memorandum

Hewlett-Packard Company
3000 Hanover Street
Palo Alto, CA 94304-1185
USA
www.hp.com

T10/07-382r0

To	From	Subject	Date
INCITS T10 Committee	Michael Banther, HP	SSC-3 MAM and Write Protect	18 September 2007

Revision History

Revision 0 – Initial document

Reference documents

SCSI Stream Commands – 3 (SSC-3), Project 1611-D, Revision 03c, 13 April 2007.

Background

Presently SSC-3 (and SPC-4) is silent regarding the effect that Write Protection has on accessibility to the Host Attributes in Medium Auxiliary Memory (MAM). HP is aware that some tape drive products allow and some products disallow WRITE ATTRIBUTE commands for a Host Attribute to complete with GOOD status when write protection has been applied to a loaded medium.

This proposal clarifies the SSC-3 standard with regard to the interactions between write protection and WRITE ATTRIBUTE commands. Incidentally, this proposal corrects some ambiguity in the reporting of the Additional Sense Code value when a device server that does not support WORM mode has detected the mounting of an archive tape, some other form of write protection is also in effect for the medium, and an attempt to alter the medium contents occurs.

In this document, new proposed text appears in blue and proposed deleted text appears in ~~red strikeout~~. Notes that do not form part of the proposed text appear in pink.

Changes to the SSC-3 draft standard

4.2.11.4 Error conditions

Table 5 – Error conditions and sense keys

Condition	Sense Key
[Note: Not all rows of table 5 shown.]	
Attempt to perform an erase, format, partition, set capacity, or write-type operation on write protected medium.	DATA PROTECT
Processing a WRITE ATTRIBUTE command that would result in alteration of a write protected medium.	MEDIUM ERROR (see SPC-4)
Deferred write error.	MEDIUM ERROR

4.2.12.1 Write protection introduction

Write protection of the medium prevents the alteration of logical objects on the medium and any change to the accessibility of logical objects on the medium, by commands issued to the device server. If processing a WRITE ATTRIBUTE command results in alteration of the medium, write protection of the medium prevents the alteration of that medium auxiliary medium attribute. Write protection is usually controlled by the user of the medium through manual intervention (e.g., mechanical lock) or may result from hardware controls (such as tabs on the media housing), conditions such as positioning within unrecoverable data, or software write protections. All sources of write protection are independent. When present, any write protection shall cause otherwise valid commands, except for WRITE ATTRIBUTE (see SPC-4), that request alteration of logical objects on the medium, or affect the accessibility of logical objects on the medium, to be rejected with a CHECK CONDITION status with the sense key set to DATA PROTECT (see 4.2.12.2). Only when all write protections are disabled shall the device server process commands that request alteration of logical objects on the medium, or commands that may affect the accessibility of logical objects on the medium.

4.2.12.2 Write protection additional sense code use

The additional sense code associated with the DATA PROTECT sense key depends on the write protection in effect at the time. Table 6 specifies the preferred additional sense code for the given write protection. Alternatively, the generic additional sense code of WRITE PROTECTED may be returned by the device server.

6

Table 6 – Write protect additional sense code combinations

Cause of DATA PROTECT error	Additional Sense Code
Hardware Write Protection	HARDWARE WRITE PROTECTED
Permanent Write Protection	PERMANENT WRITE PROTECT
Persistent Write Protection	PERSISTENT WRITE PROTECT
Associated Write Protection	ASSOCIATED WRITE PROTECT
Software Write Protection	LOGICAL UNIT SOFTWARE WRITE PROTECTED
Archive tape mounted (see 4.2.19.3)	CANNOT WRITE MEDIUM – INCOMPATIBLE FORMAT

If more than one condition exists, the device server shall either report the applicable condition in order of HARDWARE WRITE PROTECTED, PERMANENT WRITE PROTECT, PERSISTENT WRITE PROTECT, ASSOCIATED WRITE PROTECT, ~~and~~ LOGICAL UNIT SOFTWARE WRITE PROTECTED, and CANNOT WRITE MEDIUM – INCOMPATIBLE FORMAT, or report the generic additional sense code of WRITE PROTECTED.

4.2.19.3 WORM mode

If a device server that does not support WORM mode detects that an archive tape is mounted, it shall treat the medium as write protected (see 4.2.12). ~~Any command that attempts to alter the medium shall be terminated with CHECK CONDITION status. The sense key shall be set to DATA PROTECT and the additional sense code shall be set to CANNOT WRITE MEDIUM - INCOMPATIBLE FORMAT.~~

8.3.3 Device Configuration mode page

A software write protection (SWP) bit set to one specifies the device server shall perform a synchronize operation then enter the write-protected state (see 4.2.12, 4.2.12.2 and 4.2.12.3). ~~When the SWP bit is set to one, all commands requiring eventual writes to the medium shall return CHECK CONDITION status. The sense key shall be set to DATA PROTECT and the additional sense code should be set to LOGICAL UNIT SOFTWARE WRITE PROTECTED (see 4.2.12.2).~~ A SWP bit set to zero specifies the device server may inhibit writing to the medium, dependent on other write inhibits.

An associated write protection (ASOCWP) bit set to one specifies the logical unit shall inhibit all writing to the medium after performing a synchronize operation (see 4.2.12 and 4.2.12.4). When the ASOCWP bit is set to one, the currently mounted volume is logically write protected until the volume is de-mounted (see 4.2.12, 4.2.12.2 and 4.2.12.4). ~~When the ASOCWP bit is set to one, all commands requiring eventual writes to the medium shall return CHECK CONDITION status. The sense key shall be set to DATA PROTECT and the additional sense code should be set to ASSOCIATED WRITE PROTECT (see 4.2.12.2).~~ An ASOCWP bit set to zero specifies the currently mounted volume is not write protected by the associated write protection. The ASOCWP bit shall be set to zero by the device server when the volume is de-mounted. This change of state shall not cause a unit attention condition. If the application client sets the ASOCWP bit to one while no volume is mounted, the device server shall terminate the MODE SELECT command with CHECK CONDITION status. The sense key shall be set to NOT READY and the additional sense code shall be set to MEDIUM NOT PRESENT. If the Device Configuration mode page is savable, the ASOCWP bit shall be saved as zero, regardless of the current setting.

A persistent write protection (PERSWP) bit set to one specifies the currently mounted volume is logically write protected (see 4.2.12, 4.2.12.2 and 4.2.12.5). ~~When the PERSWP bit is set to one, all commands requiring eventual writes to the medium shall return CHECK CONDITION status. The sense key shall be set to DATA PROTECT and the additional sense code should be set to PERSISTENT WRITE PROTECT (see 4.2.12.2).~~ A PERSWP bit set to zero specifies the currently mounted volume is not write protected by the persistent write protection. The PERSWP bit shall be set to zero by the device server when the volume is de-mounted or when a volume is mounted with persistent write protection disabled. The PERSWP bit shall be set to one by the device server when a volume is mounted with persistent write protection enabled. These changes of state shall not cause a unit attention condition. If the application client sets the PERSWP bit to one while no volume is mounted, the device server shall terminate the MODE SELECT command with CHECK CONDITION status. The sense key shall be set to NOT READY and the additional sense code shall be set to MEDIUM NOT PRESENT. If the application client sets the PERSWP bit to one when the logical position is not at BOP 0, the device server shall return CHECK CONDITION status. The sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to POSITION PAST BEGINNING OF MEDIUM. If the Device Configuration mode page is savable, the PERSWP bit shall be saved as zero, regardless of the current setting.

6 A permanent write protection (PRMWP) bit set to one specifies the currently mounted volume is logically write protected (see 4.2.12, 4.2.12.2 and 4.2.12.6). ~~When the PRMWP bit is set to one, all commands requiring eventual writes to the medium shall return CHECK CONDITION status. The sense key shall be set to DATA PROTECT and the additional sense code should be set to PERMANENT WRITE PROTECT (see 4.2.12.2).~~ A PRMWP bit set to zero specifies the currently mounted volume is not write protected by the permanent write protection. The PRMWP bit shall be set to zero by the device server when the volume is de-mounted or when a volume is mounted with permanent write protection disabled. The PRMWP bit shall be set to one by the device server when a volume is mounted with permanent write protection enabled. These changes of state shall not cause a unit attention condition. If the application client sets the PRMWP bit to one while no volume is mounted, the device server shall terminate the MODE SELECT command with CHECK CONDITION status. The sense key shall be set to NOT READY and the additional sense code shall be set to MEDIUM NOT PRESENT. If the application client sets the PRMWP bit to one when the logical position is not at BOP 0, the device server shall return CHECK CONDITION status. The sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to POSITION PAST BEGINNING OF MEDIUM. If the application client attempts to change the PRMWP bit from one to zero, the device server shall terminate the MODE SELECT command with CHECK CONDITION status. The sense key shall be set to DATA PROTECT and the additional sense code shall be set to PERMANENT WRITE PROTECT. If the Device Configuration mode page is savable, the PRMWP bit shall be saved as zero, regardless of the current setting.