To: T10 Technical Committee
From: Rob Elliott, HP (elliott@hp.com)
Date: 5 November 2004
Subject: 04-349r0 SPC-3 MMC-5 Merge PREVENT ALLOW MEDIUM REMOVAL commands

Revision history
Revision 0 (5 November 2004) First revision

Related documents
spc3r16 - SCSI Primary Commands - 3 revision 21
mmc5r00 - SCSI Multimedia Commands - 5 revision 0

Overview
MMC-5 defines its own version of the PREVENT ALLOW MEDIUM REMOVAL command, despite the fact that it is already defined in SPC-3. MMC-5 includes a "Persistent Prevent" feature that is not defined in SPC-3.

Fortunately, the feature does not overlap and can be integrated into the SPC-3 rendition.

Suggested changes to SPC-3

5.6.10 Releasing persistent reservations and removing registrations

5.6.10.5 Preempting and aborting

If no reservation conflict occurred, the device server shall perform the following uninterrupted series of actions:

> ...
> f) For logical units that implement the PREVENT ALLOW MEDIUM REMOVAL command, the device server shall ~~perform an action equivalent to the processing of a PREVENT ALLOW MEDIUM REMOVAL command with the PREVENT field equal to zero received on the~~ set the DTE prevent state to its default value for each of the I_T nexuses associated with the persistent reservation being preempted (see 6.13).

...

6.13 PREVENT ALLOW MEDIUM REMOVAL command

The PREVENT ALLOW MEDIUM REMOVAL command (see table 116) requests that the logical unit enable or disable the removal of the medium by an operator (e.g., with a manual eject button), by a medium changer, and/or by a START STOP UNIT command (see SBC-2, RBC, or MMC-4). ~~The logical unit shall not allow medium removal if any initiator port currently has medium removal prevented~~ The method used by the logical unit to prevent medium removal is vendor specific.

Table 1 — PREVENT ALLOW MEDIUM REMOVAL command

Byte\Bit	7	6	5	4	3	2	1	0
0	OPERATION CODE (1Eh)							
1	Reserved							
2	Reserved							
3	Reserved							
4	Reserved						PREVENT	
5	CONTROL							

The device server shall maintain a data transfer element (DTE) prevent state for each I_T nexus set to true or false.

If MCHNGR is set to zero in the standard INQUIRY data (see 6.4.2) (i.e., a medium changer is not present)(e.g., it is an MMC-4 peripheral device), the device server may maintain a persistent data transfer element (PDTE) prevent state for each I_T nexus set to true or false.

If MCHNGR is set to one in the standard INQUIRY data (see 6.4.2) (i.e., a medium changer is present), the device server may maintain a medium changer prevent state for each I_T nexus set to true or false.

The PDTE prevent state, the DTE prevent state, and the medium changer prevent state shall each be set to their vendor-specific default values on I_T nexus loss, logical unit reset, hard reset, power on, and a persistent reservation PREEMPT AND ABORT service action (see 5.6.10.5). The default values should each be false.

Editor's Note 1: Is the PDTE prevent status default acceptable as "shall be false"?

Table 115 defines the PREVENT field values and their meanings.

Table 2 — PREVENT field [replaces current table 117]

Code	MCHNGR bit in standard INQUIRY data	Effect on prevent states		
		PDTE prevent state	**DTE prevent state**	**Medium changer prevent state**
00b	0 or 1	no change	set to false	set to false
01b	0 or 1	no change	set to true	set to false
10b	0	set to true [a]	no change	no change
	1	no change	set to false	set to true [b]
11b	0	set to true [a]	no change	no change
	1	no change	set to true	set to true [b]

[a] If the device server does not support the PDTE prevent state, it shall terminate the PREVENT ALLOW MEDIUM REMOVAL command with CHECK CONDITION status with the sense key set to ILLEGAL REQUEST and the additional sense code set to INVALID FIELD IN CDB.
[b] If the device server does not support the medium changer prevent state, it shall terminate the PREVENT ALLOW MEDIUM REMOVAL command with CHECK CONDITION status with the sense key set to ILLEGAL REQUEST and the additional sense code set to INVALID FIELD IN CDB.

Table 3 defines the handling of insertion and ejection events when each of the prevent states is set to true. If at least one prevent state for at least one I_T nexus disables handling of an event, then the device server shall disable handling of that event (i.e., disable has priority over enable)(e.g., if the DTE prevent state is set to true

for at least one I_T nexus, insertion by an operator is disabled regardless of the PDTE prevent state value for that I_T nexus or the DTE prevent state values for other I_T nexuses).

Table 3 — Handling of insertion and ejection events [new]

Prevent state	Event				
	Insertion by operator	Insertion by medium changer	Ejection by operator	Ejection by medium changer	Ejection by START STOP UNIT command
PDTE prevent state is true	enabled	no restriction	For MMC-4 peripheral devices, enabled until the NewMedia event has been reported for the medium and disabled after the NewMedia event has been reported for the medium (see MMC-4). For other peripheral devices, disabled.	no restriction	enabled
DTE prevent state is true	disabled	no restriction	disabled	no restriction	disabled
Medium changer prevent state is true	no restriction	disabled	no restriction	disabled	no restriction

~~PREVENT values 10b and 11b are valid only when the RMB bit and the MCHNGR bit are both equal to one in the standard INQUIRY data.~~

~~The prevention of medium removal shall begin when any application client issues a PREVENT ALLOW MEDIUM REMOVAL command with a PREVENT field of 01b or 11b (i.e., medium removal prevented). The prevention of medium removal for the logical unit shall terminate:~~

~~a) After all initiator ports with application clients that previously prevented medium removal issue PREVENT ALLOW MEDIUM REMOVAL commands with a PREVENT field of 00b or 10b, and the device server has successfully performed a synchronize cache operation; or~~
~~b) Upon a logical unit reset.~~

Before changing from ejection being disabled to enabled, the device server shall flush any cached data to medium.

The persistent reservation PREEMPT AND ABORT service action sets the DTE prevent state to its default value (see 5.6.10.5).

~~For an initiator port that has executed a PERSISTENT RESERVE OUT command with a service action of RESERVE, REGISTER AND IGNORE EXISTING KEY, or REGISTER service action, the PREVENT field shall be set to zero as part of the uninterrupted sequence of events performed by a PERSISTENT RESERVE OUT command with a service action of PREEMPT AND ABORT using that the registration value associated with the initiator port associated with that I_T nexus in the SERVICE ACTION RESERVATION KEY field. This allows an application client to override the prevention of medium removal function for an initiator port that is no longer operating correctly.~~

~~While a prevention of medium removal condition is in effect, the logical unit shall inhibit mechanisms that normally allow removal of the medium by an operator.~~

Suggested changes to MMC-5

4.1.7 Removable medium

A disc has an attribute of either being mounted or unmounted on a suitable transport mechanism. A disc is mounted when the Logical Unit is capable of performing read operations to the medium. A mounted disc may not be accessible by an Initiator, if another Initiator has reserved it. A disc is unmounted at any other time (e.g. during loading, unloading, or storage). An Initiator may check the mounted status by issuing a TEST UNIT READY command.

The REMOVABLE MEDIUM Feature provides the Initiator with commands to load or eject media and to prevent the removal of any media.

The PREVENT ALLOW MEDIUM REMOVAL command allows an Initiator to restrict the de-mounting of the disc. This is useful in maintaining system integrity. If the Logical Unit implements cache memory, it shall ensure that all logical blocks of the medium contain the most recent data prior to permitting de-mounting of the disc. If the Initiator issues a START STOP UNIT command to eject the disc, and is prevented from de-mounting by the PREVENT ALLOW MEDIUM REMOVAL command, the START/STOP UNIT command is rejected by the Logical Unit.

When the ~~Persistent Prevent~~ PDTE prevent state is entered, the media shall remain locked in the Logical Unit, until the Initiator issues an eject request, or a power on or hard reset condition occurs. The ~~Persistent Prevent~~ PDTE prevent state shall be maintained after the eject request. New media that is inserted into the Logical Unit shall be locked in the Logical Unit after the Logical Unit reports the NEW MEDIA event. Prior to reporting the NEW MEDIA event, the Logical Unit may eject media without an explicit eject command from the Initiator. This allows the user to remove incorrectly inserted media without having to wait for Initiator intervention.

While in the ~~Persistent prevent~~ PDTE prevent state, the Logical Unit shall generate Events upon receipt of a User Eject request. The Logical Unit shall not eject the media on receipt of these requests if the Logical Unit has already reported a NEW MEDIA event for this media. If a Logical Unit allows an eject between generating and reporting the NEW MEDIA event, the Logical Unit shall remove the NEW MEDIA event(s) from the Event queue. When the Initiator receives the Eject Request and determines that it is safe to eject the medium, an eject command (START STOP UNIT command with LoEj bit set to one) should be issued. At that time the Logical Unit shall eject the medium. The ~~Persistent Prevent State shall be retained~~ PDTE prevent state shall not be changed.

The Logical Unit shall only generate GET EVENT STATUS NOTIFICATION (EJECT REQUEST) events after reporting a GET EVENT STATUS NOTIFICATION (NEW MEDIA) event, and prior to reporting a GET EVENT STATUS NOTIFICATION (MEDIA REMOVAL) event for the given media.

To maintain compatibility with existing BIOS implementations and operating systems, the Logical Unit shall default to ~~Persistent Prevent disabled~~ a PDTE prevent state set to false. When the Initiator enables the support using the PREVENT ALLOW MEDIUM REMOVAL command, the Logical Unit shall respond as described in this specification. When the Initiator disables this Feature, the Logical Unit shall default to normal operating modes. A power on or hard reset shall cause the Logical Unit to return to the default value of the PDTE prevent state.

> Editor's Note 2: is the default value "shall be false" per the above, or "should be false" as described in 6.18.1 below the PREVENT table? If shall, then get rid of "default" mentions, e.g., replace the last sentence with "A power on or hard reset shall cause the Logical Unit to set the PDTE prevent state to false."

If the Logical Unit is unable to maintain media status information across a reset or power cycle, the Logical Unit shall generate a NEW MEDIA event.

Commands shall be processed exactly the same as if ~~Persistent Prevent was not enabled~~ the PDTE prevent state was set to false. For compatibility reasons, a unit attention condition shall be generated. Execution of the GET EVENT STATUS NOTIFICATION command does not include terminating with CHECK CONDITION status when a unit attention condition is pending. e.g., if the user inserts a new medium and the Logical Unit

is accessed with a command, a unit attention condition shall be generated, but the Logical Unit shall also report the NEW MEDIA Event with the next available GET EVENT STATUS NOTIFICATION (Media Status) command.

5.3.3 Morphing Feature (0002h)

This Feature identifies the ability of the Logical Unit to notify an Initiator about operational changes and accept Initiator requests to prevent operational changes.

Support for this Feature is enabled using the PREVENT ALLOW MEDIUM REMOVAL command ~~(Persistent Bit)~~and its PDTE prevent state, and the media status is retrieved using the GET EVENT STATUS NOTIFICATION command.

...

Logical Units that support this Feature shall implement the commands specified in Table 83.

Table 4 — Morphing Feature Commands

Op Code	Command description	Reference
46h	GET CONFIGURATION	6.6
4Ah	GET EVENT STATUS NOTIFICATION	6.7
1Eh	PREVENT ALLOW MEDIUM REMOVAL ~~(with Persistent bit set to one)~~ and the PDTE prevent state	6.18

5.3.4 Removable Medium Feature (0003h)

This Feature identifies a Logical Unit that has a medium that is removable. Media shall be considered removable if it is possible to remove it from the loaded position, i.e., a single mechanism changer, even if the media is captive to the changer.

...

The Pvnt Jmpr bit, when set to zero, shall indicate that the Prevent Jumper is present. The Logical Unit shall ~~power up to the allow state and locking the Logical Unit with the PREVENT ALLOW MEDIUM REMOVAL command shall not prevent insertion of the media~~set the default value of the DTE prevent state to zero (see 6.18 and SPC-3). When set to one, the Prevent Jumper is not present. The Logical Unit shall ~~power up to the prevent state (locked) and shall not accept new media or allow the ejection of media already loaded until a PREVENT ALLOW MEDIUM REMOVAL (allow) command is issued~~set the default value of the DTE prevent state to zero (see 6.18 and SPC-3). The Pvnt Jmpr bit shall not change state, even if the physical jumper is added or removed during operation. Logical Units that do not have a Prevent Jumper available should set this bit to 0 to indicate that the Logical Unit behaves as described for a jumper being present.

...

Logical Units that support the Removable Medium Feature shall implement the commands specified in Table 86.

Table 5 — Removable Medium Feature Commands

Op Code	Command description	Reference
BDh	MECHANISM STATUS	6.11
1Eh	PREVENT ALLOW MEDIUM REMOVAL ~~with the Persistent Prevent bit set to zero~~and the DTE prevent state	6.18
1Bh	START STOP UNIT and load eject (LOEJ) bit	6.45

5

6.18 PREVENT ALLOW MEDIUM REMOVAL Command

6.18.1 Introduction

The PREVENT/ALLOW MEDIUM REMOVAL Command requests that the Logical Unit enable or disable the removal of the medium in the Logical Unit. The Logical Unit shall not allow medium removal if any Initiator currently has medium removal prevented. The method of prevention of medium removal is vendor specific.

The PREVENT ALLOW MEDIUM REMOVAL command (see table 116) requests that the logical unit enable or disable the removal of the medium by an operator (e.g., with a manual eject button), by a medium changer, and/or by a START STOP UNIT command (see SBC-2, RBC, or MMC-4). The method used by the logical unit to prevent medium removal is vendor specific.

SPC-3 describes a PREVENT ALLOW MEDIUM REMOVAL command, however, the SPC-3 description does not apply to MM devices.

The PREVENT ALLOW MEDIUM REMOVAL command is described in SPC-3.

Table 326 shows the Features associated with the PREVENT ALLOW MEDIUM REMOVAL command.

Table 6 — Features associated with the PREVENT ALLOW MEDIUM REMOVAL command

Feature Number	Feature Name	Command Requirement
0002h	Morphing	Mandatory
0003h	Removable Medium	Mandatory

6.18.2 The CDB and its Parameters

The PREVENT ALLOW MEDIUM REMOVAL CDB is shown in Table 327.

Table 7 — PREVENT ALLOW MEDIUM REMOVAL CDB

Byte\Bit	7	6	5	4	3	2	1	0
0	OPERATION CODE (1Eh)							
1	Reserved							
2	Reserved							
3	Reserved							
4	Reserved						PERSISTENT	PREVENT
5	CONTROL							

The Logical Unit maintains two separate Prevent states: Prevent and Persistent Prevent as described in 4.1.7. The Persistent and Prevent bits are used to independently select values for these states. See Table 328.

Table 8 — PREVENT ALLOW MEDIUM REMOVAL PREVENT field

Persistent	Prevent	Meaning
0	0	Prevent State shall be cleared (Unlocked)
0	1	Prevent State shall be set (Locked)
1	0	Persistent Prevent State shall be cleared (Persistent Allow)
1	1	Persistent Prevent State shall be set (Persistent Prevent)

The recommended default state at power-on or hard reset is Prevent State cleared and Persistent Prevent State cleared.

> Editor's Note 3: Later descriptions state that the persistent prevent status is "reset" on power on. Is that just back to the default, whatever it might be? later description doesn't mention power-on for the Prevent state. Other text says Persistent Prevent shall default to 0.

6.18.3 Command Execution

6.18.3.1 Overview

The selected state begins upon successful completion of the PREVENT ALLOW MEDIUM REMOVAL command.

6.18.3.2 Persistent Prevent state

Upon entering the Persistent Prevent state, the logical unit shall disable any eject mechanisms, and all media after initial media spin up shall remain locked in the Logical Unit until:

   a) the Initiator issues an eject request; or
   b) the Persistent Prevent status is reset and the hardware eject mechanism again becomes available.

The Persistent Prevent status shall be reset upon:

   a) receipt of a PREVENT/ALLOW MEDIUM REMOVAL command (from the same Initiator that originally set the Persistent Prevent state) with the Persistent bit set and the Prevent bit cleared (i.e., a value of 10b);
   b) a bus reset; or
   c) a power reset condition.

Upon insertion of new media, under Persistent Prevent conditions, the logical unit eject controls shall remain functional up until the Logical Unit generates or reports a New Media event as defined in the Media Events section. After this event has been generated or reported, the media shall remain locked as defined above. The logical unit is allowed to morph from the no medium present state to the medium present state without explicit direction from the Initiator.

The logical unit shall not report a New Media Event if the medium is removed between the generation of the Event and the next GET EVENT/STATUS NOTIFICATION command issued.

The Persistent Prevent state shall not prevent an eject request from the Initiator from succeeding.

6.18.3.3 Prevent State

The Prevent State (Locked) is entered upon successful completion of the PREVENT/ALLOW MEDIUM REMOVAL command where Prevent State is set.

The prevention of medium removal for the Logical Unit shall terminate:

   1) After the Initiator has issued a PREVENT/ALLOW MEDIUM REMOVAL command clearing Prevent State and the Logical Unit has successfully performed a flush cache operation; or
   2) Upon a Hard Reset condition; or
   3) Upon a DEVICE RESET in an ATAPI environment; or

While a prevention of medium removal condition is in effect the Logical Unit shall inhibit mechanisms that normally allow removal of the medium by an operator. This is also the case for changers.

> Editor's Note 4: MCHNGR is required to be 0 by MMC. I assume the previous sentence means changers that the Logical Unit knows nothing about (e.g. that just press the eject button mechanically).

Unlocked is the recommended default state of the Logical Unit at power on.

This command affects the actions of the START/STOP UNIT command (6.45) and other mechanisms (e.g. manual ejection / media removal systems).

Table 9 — Actions for Lock/Unlock/Eject

Operation	Current Prevent State	No Media Present	Media Present and READY
Unlock	Unlocked	No error	No error.
Unlock	Locked	No error, medium may be inserted	No error, medium may be removed
Lock	Unlocked	No error, media insertion is not permitted	No error, media to be removal is not permitted
Lock	Locked	No error	No error
Start/Stop Unit with Start=0 and LoEj=1	Unlocked	No error. Media mount mechanism is opened.	No error. Media is ejected.
Start/Stop Unit with Start=0 and LoEj=1	Locked	CHECK CONDITION	CHECK CONDITION
Manual Eject	Unlocked	Media mount mechanism is opened.	Media is ejected.
Manual Eject	Locked	No visible operation occurs	No visible operation occurs.

Editor's Note 5: I assume that "Unlock" means running the command with 00b, and "Lock" means running it with 01b

6.18.4 Timeouts

The PREVENT ALLOW MEDIUM REMOVAL command belongs to timeout group 1. If the command is terminated with CHECK CONDITION status due to a timeout, sense bytes SK/ASC/ASCQ shall be set to UNIT ATTENTION/INSUFFICIENT TIME FOR OPERATION.

6.18.5 Error Reporting

Recommended error reporting for the PREVENT ALLOW MEDIUM REMOVAL command is defined in Table 330.

Table 10 — Recommended errors for PREVENT ALLOW MEDIUM REMOVAL command

Error	Reference
Unit Attention conditions	Table F.1
CDB or parameter list validation errors	Table F.2
Hardware failures	Table F.8

A.2.6 Mapping of Reset Functions

Table A.4 shows how the different reset functions specified in the SCSI standards are used in this standard. This table is not intended to show all possible resets or their mapping.

Table 11 — Example Reset Function Mapping in ATAPI

Reset Type	ATAPI
Power-On Reset	Same as SCSI Power-On Reset
Hard Reset	Hard Reset
	ATA SRST. This is a channel reset and as such is treated as a Hard Reset. However, the SRST does not reset any mode parameters to the default state.
Logical Unit Reset	ATA DEVICE RESET command.

Annex E Legacy Specifications

E.3 MODE PARAMETERS

E.3.3 MM Capabilities and Mechanical Status Page (Page Code 2Ah)

The MM Capabilities and Mechanical Status Page (Table E.20) is read only and should not be set with Mode Select.

...

When Lock is set to one, the Logical Unit should support ~~locking the media within the physical Logical Unit via~~ the PREVENT ALLOW MEDIUM REMOVAL command.

When Lock is set to one and Lock State is set to zero, the ~~Logical Unit is currently in the allow (unlocked) state~~DTE prevent state is currently true for the I_T nexus being used for the MODE SENSE command. When Lock is set to one and Lock State is set to one, the ~~Logical Unit is currently in the prevent (locked) state~~DTE prevent state is currently true for the I_T nexus being used for the MODE SENSE command. When Lock is set to zero, Lock State has no meaning.

~~When Prevent Jumper is set to zero, the Logical Unit has a physical jumper named the Prevent/Allow Jumper and the jumper is present.~~ A Prevent Jumper bit set to zero indicates that the Logical Unit has a physical jumper named the Prevent/Allow Jumper, the jumper is present, and the default DTE prevent state value is false. ~~At power on time, the default loading mechanism state should be allow (unlocked). Locking the Logical Unit with the PREVENT ALLOW MEDIUM REMOVAL command should not prevent the insertion of media.~~

> Editor's Note 6: In the last sentence, allowing "Locking" (assuming that means setting the Prevent state=1) to not prevent insertion violates all the descriptions in the PAMR command itself. Does this really intend to describe setting Persistent Prevent=1 instead? Note 37 implies that jumper present means normal behavior, so I suspect this sentence is just wrong.

~~When Prevent Jumper is set to one, the Logical Unit has a physical jumper named the Prevent/Allow Jumper and the jumper is not present.~~ A Prevent Jumper bit set to one indicates that the Logical Unit has a physical jumper named the Prevent/Allow Jumper, the jumper is not present, and the default DTE prevent state value is true. ~~At power on time, the default loading mechanism state should be prevent (locked). . The Logical Unit should not accept new media or allow the ejection of media already loaded until an allow command is issued.~~

> ~~NOTE 37: The Prevent Jumper is optional. If the Logical Unit does not implement the prevent Jumper, then it should respond as if the jumper was present .~~