRYPT. Include the key and any key-associated data (for example a key identifier) and set the KAD FORMAT field to indicate the format of the key identifier. If in a multi-initiator environment, the LOCK bit should be set to 1 so that the application is notified if there are any changes to the encryption parameters.

Disabling encryption

Use the `SECURITY PROTOCOL OUT` command, setting the SCOPE to PUBLIC and both Encryption and Decryption Modes to DISABLE. With these settings, the key length can be set to 0 and no key need be supplied.

Persistent reservation

It is strongly recommended that initiators employing encryption use reservations (persistent or “classic”) to prevent other initiators from changing encryption parameters whilst writing/reading data. Note that using LOCAL scope will reduce the risk of this; however it is still prudent to reserve the drive before writing or reading.

Tape copying

With the advent of encryption, it is no longer possible to create a “simple” tape copy because the key used for encryption must be supplied to the reading drive to decrypt the data, and also the writing drive in order to re-encrypt the data onto the new tape copy. Providing the key to both drives is one solution, a “keyless copy” may be possible using Raw decryption mode and External encryption mode as defined in the T10 draft SSC-5 standard. This permits an application with no knowledge of the key to read the encrypted data stream directly from the source drive (in Raw mode), and send it

to the target drive where it can be written as-is (External mode) without further data processing. However there are several issues with this:

- There is format-specific encryption information to be transferred between tape drives, which must be done correctly to allow the new tape to be read and decrypted. This places a significant burden on the software application performing the keyless copy.
- There is a potential security hole opened up by allowing the encrypted data stream to be extracted intact, allowing the theoretical possibility of an offline security attack and potentially discovering the encryption key.
- Data could be modified before being written to the destination drive; record re-ordering or deletion cannot be prevented during keyless copy.

For these reasons, Hewlett Packard Enterprise does not recommend supporting keyless copy in applications. The safest way to successfully and securely create copies of encrypted tapes is to use the encryption key when reading, transfer the data to the new tape in the clear, and re-encrypt it in the destination tape drive using the same key (and key-associated data).

If it is desired to create a keyless copy solution, there are several security features in the LTO tape format which must be considered.

Tagging externally encrypted data

The LTO formats include a special tag to any data written in External encryption mode. When reading back, the drive can differentiate between data written in Encrypt mode and data written in External mode. By controlling how this tag is treated during reading, the application can prevent the drive from returning Read data that was written in External mode. This may be desirable since the integrity of the data cannot be guaranteed by the drive, as it was encrypted by another agent outside the knowledge of the reading drive. The CEEM field in the Set Data Encryption page controls this behavior.

The default behavior of LTO-8 drives is to ignore the special tag, allowing reading of blocks written in External mode. This change from earlier generations, which defaulted to disallowing reads of blocks written in External mode. To disable reading of External-written blocks, set the CEEM field to 10b in the Set Data Encryption page which is sent using the `SECURITY PROTOCOL OUT` command to enable decryption mode.

Tagging data to disallow raw reads

A second feature of the LTO format adds another tag to data written by the drive. The application can specify that this data is not to be returned in Raw read mode, preventing keyless copy with its associated risks. This mode is specified by the application, through the RDMC field in the Set Data Encryption page.

The default behavior of LTO-8 drives is to mark each data block such that reads in Raw decrypt mode are allowed. This is a change from earlier generations, which defaulted to disallowing Raw reads. Use the RDMC field in the Set Data Encryption page sent to enter encryption mode.

Keyless copy recommendations

Because of the potential vulnerability of allowing RAW mode reads, Hewlett Packard Enterprise does not recommend performing keyless copies. However if it is desired to implement this feature, then the following points should be considered:

Always set CEEM and RDMC to the desired values in the Security Protocol Out page, rather than relying on the drive default behavior (i.e. do not leave them at 00). The drive default behavior is vendor-unique and varies between generations, so the recommended way to ensure the desired behavior is to select it explicitly.

Use the values of CEEM and RDMC shown in the table below to obtain the desired behavior:

Table 57: Keyless copy controls

Desired behavior	RDMC	CEEM
Permit future keyless copy of tape being created	10b	X
Prevent future keyless copy of tape being created	11b	X
Permit reads of externally-written data to succeed	X	01b
Force reads of externally-written data to fail	X	10b

The SSC-5 draft standard includes a simplified flowchart of a keyless copy operation. A thorough understanding of the process is required before attempting to implement this complex functionality.

Key management

The key management tools provided by the backup application should be suited to the sophistication of the user and the level of security required. Standards and guidelines on all aspects of data encryption including key management recommendation, can be found on the US National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC) website: **http://csrc.nist.gov/CryptoToolkit/**.

Minimum key management requirements are:

- Generate a 256bit key
- Guided manual key management by the user e.g.
  - Single key used for all backups until changed by user
  - User back up key /passphrase manually (i.e. writes it down)
- Limited key resolution e.g. key change limited to per media or backup session

More sophisticated key management value add could include:

- Generation of a random key (more secure than passphrase based keys)
- Configurable key resolution – key per user, schedule, file etc
- Secure deletion – key per retention policy enables secure deletion of data by key deletion
- Tools for secure key storage and backup internal and/or external to the application
- Alternative key generation options, e.g. true RNG keys
- Audit logs – required to prove the data was encrypted
- Keyless tape copying (should RAW and EXTERNAL modes of operation be supported)
- Support for external key management applications/appliances

IMPORTANT:

Passphrase generated encryption keys appear to provide the simplest key management option for users and application developers. However passphrase generated keys are only as secure as the passphrase length and unpredictability. They will be vastly less secure than keys generated with cryptographically sound random bit generators, and may mislead users with a level of security that is weaker than it should be.

For strong security Hewlett Packard Enterprise would **always** recommend generating a genuinely random encryption key.

Frequently asked questions

Can I encrypt data on all LTO tapes?

Yes, for LTO-8 drives. All cartridge formats compatible with LTO-8 support data encryption.

The application writes a header onto the media to identify it as being written by this application. Ideally, we want to leave the header in cleartext and then turn on encryption only for the rest of the data - would this be possible?

Yes, any combination of encrypted and unencrypted data is possible. MAM attributes 0224h and 0225h can be used to determine if the header is in cleartext and all other data is encrypted.

Can the application intersperse cleartext and encrypted text?

Yes, as previously stated.

Is it possible to use multiple keys to encrypt a single piece of media?

Yes, any number of keys can be used on a single piece of media. Be aware of the capacity and performance impacts of changing the key too frequently.

How does the application know which blocks are encrypted and with which keys?

The Next Block Encryption Status (NBES) page can be read to determine whether the next logical block is encrypted. When setting encryption parameters, applications may also include key-associated data (KAD) containing a unique key identifier. This identifier will be stored on tape and can also be read using the NBES page, which then allows the application to retrieve the correct key. For more information, see **Next block encryption status page (0021h)**.

What is the impact on performance of switching keys or switching between encrypted and nonencrypted data?

Negligible if it only happens occasionally. Frequent key changes or encryption boundaries may result in some loss of capacity and also of performance.

What is the impact on the lifetime of the drive/media?

There is no impact.

What is the impact on capacity using encryption?

The only impact encryption could have on capacity is if you use small block sizes and/or change keys frequently:

- Encryption adds about 72 bytes to a block so the approximate capacity loss can be determined (for example, 64kB blocks containing uncompressible data will add about 0.11%).
- A key change results in a dataset flush. A dataset is a data container defined in the Ultrium logical tape format. Every time the key is changed, the dataset is padded out regardless of how much it contains, wasting some capacity. However if the key does not change, or changes only a few times per cartridge, then the loss is negligible.

Logical block protection

Standards and references

The End-to-End Logical Block Protection is based on the following standards:

- T10 draft SSC-5 standard (Logical block protection, Control Data Protection mode page)
- T10 draft SPC-4 standard (Standard INQUIRY data, Extended INQUIRY Data VPD page)

Minimum requirements

An application which supports the End-to-End Logical Block Protection feature will need as a minimum to:

- Support the Control Data Protection Mode page 0Ah sub-page F0h - as a means to oversee the synchronisation of E2E-LBP mode of operation between the ISV application and the tape drive
- Interpret the protect bit in Standard Inquiry data
- Interpret the supported protection type (SPT) field in Extended INQUIRY Data VPD page
- Calculate and add CRC information to each SCSI data block to be written to the tape drive in E2E-LBP mode
- Implement checking and removal of CRC bytes from incoming restore data blocks, and in the event of detecting an E2E-LBP CRC error, execute subsequent error handling (restore / verify failure)
- Allow for flexible SCSI block size handling - with enablement or disablement of E2E-LBP transfers (assuming both modes of operation are supported) - i.e. handling inclusion or non-inclusion of CRC information in block transfers
- Interpret E2E-LBP related SCSI CHECK CONDITION Sense Data reported by the tape drive in the event of a WRITE or READ E2E-LBP CRC error and manage subsequent error handling (backup or restore failure)

General operation overview

Set-up

The backup/archive application discovers a tape drive's support status for End-to-End Logical Block Protection through the PROTECT bit in the standard INQUIRY page as well as the SUPPORTED PROTECTION TYPE (SPT) field in Extended INQUIRY Data VPD page.

The ISV application configures the tape drive for participation in End-to-End Logical Block Protection through the Control Data Protection mode page. For LTO-8, the protection method may be set to 01h (Logical Block Protection enabled, using Reed-Solomon CRC), or 02h (Logical Block Protection enabled, using Castagnoli CRC32C). Setting the protection method to 00h disables Logical Block Protection mode.

If using Fixed mode, the ISV application configures the fixed block size to be 4 bytes greater than the desired data transfer (to allow for the CRC bytes) through the Block Length field in the Mode Block Descriptor.

E2E-LBP enablement is compatible with Ultrium data encryption enabled or disabled; and with Ultrium hardware data compression enable or disabled.

E2E-LBP settings are specific to a particular I-T-L Nexus

Backup

During each SCSI WRITE operation the application calculates and appends four CRC bytes to the tail end of each SCSI data block to be transferred. The four CRC bytes are included in the overall SCSI block size for transfer.

The incoming CRC bytes are checked by the tape drive before the data is written to tape media, and the tape drive retains the added CRC information with each data block to be written to tape media.

Any WRITE CRC errors are reported with CHECK CONDITON status by the tape drive to indicate that the backup has failed.

Restore / Verify

During a READ operation, the tape drive retrieves each data block with its stored CRC from tape and checks the CRC against the data block prior to sending it to the host.

Any READ CRC errors are reported with CHECK CONDITON status by the tape drive to indicate that the restore has failed.

ISV application checks the CRC bytes in each incoming SCSI block upon receiving them, strips off the CRC bytes and relays data to its ultimate restore destination.

Any READ CRC error detected by the ISV application triggers a restore failure.

Backup with E2E-LPB disabled

ISV checks/disables E2E-LBP for WRITEs in the tape drive via Control Data Protection Mode page.

The tape drive receives the unprotected WRITE data blocks and generates the CRC protection bytes internally prior to writing each data block + CRC to tape.

Restore / Verify with E2E-LPB disabled

ISV checks/disables E2E-LBP for READs in the tape drive via Control Data Protection Mode page.

The tape drive retrieves data blocks + CRCs from tape, checks the CRC bytes and reports any errors, similar to E2E-LBP enabled case.

The tape drive then strips off the CRC bytes prior to returning data blocks to the application.

Specific SCSI behavioral changes

WRITE(6)

When E2E-LBP is enabled for WRITE operations, 4 additional CRC bytes are appended to the tail end of the data block. The declared SCSI block size for each WRITE operation is increased by +4 - whether in variable mode (via the WRITE CDB Transfer Length field) - or in fixed block mode (via Block Length field in a Mode Block Descriptor). Note that in fixed mode, every fixed block must include its own CRC bytes; hence a write of m fixed blocks each of declared block length **n** will transfer (**m***__n__) bytes, of which (4*__m__) will be CRC bytes.

The combined E2E-LBP data block with declared block length **n** is illustrated in the table below.

Table 58: Logical data block with E2E-LBP CRC bytes (combined length n bytes)

	7	6	5	4	3	2	1	0
0…	DATA							
n-5								
n-4	E2E-LBP CRC (4 BYTES)							
n-1								

READ(6)

Similarly with E2E-LBP enabled for READ operations the declared SCSI block size for each READ operation is increased by +4 - whether in variable mode (via the READ CDB Transfer Length field) or in fixed block mode (via Block Length field in a Mode Block Descriptor). The combined E2E-LBP data block with declared block length **n** is illustrated in the table above.

READ BLOCK LIMITS

With E2E-LBP enabled the MAXIMUM BLOCK LENGTH LIMIT field the drive returns in response to READ BLOCK LIMITS is reduced by 4 bytes - i.e. 16777211 bytes (16777215 minus 4 E2E-LPB CRC bytes).

INQUIRY

Standard Inquiry data (ref. SPC-4): The PROTECT bit is set to one to indicate that the logical unit supports E2E-LBP.

Extended INQUIRY Data VPD page (ref. SPC-4): Supported protection type (SPT) field has value 001b to indicate that E2E-LBP is supported.

Control data protection mode page

When enabling E2E-LBP in the tape drive, the ISV application establishes the following **Control Data Protection mode page** settings (ref SPC-4):

- LOGICAL BLOCK PROTECTION METHOD field = 01h (Reed-Solomon) or 02h (Castagnoli);
- LOGICAL BLOCK PROTECTION INFORMATION LENGTH = 04h; and
- LBP_W =1b, LBP_R=1b to enable protection for both WRITE and READ

Setting all the above fields to 0 will disable E2E-LBP.

Note that RPDP (Recover Buffered Data Protected) is not supported and must be set to 0b.

Sense data

When E2E_LBP is **enabled** for READ operations, the tape drive checks the E2E-LBP CRC against each data block retrieved from tape. In the event of a CRC validation failure the drive terminates the transfer and reports CHECK CONDITION status with the following sense data:

Sense key 04h HARDWARE ERROR - ASC/Q 10 01 LOGICAL BLOCK GUARD CHECK FAILED.

42data block retrieved from tape. In the event of a CRC validation failure the drive terminates the transfer and reports CHECK CONDITION status with the following sense data:

Sense key 03h MEDIUM ERROR - ASC/Q 31 00 MEDIUM FORMAT CORRUPTED

When E2E_LBP is **enabled** for WRITE operations, the tape drive checks the E2E-LBP CRC against each incoming data block. In the event of a CRC validation failure the drive terminates the transfer and reports CHECK CONDITION status with the following sense data:

Sense key 04h HARDWARE ERROR - ASC/Q 10 01 LOGICAL BLOCK GUARD CHECK FAILED.

E2E-LBP CRC algorithm

E2E-LBP uses either the Reed-Solomon CRC as specified in ECMA-319 (Ultrium-1 format) or the CRC32C (Castagnoli) CRC used by iSCSI and specified in RFC 7143 and RFC 3385. Sample C programs to generate either CRC are included in an Annex to the T10 SSC-5 draft standard.

Error handling and deferred errors

Key considerations

- Ultrium drives implement deferred error reporting when writing data using the recommended Buffered Mode of operation. Hence the reporting of a WRITE E2E-LBP CRC validation failure may be delayed to a later SCSI command; this being after the affected WRITE data block has been released from the drive's write data cache for CRC checking.
- In certain circumstances an Ultrium drive may repeat a CHECK CONDITION status report upon detection of a single Write-Behind deferred error. For example for a corrupted E2E-LBP WRITE data block, the deferred error may be reported twice. Similar consideration may also be given to optimized error handling in the broader scope of Write-Behind deferred error reporting.

  NOTE: As indicated by SPC-4 such scenarios are not limited to the Ultrium E2E-LBP implementation; for instance Ultrium drives handle other deferred Write Behind errors in a similar manner.

- In view of the above, ISV application developers may need to consider how to ensure deferred errors are detected in a timely manner. Routine post-backup SCSI operations may be sufficient to elicit the deferred CHECK CONDITION status if certain SCSI operations can be guaranteed. Alternatively deterministic early 'flushing out' of any latent deferred CHECK CONDITION status may be desirable following completion of a backup or restore operation. The following commands ensure the tape drive's write data cache gets flushed to tape, forcing E2E-LBP CRC checking.

  `Write Filemark`, `Rewind`, `Space`, `Locate`, `Unload`, `Read`, `Verify`, `Mode Select`, `Prevent/Allow Medium Removal`, `Read Position` commands.

- Then in response to a first CHECK CONDITION 04h - ASC/Q 10 01 – a Test Unit Ready command will deterministically flush out any latent repeated 2nd CHECK CONDITION status (plus further TURs may be issued to confirm GOOD status).
- ISV's receipt of the any of the above CHECK CONDITION status conditions, or CRC validation failure directly detected by the ISV application is assumed to trigger a hard backup failure or hard restore failure as no provision is made for on-the-fly error correction in the E2E-LBP scheme.

Background to deferred error handling

Hewlett Packard Enterprise recommends that SCSI WRITE operations are executed in Buffered Mode (the Buffered Mode field set to '001b' in a prior MODE SELECT's Block Descriptor Header). This enables immediate reporting by the tape drive and provides optimum performance.

This typically results in GOOD SCSI status being returned by the tape drive upon successful receipt of a `WRITE` command's data into the drive's host interface data buffer. WRITE data blocks are thus buffered (as 'Write-behind data') until ready to be efficiently processed further by the tape drive. The post-buffering processing phase would include the required E2E-LBP CRC check in an E2E-LBP Ultrium tape drive. If the CRC check happens to uncover a corrupted data block at this point, when the drive has already returned GOOD status for the `WRITE` command as outlined above, then the CHECK CONDITION will be returned in response to a later SCSI command. The T10 draft standard SPC-43 specification describes the appropriate formats of Sense data reporting for such deferred errors.

In some scenarios the reporting of the error will result in a first instance of CHECK CONDITION associated with Current information Sense Data, and then followed by a second CHECK CONDITION for a subsequent SCSI command associated with Deferred information Sense Data.

NOTE:

See SPC-4 rev. 34 section 4.5.5 for more information on Deferred errors and on scenarios where a Deferred error can follow on from a Current error.

Data transfer performance and Server CPU loading considerations

Summary

The following sections examine potential trade-offs in ISV backup/restore performance and Backup Server CPU loading that may be experienced when implementing T10 SSC4 End-to-End Logical Block Protection (E2E-LBP) with Ultrium 6 tape drive.

Reference is made to findings from experimental testing and analysis carried out by comparing various E2E-LBP (on and off) scenarios; using the T10 E2E-LBP software algorithm implemented in a software test utility, independently of ISV software. All the results were obtained using the Reed-Solomon CRC. The findings of the investigation can be summarized as shown in the following sections.

Backup/Restore performance

The T10 E2E-LBP CRC software algorithm can introduce noticeable delays when processing E2E-LBP SCSI READ or WRITE data operations. The effect of this is found to vary with different modelled use-case scenarios. There is no evidence of any corresponding delays in the hardware-based CRC processing within the Ultrium 6 tape drive.

For example backup / restore use cases using low compressibility data and using larger SCSI block sizes (>256KB) are likely to show little or no noticeable data transfer performance impact using E2E-LBP.

On the other hand high bandwidth hardware systems using high compressibility data are likely to see a significant data transfer performance impact of using E2E-LPB.

It is important to note that the experimental findings herewith exclude certain other factors that may contribute to real-world data transfer performance pipelines and which may offset any noticeable relative E2E-LBP effect. For example Disk subsystem access performance and OS file system access can in practice represent a bottleneck to the Ultrium 6 drive.

Backup Server CPU loading

Monitoring of CPU loading on Proliant servers shows noticeable increased activity attributable to E2E-LPB processing. However for the Proliant servers tested this was found to be typically only a fraction of a single CPU core bandwidth per backup/restore.

Experiments showed a fairly wide range of around 2-20% additional CPU time per backup/restore when extrapolated to a single CPU core. This loading is found to be linearly scalable with more than 1 backup or restore running using E2E-LBP. Hence some CPU budgeting allowance may be required for already heavily loaded systems incrementally running one or more E2E-LBP operations.

Experimental findings for data transfer performance and server CPU loading

Backup / Restore Raw Performance - comparing E2E-LBP on vs. E2E-LBP off

Figure 5: LTO-6 SAS Raw Performance charts(memory to/from tape – variable SCSI block mode) below shows some typical comparative LTO-6 Raw Performance charts (memory to/from tape).

Details of experimental test configurations used may be found in **Experimental configurations for E2E-LBP data transfer performance and server CPU loading** below.

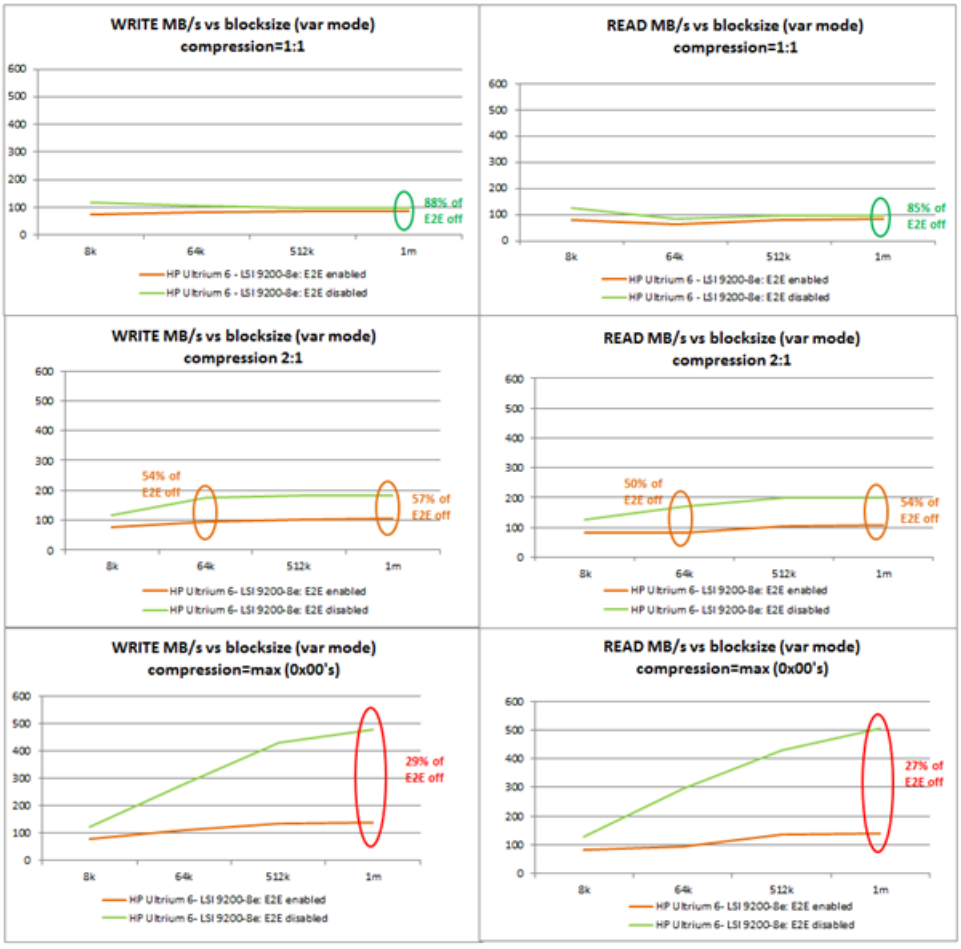

Figure 5: LTO-6 SAS Raw Performance charts(memory to/from tape – variable SCSI block mode)

The following observations are referenced to the above charts:

1:1 data-compressibility (top 2 charts - **Figure 5: LTO-6 SAS Raw Performance charts(memory to/from tape – variable SCSI block mode)**

E2E-enabled

backups and restores using **uncompressible** data i.e. and with large blocksizes (> 512KB) in the experiments typically exhibited data transfer performance of a similar order to **E2E-disabled**. E2E-enabled performance being typically 80-90% of E2E-enabled raw performance.

- Overall there is a relatively low base-level performance 'ceiling' prior to E2E-LBP enablement. This is consistent with the following anticipated performance factors

  With larger SCSI data blocksizes, E2E-CRC processing is required for fewer blocks per Gigabyte and CRC processing overhead is consequently minimized.

If the data were compressible Ultrium 6 Data Hardware Compression has the potential to enhance backup and restore data transfer performance across the host interface at the tape drive. This benefit is not realized with 1:1 DC data and this effectively lowers the relative performance 'ceiling' for E2E-LBP-**disabled**.

Maximum data-compressibility (bottom 2 charts – **Figure 5: LTO-6 SAS Raw Performance charts(memory to/from tape – variable SCSI block mode)**)

- Conversely experimental cases using **maximallycompressible** data (all zeros data), used in combination with larger SCSI blocksizes and simulating **high bandwidth hardware** (i.e. Raw memory to tape) showed a significant data transfer performance impact –whereby E2E-enabled performance can be lower than 30% of E2E-disabled.
- Overall there is a relatively High base-level performance 'ceiling' prior to E2E-LBP enablement which emphasizes the relative effect of E2E-CRC processing delays. This is consistent with the following anticipated performance factors.

Larger SCSI blocksizes normally benefit from reduced SCSI block processing overhead in the E2E-**disabled** case, but this benefit is apparently overridden when E2E-CRC processing delays are in the pipeline.

Potential high DC performance benefits from Ultrium 6 hardware compression engine as seen in the E2E-**disabled** case are apparently bottlenecked by E2E-CRC processing delays.

2:1 data-compressibility and 64k blocksize (middle 2 charts – **Figure 5: LTO-6 SAS Raw Performance charts(memory to/from tape – variable SCSI block mode)**)

A common usage model using around 2:1 data compressibility and 64K blocksizes was found to be in between the above two scenarios, showing around 50% relative Raw performance impact due to E2E-CRC processing delays.

Other Potential Real World Performance Factors

It is important to note that the above experimental findings exclude certain other factors that may contribute to real-world data transfer performance pipelines and which may offset any noticeable **relative** E2E-LBP effect. For example Disk subsystem access performance and OS file system access can in practice represent a bottleneck to the Ultrium 6 drive.

Measured CPU loading due to E2E-LBP processing

CPU loading measurements in the form of **% processor time** were taken comparing E2E-LBP-enabled and E2E-LBP-disabled backups and restores. Two different Proliant server models were tested using two different 6Gb SAS HBA models and two Operating Systems – Windows 2008 64bit and Red Hat 6.3. Details of experimental test configurations may be found in **Experimental configurations for E2E-LBP data transfer performance and server CPU loading**below.

Figure 6: Measured CPU loading on Windows 2008 Proliant Server (2@Intel® Xeon® X5687) below shows comparative CPU loading on a Proliant DL370 G6 server running Windows 2008 Operating System. Backups (SCSI WRITEs) and Restores (SCSI READs) are compared for a single LTO-6 drive and also for 2 LTO-6 drives concurrently.

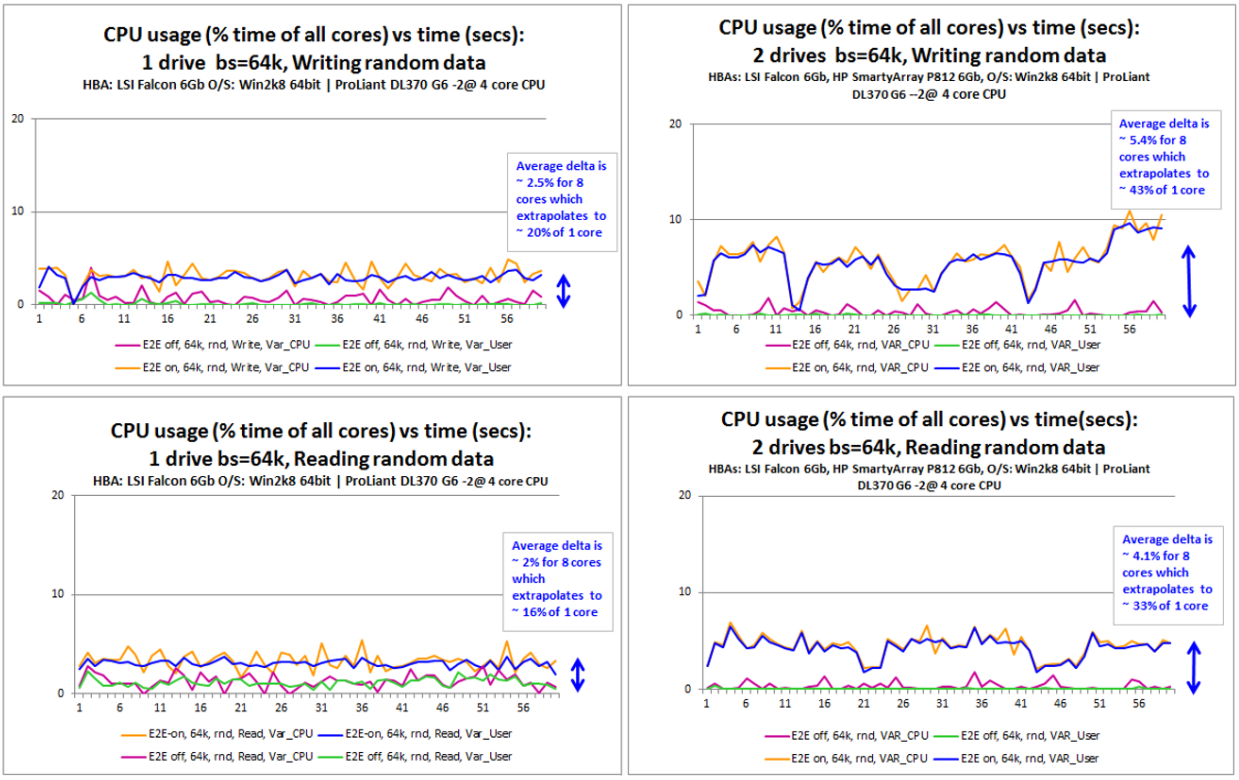

Figure 6: Measured CPU loading on Windows 2008 Proliant Server (2@Intel® Xeon® X5687)

Observations:

- Measured CPU loading (% processor time) on the Windows Proliant server shows noticeable additional activity with E2E-enabled - typically estimated at around 16-20% of a single CPU core bandwidth per backup / restore operation.
- This is scalable with more than 1 backup running. Some allowance may be required for heavily loaded systems running one or more E2E-LBP operation.

Figure 7: Measured CPU loading on Red Hat 6.3 Proliant Server (Intel® Xeon® Processor 5140) below shows comparative CPU loading on a Proliant ML370 G5 server running Red Hat 6.3 Linux Operating System. Backups (SCSI WRITEs) and Restores (SCSI READs) are compared for a single LTO-6 drive.

A different measurement process was used with the Linux setup which generates CPU % time figures which are **additive** for the 2 processor cores, and with a theoretical range 0-200% for the combined cores (whereas the above Windows measurement have a theoretical range 0-100% for combined 8 cores). This requires a slightly different extrapolation process to estimate **per-core** loading.

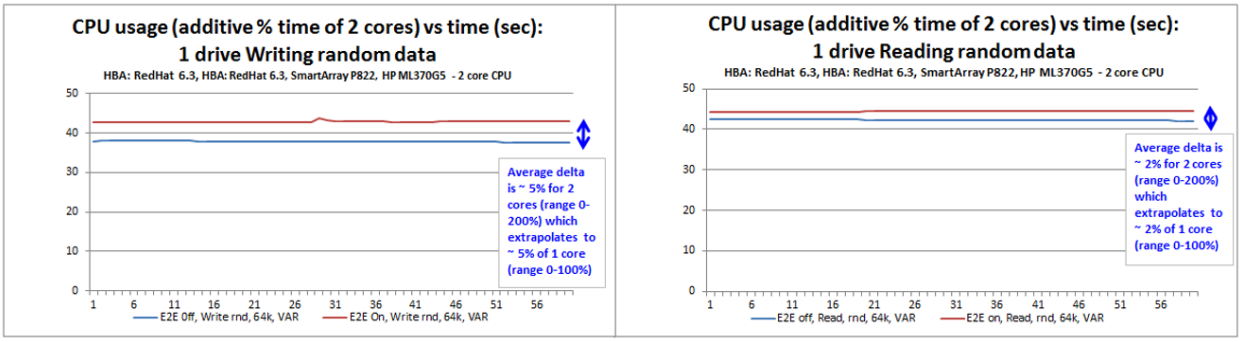

Figure 7: Measured CPU loading on Red Hat 6.3 Proliant Server (Intel® Xeon® Processor 5140)

Observations:

- Measured CPU loading (% processor time) on the Red Hat 6.3 Proliant server shows noticeable additional activity with E2E-enabled – typically estimated at around 2-5% of a single CPU core bandwidth per backup / restore operation - but apparently less CPU % time processing in comparison to the Windows setup.
- There are several differences between the Windows and Linux setups that may contribute to the difference in measurements between the 2 systems – notably: CPU measurement tool, processor power, SAS controller model, Operating System. Therefore caution is required in drawing any firm conclusions as to the causes of the differences.
- This may be rather be taken as illustrative of the range of measurable CPU loading impact.

Summary:

Measured CPU loading on both the Proliant servers tested show measurable activity due to E2E-LBP but typically only a fraction of a single CPU core bandwidth per backup/restore.

NOTE: Raw' performance is defined as Server RAM to/from LTO tape (bypassing disk system and OS file system).

Bottlenecking is principally in the Host E2E Software Algorithm

SAS traces were analyses for E2E-LBP-enabled and E2E-LBP-disabled SCSI WRITE and READ operations.

Analysis of timings in the traces indicates the additional delays associated with E2E-LBP backup data transfers can be attributed to pausing or stalling by the host server.

Modelling the event timings of single `WRITE` and `READ` command cycles and cross-correlating this with macro-level performance measurements indicates that E2E-LBP performance impact is essentially attributable to the host's delays from each command cycle.

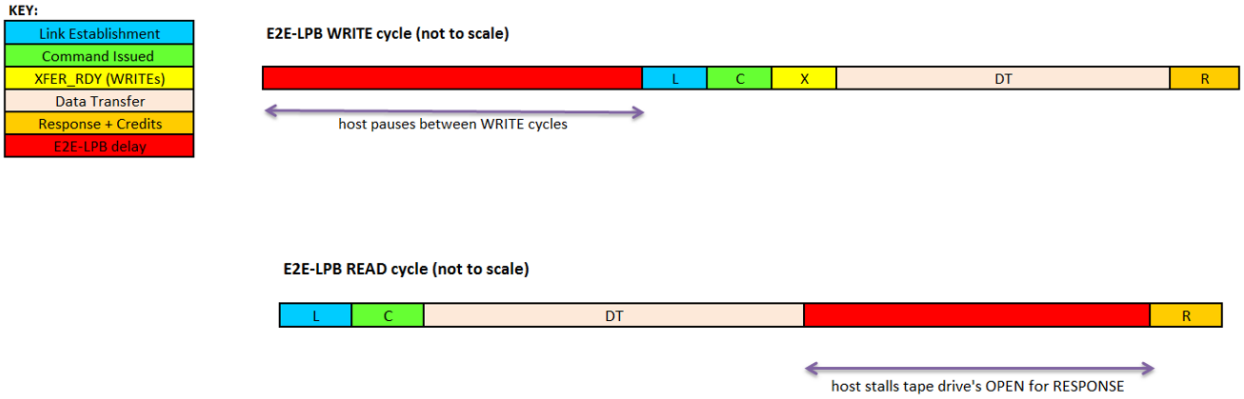

Figure 8: Logical points in process of E2E-LBP delays from SAS trace analysis

SCSI WRITE delays:

In the case of E2E-LBP WRITE operations, there is a significant delay between each SCSI command cycle; i.e. the host pauses before opening a SAS connection to send each `WRITE` command to the tape drive. This is shown diagrammatically above in **Figure 8: Logical points in process of E2E-LBP delays from SAS trace analysis** WRITE cycle.

The length of this delay cumulatively accounts for the E2E-LBP performance in the experimental cases. This delay appears to be attributable to host overhead in calculating a CRC for each SCSI data block.

SCSI READ delays:

Here the E2E-LBP delays occur **within** the SCSI command cycle; after sending the `READ` command to the tape drive and having received all the data from the tape drive; the drive then issues an OPEN with a view to sending an SSP RESPONSE frame; however the host uses the SAS OPEN_REJECT(RETRY) mechanism to temporarily stall the completion of the command.

This is shown diagrammatically above in **Figure 8: Logical points in process of E2E-LBP delays from SAS trace analysis** READ cycle.

The length of this delay associated with the OPEN_REJECT and the tape drive subsequently retrying the OPEN cumulatively accounts for the E2E-LBP performance in the experimental cases. This delay appears to be attributable to host overhead checking the CRC for each incoming SCSI data block.

Experimental configurations for E2E-LBP data transfer performance and server CPU loading

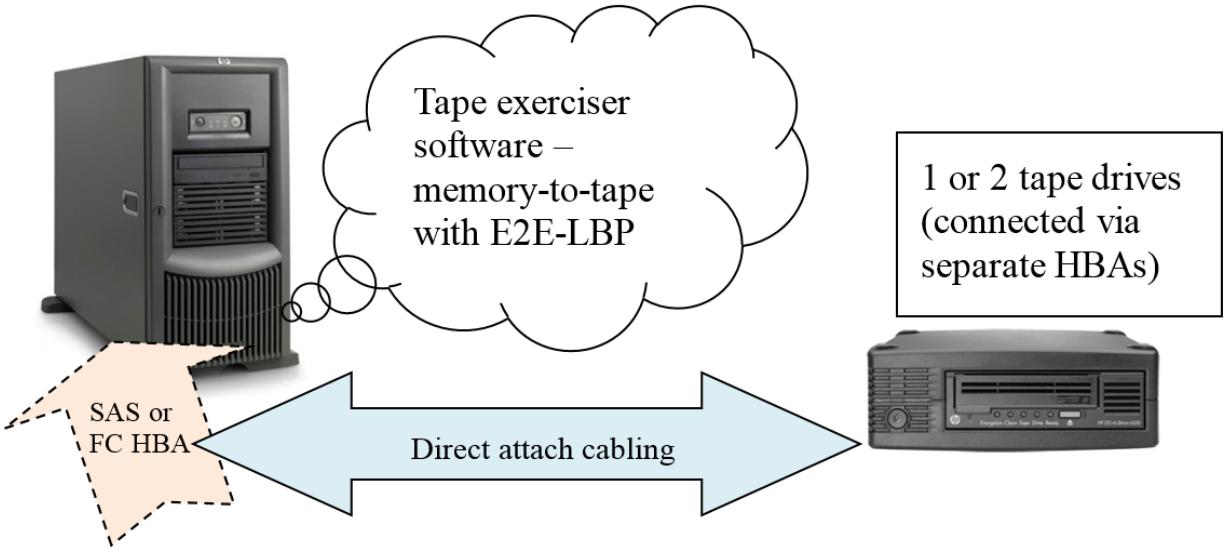

Figure 9: Data transfer performance test configurations

Table 59: Summary of raw performance configurations

Measurements	Test condition (Win 2k8 R2) FC and SAS HBAs (**listed below)	
Raw transfer rate (memory to/from tape)SAS traces analysis of delays using the LSI 9200-8e 6Gb SAS HBA and bs=64KB	E2E LBP ON (WRITE/READ)	E2E LBP OFF (WRITE/READ)
	SCSI transfer size range: 8KB to 1MB	
	Data compressibility of transfer (Ultrium HW compression): • 1:1 (random) • 2:1 Maximum (all 00h bytes)	

Table 60: Summary of CPU loading measurement configurations

Measurements	Test Condition (Win 2K8 LSI 9200-8e 6Gb SAS HBA, Red Hat 6.3)HPE SmartArray P822 SAS HBA
CPU Loading (OS native tooling): • Windows 2K8: Performance Monitor (Figure 7) • Red Hat 6.3: ps –axu (%CPU summation)	E2E LBP ON (WRITE/READ) E2E LBP OFF (WRITE/READ)
	SCSI transfer size range[1]: 64KB
	Data compressibility of transfer (Ultrium HW compression): • 1:1 (random) • Maximum (all 00h bytes)
	Background CPU Loading levels: • Minimal (Win2K8 and RHEL6.3) • Heavy (RHEL 6.3)
	Single and Dual LTO-6 drive on single server (Win 2K8)

1 Blocksize prior to addition of any E2E CRC bytes.

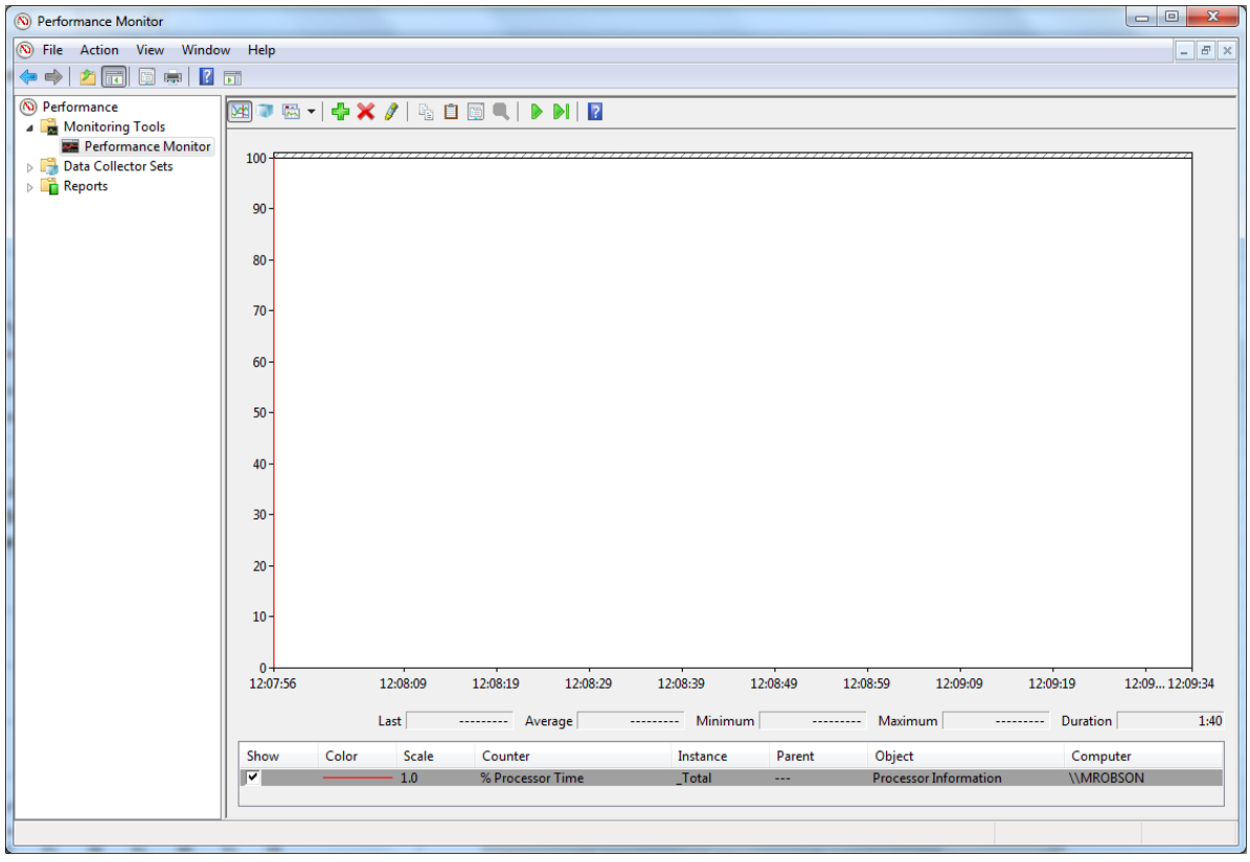

Figure 10: Windows Performance monitor

Test Software: **triffid** drive exerciser (server memory to/from tape, incorporating T10 E2E LBP algorithm)

Tape drives:

- LTO-6 Ultrium 6650 Tape Drive (SAS Full Height, JSS8 prototype)
- LTO-6 Ultrium 6250 Tape Drive (SAS Half Height, CSS8 prototype)
- LTO-6 Ultrium FC development drive (JFC8 prototype)

Host Bus Adaptors:

- **HPE SmartArray**

  6Gb SAS Controllers:

  - P812
  - H222

- **LSI**

  9200-8e 6Gb SAS

- **Emulex**

  LP11002E Dual Port 4Gb FC

References for E2E-LBP data transfer performance and server CPU loading

1. T10 SCSI Stream commands - 5 (SSC-5) rev 04 section 2.4.28
2. End-to-End Logical Block Protection in HPE Ultrium 6 Tape Drive – An Overview rev 1.1 Nov 2010 Mike Robson Hewlett Packard Enterprise SDI Bristol.