

American National Standard

Information technology - ATA/ATAPI-8 Command Set (ATA8-ACS) - Ammendment 1

Approved mm/dd/yyyy:



Secretariat: Information Technology Industry Council

American National Standard

Approval of an American National Standard requires verification by ANSI that the requirements for due process, consensus, and other criteria for approval have been met by the standards developer. Consensus is established when, in the judgment of the ANSI Board of Standards Review, substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that effort be made towards their resolution.


The use of American National Standards is completely voluntary; their existence does not in any respect preclude anyone, whether he has approved the standards or not, from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standards.


The American National Standards Institute does not develop standards and will in no circumstances give interpretation on any American National Standard. Moreover, no person shall have the right or authority to issue an interpretation of an American National Standard in the name of the American National Standards Institute. Requests for interpretations should be addressed to the secretariat or sponsor whose name appears on the title page of this standard.

CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time. The procedures of the American National Standards Institute require that action be taken periodically to reaffirm, revise, or withdraw this standard. Purchasers of American National Standards may receive current information on all standards by calling or writing the American National Standards Institute.

Summary of Comments on ACS Proposal Template

Page: 1

 Number: 1 Author: moverby Subject: Sticky Note Date: 4/16/2009 1:10:58 PM
Add adobe bookmarks for each change section


 Number: 2 Author: moverby Subject: Sticky Note Date: 4/16/2009 2:06:12 PM
Global: Remove change bars


Replace a single row in Table 6:**Table 6 — Block Size By Command (part 1 of 2)**

Command	Words Transferred per Block
CFA TRANSLATE SECTOR	256

**Insert a single row into Table 3****Table 9 — Security Command Actions (part 3 of 4)**

Command	Locked	Disabled or Unlocked	Frozen
TRUSTED NON-DATA	Command aborted	Executable	Executable

 Number: 1 Author: moverby Subject: Cross-Out Date: 4/16/2009 1:13:08 PM
This I does not belong here and if this was intended to be a 1, it is wrong as well.

 Number: 2 Author: moverby Subject: Sticky Note Date: 4/16/2009 1:14:00 PM
These changes should be reordered to be in the same order they appear in the document that this amendment applies to.

Completely replace section 4.25 with the following text:**4.25 Trusted Computing feature set**

The Trusted Computing feature set provides an interface between a horizontal security product embedded in devices whose behavior may be authorized via interaction with a trusted host system.

The following commands are mandatory for devices implementing the Trusted Computing feature set:

- a) TRUSTED SEND;
- b) TRUSTED SEND DMA;
- c) TRUSTED RECEIVE;
- d) TRUSTED RECEIVE DMA; and
- e) TRUSTED NON-DATA.

TRUSTED SEND and TRUSTED SEND DMA may be used interchangeably. The two commands only differ by the type of data transport protocol used (i.e., PIO Data-Out Command or DMA Command). Similarly, TRUSTED RECEIVE and TRUSTED RECEIVE DMA are interchangeable (i.e., PIO Data-In Command or DMA Command). IDENTIFY DEVICE data word 48 bit 0 indicates whether or not this feature set is supported.

The DEVICE CONFIGURATION OVERLAY SET command provides a mechanism to remove support for this feature set.

The data streams and subsequent actions resulting from these commands are defined by the security protocol identified in the command parameters. These protocols may be defined by groups outside of this standard. The intent is to standardize the data content so it is identical across both ATA and SCSI interfaces.

This page contains no comments

Completely replace section 4.27 with the following text:**4.27 Write-Read-Verify feature set**

The optional ¹Write-Read-Verify feature set allows a host to control ²Read After Write behavior in a device.

To enable or disable the feature of ³Write/Read/Verify, the host ~~may issue~~ a SET FEATURES command with one of two subcommand codes.

It is possible that the device may experience a ⁴performance ~~degradation~~ when the Write-Read-Verify feature set is enabled.

These commands are affected by this feature:

- a) WRITE DMA
- b) WRITE DMA EXT
- c) WRITE DMA FUA EXT
- d) WRITE DMA QUEUED
- e) WRITE DMA QUEUED EXT
- f) WRITE DMA QUEUED FUA EXT
- g) WRITE FPDMA QUEUED
- h) WRITE MULTIPLE
- i) WRITE MULTIPLE EXT
- j) WRITE MULTIPLE FUA EXT
- k) WRITE SECTOR(S)
- l) WRITE SECTOR(S) EXT

⁶See 7.52.10 for a description of device behavior when this feature set is supported and enabled.

⁷The IDENTIFY DEVICE command shall reflect the supported and enabled or disabled state of this feature set.

When the device's volatile write cache is enabled, the device may report command completion with no error to the host even if the data is in the device volatile write cache and not written and verified to the non-volatile media. This is ~~important to reduce~~ ⁹the ¹⁰performance ~~degradation~~ when the Write-Read-Verify feature set is enabled.

If:



- a) the volatile write cache is disabled and any write command is processed by the device;
- b) a forced unit access write command is processed by the device; or
- c) a flush cache command is processed by the device,










then the device shall only report command completion after the data has been verified.

If the Write-Read-Verify feature set is enabled and the device has not already verified the maximum number of logical sectors configured for this feature set, then after after the device has written the sectors to the non-volatile media, the device shall read the data from the non-volatile media and verify that there are no errors. A read from the non-volatile media shall be performed before verification. The verification of sectors is defined as vendor specific.

If the Write-Read-Verify feature set is disabled, or if the device has already verified the maximum number of logical sectors configured for this feature set, then no verification by this feature set shall be performed after the device has written the sectors to the non-volatile media.

If an unrecoverable error condition is encountered by the device during the write, read, or verify operation, the device shall set the Device Fault bit ¹¹(See 6.2.7) to one.

-
-  Number: 1 Author: moverby Subject: Highlight Date: 4/16/2009 1:24:13 PM
Is it Write-Read-Verify or Write/Read/Verify. It is used both ways. To be consistent with the feature set name, it should be Write-Read-Verify.
-
-  Number: 2 Author: moverby Subject: Highlight Date: 4/16/2009 1:19:46 PM
s/b
read after write

There is no need for non-standard case.
-
-  Number: 3 Author: moverby Subject: Highlight Date: 4/16/2009 1:24:17 PM
Is it Write-Read-Verify or Write/Read/Verify. It is used both ways. To be consistent with the feature set name, it should be Write-Read-Verify.
-
-  Number: 4 Author: moverby Subject: Cross-Out Date: 4/16/2009 1:28:05 PM
-
-  Number: 5 Author: moverby Subject: Replacement Text Date: 4/16/2009 1:27:58 PM
s/b
reduced
-
-  Number: 6 Author: moverby Subject: Highlight Date: 4/16/2009 1:31:16 PM
This cross reference is to the sleep command in ATA8-ACS r6a (the last draft). This is incorrect.
-
-  Number: 7 Author: moverby Subject: Highlight Date: 4/16/2009 1:31:59 PM
Do we need to say this? Isn't this already covered in IDENTIFY DEVICE? Suggest deletion.
-
-  Number: 8 Author: moverby Subject: Cross-Out Date: 4/16/2009 1:45:20 PM
-
-  Number: 9 Author: moverby Subject: Replacement Text Date: 4/16/2009 1:44:58 PM
s/b
mitigates
-
-  Number: 10 Author: moverby Subject: Inserted Text Date: 4/16/2009 1:45:17 PM
reduced
-
-  Number: 11 Author: moverby Subject: Highlight Date: 4/16/2009 1:56:24 PM
This cross reference is wrong against ATA8-ACS r6a (the last draft). It appears this should be 6.2.6. 6.2.7 is the device ready bit.

Completely replace section 7.48.10 with the following text:

7.48.10 Enable/Disable Write-Read-Verify feature set

Subcommand code 0Bh enables the Write-Read-Verify feature set.

Bits (7:0) of the LBA field in the SET FEATURES command specify the Write-Read-Verify mode.¹ Table 1 defines the Write-Read-Verify modes.

² Table 1 — Write-Read-Verify Modes


Mode	Description
00h ^a	Always enabled (i.e., the device shall perform a Write-Read-Verify for all logical sectors for all write commands).
01h ^a	The device shall perform a Write-Read-Verify on the first 65,536 logical sectors written by the host after: <ul style="list-style-type: none"> d) spin-up; or e) the device completes a SET FEATURES command setting the Write-Read-Verify mode without error.
02h ^a	The number of logical sectors on which a device performs a Write-Read-Verify is vendor specific.
03h	The device shall perform a Write-Read-Verify on the first (number specified by the Count field in the SET FEATURES command x 1,024) logical sectors written by the host after: <ul style="list-style-type: none"> a) spin-up; or b) the device completes a SET FEATURES command setting the Write-Read-Verify mode without error.
04h-FFh	Reserved
^a the Count field shall be ignored.	

Subcommand code 8Bh disables the Write-Read-Verify feature set.


A device shall set the Write-Read-Verify feature set to its factory default setting after processing of a power-on reset or if the Software Settings Preservation feature set is disabled and a hardware reset is processed. If the Software Settings Preservation feature set is enabled and a hardware reset is processed, the device shall not change the settings of the Write-Read-Verify feature set.

If a device is in the reverting to defaults enabled mode (see 7.48.16), then the device shall set the Write-Read-Verify feature set to its factory default setting after processing of a software reset.

If a device is in the reverting to defaults disabled mode (see 7.48.16), then the device shall not change the settings of the Write-Read-Verify feature set after processing of a software reset.

 Number: 1 Author: moverby Subject: Highlight Date: 4/16/2009 1:57:56 PM

This is wrong. The Table has to be table 55 so that if this were to be inserted into a document you wouldn't have two table 1 entries.

 Number: 2 Author: moverby Subject: Highlight Date: 4/16/2009 1:58:08 PM

s/b
Table 55

Completely replace section 7.49.6 with the following text:**7.49.6 SET MAX UNLOCK - F9h/03h, PIO Data-Out****7.49.6.1 Feature Set**

This 28-bit command is mandatory for devices that implement the HPA Security Extensions.

7.49.6.2 Description

This command requests a transfer of a single 512-byte block of data from the host. Table 59 defines the content of this data.

The password supplied in the data transferred shall be compared with the password set by the SET MAX SET PASSWORD command.

If the device is locked from HPA commands and the password compare fails, then the device shall return command aborted and decrement the HPA Security Extensions unlock counter. This counter shall be decremented for each password mismatch when SET MAX UNLOCK is issued and the device is locked from HPA commands. When this counter reaches zero in a device, then the device shall return command aborted for all subsequent SET MAX UNLOCK commands until after the device has processed a power-on reset.

NOTE 1 — The HPA Security Extensions unlock counter is not related to the Security feature set unlock counter.

If the device is HPA Locked, the HPA Security Extensions unlock counter is not zero, and the password compare matches, then the device is HPA Unlocked and all SET MAX commands shall be accepted.

This command should not be immediately preceded by a READ NATIVE MAX ADDRESS command. If this command is immediately preceded by a READ NATIVE MAX ADDRESS command, it shall be interpreted as a SET MAX ADDRESS command.

7.49.6.3 Inputs


Name	Description
Feature	03h
Count	N/A
LBA	N/A
Device	<p>Bit Description</p> <p>7 Obsolete</p> <p>6 N/A</p> <p>5 Obsolete</p> <p>4 Transport Dependent - See 6.2.11</p> <p>3:0 Reserved</p>
Command	7:0 F9h

7.49.6.4 Normal Outputs

See table 99.

7.49.6.5 Error Outputs

If a device is not HPA Locked, then the device shall return command aborted. A device may return command completion with the Error bit set to one if an Interface CRC error has occurred. See table 126.ee table 99.

 Number: 1 Author: moverby Subject: Highlight Date: 4/16/2009 2:00:59 PM
This NOTE should be the correct sequential number for where it belongs. Not NOTE-1.

r6a indicates that it should be NOTE 24.

7.49.6.6 Output From the Host to the Device Data Structure

See Table 59

This page contains no comments