



ISO/IEC 17760-101

Edition 1.0 2015-06

INTERNATIONAL STANDARD



Information technology – AT attachment 8 –
Part 101: ATA/ATAPI Command Set (ACS)



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2015 ISO/IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about ISO/IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

IEC Central Office
3, rue de Varembe
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue

The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,...). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

More than 60 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.



ISO/IEC 17760-101

Edition 1.0 2015-06

INTERNATIONAL STANDARD



**Information technology – AT attachment 8 –
Part 101: ATA/ATAPI Command Set (ACS)**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 35.200

ISBN 978-2-8322-2695-7

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

FOREWORD.....	14
INTRODUCTION	16
1 Scope	17
2 Normative references	17
3 Terms, definitions and conventions	18
3.1 Terms and definitions	18
3.2 Conventions	25
3.2.1 Overview	25
3.2.2 Precedence	25
3.2.3 Lists	26
3.2.4 Keywords	26
3.2.5 Numbering	27
3.2.6 Bit conventions	28
3.2.7 State diagram conventions	28
3.2.8 Byte, word, DWord, and QWord Relationships	29
3.2.9 ATA string convention	31
4 Feature set definitions	32
4.1 Overview	32
4.2 General feature set	32
4.3 The PACKET feature set	33
4.3.1 Overview	33
4.3.2 Identification of PACKET feature set devices	34
4.3.3 Signature for ATAPI devices	34
4.3.4 The PACKET command	34
4.4 48-bit Address feature set	34
4.5 Advanced Power Management (APM) feature set	35
4.6 Automatic Acoustic Management (AAM) feature set	35
4.7 CompactFlash Association (CFA) feature set	35
4.8 Device Configuration Overlay (DCO) feature set	36
4.9 Free-fall Control feature set	38
4.10 General Purpose Logging (GPL) feature set	38
4.11 Host Protected Area (HPA) feature set	39
4.11.1 HPA overview	39
4.11.2 HPA security extensions	39
4.11.3 28-bit and 48-bit HPA commands interactions	39
4.11.4 IDENTIFY DEVICE data	41
4.11.5 Determination of SET MAX security extension status	41
4.11.6 HPA State Transition Diagrams	41
4.12 Long Logical Sector (LLS) feature set	56
4.13 Long Physical Sector (LPS) feature set	58
4.14 Media Card Pass Through Command feature set	60
4.15 Native Command Queuing (NCQ) feature set	60
4.15.1 Overview	60
4.15.2 Command Phases	61

4.16 NV Cache feature set	61
4.16.1 Overview	61
4.16.2 Pinning	61
4.16.3 NV Cache Management	62
4.16.4 Rotating media state after power-on event	62
4.17 NV Cache Power Management feature set	62
4.18 Power Management feature set	63
4.18.1 Overview	63
4.18.2 Power management commands	63
4.18.3 Standby timer	64
4.18.4 Power modes	64
4.19 Power-Up In Standby (PUIS) feature set	66
4.20 Security feature set	66
4.20.1 Overview	66
4.20.2 Passwords	67
4.20.3 Master Password Capability	67
4.20.4 Frozen Mode	67
4.20.5 Commands	67
4.20.6 IDENTIFY DEVICE data	67
4.20.7 Security initial setting	68
4.20.8 Password rules	68
4.20.9 Password attempt counter	68
4.20.10 Security states	69
4.20.11 Master Password Identifier feature	78
4.21 Self-Monitoring, Analysis, and Reporting Technology (SMART) feature set	79
4.21.1 Overview	79
4.21.2 Device SMART data structure	79
4.21.3 Background data collection	79
4.21.4 Off-line/Captive mode data collection	79
4.21.5 Threshold exceeded condition	79
4.21.6 SMART feature set commands	79
4.21.7 SMART operation with power management modes	79
4.21.8 SMART device error log reporting	80
4.22 Software Settings Preservation (SSP) feature set	80
4.23 Streaming feature set	81
4.23.1 Streaming feature set overview	81
4.23.2 Streaming commands	81
4.24 Tagged Command Queuing (TCQ) feature set	82
4.24.1 Overview	82
4.24.2 Queueing	83
4.25 Trusted Computing feature set	83
4.26 Write-Read-Verify feature set	84
5 ATA protocols	86
6 Normal and Error Output field descriptions	87
6.1 Overview	87
6.2 Status field	87
6.2.1 Overview	87
6.2.2 Busy bit	87
6.2.3 Check Condition bit	87

6.2.4 Data Request bit	87
6.2.5 Deferred Write Error bit	87
6.2.6 Device Fault bit	88
6.2.7 Device Ready bit	88
6.2.8 Error bit	88
6.2.9 Service bit	88
6.2.10 Stream Error bit	88
6.2.11 Transport Dependent (TD)	88
6.3 Error field	89
6.3.1 Overview	89
6.3.2 Abort bit	89
6.3.3 Attempted Partial Range Removal bit	89
6.3.4 Command Completion Time Out bit	89
6.3.5 End of Media bit	89
6.3.6 ID Not Found bit	89
6.3.7 Illegal Length Indicator bit	90
6.3.8 Insufficient LBA Range Entries Remaining bit	90
6.3.9 Insufficient NV Cache Space bit	90
6.3.10 Interface CRC bit	90
6.3.11 Media Error bit	90
6.3.12 Sense Key field	90
6.3.13 Uncorrectable Error bit	90
6.4 Interrupt Reason field	90
6.4.1 Overview	90
6.4.2 Command/Data bit	90
6.4.3 Input/Output (I/O) bit	90
6.4.4 Release bit	91
6.4.5 Tag field	91
6.5 Count field	91
6.5.1 Overview	91
6.5.2 NCQ Tag field	91
6.6 SActive field	91
6.7 SATA Status	91
7 Command descriptions	92
7.1 Command description introduction	92
7.1.1 Overview	92
7.1.2 Command Name - Command Code [/Subcommand Code], Command Protocol	92
7.1.3 Feature Set	92
7.1.4 Inputs	93
7.1.5 Normal Outputs	93
7.1.6 Error Outputs	94
7.1.7 Input From the Device to the Host Data Structure	94
7.1.8 Output From the Host to the Device Data Structure	95
7.1.9 Unsupported commands	95
7.2 CFA ERASE SECTORS - C0h, Non-Data	95
7.3 CFA REQUEST EXTENDED ERROR CODE - 03h, Non-Data	96
7.4 CFA TRANSLATE SECTOR - 87h, PIO Data-In	98
7.5 CFA WRITE MULTIPLE WITHOUT ERASE - CDh, PIO Data-Out	99
7.6 CFA WRITE SECTORS WITHOUT ERASE - 38h, PIO Data-Out	100

7.7 CHECK MEDIA CARD TYPE - D1h, Non-Data	101
7.8 CHECK POWER MODE - E5h, Non-Data	102
7.9 CONFIGURE STREAM - 51h, Non-Data	103
7.10 Device Configuration Overlay (DCO)	104
7.10.1 DCO Overview	104
7.10.2 DEVICE CONFIGURATION FREEZE LOCK - B1h/C1h, Non-Data	105
7.10.3 DEVICE CONFIGURATION IDENTIFY - B1h/C2h, PIO Data-In	106
7.10.4 DEVICE CONFIGURATION RESTORE - B1h/C0h, Non-Data	110
7.10.5 DEVICE CONFIGURATION SET - B1h/C3h, PIO Data-Out	111
7.11 DEVICE RESET - 08h, Device Reset	118
7.12 DOWNLOAD MICROCODE - 92h, PIO Data-Out/Non-Data	119
7.13 EXECUTE DEVICE DIAGNOSTIC - 90h, Execute Device Diagnostic	121
7.14 FLUSH CACHE - E7h, Non-Data	122
7.15 FLUSH CACHE EXT - EAh, Non-Data	124
7.16 IDENTIFY DEVICE - ECh, PIO Data-In	125
7.17 IDENTIFY PACKET DEVICE - A1h, PIO Data-In	163
7.18 IDLE - E3h, Non-Data	181
7.19 IDLE IMMEDIATE - E1h, Non-Data	182
7.20 Non-Volatile Cache	183
7.20.1 NV Cache Overview	183
7.20.2 NV Cache Power Management Overview	184
7.20.3 ADD LBA(S) TO NV CACHE PINNED SET - B6h/10h, DMA.....	184
7.20.4 FLUSH NV CACHE - B6h/14h, Non-Data	186
7.20.5 NV CACHE DISABLE- B6h/16h, Non-Data.....	187
7.20.6 NV CACHE ENABLE - B6h/15h, Non-Data.....	188
7.20.7 QUERY NV CACHE MISSES - B6h/13h, DMA	189
7.20.8 QUERY NV CACHE PINNED SET - B6h/12h, DMA	191
7.20.9 REMOVE LBA(S) FROM NV CACHE PINNED SET - B6h/11h, DMA/Non-Data.....	192
7.20.10 RETURN FROM NV CACHE POWER MODE - B6h/01h, Non-Data	194
7.20.11 SET NV CACHE POWER MODE - B6h/00h, Non-Data.....	195
7.21 NOP - 00h, Non-Data	196
7.22 PACKET - A0h, Packet	197
7.23 READ BUFFER - E4h, PIO Data-In	199
7.24 READ DMA - C8h, DMA	200
7.25 READ DMA EXT - 25h, DMA	201
7.26 READ DMA QUEUED - C7h, DMA Queued	202
7.27 READ DMA QUEUED EXT- 26h, DMA Queued	203
7.28 READ FPDMA QUEUED - 60h, DMA Queued	205
7.29 READ LOG EXT - 2Fh, PIO Data-In	206
7.30 READ LOG DMA EXT - 47h, DMA	207
7.31 READ MULTIPLE - C4h, PIO Data-In	208
7.32 READ MULTIPLE EXT - 29h, PIO Data-In	209
7.33 READ NATIVE MAX ADDRESS - F8h, Non-Data	210
7.34 READ NATIVE MAX ADDRESS EXT - 27h, Non-Data	211
7.35 READ SECTOR(S) - 20h, PIO Data-In	212
7.36 READ SECTOR(S) EXT - 24h, PIO Data-In	213
7.37 READ STREAM DMA EXT - 2Ah, DMA	214

7.38 READ STREAM EXT - 2Bh, PIO Data-In	216
7.39 READ VERIFY SECTOR(S) - 40h, Non-Data	217
7.40 READ VERIFY SECTOR(S) EXT - 42h, Non-Data	218
7.41 SECURITY DISABLE PASSWORD - F6h, PIO Data-Out	219
7.42 SECURITY ERASE PREPARE - F3h, Non-Data	220
7.43 SECURITY ERASE UNIT - F4h, PIO Data-Out	221
7.44 SECURITY FREEZE LOCK - F5h, Non-Data	223
7.45 SECURITY SET PASSWORD - F1h, PIO Data-Out	224
7.46 SECURITY UNLOCK - F2h, PIO Data-Out	225
7.47 SERVICE - A2h, DMA Queued	227
7.48 SET FEATURES - EFh, Non-Data	228
7.48.3 Enable/disable 8-bit PIO data transfer	230
7.48.4 Enable/disable volatile write cache	230
7.48.5 Set transfer mode	230
7.48.6 Enable/disable the APM feature set	231
7.48.7 Enable/disable the PUIS feature set	232
7.48.8 PUIS feature set device spin-up	232
7.48.9 Enable/disable CFA power mode 1	232
7.48.10 Enable/Disable Write-Read-Verify feature set	233
7.48.11 Enable/disable the AAM feature set	233
7.48.12 Set Maximum Host Interface Sector Times	234
7.48.13 Enable/disable read look-ahead	234
7.48.14 Enable/disable release interrupt	235
7.48.15 Enable/disable SERVICE interrupt	235
7.48.16 Enable/disable reverting to defaults	235
7.48.17 Enable/Disable the Free-fall Control feature set	235
7.48.18 Enable/Disable SATA feature	235
7.49 SET MAX	237
7.49.2 SET MAX ADDRESS - F9h, Non-Data.....	238
7.49.3 SET MAX FREEZE LOCK – F9h/04h, Non-Data	240
7.49.4 SET MAX LOCK - F9h/02h, Non-Data	241
7.49.5 SET MAX SET PASSWORD - F9h/01h, PIO Data-Out.....	242
7.49.6 SET MAX UNLOCK - F9h/03h, PIO Data-Out.....	243
7.50 SET MAX ADDRESS EXT - 37h, Non-Data	245
7.51 SET MULTIPLE MODE - C6h, Non-Data	246
7.52 SLEEP - E6h, Non-Data	247
7.53 SMART	248
7.53.2 SMART DISABLE OPERATIONS - B0h/D9h, Non-Data.....	249
7.53.3 SMART ENABLE/DISABLE ATTRIBUTE AUTOSAVE - B0h/D2h, Non-Data	250
7.53.4 SMART ENABLE OPERATIONS - B0h/D8h, Non-Data.....	251
7.53.5 SMART EXECUTE OFF-LINE IMMEDIATE - B0h/D4h, Non-Data	253
7.53.6 SMART READ DATA - B0h/D0h, PIO Data-In	257
7.53.7 SMART READ LOG - B0h/D5h, PIO Data-In	262
7.53.8 SMART RETURN STATUS - B0h/DAh, Non-Data.....	263
7.53.9 SMART WRITE LOG - B0h/D6h, PIO Data-Out.....	264
7.54 STANDBY - E2h, Non-Data	265
7.55 STANDBY IMMEDIATE - E0h, Non-Data	266
7.56 TRUSTED NON-DATA - 5Bh, Non-Data	267

7.57 TRUSTED RECEIVE - 5Ch, PIO Data-In	268
7.58 TRUSTED RECEIVE DMA - 5Dh, DMA	271
7.59 TRUSTED SEND - 5Eh, PIO Data-Out	273
7.60 TRUSTED SEND DMA - 5Fh, DMA	275
7.61 WRITE BUFFER - E8h, PIO Data-Out	276
7.62 WRITE DMA - CAh, DMA	277
7.63 WRITE DMA EXT - 35h, DMA	278
7.64 WRITE DMA FUA EXT - 3Dh, DMA	279
7.65 WRITE DMA QUEUED - CCh, DMA Queued	279
7.66 WRITE DMA QUEUED EXT - 36h, DMA Queued	282
7.67 WRITE DMA QUEUED FUA EXT - 3Eh, DMA Queued	284
7.68 WRITE FPDMA QUEUED - 61h, DMA Queued	285
7.69 WRITE LOG EXT - 3Fh, PIO Data-Out	286
7.70 WRITE LOG DMA EXT - 57h, DMA	287
7.71 WRITE MULTIPLE - C5h, PIO Data-Out	288
7.72 WRITE MULTIPLE EXT - 39h, PIO Data-Out	289
7.73 WRITE MULTIPLE FUA EXT - CEh, PIO Data-Out	290
7.74 WRITE SECTOR(S) - 30h, PIO Data-Out	291
7.75 WRITE SECTOR(S) EXT - 34h, PIO Data-Out	292
7.76 WRITE STREAM DMA EXT - 3Ah, DMA	293
7.77 WRITE STREAM EXT - 3Bh, PIO Data-Out	295
7.78 WRITE UNCORRECTABLE EXT - 45h, Non-Data	296
8 SCT Command Transport	298
8.1 Overview	298
8.1.1 General	298
8.1.2 SCT command nesting and interspersing with standard commands	298
8.1.3 Resets	298
8.2 Processing SCT commands	299
8.2.1 Processing SCT commands overview	299
8.2.2 SCT capability identification	299
8.2.3 SCT command transfer	299
8.2.4 SCT data transfer	303
8.2.5 SCT status	305
8.3 SCT Command Set	309
8.3.1 Overview	309
8.3.2 SCT Read/Write Long command.....	310
8.3.3 SCT Write Same command.....	312
8.3.4 SCT Error Recovery Control command.....	315
8.3.5 SCT Feature Control command.....	317
8.3.6 SCT Data Table command.....	320
9 Normal and Error Outputs	324
9.1 Overview	324
9.2 Normal Outputs	324
9.3 Error Outputs	344
Annex A (normative) – Log definitions	386

Annex B (informative) – Command Set summary.....	407
Annex C (informative) – Design and programming considerations for large physical sector devices.....	432
Annex D (informative) – How to use SCT commands	434
Annex E (informative) – Implementation Guidelines For 1 024/4 096 Byte Sector Sizes	442
Bibliography	448

FIGURES

Figure 1 – ATA document relationships	16
Figure 2 – State diagram convention	28
Figure 3 – Byte, word, DWord and QWord relationships	29
Figure 4 – Device Configuration Overlay state diagram	37
Figure 5 – HPA Not Set	42
Figure 6 – HPA Set (28).....	43
Figure 7 – HPA Set (48).....	44
Figure 8 – HPA Locked (28)	45
Figure 9 – HPA Locked (48)	46
Figure 10 – LLS and LPS Example.....	59
Figure 11 – Alignment 0	59
Figure 12 – Alignment 1	59
Figure 13 – Alignment 3	59
Figure 14 – Power management state diagram	64
Figure 15 – Security state diagram	73
Figure 16 – Selective self-test span example	255
Figure C.1 – Unaligned Write Example.....	4 3 3
Figure D.1 – Example flowchart for SCT commands.....	435
Figure D.2 – Example sequence for foreground write same with a repeating pattern	436
Figure D.3 – Example sequence for foreground write same with a repeating sector	436
Figure D.4 – Example sequence for writing data using an SCT command with no background activity	436
Figure D.5 – Example sequence for reading data using an SCT command with no background activity	437
Figure D.6 – Example Sequence for a Non-Data SCT command with no background activity	437
Figure D.7 – Example sequence for writing data using an SCT command with background activity	438
Figure D.8 – Example sequence for a Non-Data SCT command with background activity	439
Figure E.1 – System Dependency Chain.....	442
Figure E.2 – Mapping Proposals.....	443
Figure E.3 – Logical to Physical Mapping.....	4 43
Figure E.4 – Uncorrectable Error Handling	445
Figure E.5 – Typical HDD Layout Using A Master Boot Record	446

TABLES

Table 1 – Numbering conventions examples.....	28
Table 2 – ATA string byte swapping	31
Table 3 – ATA firmware revision example	31
Table 4 – Feature Set Summary	32
Table 5 – Block Size By Command	57
Table 6 – Media Card type references.....	60
Table 7 – Summary of Security States and Characteristics.....	69
Table 8 – Security Command Actions.....	70
Table 9 – IDENTIFY settings for Security state SEC1.....	74
Table 10 – IDENTIFY settings for Security state SEC2.....	75
Table 11 – IDENTIFY settings for Security state SEC4.....	76
Table 12 – IDENTIFY settings for Security state SEC5.....	77
Table 13 – IDENTIFY settings for Security state SEC6.....	78
Table 14 – Preserved Feature Sets and Settings	80
Table 15 – Status field	87
Table 16 – Error field	89
Table 17 – Interrupt Reason Field	90
Table 18 – Count field.....	91
Table 19 – Example Inputs	93
Table 20 – Example Normal Output.....	93
Table 21 – Example Error Output	94
Table 22 – Extended error codes.....	96
Table 23 – CFA TRANSLATE SECTOR data.....	98
Table 24 – Device Configuration Overlay Feature field values.....	104
Table 25 – Device Configuration Identify data structure	107
Table 26 – Device Configuration Overlay (DCO) data structure	112
Table 27 – Count field output for DOWNLOAD MICROCODE requesting the offset transfer method	120
Table 28 – Diagnostic codes.....	122
Table 29 – IDENTIFY DEVICE data	126
Table 30 – Specific Configuration	143
Table 31 – Minor version number	149
Table 32 – Normal Erase Mode Time	155
Table 33 – Enhanced Erase Mode Time	155
Table 34 – IDENTIFY DEVICE data World Wide Name field (word-based view)	158
Table 35 – IDENTIFY DEVICE data World Wide Name field (byte-based view)	158
Table 36 – Device Nominal Form Factor	160
Table 37 – Nominal Media Rotation Rate	161
Table 38 – Transport minor version number	162
Table 39 – IDENTIFY PACKET DEVICE data.....	164
Table 40 – Standby timer periods	181
Table 41 – NV Cache Commands	184
Table 42 – NV Cache Power Management Commands	184
Table 43 – Request Pin Data.....	186
Table 44 – Cache Miss Data.....	190
Table 45 – Pin Set Data.....	191
Table 46 – Remove Pin Data.....	193
Table 47 – NOP Subcommand Code	196

Table 48 – SECURITY DISABLE PASSWORD data content.....	220
Table 49 – SECURITY ERASE UNIT data content	222
Table 50 – SECURITY SET PASSWORD data content	225
Table 51 – SECURITY UNLOCK data content	226
Table 52 – SET FEATURES Feature field definitions	228
Table 53 – Transfer modes	231
Table 54 – APM levels	231
Table 55 – Write-Read-Verify Modes.....	233
Table 56 – AAM levels	234
Table 57 – SATA Features	235
Table 58 – SET MAX Feature field values	237
Table 59 – SET MAX SET PASSWORD data content	242
Table 60 – SMART Feature field values	248
Table 61 – SMART EXECUTE OFF-LINE IMMEDIATE Subcommands	253
Table 62 – Device SMART data structure	258
Table 63 – Off-line data collection status byte values.....	259
Table 64 – Self-test execution status values	259
Table 65 – Offline Data Collection Capabilities.....	260
Table 66 – TRUSTED RECEIVE Security Protocol field description	269
Table 67 – Security Protocol 00h - SP Specific field descriptions for Protocol 00h	270
Table 68 – TRUSTED RECEIVE parameter data for SP Specific=0000h	270
Table 69 – TRUSTED RECEIVE parameter data for SP Specific=0001h	271
Table 70 – TRUSTED SEND - Security Protocol field description.....	274
Table 71 – Fields to issue an SCT command using SMART WRITE LOG.....	299
Table 72 – Fields to issue an SCT command using WRITE LOG (DMA) EXT	300
Table 73 – Successful SCT command response.....	301
Table 74 – SCT command error response.....	302
Table 75 – Extended Status codes	303
Table 76 – SCT data transfer using SMART READ LOG or SMART WRITE LOG	304
Table 77 – SCT data transfer using the GPL feature set.....	305
Table 78 – SCT status request using SMART READ LOG	306
Table 79 – SCT status request using the GPL feature set	307
Table 80 – Format of SCT status response	307
Table 81 – SCT command format.....	309
Table 82 – SCT Action Codes	309
Table 83 – SCT Read/Write Long command	310
Table 84 – SCT Read/Write Long command status response.....	310
Table 85 – SCT Read/Write Long command Format.....	311
Table 86 – SCT Write Same command	313
Table 87 – SCT Write Same command status response.....	314
Table 88 – SCT Error Recovery Control command	315
Table 89 – SCT Error Recovery Control command status response.....	316
Table 90 – SCT Feature Control command	317
Table 91 – Feature Code List	318
Table 92 – SCT Feature Control command status response.....	319
Table 93 – SCT Data Table command	320
Table 94 – SCT Data Tables (by Table Identifier)	320
Table 95 – Absolute HDA Temperature.....	321
Table 96 – SCT Data Table command status response	323
Table 97 – Error Bit Defined For Normal Output.....	324
Table 98 – Extended Error Code for Normal Output.....	324

Table 99 – Generic Normal Output (No LBA Return Value) for Normal Output.....	326
Table 100 – CFA Normal Output	327
Table 101 – Media Card Type Normal Output	328
Table 102 – Check Power Mode Normal Output	329
Table 103 – Stream Normal Output	330
Table 104 – Device Signatures for Normal Output	331
Table 105 – IDLE Unload Normal Output	332
Table 106 – ATAPI Normal Output	333
Table 107 – Queued Normal Output.....	334
Table 108 – HPA Normal Output	335
Table 109 – SMART Off-Line Immediate Normal Output	336
Table 110 – SMART Return Status Normal Output	337
Table 111 – Generic Extended Normal Output.....	338
Table 112 – SETMAX Extended Normal Output.....	339
Table 113 – Queued Extended Normal Output.....	340
Table 114 – NV Cache Normal Output	341
Table 115 – NV Cache Flush Normal Output	342
Table 116 – NCQ Command Acceptance Normal Output	343
Table 117 – NCQ Normal Outputs.....	343
Table 118 – Unsupported Command Error	344
Table 119 – CFA Erase Error	345
Table 120 – CFA Write Error	346
Table 121 – CFA & Check Power Mode Abort Error	347
Table 122 – Generic Abort wo/ICRC Error	348
Table 123 – Generic Abort Error	349
Table 124 – Trusted Abort Error	350
Table 125 – Generic SET MAX Error.....	351
Table 126 – SET MAX Unlock Error	352
Table 127 – Configure Stream Error.....	353
Table 128 – Flush Cache Error.....	354
Table 129 – Flush Cache Ext Error.....	355
Table 130 – Read DMA Error	356
Table 131 – Read DMA Ext Error	357
Table 132 – Read Log Ext Error	358
Table 133 – Read PIO Error	359
Table 134 – Read Stream Error.....	360
Table 135 – HPA Error.....	361
Table 136 – Write Log Error.....	362
Table 137 – Write Log Ext Error	363
Table 138 – SMART Error	364
Table 139 – Write Extended Error	365
Table 140 – Write Stream Error	366
Table 141 – DCO Set Error.....	367
Table 142 – NOP Error	368
Table 143 – PACKET command Error.....	369
Table 144 – Read DMA Queued Error.....	370
Table 145 – Read DMA Queued Extended Error	371
Table 146 – SMART Read Log/SMART Read Data Error	372
Table 147 – Read PIO Extended Error	373
Table 148 – Read Native Max Extended Error	374
Table 149 – SETMAX Extended Error	375

Table 150 – Write Error.....	376
Table 151 – Write DMA Error.....	377
Table 152 – Write DMA Queued Error.....	378
Table 153 – NV Cache Add Abort Error.....	379
Table 154 – NV Cache Remove Abort Error.....	380
Table 155 – NV Cache Abort Error.....	381
Table 156 – NV Cache Abort with Data Transfer Error.....	382
Table 157 – NCQ Command Acceptance Error.....	383
Table 158 – NCQ Write Command Aborted Error	384
Table 159 – NCQ Read Command Aborted Error	385
Table A.1 – Example Log Structure	386
Table A.2 – Log address definition	387
Table A.3 – General Purpose Log Directory	388
Table A.4 – SMART Log Directory.....	388
Table A.5 – Comprehensive error log	389
Table A.6 – General Statistics	390
Table A.7 – Extended Comprehensive SMART error log	391
Table A.8 – Extended Error log data structure.....	392
Table A.9 – Command data structure	392
Table A.10 – Error data structure.....	393
Table A.11 – State field values	393
Table A.12 – Extended Self-test log data structure	394
Table A.13 – Extended Self-test log descriptor entry.....	395
Table A.14 – NCQ Command Error Log	396
Table A.15 – Read Stream Error Log	397
Table A.16 – Stream Error Log Entry.....	398
Table A.17 – SATA Phy Event Counters Format.....	399
Table A.18 – Selective self-test log.....	400
Table A.19 – Selective self-test feature flags.....	401
Table A.20 – Self-test log data structure.....	401
Table A.21 – Self-test log descriptor entry	402
Table A.22 – Summary SMART Error log.....	403
Table A.23 – Error log data structure	404
Table A.24 – Command data structure	404
Table A.25 – Error data structure.....	405
Table A.26 – State field values	405
Table A.27 – Write Stream Error Log.....	406
Table B.1 – Command Matrix	407
Table B.2 – Command codes (sorted by command code).....	408
Table B.3 – Command codes (sorted by command name)	412
Table B.4 – Historical Command Assignments.....	415
Table B.5 – Historical SET FEATURE Code Assignments.....	423
Table D.1 – SCT command using SMART WRITE LOG command	440
Table D.2 – SCT command using WRITE LOG EXT command.....	440

INFORMATION TECHNOLOGY –

AT ATTACHMENT 8 –

Part 101: ATA/ATAPI Command Set (ACS)

FOREWORD

- 1) ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.
- 2) The formal decisions or agreements of IEC and ISO on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC and ISO member bodies.
- 3) IEC, ISO and ISO/IEC publications have the form of recommendations for international use and are accepted by IEC National Committees and ISO member bodies in that sense. While all reasonable efforts are made to ensure that the technical content of IEC, ISO and ISO/IEC publications is accurate, IEC or ISO cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees and ISO member bodies undertake to apply IEC, ISO and ISO/IEC publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any ISO, IEC or ISO/IEC publication and the corresponding national or regional publication should be clearly indicated in the latter.
- 5) ISO and IEC do not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. ISO or IEC are not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or ISO or its directors, employees, servants or agents including individual experts and members of their technical committees and IEC National Committees or ISO member bodies for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication of, use of, or reliance upon, this ISO/IEC publication or any other IEC, ISO or ISO/IEC publications.
- 8) Attention is drawn to the normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this ISO/IEC publication may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

International Standard ISO/IEC 17760-101 was prepared by subcommittee 25: Interconnection of information technology equipment, of ISO/IEC joint technical committee 1: Information technology.

The list of all currently available parts of the ISO/IEC 17760 series, under the general title *Information technology – ATA attachment 8*, can be found on the IEC web site.

This International Standard has been approved by vote of the member bodies, and the voting results may be obtained from the address given on the second title page.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2, as far as was practicable.

IMPORTANT – The “colour inside” logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this publication using a colour printer.

INTRODUCTION

This International Standard standard encompasses the following:

- Clause 1 describes the scope.
- Clause 2 provides normative references for the entire standard.
- Clause 3 provides terms and definitions, abbreviations, and conventions used within the entire standard.
- Clause 4 describes the general operating requirements of the command layer.
- Clause 5 describes the ATA protocols used by the commands in this standard.
- Clause 6 describes Normal and Error Output fields.
- Clause 7 describes commands.
- Clause 8 describes the SCT Command Transport.
- Clause 9 describes command normal and error outputs.
- Annex A describes logs.
- Annex B provides command summaries.
- Annex C describes considerations for using devices with non-512 byte sectors.
- Annex D provides a tutorial on how to use SCT.
- Annex E provides implementation guidelines for 1 024/4 096 byte sectors.

Windows is a registered trademark of Microsoft Corporation in the United States and/or other countries.

ATA document relationships

The set of AT Attachment standards consists of this standard and the ATA implementation standards described in AT Attachment - 8 ATA/ATAPI Architecture Model (ATA8-AAM). Figure 1 shows the relationship of this standard to the other standards and related projects in the ATA and SCSI families of standards and specifications.

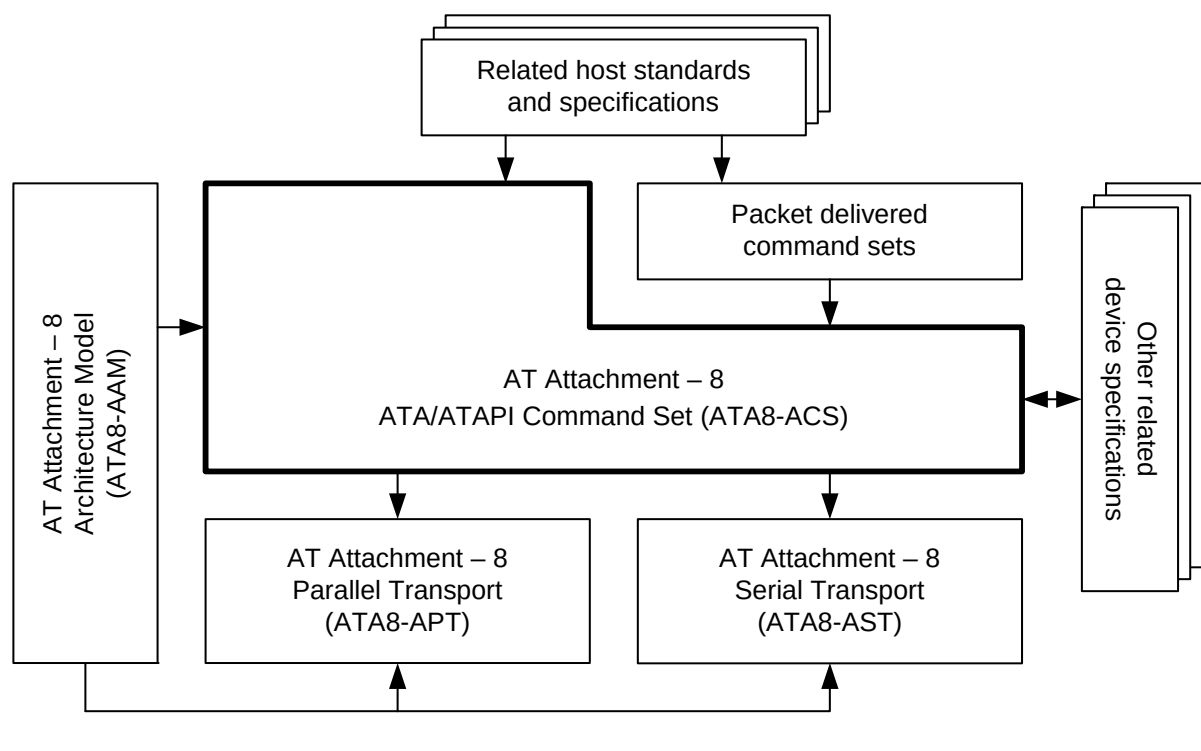


Figure 1 — ATA document relationships

INFORMATION TECHNOLOGY – AT ATTACHMENT 8 –

Part 101: ATA/ATAPI Command Set (ACS)

1 Scope

This part of ISO/IEC 17760 (ATA8-ACS) specifies the command set host systems use to access storage devices. It provides a common command set for systems manufacturers, system integrators, software suppliers, and suppliers of intelligent storage devices.

This International Standard maintains compatibility with the AT Attachment with Packet Interface - 7 standard (ATA/ATAPI-7), ISO/IEC 24739, while providing additional functions.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 14776-453, *Information technology - SCSI Primary Commands - 3 (SPC-3)*¹

ISO/IEC 24739 (all parts), *Information technology – AT Attachment with Packet Interface - 7 (ATA/ATAPI-7 V1 to V3)*²

ISO 7779:1999, *Acoustics - Measurement of airborne noise emitted by information technology and telecommunications equipment*

ANSI INCITS.397-2005/AM 1-2006, *ATA/ATAPI-7 Amendment 1*

ANSI INCITS.452-2008, *AT Attachment-8 - ATA/ATAPI Architecture Model (ATA8-AAM)*

INCITS T13/1697D, *AT Attachment-8 - ATA Serial Transport (ATA8-AST)*

INCITS T13/1698D, *AT Attachment-8 - Parallel Transport (ATA8-APT)*

Serial ATA 2.6 (SATA 2.6) specification. February 2007

Serial ATA 2.5 (SATA 2.5) specification. October 2005

NOTE 1 - For information on the current status of Serial ATA documents, see the Serial ATA International Organization at <http://www.sata-io.org>.

NOTE 2 - For more information on the current status of T10 documents, contact the INCITS Secretariat at 202-737-8888 (phone), 202-638-4922 (fax) or via e-mail at incits@itic.org. To obtain copies of this document, contact Global Engineering at 15 Inverness Way, East Englewood, CO 80112-5704 at 303-792-2181 (phone), 800-854-7179 (phone), or 303-792-2192 (fax), or see <http://www.incits.org>.

CompactFlash Association Specification, Revision 4.1

NOTE 3 - For the CompactFlash Association Specification published by the CompactFlash Association, contact the CompactFlash Association at <http://www.compactflash.org>.

RFC 3280, *Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile*, IETF, 2002

RFC 3281, *An Internet Attribute Certificate: Profile for Authorization*, IETF, 2002

NOTE 4 - For RFCs contact the Internet Engineering Task Force at <http://www.ietf.org>.

1. ANSI INCITS 408-2005
2. ANSI INCITS 397-2005

3 Terms, definitions and conventions

3.1 Terms and definitions

For the purposes of this document the following terms and definitions apply.

3.1.1

28-bit command

command that uses Feature (7:0), Count (7:0), LBA (27:0), Device (15:8) and Command (7:0) to specify its arguments

3.1.2

48-bit command

command that uses Feature (15:0), Count (15:0), LBA (47:0), Device (15:8) and Command (7:0) to specify its arguments

3.1.3

application client

object in the host that is the source of commands and device management functions

Note 1 to entry: See ATA8-AAM

3.1.4

ASCII

American Standard Code for Information Interchange

Note 1 to entry: See ANSI INCITS 4-1986 (R2002).

3.1.5

ASCII character

byte containing a 7-bit ASCII pattern in bits (6:0) with bit 7 cleared to zero

3.1.6

acoustics

measurement of airborne noise emitted by information technology and telecommunications equipment

Note 1 to entry: See ISO 7779:1999.

3.1.7

ATA device

AT Attachment device

device implementing the general feature set (see 4.2)

3.1.8

ATA string

set of ASCII characters (see 3.1.5) in the format specified in 3.2.9

3.1.9

ATAPI device

AT Attachment Packet Interface device

device implementing the PACKET feature set (see 4.3)

3.1.10

Audio-Video

AV

audio-video applications use data that are related to video images and/or audio

Note 1 to entry: The distinguishing characteristic of this type of data is that accuracy is of lower priority than timely transfer of the data.

3.1.11**Background Activities**

activities initiated by a command that occur after command completion has been reported

3.1.12**Basic Input/Output System****BIOS**

initial application client run by a computer when power is applied

Note 1 to entry: The primary function of BIOS is to initialize various components of the system, including storage devices.

3.1.13**Block Data**

data transferred to or from the device using SCT read/write log capabilities

3.1.14**byte**

sequence of eight contiguous bits considered as a unit (see 3.2.8)

3.1.15**cache**

data storage area outside the area accessible by application clients that may contain a subset of the data stored in the non-volatile data storage area

3.1.16**CFA Device**

device implementing the CFA feature set (see 4.7)

3.1.17**check condition**

for ATAPI devices, this indicates an error or exception condition has occurred

3.1.18**Cylinder-Head-Sector****CHS**

obsolete method of addressing the data on the device by cylinder number, head number, and sector number

3.1.19**command aborted**

command completion with the Error bit set to one in the Status field and Abort bit set to one in the Error field

3.1.20**command acceptance**

positive acknowledgement of a command being received by a device

Note 1 to entry: See the appropriate transport standard for a definition of positive acknowledgement.

3.1.21**command completion**

completion by the device of the action requested by the command or the termination of the command with an error, the setting of the appropriate bits in the Error field, and the setting of the appropriate bits in the Status field

3.1.22**command packet**

data structure transmitted to the device during the processing of a PACKET command that includes the command and command parameters

3.1.23**COMRESET**

commanded hardware reset in the Serial ATA transport

Note 1 to entry: See SATA 2.6.

3.1.24**device**

data storage peripheral (see 3.1.7 and see 3.1.9)

Note 1 to entry: For example a disk drive is such a device.

3.1.25**DMA data transfer****direct memory access data transfer**

means of data transfer between device and host memory without host processor intervention

3.1.26**DRQ data block****Data Request data block**

unit of data words associated with available status when using either the PIO Data-In command protocol or the PIO Data-Out command protocol

3.1.27**DWord**

sequence of four contiguous bytes considered as a unit (see 3.2.8)

3.1.28**FIS**

Frame Information Structure for the serial ATA interface

Note 1 to entry: See ATA8-AST.

3.1.29**hardware reset**

routine performed by a device after a hardware reset event as defined in ATA8-AAM

Note 1 to entry: The hardware reset routine performed by the device includes the actions performed by the device for a software reset, and the actions defined in ATA8-AAM, this standard, and the applicable transport standards.

3.1.30**HPA Locked**

condition of a device in the H2, HL1-HL6 or HEL1-HEL6 state

3.1.31**HPA Unlocked**

condition of a device in the H0, H1, H3, HS1-HS6, or HES1-HES6 state (i.e., states where the password may or may not be set)

3.1.32**host**

object that originates commands and device management functions

Note 1 to entry: See ATA8-AAM.

3.1.33

host adapter

implementation of the host transport, link, and physical layers

3.1.34

Logical Block Address

LBA

value used to reference a logical sector

3.1.35

logical sector

sector

set of logical words accessed and referenced as a unit (see IDENTIFY DEVICE data words 118:117)

Note 1 to entry: These units are referenced by LBA (see 3.1.34).

3.1.36

log

named sequence of one or more log pages (see Annex A)

3.1.37

log address

numeric value that a log command uses to identify a specific log

3.1.38

log command

SMART READ LOG command (see 7.53.7), SMART WRITE LOG command (see 7.53.9), or GPL feature set (see 4.10) command

3.1.39

log page

unit of measure for determining the size of a log; each log page is a 512-byte block of data

Note 1 to entry: Log consists of one or more pages.

3.1.40

Least Significant Bit

LSB

<binary code> bit or bit position with the smallest numerical weighting in a group of bits that, when taken as a whole, represent a numerical value

Note 1 to entry: For example in the numerical value 0001b, the bit that is set to one.

3.1.41

Master Password Capability

Security Level

master password may or may not be used to unlock the device

3.1.42

Media

material on which data is stored

3.1.43

Media Access Command

any command that causes the device to access non-volatile media

3.1.44

Most Significant Bit

MSB

<binary code> bit or bit position with the largest numerical weighting in a group of bits that, when taken as a whole, represent a numerical value

Note 1 to entry: For example in the numerical value 1000b, the bit that is set to one.

3.1.45

native max address

highest LBA that a device accepts as reported by DEVICE CONFIGURATION IDENTIFY data or as reduced by the DEVICE CONFIGURATION SET command

Note 1 to entry: That is, the highest LBA that is accepted by a device using the SET MAX ADDRESS command (see 7.49.2) or, if the 48-bit Address feature set is supported, then the highest value accepted by a device using the SET MAX ADDRESS EXT command (see 7.50)

3.1.46

Non-Volatile cache

cache that retains data through all reset events (e.g., power-on reset) and is a subset of the non-volatile media

3.1.47

Non-Volatile Media

physical storage media that retains data written to it for subsequent read operations through all power and reset events

Note 1 to entry: Non-Volatile Media are for example, magnetic media, optical media, flash media.

3.1.48

NV Cache Pinned Set

set of logical blocks specified by the application client for which all user data accesses associated with those logical blocks are written to or read from the non-volatile cache

3.1.49

NV Cache Set

set of logical blocks currently represented in the device's entire NV Cache

3.1.50

NV Cache Set Data

data structure representing the standard format of transmitting logical blocks in the form of a list of LBA Range Entries

3.1.51

NV Cache Unpinned Set

set of logical blocks that are represented in the NV Cache Set but not represented in the NV Cache Pinned Set

Note 1 to entry: The NV Cache Pinned Set and the NV Cache Unpinned Set are mutually exclusive. An NV Cache Unpinned Set is managed by the device and logical blocks represented in the NV Cache Unpinned Set may be added or removed from the NV Cache Set at any time.

3.1.52

Password Attempt Counter Exceeded

name associated with IDENTIFY DEVICE, word 128, bit 4 (see 7.16.7.64)

3.1.53

PATA device

Parallel ATA device

device implementing the parallel ATA transport

Note 1 to entry: See ATA8-APT.

3.1.54

physical sector

one or more contiguous logical sectors that are read from or written to the device media in a single operation

3.1.55

PIO data transfer

programmed input/output data transfer

data transfers performed using PIO commands and protocol

3.1.56

power cycle

period from when power is removed from a host or device until the subsequent power-on event

Note 1 to entry: See ATA8-AAM.

3.1.57

power-on reset

host specific routine performed by the host or the routine performed by a device after detecting a power-on event

Note 1 to entry: The power-on reset routine performed by a device includes the actions performed by the device for a hardware reset and a software reset, and the actions defined in ATA8-AAM, this standard, and the applicable transport standards.

3.1.58

Queued Command

TCQ or NCQ command that has reported command acceptance but not command completion

3.1.59

QWord

sequence of eight contiguous bytes considered as a unit (see 3.2.8)

3.1.60

read command

command that causes the device to transfer data from the device to the host

EXAMPLES: READ DMA, READ DMA EXT, READ DMA QUEUED, READ DMA QUEUED EXT, READ FPDMA QUEUED, READ MULTIPLE, READ MULTIPLE EXT, READ SECTOR(S), READ SECTOR(S) EXT, READ STREAM EXT, READ STREAM DMA EXT, READ VERIFY SECTOR(S), or READ VERIFY SECTOR(S) EXT

3.1.61

release

action by a device implementing the TCQ feature set (see 4.24) that allows a host to select an alternate device or deliver another TCQ command (see 4.24)

3.1.62

SATA device

Serial ATA device

device implementing the serial ATA transport

Note 1 to entry: See ATA8-AST and SATA 2.6.

3.1.63

SCT Command

command that writes to the SCT command/status log (see clause 8)

3.1.64

SCT Status

command that reads from the SCT command/status log (see clause 8)

3.1.65

Serial ATAPI device

device implementing the serial ATA transport and the PACKET feature set

Note 1 to entry: For the serial ATA transport, see ATA8-AST.

3.1.66

signature

unique set of values placed in the return parameters used to distinguish device types

Note 1 to entry: Such device types are General, ATAPI device, Port Multiplier (see table 104).

3.1.67

software reset

routine performed by a device after a software reset event as defined in ATA8-AAM

Note 1 to entry: The software reset routine includes the actions defined in ATA8-AAM, this standard, and the applicable transport standards.

3.1.68

spin-down

process of bringing a rotating media device's media to a stop

3.1.69

spin-up

process of bringing a rotating media device's media to operational speed

3.1.70

Stream

set of operating parameters specified by a host using the CONFIGURE STREAM command (see 7.9) to be used for subsequent READ STREAM commands and WRITE STREAM commands

3.1.71

Trusted Computing Group

TCG

organization that develops and promotes open standards for hardware-enabled trusted computing and security technologies

Note 1 to entry: See <https://www.trustedcomputinggroup.org> for more information.

3.1.72

transport

mechanism used to communicate with a device

Note 1 to entry: See ATA8-APT and ATA8-AST.

3.1.73

unaligned write

write command that does not start at the first logical sector of a physical sector or does not end at the last logical sector of a physical sector

3.1.74**unrecoverable error**

condition that occurs when the device sets either the Error bit or the Device Fault bit to one in the Status field at command completion

3.1.75**Volatile Cache**

cache that does not retain data through power cycles

3.1.76**vendor specific**

<values> bits, bytes, fields, and code values that are reserved for vendor specific purposes

Note 1 to entry: These bits, bytes, fields, and code values are not described in this standard, and implementations may vary among vendors.

3.1.77**vendor specific**

<functionality> levels of functionality whose definition is left to the vendor

3.1.78**word**

sequence of two contiguous bytes considered as a unit (see 3.2.8)

3.1.79**write command**

command that causes the device to transfer data from the host to the device

EXAMPLES: SCT Write Same, SCT Write Long, WRITE DMA, WRITE DMA EXT, WRITE DMA FUA EXT, WRITE DMA QUEUED, WRITE DMA QUEUED EXT, WRITE DMA QUEUED FUA EXT, WRITE FPDMA QUEUED, WRITE MULTIPLE, WRITE MULTIPLE EXT, WRITE MULTIPLE FUA EXT, WRITE SECTOR(S), WRITE SECTOR(S) EXT, WRITE STREAM DMA EXT, or WRITE STREAM EXT)

3.1.80**World Wide Name****WWN**

64-bit worldwide unique name based upon a company's IEEE organizationally unique identifier (OUI), reported in IDENTIFY DEVICE data words 108-111 (see 7.16.7.56) and IDENTIFY PACKET DEVICE data words 108-111 (see 7.17.6.44)

3.2 Conventions**3.2.1 Overview**

Lowercase is used for words having the normal English language meaning. Certain words and terms used in this standard have a specific meaning beyond the normal English language meaning. These words and terms are defined either in clause 3 or in the text where they first appear.

The names of abbreviations, commands, fields, and acronyms used as signal names are in all uppercase (e.g., IDENTIFY DEVICE). Fields containing only one bit are usually referred to as the "name" bit instead of the "name" field. (See 3.2.6 for the naming convention used for naming bits.)

Names of device fields begin with a capital letter (e.g., Count).

The expression "word n" or "bit n" shall be interpreted as indicating the content of word n or bit n.

3.2.2 Precedence

If there is a conflict between text, figures, and tables, the precedence shall be tables, figures, then text.

3.2.3 Lists

3.2.3.1 Lists overview

Lists shall be introduced by a complete grammatical proposition followed by a colon and completed by the items in the list.

Lists are associated with an introductory paragraph or phrase, and are numbered relative to that paragraph or phrase (i.e., all lists begin with an a) or 1) entry).

Each item in a list shall be preceded by an identification with the style of the identification being determined by whether the list is intended to be an ordered list or an unordered list.

If the item in a list is not a complete sentence, then the first word in the item shall not be capitalized. If the item in a list is a complete sentence, then the first word in the item shall be capitalized,

Each item in a list shall end with a semicolon, except the last item, which shall end in a period. The next to the last entry in the list shall end with a semicolon followed by an “and” or an “or” (i.e., “...; and”, or “...; or”). The “and” is used if all the items in the list are required. The “or” is used if only one or more items in the list are required.

3.2.3.2 Unordered lists

An unordered list is one in which the order of the listed items is unimportant (i.e., it does not matter where in the list an item occurs as all items have equal importance). Each list item shall start with a lower case letter followed by a close parenthesis. If it is necessary to subdivide a list item further with an additional unordered list (i.e., have a nested unordered list), then the nested unordered list shall be indented and each item in the nested unordered list shall start with an upper case letter followed by a close parenthesis.

EXAMPLE – The following is an example of an unordered list with a nested unordered list.

The following are the items for the assembly:

- a) a box containing:
 - A) a bolt;
 - B) a nut; and
 - C) a washer;
- b) a screwdriver; and
- c) a wrench.

3.2.3.3 Ordered lists

An ordered list is one in which the order of the listed items is important (i.e., item n is required before item n+1). Each listed item starts with an Western-Arabic numeral followed by a close parenthesis. If it is necessary to subdivide a list item further with an additional unordered list (i.e., have a nested unordered list), then the nested unordered list shall be indented and each item in the nested unordered list shall start with an upper case letter followed by a close parenthesis.

EXAMPLE – The following is an example of an ordered list with a nested unordered list.

The following are the instructions for the assembly:

- 1) Remove the contents from the box;
- 2) Assemble the item;
 - A) Use a screwdriver to tighten the screws; and
 - B) Use a wrench to tighten the bolts;and
- 3) Take a break.

3.2.4 Keywords

3.2.4.1

expected A keyword used to describe the behavior of the hardware or software in the design models assumed by this standard. Other hardware and software design models may also be implemented.

3.2.4.2 mandatory A keyword indicating items to be implemented as defined by this standard.

3.2.4.3 may A keyword that indicates flexibility of choice with no implied preference.

3.2.4.4 N/A A keyword that indicates a field is not applicable and has no defined value and should not be checked by the host or device.

3.2.4.5 obsolete A keyword indicating that the designated bits, bytes, words, fields, and code values that may have been defined in previous standards are not defined in this standard and shall not be reclaimed for other uses in future standards. However, some degree of functionality may be required for items designated as “obsolete” to provide for backward compatibility.

Obsolete commands should not be used by the host. Commands defined as obsolete may be command aborted by devices conforming to this standard. However, if a device does not return command aborted for an obsolete command, then the device shall return command completion for the command.

3.2.4.6 optional A keyword that describes features that are not required by this standard. However, if any optional feature defined by the standard is implemented, the feature shall be implemented in the way defined by the standard.

3.2.4.7 prohibited A keyword indicating that an item shall not be implemented by an implementation.

3.2.4.8 reserved A keyword indicating reserved bits, bytes, words, fields, and code values that are set aside for future standardization. Their use and interpretation may be specified by future extensions to this or other standards. A reserved bit, byte, word, or field shall be cleared to zero, or in accordance with a future extension to this standard. The recipient shall not check reserved bits, bytes, words, or fields. Receipt of reserved code values in defined fields shall be treated as a command parameter error and reported by returning command aborted.

3.2.4.9 retired A keyword indicating that the designated bits, bytes, words, fields, and code values that had been defined in previous standards are not defined in this standard and may be reclaimed for other uses in future standards. If retired bits, bytes, words, fields, or code values are used before they are reclaimed, they shall have the meaning or functionality as described in previous standards.

3.2.4.10 shall A keyword indicating a mandatory requirement. Designers are required to implement all such mandatory requirements to ensure interoperability with other products that conform to this standard.

3.2.4.11 should A keyword indicating flexibility of choice with a strongly preferred alternative. Equivalent to the phrase “it is recommended”.

3.2.5 Numbering

Numbers that are not immediately followed by a lowercase “b” or “h” are decimal values. This standard uses the following conventions for representing decimal numbers:

- a) the decimal separator (i.e., separating the integer and fractional portions of the number) is a period;
- b) the thousands separator (i.e., separating groups of three digits in a portion of the number) is a space;
- c) the thousands separator is used in both the integer portion and the fraction portion of a number; and
- d) the decimal representation for a year is 1999 not 1 999.

Numbers that are immediately followed by a lowercase “b” (e.g., 01b) are binary values. Numbers that are immediately followed by a lowercase “h” (e.g., 3Ah) are hexadecimal values.

Underscores or spaces may be included in number representations to increase readability or delineate field boundaries (e.g., FFFF_FFFFh, FFFF FFFFh, and FFFFFFFFh represent the same number).

The table 1 below shows some examples of decimal numbers represented using various conventions.

Table 1 — Numbering conventions examples

ISO/IEC	US	This standard
0,6	0.6	0.6
3,141 592 65	3.14159265	3.141 592 65
1 000	1,000	1 000
1 323 462,95	1,323,462.95	1 323 462.95

3.2.6 Bit conventions

Name (n:m), where n shall be greater than m, denotes a set of bits (e.g., Feature (7:0)). n:m where n shall be greater than m denotes a bit range in a table.

3.2.7 State diagram conventions

State diagrams shall be as shown in Figure 2.

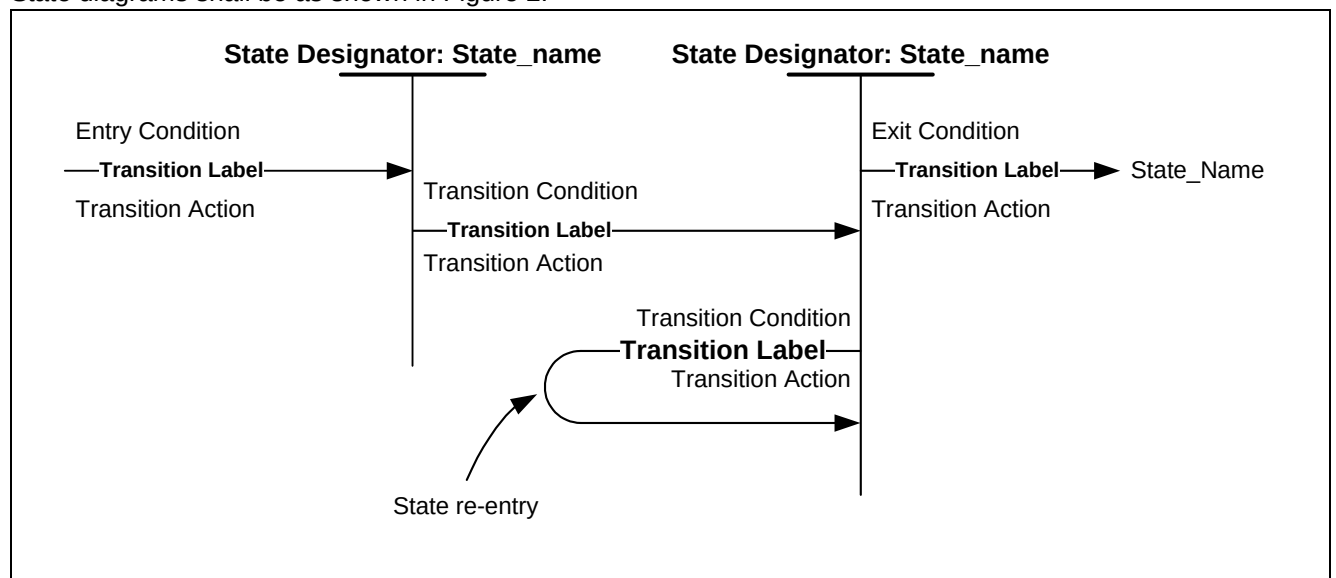


Figure 2 — State diagram convention

Each state is identified by a state designator and a state name. The state designator is unique among all states in all state diagrams in this document. The state designator consists of a set of letters that are capitalized in the title of the figure containing the state diagram followed by a unique number. The state name is a brief description of the primary action taken during the state, and the same state name may appear in other state diagrams. If the same primary function occurs in other states in the same state diagram, they are designated with a unique letter at the end of the name. Additional actions may be taken while in a state and these actions are described in the state description text.

Each transition is identified by a transition label and a transition condition. The transition label consists of the state designator of the state from which the transition is being made followed by the state designator of the state to which the transition is being made. In some cases, the transition to enter or exit a state diagram may come from or go to a number of state diagrams, depending on the command being processed. In this case, the state designator is labeled State_name. The transition condition is a brief description of the event or condition that causes the transition to occur and may include a transition action, indicated in italics, that is taken when the transition occurs. This action is described in the transition description text.

Upon entry to a state, all actions to be processed in that state are processed. If a state is re-entered from itself, all actions to be processed in the state are processed again.

Transitions from state to state shall be instantaneous.

3.2.8 Byte, word, DWord, and QWord Relationships

Figure 3 illustrates the relationship between bytes, words, DWords, and QWords.

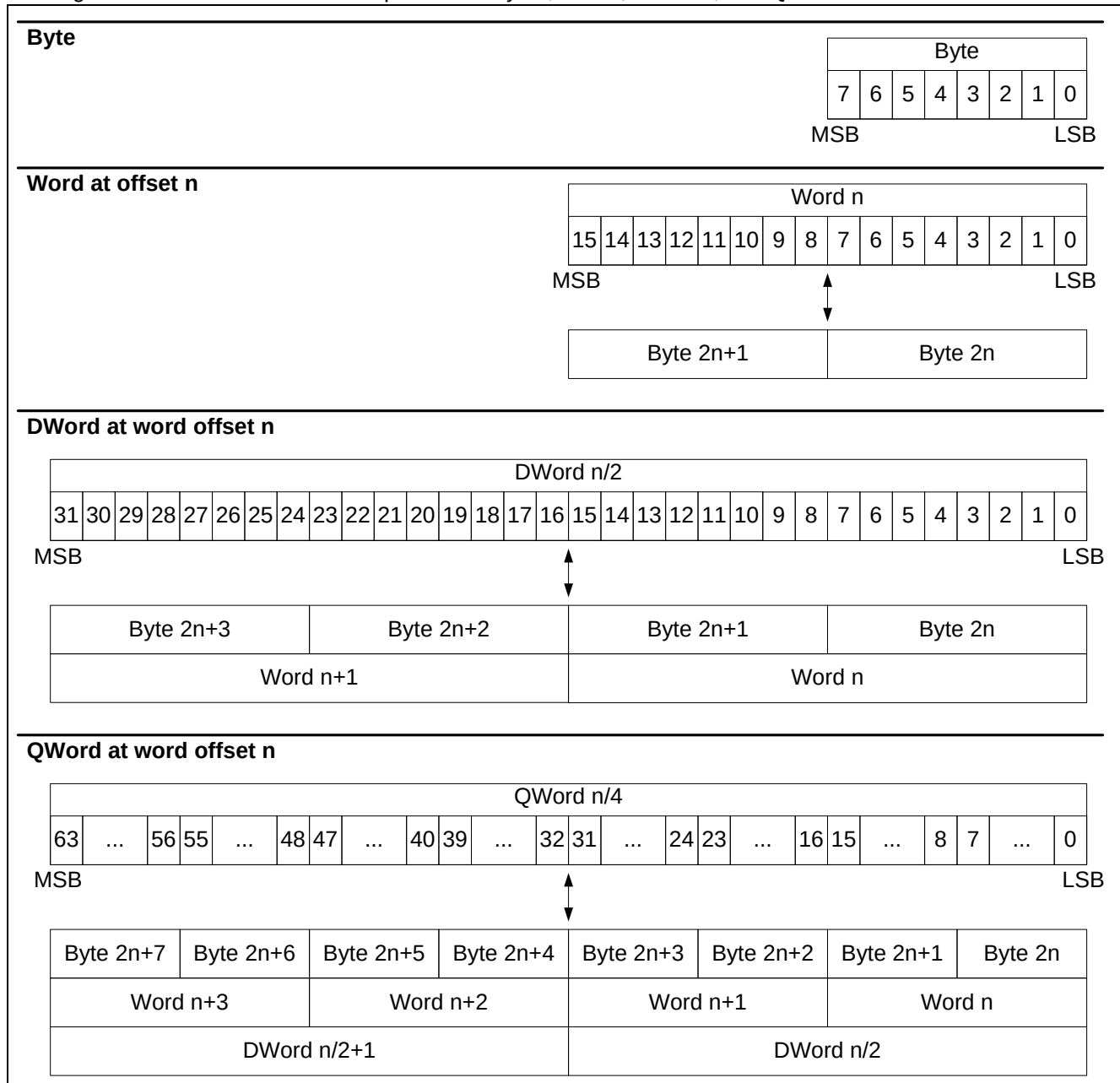


Figure 3 — Byte, word, DWord and QWord relationships

Unless stated or defined otherwise, in a field containing a multi-byte value (e.g., a word, DWord, or QWord), the byte containing the LSB is stored at the lowest offset and the byte containing the MSB is stored at the highest offset. Examples following this convention include:

- Device Configuration Identify data (see table 25) and Device Configuration Overlay data (see table 26) 7.10.5.6;
- IDENTIFY DEVICE data (see table 29);
- IDENTIFY PACKET DEVICE data (see table 39);
- Request Pin data (see table 43), Cache Miss Data (see table 44), Pin Set Data (see table 45), and Remove Pin Data (see table 46) used by Non-Volatile Cache commands (see 7.10.6).

- e) Device SMART data (see table 62);
- f) SCT status response (see table 80) and SCT command (see table 81); and
- g) Logs defined in Annex A.

EXAMPLE 1 –

- a) if the two-byte field (i.e., word) in SCT command (see table 81) word 0 contains 0007h, then:
 - A) byte 0 contains 07h; and
 - B) byte 1 contains 00h;
- b) if the four-byte field (i.e., DWord) at IDENTIFY DEVICE data words 60-61 (see table 29) contains 8001_0203h (i.e., 2 147 549 699), then:
 - A) byte 120 contains 03h;
 - B) byte 121 contains 02h;
 - C) byte 122 contains 01h; and
 - D) byte 123 contains 80h;

and
- c) if an eight-byte field (i.e., QWord) in the WRITE SAME command words 2-5 (see table 86) contains 0000_0504_0302_0100h, then:
 - A) byte 4 contains 00h;
 - B) byte 5 contains 01h;
 - C) byte 6 contains 02h;
 - D) byte 7 contains 03h;
 - E) byte 8 contains 04h;
 - F) byte 9 contains 05h;
 - G) byte 10 contains 00h; and
 - H) byte 11 contains 00h.

Exceptions to this convention include:

- a) each field containing an ATA string (e.g., the IDENTIFY DEVICE data and IDENTIFY PACKET DEVICE data Serial number, Firmware revision, and Model number fields) is considered to be an array of bytes, not a multi-byte value, and is handled as described in 3.2.9;
- b) the IDENTIFY DEVICE data and IDENTIFY PACKET DEVICE data World Wide Name field is treated as four word fields rather than one QWord field and is handled as described in 7.16.7.56; and
- c) the CFA TRANSLATE SECTOR data LBA and logical sector write cycles count fields (see table 23);
- d) the command packet in the PACKET command (see 7.22) is formatted as defined by the applicable command standard; and
- e) parameter data in the TRUSTED RECEIVE (see 7.57), TRUSTED RECEIVE DMA (see 7.58), TRUSTED SEND (see 7.59), and TRUSTED SEND DMA commands (see 7.60) is formatted as defined in those sections or in the standard defining the security protocol.

EXAMPLE 2 –

- a) if the two-byte field (i.e., a word) in TRUSTED RECEIVE parameter data for SP Specific=0000h (see table 68) contains 01FFh, then:
 - A) byte 6 contains 01h; and
 - B) byte 7 contains FFh;

and
- b) if a command packet in the PACKET command contains a SCSI INQUIRY command (see SPC-3) requesting the standard INQUIRY data with the allocation length field set to 01FFh, then:
 - A) byte 0 (i.e., the operation code field) contains 12h;
 - B) byte 1 (i.e., the byte containing the evpd bit) contains 00h;
 - C) byte 2 (i.e., the page code field) contains 00h;
 - D) byte 3 (i.e., the byte containing the MSB of the allocation length field) contains 01h;
 - E) byte 4 (i.e., the byte containing the LSB of the allocation length field) contains FFh;
 - F) byte 5 (i.e., the control field) contains 00h;
 - G) if IDENTIFY PACKET DEVICE data word 0 bits (1:0) are set to 00b (i.e., 12 byte command packet), bytes 6 through 11 each contain 00h; and
 - H) if IDENTIFY PACKET DEVICE data word 0 bits (1:0) are set to 01b (i.e., 16 byte command packet), bytes 6 through 15 each contain 00h.

3.2.9 ATA string convention

ATA strings are sequences of bytes containing ASCII graphic characters in the range of 20h-7Eh. ATA strings shall not contain values in the range of 00h-1Fh or 7Fh-FFh.

The following fields in IDENTIFY DEVICE data (see 7.16.7) and IDENTIFY PACKET DEVICE data (see 7.17.6) contain ATA strings:

- a) Serial number (words 10-19) (see 7.16.7.10);
- b) Firmware revision (words 23-26) (see 7.16.7.13);
- c) Model number (words 27-46) (see 7.16.7.14); and
- d) Current media serial number (words 176-205) (see 7.16.7.70).

Each pair of bytes in an ATA string is swapped as shown in table 2.

Table 2 — ATA string byte swapping

Word	Byte	Character in string
0	0	Second character
	1	First character
1	2	Fourth character
	3	Third character
...	...	...
n	2n	Last character
	2n+1	Second-to-last character

If the Firmware revision field (i.e., words 23-26) contains the string “abcdefg”, including one padding space character at the end, then the word and byte representations for the field are shown in table 3.

Table 3 — ATA firmware revision example

Word	Value	Byte	Value
23	6162h (i.e., “ba”)	36	62h (i.e., ‘b’)
		37	61h (i.e., ‘a’)
24	6364h (i.e., “dc”)	38	64h (i.e., ‘d’)
		39	63h (i.e., ‘c’)
25	6566h (i.e., “fe”)	40	66h (i.e., ‘f’)
		41	65h (i.e., ‘e’)
26	6720h (i.e., “ g”)	42	20h (i.e., ‘ ’, the space character)
		43	67h (i.e., ‘g’)

4 Feature set definitions

4.1 Overview

Table 4 lists the feature sets in alphabetical order and shows whether a feature set is mandatory, optional, prohibited, or not defined for ATA devices and ATAPI devices.

Table 4 — Feature Set Summary

Feature Set	ATA Devices	ATAPI Devices
48-Bit Address feature set (see 4.4)	O	P
Advanced Power Management (APM) feature set (see 4.5)	O	O
Automatic Acoustic Management (AAM) feature set (see 4.6)	O	O
CompactFlash Association (CFA) feature set (see 4.7)	N	N
Device Configuration Overlay (DCO) feature set (see 4.8)	O	O
Free-fall Control feature set (see 4.9)	O	P
General feature set (see 4.2)	M	P
General Purpose Logging (GPL) feature set (see 4.10)	O	O
Host Protected Area (HPA) feature set (see 4.11)	O	O
Long Logical Sector (LLS) feature set (see 4.12)	O	P
Long Physical Sector (LPS) feature set (see 4.13)	O	P
Media Card Pass Through Command feature set (see 4.14)	N	P
Native Command Queuing (NCQ) feature set (see 4.15)	O	P
NV Cache feature set (see 4.16)	O	P
NV Cache Power Management feature set (see 4.17)	O	P
PACKET feature set (see 4.3)	P	M
Power Management feature set (see 4.18)	M	O
Power-Up In Standby (PUIS) feature set (see 4.19)	O	O
Security feature set (see 4.20)	O	O
Self-Monitoring, Analysis, and Reporting Technology (SMART) feature set (see 4.21)	O	P
Software Settings Preservation (SSP) feature set (see 4.22)	O	P
Streaming feature set (see 4.23)	O	P
Tagged Command Queuing (TCQ) feature set (see 4.24)	O	P
Trusted Computing feature set (see 4.25)	O	P
Write-Read-Verify feature set (see 4.26)	O	P
Key: M – Mandatory, O – Optional, P – Prohibited, N – Not defined		

4.2 General feature set

The following General feature set commands are mandatory for all devices that are capable of both reading and writing their media:

- a) EXECUTE DEVICE DIAGNOSTIC;
- b) FLUSH CACHE;
- c) IDENTIFY DEVICE;
- d) READ DMA;
- e) READ MULTIPLE;
- f) READ SECTOR(S)
- g) READ VERIFY SECTOR(S);
- h) SET FEATURES;
- i) SET MULTIPLE MODE;

- j) WRITE DMA;
- k) WRITE MULTIPLE; and
- l) WRITE SECTOR(S).

The following General feature set commands are mandatory for all devices that are capable of only reading their media:

- a) EXECUTE DEVICE DIAGNOSTIC;
- b) IDENTIFY DEVICE;
- c) READ DMA;
- d) READ MULTIPLE;
- e) READ SECTOR(S);
- f) READ VERIFY SECTOR(S);
- g) SET FEATURES; and
- h) SET MULTIPLE MODE.

The following General feature set commands are optional:

- a) DOWNLOAD MICROCODE;
- b) NOP;
- c) READ BUFFER;
- d) WRITE BUFFER; and
- e) WRITE UNCORRECTABLE EXT.

All other commands that are contained in the PACKET feature set shall not be implemented.

4.3 The PACKET feature set

4.3.1 Overview

ATAPI devices use DEVICE RESET and PACKET commands as well as a subset of the General feature set to control the device.

The content of command packets delivered during execution of the PACKET command are defined in the standard indicated by IDENTIFY PACKET DEVICE data word 0 5bits (12:8) (see 7.17.6.2) and are not described in this standard.

The optional PACKET feature set provides for ATAPI devices that require command parameters that are too extensive to be expressed in the return data structure. Devices implementing the PACKET feature set exhibit responses different from those exhibited by devices not implementing this feature set.

The following commands are mandatory for all devices implementing the PACKET feature set:

- a) PACKET;
- b) DEVICE RESET;
- c) EXECUTE DEVICE DIAGNOSTIC;
- d) IDENTIFY DEVICE;
- e) IDENTIFY PACKET DEVICE;
- f) NOP;
- g) READ SECTOR(S); and
- h) SET FEATURES.

NOTE 5 - For ATAPI devices, the IDENTIFY DEVICE command (see 7.16) and the READ SECTOR(S) command (see 7.35) are command aborted and return the ATAPI device signature (see table 104).

The following commands are optional for all devices implementing the PACKET feature set:

- a) FLUSH CACHE;
- b) READ LOG EXT;
- c) WRITE LOG EXT;
- d) READ LOG DMA EXT; and
- e) WRITE LOG DMA EXT.

All other commands that are contained in the General feature set shall not be implemented.

4.3.2 Identification of PACKET feature set devices

The IDENTIFY PACKET DEVICE command is used by the host to get identifying parameter information for a device implementing the PACKET feature set (see 7.16.5 and 7.17).

4.3.3 Signature for ATAPI devices

ATAPI devices return a signature that differentiate them from other device types (see table 104).

4.3.4 The PACKET command

The PACKET command allows a host to send a command to the device via a command packet. The command packet contains the command and command parameters that the device is to process (see clause 1).

The protocol for handling the transmission of the PACKET command and associated data is transport specific.

4.4 48-bit Address feature set

The optional 48-bit Address feature set allows devices with capacities up to 281 474 976 710 655 logical sectors. This allows device capacity up to 144 115 188 075 855 360 bytes for a 512-byte logical block device. In addition, the number of logical sectors that may be transferred by a single command are increased to 65 536.

The following commands are mandatory for devices that implement the 48-bit address feature set:

- a) FLUSH CACHE EXT;
- b) READ DMA EXT;
- c) READ MULTIPLE EXT;
- d) READ SECTOR(S) EXT;
- e) READ VERIFY SECTOR(S) EXT;
- f) WRITE DMA EXT;
- g) WRITE DMA FUA EXT;
- h) WRITE MULTIPLE EXT;
- i) WRITE MULTIPLE FUA EXT; and
- j) WRITE SECTOR(S) EXT.

Devices implementing the 48-bit Address feature set shall also implement commands that use 28-bit addressing. 28-bit and 48-bit commands may be intermixed (see 7.1.3).

The device shall indicate support of the 48-bit Address feature set in the IDENTIFY DEVICE data. In addition, IDENTIFY DEVICE data words 100-103 contain the maximum user LBA + 1 that is accessible by 48-bit addressable commands.

See 4.11.4 for a description of how to set IDENTIFY DEVICE data words 60-61 and 100-103.

When the 48-bit Address feature set is implemented, the native max address is the highest LBA accepted by the device in the factory default condition using a 48-bit Address feature set command. The native max address is the value returned by a READ NATIVE MAX ADDRESS EXT command. If the native max address of a device is equal to or less than 268 435 454, a READ NATIVE MAX ADDRESS shall return the native max address. If the native max address is greater than 268 435 454, a READ NATIVE MAX ADDRESS command shall cause the device to return a maximum value of 268 435 454.

When the 48-bit Address feature set is implemented, the device shall process the SET MAX ADDRESS command as described in 7.49.2. However, in addition to modifying the content of IDENTIFY DEVICE data words 60-61, the new content of IDENTIFY DEVICE data words 60-61 shall also be placed in IDENTIFY DEVICE data words 100-103. When a SET MAX ADDRESS EXT command is issued and the LBA requested is greater than 268 435 455, IDENTIFY DEVICE data words 100-103 shall be modified to reflect the requested value but IDENTIFY DEVICE data words 60-61 shall not be modified. When a SET MAX ADDRESS EXT command is issued and the LBA requested is equal to or less than

268 435 455, IDENTIFY DEVICE data words 100-103 shall be modified to reflect the requested value and IDENTIFY DEVICE data words 60-61 shall be modified as described in 7.49.2.1.

4.5 Advanced Power Management (APM) feature set

The Advanced Power Management feature set is an optional feature set that allows the host to select a power management level in a device. The power management level is specified using a scale from the lowest power consumption setting of 01h to the maximum performance level of FEh, see table 54 in 7.48.6. Device performance may increase with increasing power management levels. Device power consumption may increase as the power management setting numerically increases. A device may implement one power management method for two or more contiguous power management levels (e.g., a device may implement one power management method from level 80h to A0h and a higher performance, higher power consumption method from level A1h to FEh). APM levels 80h and higher do not permit a device with rotating media to spin down to save power.

The APM feature set uses the following functions:

- a) A SET FEATURES subcommand to enable APM; and
- b) An optional SET FEATURES subcommand to disable APM.

APM is independent of the Standby timer (see 4.18.3). If both APM and the Standby timer are set, the device shall go to the Standby state when the timer times out or the device's APM algorithm indicates that the Standby state should be entered.

The IDENTIFY DEVICE and IDENTIFY PACKET DEVICE data indicate whether the feature is supported, whether the feature is enabled, and the current settings.

The NV Cache Power management feature set may change the operation of the APM feature set (see 7.20.11).

4.6 Automatic Acoustic Management (AAM) feature set

The Automatic Acoustic Management feature set is an optional feature set that allows the host to select an acoustic management level. The acoustic management level ranges from the setting of 00h to FFh, although many levels are retired (see table 56). Device performance and acoustic emanation may increase with increasing acoustic management levels. The acoustic management levels may contain discrete bands (e.g., a device may implement one acoustic management method from level 80h to A0h, and a higher performance, higher acoustic emanation method from level A1h to FEh).

The Automatic Acoustic Management feature set uses the following functions:

- a) A SET FEATURES subcommand to enable the AAM feature set; and
- b) A SET FEATURES subcommand to disable the AAM feature set.

The IDENTIFY DEVICE or IDENTIFY PACKET DEVICE data indicates if the AAM feature set is supported, if the AAM feature set is enabled, and the current AAM level if the AAM feature set is enabled.

The AAM setting may impact word 97 in IDENTIFY DEVICE data (see 7.16.7.49).

4.7 CompactFlash Association (CFA) feature set

The optional CompactFlash Association (CFA) feature set provides support for devices that implement the CFA specifications. A device that implements the CFA feature set shall implement the following minimum set of commands:

- a) CFA REQUEST EXTENDED ERROR CODE;
- b) CFA WRITE SECTORS WITHOUT ERASE;
- c) CFA ERASE SECTORS;
- d) CFA WRITE MULTIPLE WITHOUT ERASE;
- e) CFA TRANSLATE SECTOR; and
- f) SET FEATURES Enable/Disable 8-bit transfer.

Devices reporting the value 848Ah in IDENTIFY DEVICE data word 0 or devices having bit 2 of IDENTIFY DEVICE data word 83 set to one shall support the CFA feature set. If the CFA feature set is implemented, all the CFA commands and the Enable/Disable 8-Bit transfers shall be implemented.

Support of DMA commands is optional for devices that support the CFA feature set.

The CFA ERASE SECTORS command preconditions the logical sector for a subsequent CFA WRITE SECTORS WITHOUT ERASE or CFA WRITE MULTIPLE WITHOUT ERASE command to achieve higher performance during the write operation. The CFA TRANSLATE SECTOR command provides information about a logical sector (e.g., the number of write cycles performed on that sector and an indication of the logical sector's erased precondition). The CFA REQUEST EXTENDED ERROR CODE command provides more detailed error information.

4.8 Device Configuration Overlay (DCO) feature set

The optional DCO feature set allows a utility program to reduce the capability of the device by modifying some of the optional commands, modes, and feature sets that a device reports as supported in the IDENTIFY DEVICE or IDENTIFY PACKET DEVICE data as well as the capacity reported.

Commands unique to the DCO feature set use a single command code and are differentiated from one another by the value placed in the Feature field. These commands are:

- a) DEVICE CONFIGURATION FREEZE LOCK;
- b) DEVICE CONFIGURATION IDENTIFY;
- c) DEVICE CONFIGURATION RESTORE; and
- d) DEVICE CONFIGURATION SET.

The DCO feature set may affect words in IDENTIFY DEVICE data, IDENTIFY PACKET DEVICE data, and other commands. Certain bits in these words that indicate that a command, mode, capacity, or feature set is supported and enabled may be cleared by a DEVICE CONFIGURATION SET command. For a particular command, mode, capacity, or feature set, when a bit is changed from one to zero requesting that the device shall not indicate support for the feature, the device shall not provide the feature.

The DEVICE CONFIGURATION SET command may be used to reduce the maximum capacity of the device. Since a Host Protected Area may be lost if the capacity of the device is reduced, when a Host Protected Area is set the DEVICE CONFIGURATION SET command shall cause the device to return command aborted. The LBA value returned by a READ NATIVE MAX ADDRESS or READ NATIVE MAX ADDRESS EXT command is modified by the DEVICE CONFIGURATION SET command modifying the maximum capacity of the device.

After processing of a power-on reset or hardware reset, a device shall not change the settings made by a DEVICE CONFIGURATION SET command.

The DEVICE CONFIGURATION IDENTIFY data indicates the selectable commands, modes, capacity, and feature sets that may be disabled in the device. After the execution of a DEVICE CONFIGURATION SET command this information is no longer available from an IDENTIFY DEVICE or IDENTIFY PACKET DEVICE command but the data that the DEVICE CONFIGURATION IDENTIFY command returns is not changed by the DEVICE CONFIGURATION SET or DEVICE CONFIGURATION RESTORE commands.

A DEVICE CONFIGURATION RESTORE command enables all capabilities that have been disabled by DEVICE CONFIGURATION SET command and returns the IDENTIFY DEVICE or IDENTIFY PACKET DEVICE data to that indicated by the DEVICE CONFIGURATION IDENTIFY command. If the value returned in IDENTIFY DEVICE data words 100-103 is less than the native max address for a device (i.e., a host protected area has been established), then the device shall return command aborted for a DEVICE CONFIGURATION RESTORE command.

If a device has not completed a DEVICE CONFIGURATION SET command without error, then a device shall be in the DCO Factory_config state after processing a power-on reset. If a device has completed a DEVICE CONFIGURATION SET command without error, then a device shall be in the DCO Reduced_config state after processing a power-on reset.

After completing a DEVICE CONFIGURATION FREEZE LOCK command without error, a device shall abort all DEVICE CONFIGURATION SET, DEVICE CONFIGURATION IDENTIFY, and DEVICE CONFIGURATION RESTORE commands until after completing the subsequent power-on reset. If a device is in the DCO_locked state, then processing a hardware reset or software reset does not cause the device to change state.

Figure 4 and the text in this subclause describe the operation of the DCO feature set.

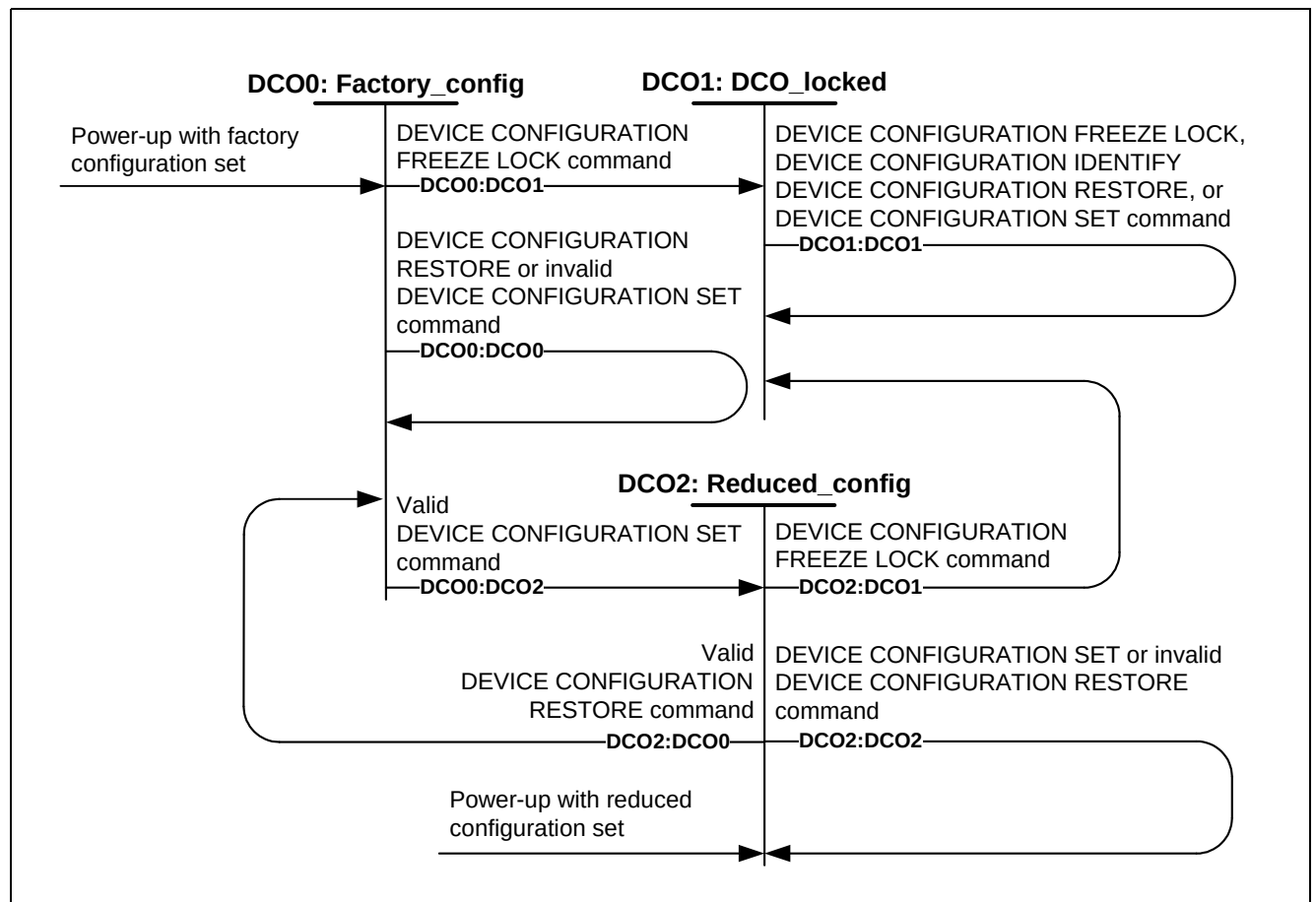


Figure 4 — Device Configuration Overlay state diagram

DCO0: Factory_config State: This state is entered when the device powers-up with the factory configuration set or a valid **DEVICE CONFIGURATION RESTORE** command is received.

When in this state, the device shall support all commands, modes, feature sets, and the capacity indicated by the response to a **DEVICE CONFIGURATION IDENTIFY** command.

Transition DCO0:DCO1: When a **DEVICE CONFIGURATION FREEZE LOCK** command is received, the device shall return successful command completion and transition to the **DCO1: DCO_locked** state.

Transition DCO0:DCO2: When a valid **DEVICE CONFIGURATION SET** command is received, the device shall return successful command completion and transition to the **DCO2: Reduced_config** state. See Transition **DCO0:DCO0** for the definition of conditions that make a **DEVICE CONFIGURATION SET** command invalid. This transition is made even if the configuration described by the **DEVICE CONFIGURATION SET** command is the same as the factory configuration.

Transition DCO0:DCO0: When a **DEVICE CONFIGURATION RESTORE** command is received, the device shall return command aborted and transition to the **DCO0: Factory_config** state. When an invalid **DEVICE CONFIGURATION SET** command is received, the device shall return command aborted and transition to the **DCO0: Factory_config** state. A device shall return command aborted if the **DEVICE CONFIGURATION SET** command requests that a device remove support for:

- the HPA feature set (see 4.11) if a HPA has been established;
- a Multiword or Ultra DMA mode if that mode or a higher numbered mode is currently selected;
- the PUIS feature set (see 4.19) if the PUIS feature set has been enabled by a jumper;
- the Security feature set (see 4.20) if the Security feature set has been enabled;
- the SMART feature set (see 4.21) if the **DEVICE CONFIGURATION SET** output data word 7 bits (2:1) are not cleared to zero; or
- the SMART feature set (see 4.21) if the SMART feature set is enabled.

DCO1: DCO_locked State: This state is entered when a DEVICE CONFIGURATION FREEZE LOCK command is received.

When in this state, all DEVICE CONFIGURATION FREEZE LOCK, DEVICE CONFIGURATION IDENTIFY, DEVICE CONFIGURATION SET, or DEVICE CONFIGURATION RESTORE commands shall return command aborted and shall remain in the same state.

Transition DCO1:DCO1: When a DEVICE CONFIGURATION FREEZE LOCK, DEVICE CONFIGURATION IDENTIFY, DEVICE CONFIGURATION SET, or DEVICE CONFIGURATION RESTORE command is received, the device shall return command aborted and shall remain in the same state.

DCO2: Reduced_config State: This state is entered when the device powers-up with a reduced configuration set or a valid DEVICE CONFIGURATION SET command is received.

When in this state, the device shall support all commands, modes, feature sets, and the capacity specified by the DEVICE CONFIGURATION SET command that caused this state to be entered.

Transition DCO2:DCO1: When a DEVICE CONFIGURATION FREEZE LOCK command is received, the device shall return successful command completion and transition to the DCO1: DCO_locked state.

Transition DCO2:DCO0: When a valid DEVICE CONFIGURATION RESTORE command is received, the device shall return successful command completion and transition to the DCO0: Factory_config state. See Transition DCO2:DCO2 for the definition of conditions that make a DEVICE CONFIGURATION RESTORE command invalid.

Transition DCO2:DCO2: When a DEVICE CONFIGURATION SET command is received, the device shall return command aborted and transition to the DCO2: Reduced_config state. When an invalid DEVICE CONFIGURATION RESTORE command is received, the device shall return command aborted and transition to the DCO2: Reduced_config state. A DEVICE CONFIGURATION RESTORE command is invalid if a Host Protected Area has been established using the SET MAX ADDRESS command.

4.9 Free-fall Control feature set

The Free-fall Control feature allows the device to attempt to protect itself in the event of free-fall detection. When this feature is enabled, upon detecting a free-fall event the device should protect its data from the mechanical contact that may damage data on the device. The implementation of free-fall detection and protection is vendor specific.

The Free-fall Control feature set is enabled and disabled using the following SET FEATURES subcommands:

- a) SET FEATURES subcommand 41h - enable the Free-fall Control feature set; and
- b) SET FEATURES subcommand C1h - disable the Free-fall Control feature set.

The Enable/Disable Free-fall Control subcommands shall be non-volatile. After the feature is enabled, the device shall keep this feature enabled until changed by the Enable/Disable Free-fall Control subcommands.

IDENTIFY DEVICE data word 120 bit 5 or IDENTIFY PACKET DEVICE data word 120 bit 5 indicates when the Free-fall Control feature set is enabled.

4.10 General Purpose Logging (GPL) feature set

The General Purpose Logging (GPL) feature set provides a mechanism for accessing logs in a device. These logs are associated with specific feature sets (e.g., SMART (see 4.21) and Streaming (see 4.23)). Support of the individual logs (see table A.2) is determined by support of the associated feature set. If the device supports a particular feature set, support for any associated log(s) is mandatory.

Support for the GPL feature set shall not be disabled by disabling SMART. If the feature set associated with a requested log is disabled, the device shall return command aborted.

If the GPL feature set is implemented, the following commands shall be supported:

- a) READ LOG EXT; and
- b) WRITE LOG EXT.

The following commands are optional:

- a) READ LOG DMA EXT; and
- b) WRITE LOG DMA EXT.

If the GPL feature set is supported, all Host Vendor Specific logs shall be supported (see A.9).

4.11 Host Protected Area (HPA) feature set

4.11.1 HPA overview

The optional Host Protected Area (HPA) feature set provides a method for an application client to reduce the number of user accessible LBAs on a device. This method results in providing a data storage area on the device that may be used by that application client but may temporarily be inaccessible to other application clients. A device that implements the HPA feature set shall implement the following minimum set of commands:

- a) READ NATIVE MAX ADDRESS; and
- b) SET MAX ADDRESS.

A device that implements the HPA feature set and supports the 48-bit Address feature set (see 4.4) shall implement the following additional set of commands:

- a) READ NATIVE MAX ADDRESS EXT; and
- b) SET MAX ADDRESS EXT.

Devices supporting this feature set shall set IDENTIFY DEVICE data word 82 bit 10 to one.

NOTE 6 - The PARTIES standard specifies a method for managing the HPA.

4.11.2 HPA security extensions

A device supporting the HPA feature set may optionally include the HPA security extensions. The Host Protected Area security commands use a single command code and are differentiated from one another by the value placed in the Feature field:

- a) SET MAX SET PASSWORD;
- b) SET MAX LOCK;
- c) SET MAX FREEZE LOCK; and
- d) SET MAX UNLOCK.

Devices supporting these extensions shall set IDENTIFY DEVICE data word 82 bit 10 or IDENTIFY PACKET DEVICE data word 82 bit 10 to one, and shall set IDENTIFY DEVICE data word 83 bit 8 or IDENTIFY PACKET DEVICE data word 83 bit 8 to one.

Upon successful completion of a power-on reset, the HPA security extensions are disabled and IDENTIFY DEVICE data word 86 bit 8 or IDENTIFY PACKET DEVICE data word 86 bit 8 is cleared to zero. There is no valid HPA password after the device processes a power-on reset and IDENTIFY DEVICE data word 86 bit 8 or IDENTIFY PACKET DEVICE data word 86 bit 8 is cleared to zero.

When a SET MAX SET PASSWORD command is completed without error, the HPA security extensions are enabled. In addition IDENTIFY DEVICE data word 86 bit 8 or IDENTIFY PACKET DEVICE data word 86 bit 8 shall be set to one.

4.11.3 28-bit and 48-bit HPA commands interactions

The READ NATIVE MAX ADDRESS or READ NATIVE MAX ADDRESS EXT command allows the host to determine the maximum native address space of the device even when a protected area has been allocated.

The SET MAX ADDRESS or SET MAX ADDRESS EXT command allows the host to redefine the maximum LBA of the user accessible LBA space. That is, when the SET MAX ADDRESS or SET MAX ADDRESS EXT command is issued with a maximum LBA less than the native max address, the device reduces the user accessible LBA space to the maximum specified by the command, providing a protected area above that maximum LBA. See 4.11.4 for a description of how to set IDENTIFY DEVICE data after issuing a SET MAX ADDRESS or SET MAX ADDRESS EXT command.

Any read or write that attempts to access an LBA above the maximum LBA specified by the SET MAX ADDRESS or SET MAX ADDRESS EXT command shall cause command completion with the ID Not Found bit set to one and the Error bit set to one, or command aborted.

A Volatility bit in the Count field allows the host to specify if the SET MAX ADDRESS LBA field is preserved after a power-on reset or a hardware reset. After processing a power-on reset or hardware reset, the device sets the maximum LBA to the last non-volatile LBA setting regardless of subsequent volatile SET MAX ADDRESS or SET MAX ADDRESS EXT commands. If the SET MAX ADDRESS or SET MAX ADDRESS EXT command is issued with a value that exceeds the native max address, then the device shall return command aborted.

Software reset shall not:

- a) affect the HPA feature set settings in the device;
- b) change the maximum accessible LBA for the device; or
- c) change the HPA state of the device.

When the device is HPA Unlocked and has not processed a SET MAX FREEZE LOCK command, then multiple SET MAX SET PASSWORD commands may be processed. The device only keeps the password set by the last SET MAX SET PASSWORD command; previously received passwords are overwritten by the new password. There is no limit to the number of times the password may be set.

Typical use of these commands is:

After a power-on reset or a hardware reset is processed:

- 1) BIOS receives control after the reset;
- 2) BIOS issues a READ NATIVE MAX ADDRESS or READ NATIVE MAX ADDRESS EXT command to find the max capacity of the device;
- 3) BIOS issues a volatile SET MAX ADDRESS or SET MAX ADDRESS EXT command to the values returned by READ NATIVE MAX ADDRESS or READ NATIVE MAX ADDRESS EXT;
- 4) BIOS reads configuration data from the highest area on the disk; and
- 5) BIOS restores the protected area by issuing a non-volatile SET MAX ADDRESS or SET MAX ADDRESS EXT using the original LBA.

On save to disk

- 1) BIOS receives control prior to shut down;
- 2) BIOS issues a READ NATIVE MAX ADDRESS or READ NATIVE MAX ADDRESS EXT command to find the max capacity of the device;
- 3) BIOS issues a volatile SET MAX ADDRESS or SET MAX ADDRESS EXT command to the values returned by READ NATIVE MAX ADDRESS or READ NATIVE MAX ADDRESS EXT;
- 4) Memory is copied to the reserved area;
- 5) Shut down completes; and
- 6) After processing a power-on reset or hardware reset, the device sets the maximum LBA to the last non-volatile LBA setting regardless of subsequent volatile SET MAX ADDRESS or SET MAX ADDRESS EXT commands.

These commands are intended for use only by system BIOS or other low-level boot time processes. Using these commands outside BIOS controlled boot or shutdown may result in damage to file systems on the device.

The SET MAX SET PASSWORD command allows the host to define the password to be used during the current power cycle. The password does not persist after a power-on reset has been processed but does persist after a hardware reset or a software reset has been processed. This password is not related to the password used for the Security feature set (see 4.20). When the password is set the device is HPA Unlocked.

The SET MAX LOCK command provides a method for the host to disable the SET MAX commands, except SET MAX UNLOCK, until after the device has processed the next power-on reset or command completion of a SET MAX UNLOCK command. When the SET MAX LOCK command is completed the device is HPA Locked.

The SET MAX UNLOCK command changes the device from HPA Locked to HPA Unlocked.

The SET MAX FREEZE LOCK command provides a method for the host to disable the SET MAX commands, including SET MAX UNLOCK, until after the device has processed the next power-on reset.

4.11.4 IDENTIFY DEVICE data

When the host issues a SETMAX ADDRESS command or SETMAX ADDRESS EXT command, several IDENTIFY DEVICE data words may be affected. The following guidelines are used for setting IDENTIFY DEVICE data:

- a) if the 48-bit Address feature set is not supported then words 60-61 shall contain the total number of user addressable sectors and words 100-103 shall be reserved;
- b) if the 48-bit Address feature set is supported and the total number of user addressable sectors is less than or equal to 0FFF_FFFFh then Words 60-61 and 100-103 shall contain the total number of user addressable sectors; and
- c) if the 48-bit Address feature set is supported and the total number of user addressable sectors is greater than 0FFF_FFFFh then words 60-61 shall contain 0FFF_FFFFh and words 100-103 shall contain the total number of user addressable sectors.

4.11.5 Determination of SET MAX security extension status

When the device is HPA Locked IDENTIFY DEVICE data word 86 bit 8 or IDENTIFY PACKET DEVICE data word 86 bit 8 shall be set to one.

4.11.6 HPA State Transition Diagrams

4.11.6.1 State Transition Figures

The HPA state transition diagrams are in five parts: figure 5, figure 6, figure 7, figure 8, and figure 9.

In the following state transition diagrams, the notation COMMAND (value) refers to the device receiving the command with a specific value or values. For example:

- a) SET MAX ADDRESS (Non-Volatile) means the device successfully processes a SET MAX ADDRESS command with the V_V field set to one; or
- b) SET MAX ADDRESS (Native Max) means the device successfully processes a SET MAX ADDRESS command with the LBA field set to the native max address.

If a state has a transition condition that specifies native max, then any other set max conditions imply a value less than the native max value. If a state has a transition condition that specifies neither volatile nor non-volatile, then both are implied.

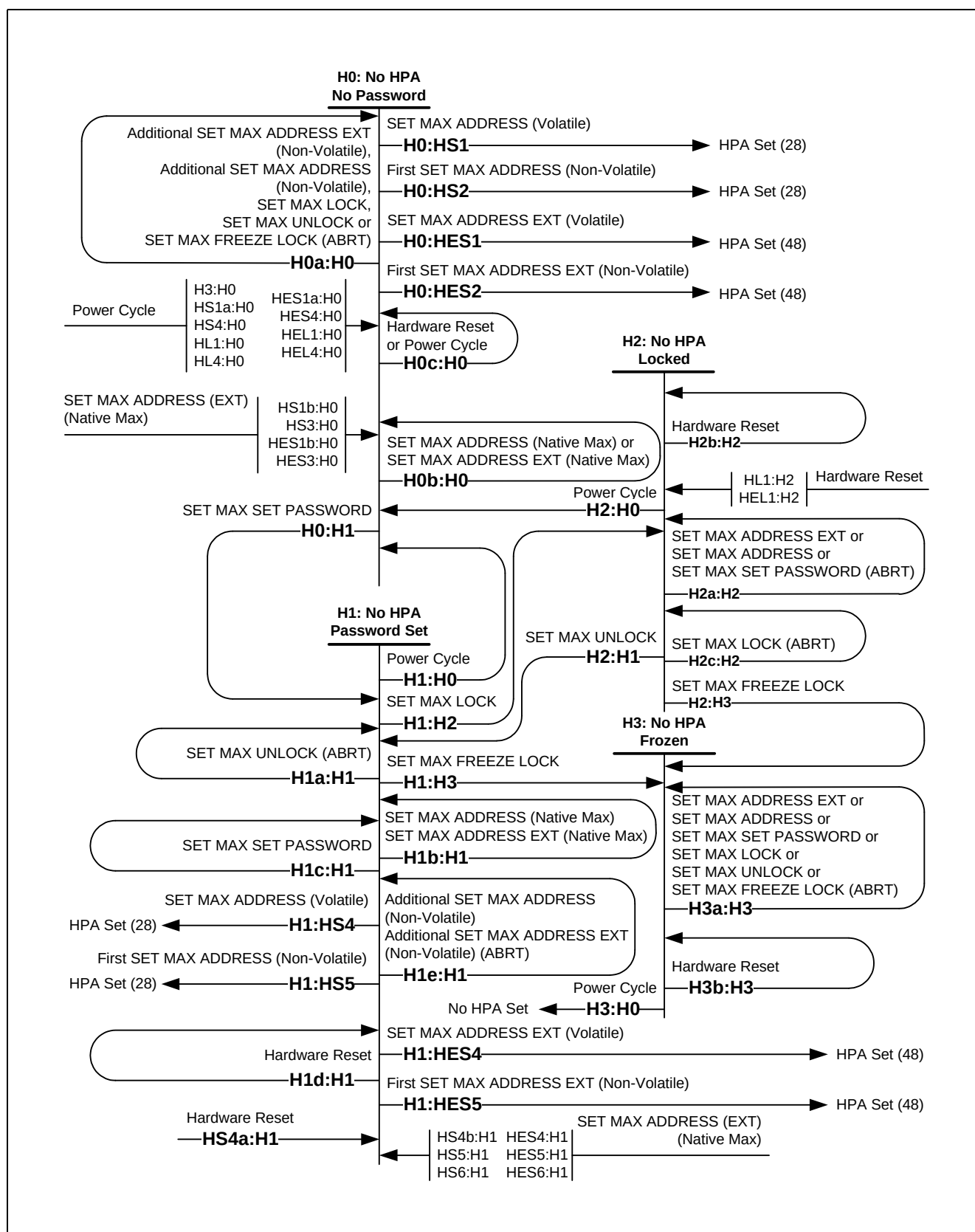


Figure 5 — HPA Not Set

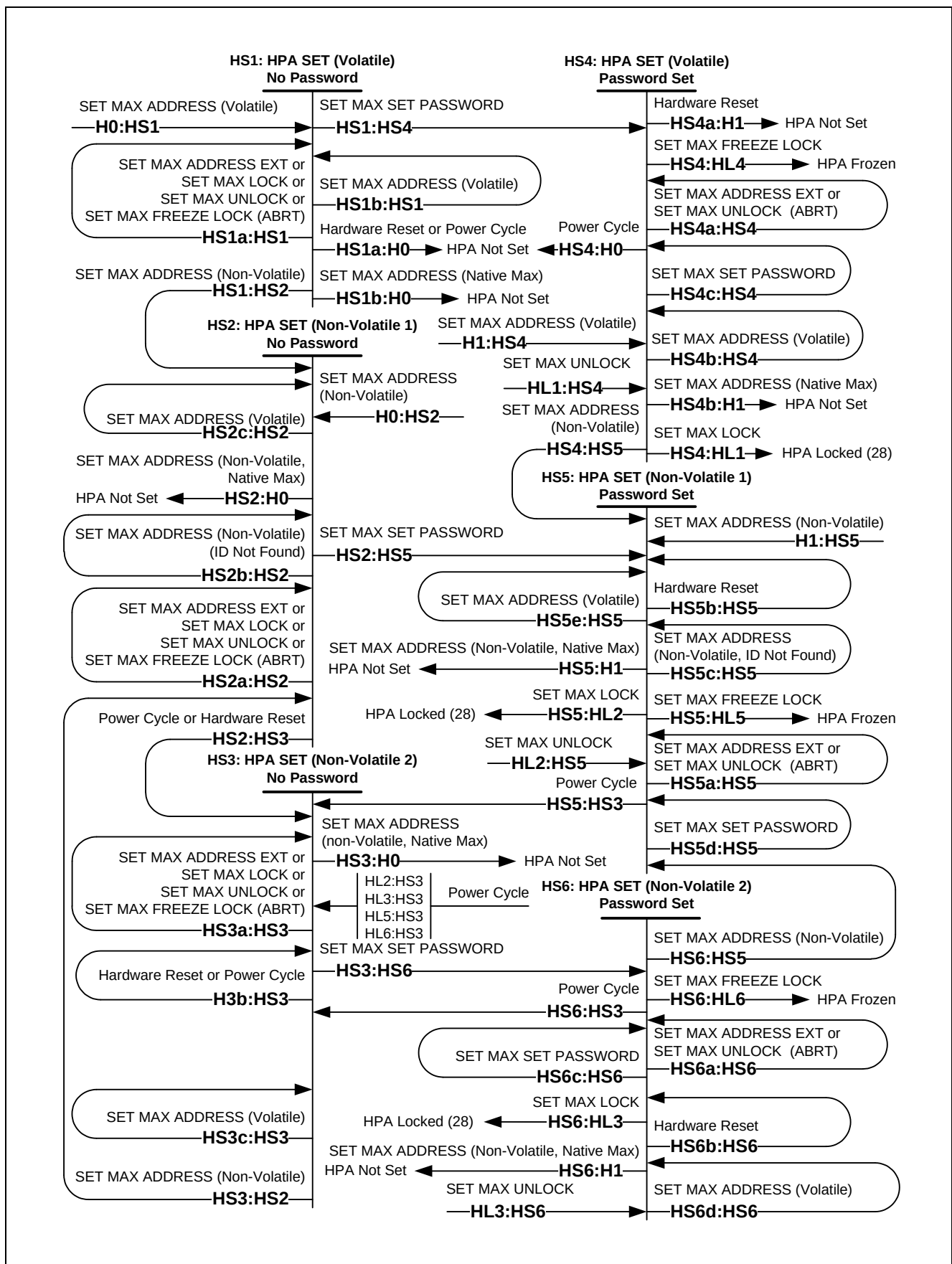


Figure 6 — HPA Set (28)

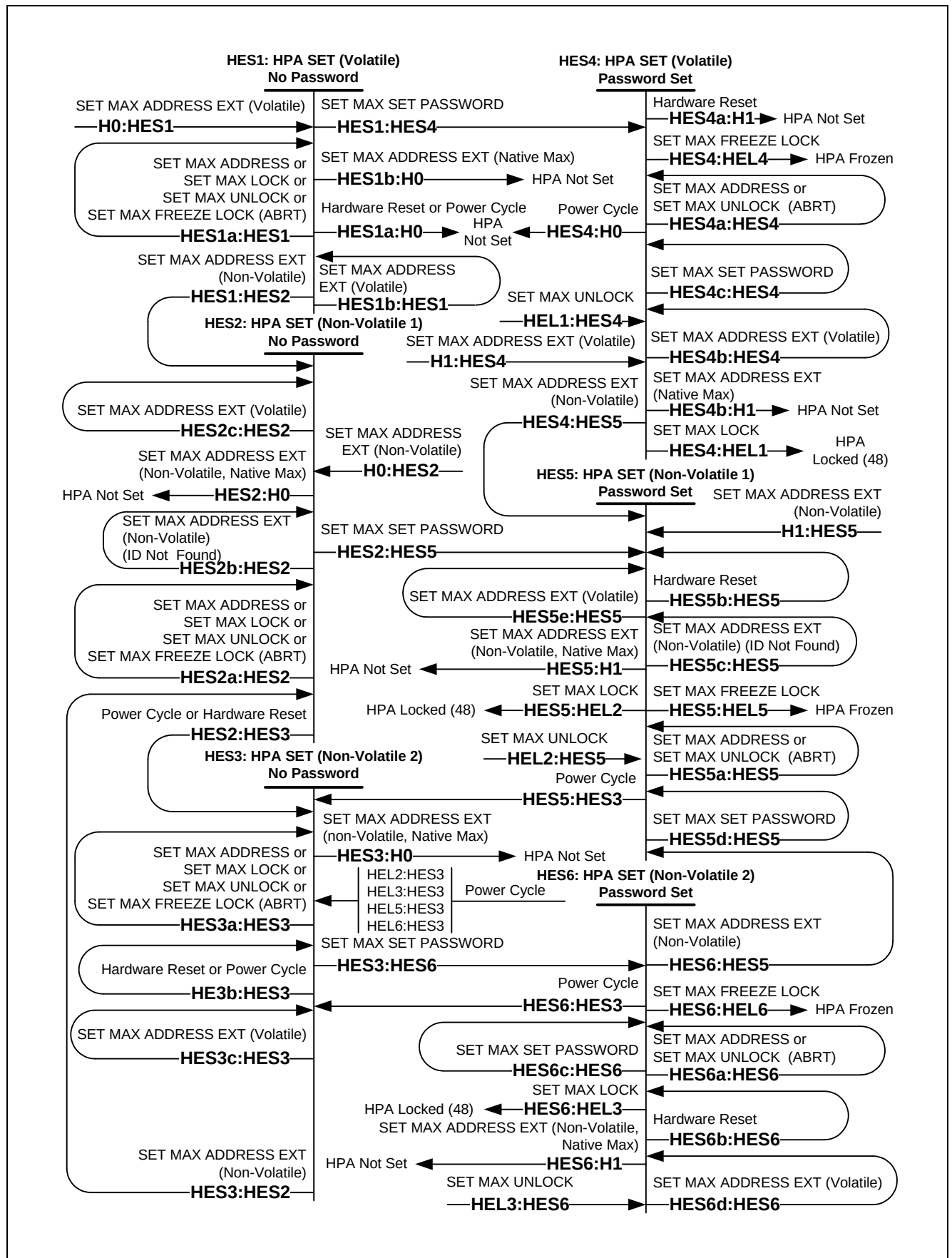


Figure 7 — HPA Set (48)

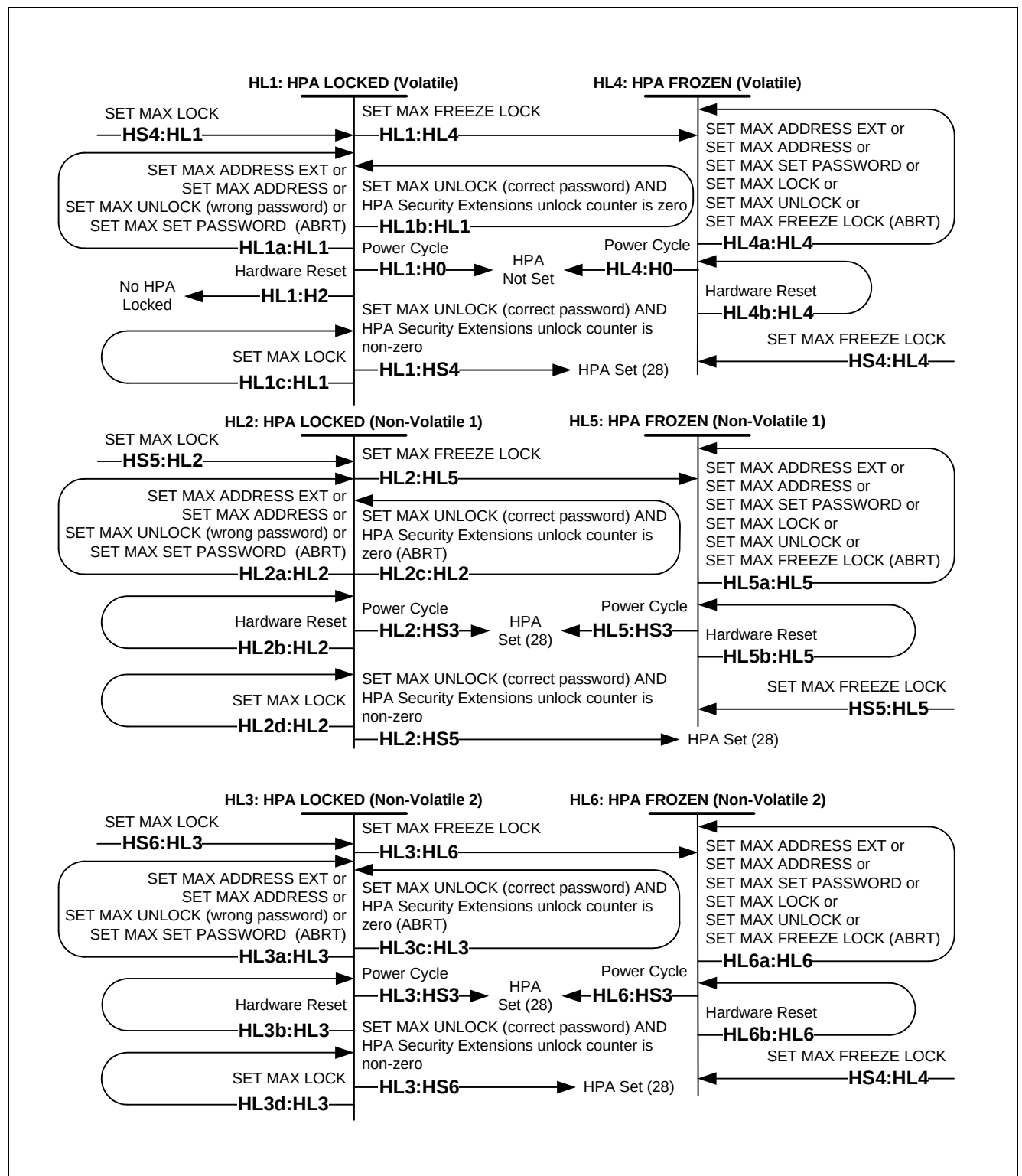


Figure 8 — HPA Locked (28)

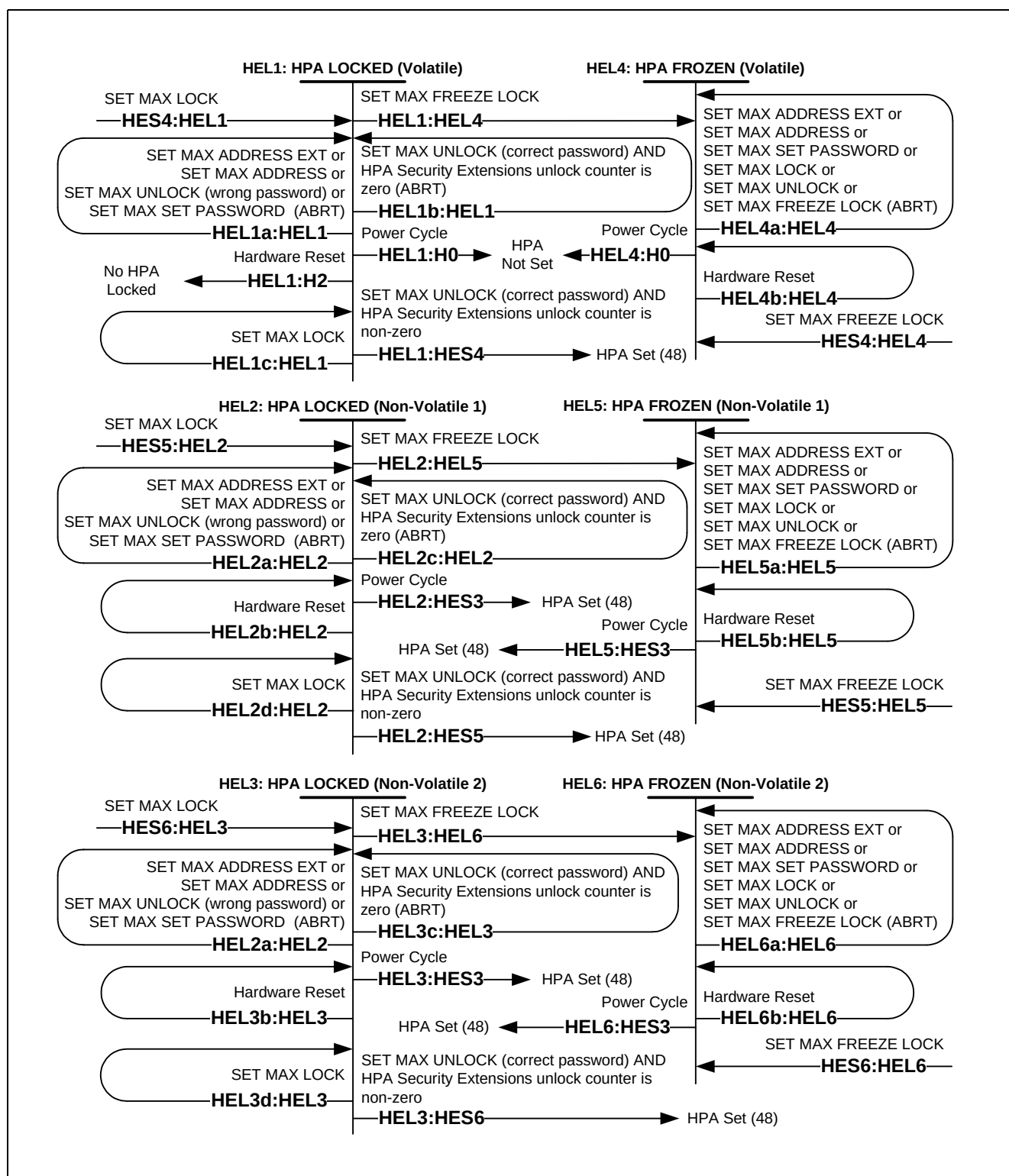


Figure 9 — HPA Locked (48)

4.11.6.2 HPA Not Set

State H0: No HPA/No Password: This state shall be entered when the device is powered on and does not have a non-volatile max address set. In this state the device has not established the HPA and the password has not been set.

Transition H0:H1: When the device successfully processes a SET MAX SET PASSWORD command without error, the device shall transition to the H1 state.

Transition H0:HS1: When the device successfully processes a SET MAX ADDRESS (Volatile) command without error, the device shall process the command and transition to the HS1 state.

Transition H0:HS2: When the device successfully processes a First SET MAX ADDRESS (non-volatile) command without error, the device shall process the command and transition to the HS2 state. A "First SET MAX ADDRESS (non-volatile) command" is the first SET MAX ADDRESS (non-volatile) command processed by the device after a Power-on reset.

Transition H0:HES1: When the device successfully processes a SET MAX ADDRESS EXT (Volatile) command without error, the device shall process the command and transition to the HES1 state.

Transition H0:HES2: When the device successfully processes a SET MAX ADDRESS EXT (Non-Volatile) command without error, the device shall process the command and transition to the HES2 state.

Transition H0a:H0: When the device successfully processes a SET MAX LOCK, SET MAX UNLOCK, SET MAX FREEZE LOCK, additional SET MAX ADDRESS EXT (non-volatile), or an additional SET MAX ADDRESS (non-volatile) command without error, the device shall return command aborted and remain in the same state. An "additional SET MAX ADDRESS (non-volatile) command" is a SET MAX ADDRESS (non-volatile) command that is processed by the device after a previous SET MAX ADDRESS (non-volatile) command has been successfully processed by the device with no intervening Power-on reset.

Transition H0b:H0: When the device successfully processes a SET MAX ADDRESS (Native Max) command or SET MAX ADDRESS EXT (Native Max) command without error, the device shall remain in the same state.

Transition H0c:H0: When the device successfully processes a hardware reset or a power-on reset, the device shall remain in the same state.

State H1: No HPA/Password Set: In this state the device has not established the HPA and the password has been set.

Transition H1:H0: When the device successfully processes a power-on reset, the device shall transition to the H0 state.

Transition H1:H2: When the device successfully processes a SET MAX LOCK command, the device shall transition to the H2 state.

Transition H1:H3: When the device successfully processes a SET MAX FREEZE LOCK command without error, the device shall transition to the H3 state.

Transition H1:HS4: When the device successfully processes a SET MAX ADDRESS (Volatile), the device shall transition to the HS4 state.

Transition H1:HES4: When the device successfully processes a SET MAX ADDRESS EXT (Volatile), the device shall transition to the HES4 state.

Transition H1:HES5: When the device successfully processes a First SET MAX ADDRESS EXT (Non-Volatile), the device shall transition to the HES5 state. A "First SET MAX ADDRESS EXT (non-volatile) command" is the first SET MAX ADDRESS (non-volatile) command processed by the device after a Power-on reset.

Transition H1:HS5: When the device successfully processes a First SET MAX ADDRESS (Non-Volatile), the device shall transition to the HS5 state. A "First SET MAX ADDRESS (non-volatile) command" is the first SET MAX ADDRESS (non-volatile) command processed by the device after a Power-on reset.

Transition H1a:H1: When the device successfully processes a SET MAX UNLOCK command, the device shall report command aborted and remain in the same state.

Transition H1b:H1: When the device successfully processes a SET MAX ADDRESS (Native Max) command or a SET MAX ADDRESS EXT (Native Max) command without error, the device shall remain in the same state.

Transition H1c:H1: When the device successfully processes a SET MAX SET PASSWORD command without error, the device shall remain in the same state.

Transition H1d:H1: If the device processes a hardware reset, the device shall remain in the same state.

Transition H1e:H1: When the device successfully processes an additional SET MAX ADDRESS EXT (non-volatile) or an additional SET MAX ADDRESS (non-volatile) command, the device shall return command aborted and remain in the same state. An "additional SET MAX ADDRESS (non-volatile) command" is a SET MAX ADDRESS (non-volatile) command that is processed by the device after a previous SET MAX ADDRESS (non-volatile) command has been successfully processed by the device with no intervening Power-on reset.

State H2: No HPA/Locked: In this state the device is HPA Locked and only the power cycle transits the state to the H0 state.

Transition H2:H0: When the device successfully processes a power-on reset, the device shall transition to the H0 state.

Transition H2:H1: When the device successfully processes a SET MAX UNLOCK command with the correct password, the device shall transition to the H1 state.

Transition H2:H3: When the device successfully processes a SET MAX FREEZE LOCK command with the correct password, the device shall transition to the H3 state.

Transition H2a:H2: When the device successfully processes a SET MAX ADDRESS EXT, SET MAX ADDRESS, or SET MAX SET PASSWORD command, the device shall return command aborted and remain in the same state.

Transition H2b:H2: If the device processes a hardware reset, then the device shall remain in the same state.

Transition H2c:H2: If the device successfully processes a SET MAX LOCK command, the device shall remain in the same state and the device may return command aborted.

State H3: No HPA FROZEN: In this state no HPA is established and the device is locked from all HPA commands. Only a power-cycle shall cause the device to change to another state.

Transition H3:H0: When the device successfully processes a power-on reset, the device shall transition to the H0 state.

Transition H3a:H3: When the device successfully processes a SET MAX ADDRESS EXT, SET MAX ADDRESS, SET MAX LOCK, SET MAX UNLOCK, SET MAX FREEZE LOCK or SET MAX SET PASSWORD command, the device shall return command aborted and remain in the same state.

Transition H3b:H3: When the device processes a hardware reset, the device shall remain in the same state.

4.11.6.3 28-bit HPA Set

State HS1: HPA SET (Volatile)/No Password: In this state the volatile 28-bit HPA is established and the password is not set.

Transition HS1:HS2: When the device successfully processes a SET MAX ADDRESS command without error in non-volatile state, the device shall transition to the HS2 state.

Transition HS1:HS4: When the device successfully processes a SET MAX SET PASSWORD command without error, the device shall transition to the HS4 state.

Transition HS1a:H0: When the device successfully processes a hardware reset or if device processes a power-on reset, the device shall transition to the H0 state.

Transition HS1b:H0: When the device successfully processes a SET MAX ADDRESS (Native Max) command without error, the device shall transition to the H0 state.

Transition HS1a:HS1: When the device successfully processes a SET MAX ADDRESS EXT, SET MAX LOCK, SET MAX UNLOCK or SET MAX FREEZE LOCK command, the device shall return command aborted and remain in the same state.

Transition HS1b:HS1: When the device successfully processes a SET MAX ADDRESS (Volatile) command, the device shall remain in the same state.