

Skylake-LP Client Platform

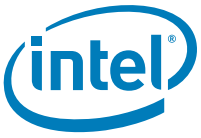
SPI Programming Guide

May 2015

Revision 0.87.0

Intel Confidential

Document Number: CDI/IBP# 550696



By using this document, in addition to any agreements you have with Intel, you accept the terms set forth below.

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

A “Mission Critical Application” is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked “reserved” or “undefined”. Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or go to: http://www.intel.com/design/literature.htm

Code names featured are used internally within Intel to identify products that are in development and not yet publicly announced for release. Customers, licensees and other third parties are not authorized by Intel to use code names in advertising, promotion or marketing of any product or services and any such use of Intel's internal code names is at the sole risk of the user.

Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families. Go to: http://www.intel.com/products/processor_number.

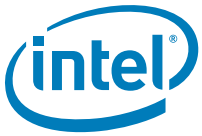
The original equipment manufacturer must provide TPM functionality, which requires a TPM-supported BIOS. TPM functionality must be initialized and may not be available in all countries.

No computer system can provide absolute security under all conditions. Built-in security features available on select Intel® Core™ processors may require additional software, hardware, services and/or an Internet connection. Results may vary depending upon configuration. Consult your PC manufacturer for more details.

Intel, Core and the Intel logo are trademarks of Intel Corporation in the U.S. and other countries.

*Other names and brands may be claimed as the property of others.

Copyright © 2015, Intel Corporation. All rights reserved.



Contents

1 Introduction 13
1.1 Overview 13
1.2 Terminology 14
1.3 Reference Documents 14

2 PCH SPI Flash Architecture 15
2.1 Descriptor Mode 15
2.2 Serial Flash Discoverable Parameter (SFDP) 15
2.3 SPI Fast Read 15
2.4 Intel® Trusted Platform Module (Intel® TPM) on SPI Bus 15
2.5 Boot Flow for Skylake PCH-LP Family 15
2.6 Flash Regions 16
2.6.1 Flash Region Sizes 16
2.7 Hardware Sequencing 16

3 PCH SPI Flash Compatibility Requirement 17
3.1 Skylake PCH-LP SPI Flash Requirements 17
3.1.1 General Requirements 17
3.1.2 Bios Requirement 18
3.1.3 Software / Firmware Requirements 18
3.1.4 JEDEC ID (Opcode 9Fh) 19
3.1.5 Multiple Page Write Usage Model 19
3.1.6 Hardware Sequencing Requirements 19
3.2 Skylake PCH-LP SPI AC Electrical Compatibility Guidelines 20
3.3 SPI Flash DC Electrical Compatibility Guidelines 22

4 Descriptor Overview 23
4.1 Flash Descriptor Content 24
4.1.1 Descriptor Signature and Map 25
4.1.1.1 FLVALSIG - Flash Valid Signature (Flash Descriptor Records) 25
4.1.1.2 FLMAP0 - Flash Map 0 Register (Flash Descriptor Records) 25
4.1.1.3 FLMAP1 - Flash Map 1 Register (Flash Descriptor Records) 26
4.1.1.4 FLMAP2—Flash Map 2 Register (Flash Descriptor Records) 26
4.1.2 Flash Descriptor Component Section 27
4.1.2.1 FLCOMP—Flash Components Register (Flash Descriptor Records) 27
4.1.2.2 FLILL—Flash Invalid Instructions Register (Flash Descriptor Records) 29
4.1.2.3 FLILL1—Flash Invalid Instructions Register (Flash Descriptor Records) 29
4.1.3 Flash Descriptor Region Section 30
4.1.3.1 FLREG0—Flash Region 0 (Flash Descriptor) Register ..... (Flash Descriptor Records) 31
4.1.3.2 FLREG1—Flash Region 1 (BIOS) Register (Flash Descriptor Records) 31
4.1.3.3 FLREG2—Flash Region 2 (Intel® ME) Register (Flash Descriptor Records) 31
4.1.3.4 FLREG3—Flash Region 3 (GbE) Register (Flash Descriptor Records) 32

4.1.3.5 FLREG4—Flash Region 4 (Platform Data) Register (Flash Descriptor Records) 32
4.1.3.6 FLREG8—Flash Region 8(Embeded Controller) Register (Flash Descriptor Records) 32
4.1.4 Flash Descriptor Master Section 33
4.1.4.1 FLMSTR1—Flash Master 1 (Host CPU/ BIOS) 33
4.1.4.2 FLMSTR2—Flash Master 2 (Intel® ME) 33
4.1.4.3 FLMSTR3—Flash Master 3 (GbE) 33
4.1.4.4 FLMSTR4—Flash Master 4 (Reserved) 34
4.1.4.5 FLMSTR5—Flash Master 5 (EC) 34
4.1.5 PCH / CPU Softstraps 34
4.1.6 Descriptor Upper Map Section 34
4.1.6.1 FLUMAP1—Flash Upper Map 1 (Flash Descriptor Records) 34
4.1.7 Intel® ME Vendor Specific Component Capabilities Table 34
4.1.7.1 JID0—JEDEC-ID 0 Register (Flash Descriptor Records) 35
4.1.7.2 VSCC0—Vendor Specific Component Capabilities 0 (Flash Descriptor Records) 35
4.1.7.3 JIDn—JEDEC-ID Register n (Flash Descriptor Records) 36
4.1.7.4 VSCCn—Vendor Specific Component Capabilities n (Flash Descriptor Records) 36
4.2 OEM Section 36
4.3 Region Access Control 36
4.3.1 Intel Recommended Permissions for Region Access 37
4.3.2 Overriding Region Access 37
4.4 Intel® ME Vendor-Specific Component Capabilities (Intel® ME VSCC) Table 38
4.4.1 How to Set a VSCC Entry in Intel® ME VSCC Table for Skylake PCH-LP Platforms 38
4.4.2 Intel® ME VSCC Table Settings for Skylake PCH-LP Family Systems 40

5 Serial Flash Discoverable Parameter (SFDP) Overview 41
5.1 Introduction 41
5.2 Discoverable Parameter Opcode and Flash Cycle 41
5.3 Parameter Table Supported on PCH 41
5.4 Detailed JEDEC Specification 42

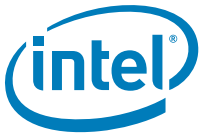
6 Configuring BIOS/GbE for SPI Flash Access 43
6.1 Unlocking SPI Flash Device Protection for Skylake PCH-LP Platform 43
6.2 Locking SPI Flash via Status Register 44
6.3 SPI Protected Range Register Recommendations 44
6.4 Recommendations for Flash Configuration Lockdown and Vendor Component Lock Bits 44
6.4.1 Flash Configuration Lockdown 44
6.4.2 Vendor Component Lock 45
6.5 Host Vendor Specific Component Control Registers (VSCC) 45
6.6 Host VSCC Register Settings 49

7 Intel® ME Disable for Debug/Flash Burning Purposes 50
7.1 Intel® ME Disable 50
7.1.1 Erasing/Programming Intel® ME Region 50

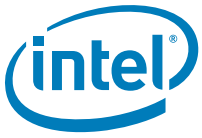
8 Recommendations for SPI Flash Programming in Manufacturing Environments 51

9 Flash Descriptor PCH / CPU Configuration Section 52
9.1 PCH Descriptor Record 0 (Flash Descriptor Records) 52
9.2 PCH Descriptor Record 1 (Flash Descriptor Records) 53
9.3 PCH Descriptor Record 2 (Flash Descriptor Records) 53

9.4 PCH Descriptor Record 3 (Flash Descriptor Records) 54
9.5 PCH Descriptor Record 4 (Flash Descriptor Records) 54
9.6 PCH Descriptor Record 5 (Flash Descriptor Records) 54
9.7 PCH Descriptor Record 6 (Flash Descriptor Records) 55
9.8 PCH Descriptor Record 7 (Flash Descriptor Records) 55
9.9 PCH Descriptor Record 8 (Flash Descriptor Records) 55
9.10 PCH Descriptor Record 9 (Flash Descriptor Records) 56
9.11 PCH Descriptor Record 10 (Flash Descriptor Records) 56
9.12 PCH Descriptor Record 11 (Flash Descriptor Records) 56
9.13 PCH Descriptor Record 12 (Flash Descriptor Records) 57
9.14 PCH Descriptor Record 13 (Flash Descriptor Records) 57
9.15 PCH Descriptor Record 14 (Flash Descriptor Records) 57
9.16 PCH Descriptor Record 15 (Flash Descriptor Records) 58
9.17 PCH Descriptor Record 16 (Flash Descriptor Records) 58
9.18 PCH Descriptor Record 17 (Flash Descriptor Records) 58
9.19 PCH Descriptor Record 18 (Flash Descriptor Records) 58
9.20 PCH Descriptor Record 19 (Flash Descriptor Records) 59
9.21 PCH Descriptor Record 20 (Flash Descriptor Records) 59
9.22 PCH Descriptor Record 21 (Flash Descriptor Records) 59
9.23 PCH Descriptor Record 22 (Flash Descriptor Records) 59
9.24 PCH Descriptor Record 23 (Flash Descriptor Records) 60
9.25 PCH Descriptor Record 24 (Flash Descriptor Records) 60
9.26 PCH Descriptor Record 25 (Flash Descriptor Records) 60
9.27 PCH Descriptor Record 26 (Flash Descriptor Records) 61
9.28 PCH Descriptor Record 27 (Flash Descriptor Records) 61
9.29 PCH Descriptor Record 28 (Flash Descriptor Records) 62
9.30 PCH Descriptor Record 29 (Flash Descriptor Records) 62
9.31 PCH Descriptor Record 30 (Flash Descriptor Records) 62
9.32 PCH Descriptor Record 31 (Flash Descriptor Records) 62
9.33 PCH Descriptor Record 32 (Flash Descriptor Records) 63
9.34 PCH Descriptor Record 33 (Flash Descriptor Records) 63
9.35 PCH Descriptor Record 34 (Flash Descriptor Records) 63
9.36 PCH Descriptor Record 35 (Flash Descriptor Records) 63
9.37 PCH Descriptor Record 36 (Flash Descriptor Records) 63
9.38 PCH Descriptor Record 37 (Flash Descriptor Records) 64
9.39 PCH Descriptor Record 38 (Flash Descriptor Records) 64
9.40 PCH Descriptor Record 39 (Flash Descriptor Records) 64
9.41 PCH Descriptor Record 40 (Flash Descriptor Records) 64
9.42 PCH Descriptor Record 41 (Flash Descriptor Records) 65
9.43 PCH Descriptor Record 42 (Flash Descriptor Records) 65
9.44 PCH Descriptor Record 43 (Flash Descriptor Records) 65
9.45 PCH Descriptor Record 44 (Flash Descriptor Records) 65
9.46 PCH Descriptor Record 45 (Flash Descriptor Records) 66
9.47 PCH Descriptor Record 46 (Flash Descriptor Records) 66
9.48 PCH Descriptor Record 47 (Flash Descriptor Records) 66
9.49 PCH Descriptor Record 48 (Flash Descriptor Records) 66
9.50 PCH Descriptor Record 49 (Flash Descriptor Records) 66
9.51 PCH Descriptor Record 50 (Flash Descriptor Records) 66
9.52 PCH Descriptor Record 51 (Flash Descriptor Records) 67
9.53 PCH Descriptor Record 52 (Flash Descriptor Records) 68
9.54 PCH Descriptor Record 53 (Flash Descriptor Records) 68
9.55 PCH Descriptor Record 54 (Flash Descriptor Records) 69
9.56 PCH Descriptor Record 55 (Flash Descriptor Records) 70
9.57 PCH Descriptor Record 56 (Flash Descriptor Records) 70
9.58 PCH Descriptor Record 57 (Flash Descriptor Records) 71



9.59 PCH Descriptor Record 58 (Flash Descriptor Records) 71
9.60 PCH Descriptor Record 59 (Flash Descriptor Records) 72
9.61 PCH Descriptor Record 60 (Flash Descriptor Records) 73
9.62 PCH Descriptor Record 61 (Flash Descriptor Records) 73
9.63 PCH Descriptor Record 62 (Flash Descriptor Records) 73
9.64 PCH Descriptor Record 63 (Flash Descriptor Records) 74
9.65 PCH Descriptor Record 64 (Flash Descriptor Records) 74
9.66 PCH Descriptor Record 65 (Flash Descriptor Records) 75
9.67 PCH Descriptor Record 66 (Flash Descriptor Records) 76
9.68 PCH Descriptor Record 67 (Flash Descriptor Records) 76
9.69 PCH Descriptor Record 68 (Flash Descriptor Records) 76
9.70 PCH Descriptor Record 69 (Flash Descriptor Records) 76
9.71 PCH Descriptor Record 70 (Flash Descriptor Records) 77
9.72 PCH Descriptor Record 71 (Flash Descriptor Records) 77
9.73 PCH Descriptor Record 72 (Flash Descriptor Records) 78
9.74 PCH Descriptor Record 73 (Flash Descriptor Records) 78
9.75 PCH Descriptor Record 74 (Flash Descriptor Records) 79
9.76 PCH Descriptor Record 75 (Flash Descriptor Records) 79
9.77 PCH Descriptor Record 76 (Flash Descriptor Records) 79
9.78 PCH Descriptor Record 77 (Flash Descriptor Records) 80
9.79 PCH Descriptor Record 78 (Flash Descriptor Records) 81
9.80 PCH Descriptor Record 79 (Flash Descriptor Records) 81
9.81 PCH Descriptor Record 80 (Flash Descriptor Records) 81
9.82 PCH Descriptor Record 81 (Flash Descriptor Records) 82
9.83 PCH Descriptor Record 82 (Flash Descriptor Records) 82
9.84 PCH Descriptor Record 83 (Flash Descriptor Records) 82
9.85 PCH Descriptor Record 84 (Flash Descriptor Records) 82
9.86 PCH Descriptor Record 85 (Flash Descriptor Records) 83
9.87 PCH Descriptor Record 86 (Flash Descriptor Records) 83
9.88 PCH Descriptor Record 87 (Flash Descriptor Records) 83
9.89 PCH Descriptor Record 88 (Flash Descriptor Records) 83
9.90 PCH Descriptor Record 89 (Flash Descriptor Records) 84
9.91 PCH Descriptor Record 90 (Flash Descriptor Records) 84
9.92 PCH Descriptor Record 91 (Flash Descriptor Records) 84
9.93 PCH Descriptor Record 92 (Flash Descriptor Records) 85
9.94 PCH Descriptor Record 93 (Flash Descriptor Records) 85
9.95 PCH Descriptor Record 94 (Flash Descriptor Records) 85
9.96 PCH Descriptor Record 95 (Flash Descriptor Records) 85
9.97 PCH Descriptor Record 96 (Flash Descriptor Records) 85
9.98 PCH Descriptor Record 97 (Flash Descriptor Records) 85
9.99 PCH Descriptor Record 98 (Flash Descriptor Records) 86
9.100 PCH Descriptor Record 99 (Flash Descriptor Records) 86
9.101 PCH Descriptor Record 100 (Flash Descriptor Records) 87
9.102 PCH Descriptor Record 101 (Flash Descriptor Records) 87
9.103 PCH Descriptor Record 102 (Flash Descriptor Records) 88
9.104 PCH Descriptor Record 103 (Flash Descriptor Records) 88
9.105 PCH Descriptor Record 104 (Flash Descriptor Records) 88
9.106 PCH Descriptor Record 105 (Flash Descriptor Records) 88
9.107 PCH Descriptor Record 106 (Flash Descriptor Records) 89
9.108 PCH Descriptor Record 107 (Flash Descriptor Records) 89
9.109 PCH Descriptor Record 108 (Flash Descriptor Records) 90
9.110 PCH Descriptor Record 109 (Flash Descriptor Records) 90
9.111 PCH Descriptor Record 110 (Flash Descriptor Records) 91
9.112 PCH Descriptor Record 111 (Flash Descriptor Records) 91
9.113 PCH Descriptor Record 112 (Flash Descriptor Records) 91

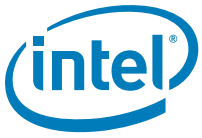


9.114 PCH Descriptor Record 113 (Flash Descriptor Records) 91
9.115 PCH Descriptor Record 114 (Flash Descriptor Records) 92
9.116 PCH Descriptor Record 115 (Flash Descriptor Records) 92
9.117 PCH Descriptor Record 116 (Flash Descriptor Records) 93
9.118 PCH Descriptor Record 117 (Flash Descriptor Records) 93
9.119 PCH Descriptor Record 118 (Flash Descriptor Records) 93
9.120 PCH Descriptor Record 119 (Flash Descriptor Records) 94
9.121 PCH Descriptor Record 120 (Flash Descriptor Records) 95
9.122 PCH Descriptor Record 121 (Flash Descriptor Records) 95
9.123 PCH Descriptor Record 122 (Flash Descriptor Records) 95
9.124 PCH Descriptor Record 123 (Flash Descriptor Records) 96
9.125 PCH Descriptor Record 124 (Flash Descriptor Records) 96
9.126 PCH Descriptor Record 125 (Flash Descriptor Records) 96
9.127 PCH Descriptor Record 126 (Flash Descriptor Records) 97
9.128 PCH Descriptor Record 127 (Flash Descriptor Records) 97
9.129 PCH Descriptor Record 128 (Flash Descriptor Records) 97
9.130 PCH Descriptor Record 129 (Flash Descriptor Records) 97
9.131 PCH Descriptor Record 130 (Flash Descriptor Records) 97
9.132 PCH Descriptor Record 131 (Flash Descriptor Records) 98
9.133 PCH Descriptor Record 132 (Flash Descriptor Records) 98
9.134 PCH Descriptor Record 133 (Flash Descriptor Records) 98
9.135 PCH Descriptor Record 134 (Flash Descriptor Records) 98
9.136 PCH Descriptor Record 135 (Flash Descriptor Records) 98
9.137 PCH Descriptor Record 136 (Flash Descriptor Records) 99
9.138 PCH Descriptor Record 137 (Flash Descriptor Records) 99
9.139 PCH Descriptor Record 138 (Flash Descriptor Records) 99
9.140 PCH Descriptor Record 139 (Flash Descriptor Records) 99
9.141 PCH Descriptor Record 140 (Flash Descriptor Records) 99
9.142 PCH Descriptor Record 141 (Flash Descriptor Records) 99
9.143 PCH Descriptor Record 142 (Flash Descriptor Records) 100
9.144 PCH Descriptor Record 143 (Flash Descriptor Records) 100
9.145 PCH Descriptor Record 144 (Flash Descriptor Records) 100
9.146 PCH Descriptor Record 145 (Flash Descriptor Records) 100
9.147 PCH Descriptor Record 146 (Flash Descriptor Records) 100
9.148 PCH Descriptor Record 147 (Flash Descriptor Records) 101
9.149 PCH Descriptor Record 148 (Flash Descriptor Records) 101
9.150 PCH Descriptor Record 149 (Flash Descriptor Records) 101
9.151 PCH Descriptor Record 150 (Flash Descriptor Records) 101
9.152 PCH Descriptor Record 151 (Flash Descriptor Records) 101
9.153 PCH Descriptor Record 152 (Flash Descriptor Records) 102
9.154 PCH Descriptor Record 153 (Flash Descriptor Records) 102
9.155 PCH Descriptor Record 154 (Flash Descriptor Records) 102
9.156 PCH Descriptor Record 155 (Flash Descriptor Records) 102
9.157 PCH Descriptor Record 156 (Flash Descriptor Records) 102
9.158 PCH Descriptor Record 157 (Flash Descriptor Records) 103
9.159 PCH Descriptor Record 158 (Flash Descriptor Records) 103
9.160 PCH Descriptor Record 159 (Flash Descriptor Records) 103
9.161 PCH Descriptor Record 160 (Flash Descriptor Records) 104
9.162 PCH Descriptor Record 161 (Flash Descriptor Records) 104
9.163 PCH Descriptor Record 162 (Flash Descriptor Records) 105
9.164 PCH Descriptor Record 163 (Flash Descriptor Records) 105
9.165 PCH Descriptor Record 164 (Flash Descriptor Records) 105
9.166 PCH Descriptor Record 165 (Flash Descriptor Records) 106
9.167 PCH Descriptor Record 166 (Flash Descriptor Records) 106
9.168 PCH Descriptor Record 167 (Flash Descriptor Records) 106

9.169 PCH Descriptor Record 168 (Flash Descriptor Records) 107
9.170 PCH Descriptor Record 169 (Flash Descriptor Records) 107
9.171 PCH Descriptor Record 170 (Flash Descriptor Records) 108
9.172 PCH Descriptor Record 171 (Flash Descriptor Records) 108
9.173 PCH Descriptor Record 172 (Flash Descriptor Records) 109
9.174 PCH Descriptor Record 173 (Flash Descriptor Records) 110
9.175 PCH Descriptor Record 174 (Flash Descriptor Records) 110
9.176 PCH Descriptor Record 175 (Flash Descriptor Records) 111
9.177 PCH Descriptor Record 176 (Flash Descriptor Records) 111
9.178 PCH Descriptor Record 177 (Flash Descriptor Records) 111
9.179 PCH Descriptor Record 178 (Flash Descriptor Records) 112
9.180 CPU Descriptor Record 0 (Flash Descriptor Records) 115
9.181 CPU Descriptor Record 1 (Flash Descriptor Records) 115
9.182 CPU Descriptor Record 2 (Flash Descriptor Records) 118

10 Configuration Dependencies 120
10.1 Descriptor Configuration Setting Enabling Dependencies 120
10.1.1 High Speed IO (HSIO) Port Enabling 120
10.1.1.1 Configuring PCIe on HSIO 123
10.1.1.2 Configure Intel® RST on PCIe 123
10.1.2 Intel® Integrated LAN Controller Enabling 125
10.1.3 Intel® Wireless LAN Controller Enabling 125
10.1.4 Deep Sx Enabling Dependencies 126
10.1.5 RPMC Enabling Dependencies 126
10.1.6 Intel® SMBus Enabling 126
10.1.7 SMLink0 Enabling Dependencies 127
10.1.8 SMLink1 Enabling Dependencies 127
10.1.9 TPM over SPI Enabling Dependencies 128
10.1.10 mSATA/M.2 / SATA Express Enabling 128
10.1.10.1 SATA0 / PCIe7 mSATA /M.2 / SATA Express Enabling HSIO 128
10.1.10.2 SATA1A / PCIe8 mSATA /M.2 / SATA Express Enabling 129
10.1.10.3 SATA1B / PCIe11 mSATA /M.2 / SATA Express Enabling 129
10.1.10.4 SATA2 / PCIe12 mSATA /M.2 / SATA Express Enabling 130

A FAQ and Troubleshooting 131

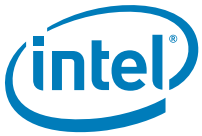


Figures

3-1 SPI Timing 21
3-2 PCH Test Load 22
4-1 Flash Descriptor (Skylake PCH-LP) 23
5-1 SFDP Read Instruction Sequence 41

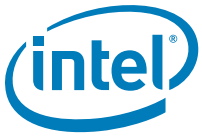
Tables

1-1 Terminology 14
1-2 Reference Documents 14
3-1 SPI Timings (20 MHz) 20
3-2 SPI Timings (33 MHz) 20
3-3 SPI Timings (50 MHz) 21
4-1 Region Access Control Table Options 36
4-2 Recommended Read/Write Settings for Platforms 37
4-3 Jidn - JEDEC ID Portion of Intel® ME VSCC Table 38
4-4 Vsccn – Vendor-Specific Component Capabilities Portion of the Skylake PCH-LP Platforms 38
6-1 VSCC0 - Vendor-Specific Component Capabilities Register for SPI Component 0 45
6-2 VSCC1 - Vendor Specific Component Capabilities Register for SPI Component 1 47
6-3 Description of How WSR and WEWS is Used 48
10-1 HSIO Lane Muxing Selection 121



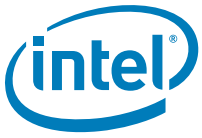
Revision History

Document Number	Revision Number	Description	Revision Date
550696	0.72	• Initial release	July 2014
550696	0.8	• Updated Chapter 10 with major changes • Update on SKL SPI architecture description, Chap2, Chap3 • PCH Strap Length (PSL) corrected to be 41h	August 2014
	0.81	• Updated 9.242 CPU Descriptor Record 0 • Updated Strap setting defaults to align with the RVP3 CRB • Added back the FIT tool setting visible column in Chapter 9	September 2014
	0.82	• Added Intel® Trace Hub Soft Enable and Intel® Trace Hub Debug Messages Enable strap settings • Added SATA / PCIe GP Select for Port setting information	October 2014
	0.83	• Corrected Offset 0x1BD reserved bit 6 which was incorrectly listed as set to '1'. • Added new CPU strap data • Default value changed for offset 0x1C0 • Added note on PCIe Controller 3 differences for Base U and Premium Y configurations.	October 2014
	0.84	• Changed setting references for Intel® Trace Hub Debug Messages Enable strap from ROM to PCH. • Integrated wired LAN Enable strap offset changed from 0x1BC to 0x1C0 • PCH Strap Length (PSL) corrected to 42h	November 2014
	0.85	• SSIC Combo Port 2 setting at offsets 0x16C, 0x17E and 0x1B9 removed no longer POR for SKL-LP. • Corrected value for offset 0x149 in the Configuration Dependencies chapter for Intel® Integrated LAN Controller Enabling. • Changed offset 0x1BF designation from t36b to tPCH33 to align with EDS • Default values changed for offsets 0x1D8 thru 0x1DD, 0x1E0 thru 1E2, 0x1E8 and 0x1EA • Default value changed for offset 0x1BC	December 2014
	0.86	• Updated offset 0x155 with additional information to properly configure SATA Express devices. • Removed 120MHz and 60MHz frequency settings offset 0x1F5 (SPI TPM Clock Frequency) not POR for Skylake. • Default value for 0x1BF bit 2 updated. • Changed default value SMLink0 Frequency (0x12A).	January 2015
	0.86.1	• Added OPI configuration settings and descriptions at offsets 0x1C4, 0x205 and 0x207. • Added ISH Supported settings and description at offset 0x1C0	January 2015
	0.86.2	• Updated CPU Strap section with updated parameter descriptions. • Updated default value for offset 0x1F4 bits [6:4] • Updated SPIBAR address offset information in section 6.3 • FLREG8 missing address offset information. • Corrected offset 0x1BF shown as bits [7:2] should be bits [7:4]. • Corrected offset 0x1B9 shown as bits [7:0] should be bits [7:2] • Added change to 0x1BF for Bit 2 noting difference in settings on A-Step and B-Step PCH.	January 2015
	0.86.3	• Removed offset 0x164 bits [4:3] feature not POR for Skylake.	February 2015
	0.86.4	• Removed RST Controller 1 settings at offsets 0x154, 0x155, 0x158, 0x19F and Configuration Dependencies Chapter 10 not POR for Skylake-LP per PCH LP EDS.	February 2015



Document Number	Revision Number	Description	Revision Date
	0.86.5	• Removed CLink setting at offset 0x140 configuration of this signal will be handled by Intel® ME firmware. • Corrected default value for offset 0x1C4 was listed as 0x0 should have been 0x10.	February 2015
	0.86.6	• Changed note on Dual Output Fast Read Supported setting. • Updated 0x1C4 with additional USB3 / SSIC setting information.	March 2015
	0.86.7	• Added APWROK Timing strap setting to 0x1BE. • Changed default value for offset 0x164 bits [4:3]. • Changed 0x116 bits [1:0] default value from 0x3 to 0x0 and the option will no longer be exposed in the FIT UI. • Corrected CPU Strap SA VR Type default value was set to 0x1 should have been 0x0 • Changed t573 (offset 0x1BD) default value from 100ms to 1ms • Changes default value for offset 0x1CC from 0x3 to 0x0. • Changed default value for offset 0x190 from 0x3 to 0x1. • Corrected offset 0x1C4 Reserved bit range incorrectly labeled [30:3] should be [31:5]	March 2015
	0.86.8	• Updated invalid instruction value defaults for FLILL and FLILL1 • Added SPI Voltage Select offset 0x1F2 bit 7. • Changed offset 0x1BD bits [1:0] designation from t573 to tPCH45 to align with EDS. • Changed offset 0x1BD bit [3:2] designation from t1001 to tPCH46 to align with EDS.	April 2015
	0.86.9	• Changed default value for offset 0x1F5 bit [7:3] was 0x0 should be 0x10 • Changed default values for Intel® RST strap settings from x2 to x4	May 2015
	0.87.0	• Changed default value for offset 0x100 bit [17] was 0x0 should be 0x1 • Changed default value for offset 0x100 bit [23] was 0x0 should be 0x1 • Corrected default value for Intel® RST strap settings back to x2 for LP	May 2015

§ §



1 Introduction

1.1 Overview

This manual is intended for OEMs and software vendors to clarify various aspects of programming the SPI flash on PCH family based platforms. The current scope of this document is for Intel® microarchitecture code name Skylake PCH-LP only.

Chapter 2, “PCH SPI Flash Architecture”

- Overview of SPI flash, Descriptor, Flash Layout, compatible SPI flash.

Chapter 3, “PCH SPI Flash Compatibility Requirement”

- Overview of compatibility requirements for Skylake PCH-LP products.

Chapter 4, “Descriptor Overview”

- Overview of the descriptor and Descriptor record definition

Chapter 5, “Serial Flash Discoverable Parameter (SFDP) Overview”

- Overview of the SFDP definition.

Chapter 6, “Configuring BIOS/GbE for SPI Flash Access”

- Describes how to configure BIOS/GbE for SPI flash access.

Chapter 7, “Intel® ME Disable for Debug/Flash Burning Purposes”

- Methods of disabling Intel Management Engine for debug purposes.

Chapter 8, “Recommendations for SPI Flash Programming in Manufacturing Environments”

- Recommendations for manufacturing environments.

Chapter 9, “Flash Descriptor PCH / CPU Configuration Section”

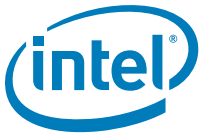
- Flash Descriptor PCH / CPU Soft Strap Section.

Chapter 10, “Configuration Dependencies”

- Descriptor configuration dependencies for enabling Skylake Hardware I/O, Bus and GPIO components.

Appendix A, “FAQ and Troubleshooting”

- Frequently asked questions and Troubleshooting tips.



1.2 Terminology

Table 1-1. Terminology

Term	Description
BIOS	Basic Input-Output System
CRB	Customer Reference Board
FPT	Flash Programming Tool - programs the SPI flash
FIT	Flash Image Tool – creates a flash image from separate binaries
FW	Firmware
FWH	Firmware Hub – LPC based flash where BIOS may reside
GbE	Intel Integrated 1000/100/10
HDCP	High-bandwidth Digital Content Protection
Intel® AMT	Intel® Active Management Technology
Skylake PCH-LP	Skylake Platform Integrated I/O
Intel® Management Engine Firmware (Intel® ME FW)	Intel firmware that adds Intel® Active Management Technology, Castle Peak, Sentry Peak, etc.
Intel PCH	Intel Platform Controller Hub
Intel PCHn family	All PCHn derivatives including PCHn (desktop) and PCHnM (mobile)
LPC	Low Pin Count Bus- bus on where legacy devices such a FWH reside
LVSCC	Lower Vendor Specific Component Capabilities
PCH	Platform Controller Hub
PCH–LP	Platform Controller Hub – Low Power
SFDP	Serial Flash Discoverable Parameter
SPI	Serial Peripheral Interface – refers to serial flash memory in this document
UVSCC	Upper Vendor Specific Component Capabilities
VSCC	Vendor Specific Component Capabilities

1.3 Reference Documents

Table 1-2. Reference Documents

Document	Document # / Location
Skylake PCH-LP External Design Specification (EDS)	Contact your Intel field representative.
Intel Flash Image Tool (FIT)	\System Tools\Flash Image Tool of latest Intel® ME kit from VIP. The Kit MUST match the platform you intend to use the flash tools for.
Intel Flash Programming Tool (FPT)	\System Tools\Flash Programming Tool of latest Intel® ME from VIP. The Kit MUST match the platform you intend to use the flash tools for.
FW Bring Up Guide	Root directory of latest Intel® Management Engine kit from VIP. The Kit MUST match the platform you intend to use the flash tools for.

§ §

2 PCH SPI Flash Architecture

2.1 Descriptor Mode

The Skylake Platform supports up to two SPI flash devices. The flash connected to Chip Select 0 must contain a valid Descriptor as defined in Section 4. The contents of the Descriptor provide platform configuration and enable the PCH to securely manage storage among multiple users/purposes.

SPI flash must be connected directly to the PCH SPI bus.

Note: **Skylake only supports Descriptor mode.**

See ***SPI Supported Feature Overview*** of the latest Intel Platform Controller Hub Family External Design Specification (EDS) for Skylake PCH-LP Family for more detailed information.

2.2 Serial Flash Discoverable Parameter (SFDP)

Serial flash with SFDP have their supported capabilities and commands stored inside the serial flash devices. The controller will discover the attributes needed to operate.

Skylake PCH-LP requires SPI flash devices support JEDEC standard JESD216 SDFDP (Serial Flash Discoverable Parameters. Revision A (JESD216A) or later is strongly recommended but not mandatory. SFDP provides a consistent method of describing the functional and feature capabilities of SPI devices in a standard set of internal parameter tables. These parameter tables can be interrogated by PCH to enable adjustment needed to accommodate divergent feature from multiple vendors.

Please refer to Chapter 5, “Serial Flash Discoverable Parameter (SFDP) Overview” for more information.

2.3 SPI Fast Read

Note: See ***SPI for Flash*** section of the latest Intel Platform Controller Hub Family External Design Specification (EDS) for Skylake PCH-LP Family for more detailed information.50-MHz support requires SPI component that meet 66-MHz timing.

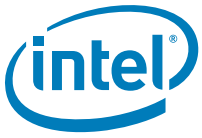
2.4 Intel® Trusted Platform Module (Intel® TPM) on SPI Bus

Skylake PCH-LP Family supports Intel TPM on the SPI bus.

See ***Serial Peripheral Interface (SPI)*** section of the latest Intel Platform Controller Hub Family External Design Specification (EDS) for Skylake PCH-LP Family for more detailed information.

2.5 Boot Flow for Skylake PCH-LP Family

See Boot BIOS strap in the **Functional Straps** of the latest Intel Platform Controller Hub Family External Design Specification (EDS) for Skylake PCH-LP Family for more detailed information.



See Chapter 4, “Descriptor Overview” for more detailed information.

2.6 Flash Regions

The controller can divide the SPI flash into separate regions below.

Region	Content
0	Descriptor
1	BIOS
2	ME – Intel® Management Engine Firmware (Intel® ME FW)
3	GbE – Location for Integrated LAN firmware and MAC address
4	PDR – Platform Data Region (Optional)[1]
8	Embedded Controller (EC)

Notes:

1. The PDR region is optional and is not applicable for Skylake PCH-LP or not required for proper platform operation.

See ***SPI Flash Regions*** section of the latest Intel Platform Controller Hub Family External Design Specification (EDS) for Skylake PCH-LP Family for more detailed information.

2.6.1 Flash Region Sizes

SPI flash space requirements differ by platform and configuration. Please refer to documentation specific to your platform for BIOS and ME Region flash size estimates.

See ***SPI Flash Regions*** section of the latest *Intel Platform Controller Hub Family External Design Specification (EDS)* for Skylake PCH-LP Family for more detailed information.

2.7 Hardware Sequencing

Host/Bios and ME may read/write /erase flash via Hardware Sequencing or Software Sequencing registers.

Skylake Hardware sequencing has been enhanced to include all operations the BIOS needs to perform.

Note: Host / Bios Software Sequencing is not supported in Skylake.

Hardware sequencing has a predefined list of opcodes, the PCH discovers the 4k and 64k erase opcodes via SFDP.

See ***Serial Peripheral Interface Memory Mapped Configuration Registers*** in *Skylake PCH-LP Family External Design Specification (EDS)* for more details.

§ §

3 PCH SPI Flash Compatibility Requirement

3.1 Skylake PCH-LP SPI Flash Requirements

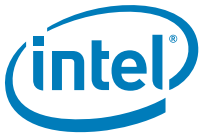
- Skylake PCH-LP Family allows for up to two SPI flash devices to store BIOS, Intel® ME FW and integrated LAN information.
  - **— Intel® ME FW is required for Skylake PCH-LP Family-based platforms**
  - — Each SPI component can support up to 64 MB (128 MB total addressable) using 26-bit addressing
- 3.3V or 1.8V SPI I/O buffer VCC
- SPI Fast Read instruction is supported and frequency of 17 MHz, 30 MHz and 48 MHz
- SPI Dual Output and Dual I/O Fast Read instruction is supported with frequency of 17 MHz, 30 MHz and 48 MHz
- SPI Quad Output and Quad I/O Fast read instruction is supported with frequency of 17 MHz, 30 MHz and 48 MHz

If there are two SPI components, both components have to support fast read in order to enable Fast Read in PCH.

Enabling Quad mode reads may require special configuration of the flash device during platform manufacturing, prior to first boot. No special configuration is required for flash devices that support Quad mode but do not contain a Quad Enable (QE) bit. Flash devices that contain a QE bit must be configured with QE=1. Several manufacturers offer SKU's with QE=1 by default.

3.1.1 General Requirements

- Erase size capability of: 4 KBytes erase must be supported uniformly across the flash array. If 64k erase is also supported, then it must be supported uniformly across the flash array.
- Serial flash device must ignore the upper address bits such that an address of FFFFFFh aliases to the top of the flash memory.
- SPI Compatible Mode 0 support: Clock phase is 0 and data is latched on the rising edge of the clock.
- If the device receives a command that is not supported or incomplete (less than 8 bits), the device must discard the cycle gracefully without any impact on the flash content.
- An erase command (page, sector, block, chip, etc.) must set all bits inside the designated area (page, sector, block, chip, etc.) to 1 (Fh).
- Status Register bit 0 must be set to 1 when a write, erase or write to status register is in progress and cleared to 0 when a write or erase is NOT in progress.
- Devices requiring the Write Enable command must automatically clear the Write Enable Latch at the end of Data Program instructions.



- The flexibility to perform a write between 1 byte to 64 bytes is required.
- SFDP fields: dword 1, bit 4 “Write Enable Instruction”. Dword 1, bit 3 “Volatile Status Register”, both bits must be 0.

Intel Management Firmware must meet the SPI flash based BIOS Requirements plus:

- 2.2 Serial Flash Discoverable Parameter (SFDP)
- 3.1.4 JEDEC ID (Opcode 9Fh)
- 3.1.5 Multiple Page Write Usage Model
- 3.1.6 Hardware Sequencing Requirements

Write protection scheme must meet guidelines as defined in SPI Flash Unlocking Requirements for Intel Management Engine.

SPI Flash Unlocking Requirements for Intel Management Engine

a. Flash devices must be globally unlocked (read, write and erase access on the ME region) from power on by writing 0 to the Block Protect bits in the flash’s status register to disable write protection.

b. If the status register must be unprotected, it must use the write enable 06h instruction.

c. Opcode 01h (write to status register) must then be used to write 0 to the Block Protect bits in the status register. If the device contains a Quad Enable bit in the status register, then firmware must perform a read-modify-write to prevent changing the state of the QE bit when writing to the status register. This must unlock the entire part. If the SPI flash’s status register has non-volatile bits that must be written to, bits [5:2] of the flash’s status register must be all 0h to indicate that the flash is unlocked.

3.1.2 Bios Requirement

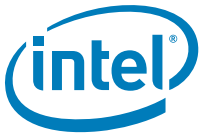
BIOS must ensure there is no SPI flash based read/write/erase protection on the GbE region. GbE firmware and drivers for the integrated LAN need to be able to read, write and erase the GbE region at all times.

3.1.3 Software / Firmware Requirements

The recommended Intel ME firmware flow for clearing block protect is:

1. Determine the location of the Quad Enable (QE) bit using the SFDP table QER field (for devices that support SFDP rev A or later) or the VSCC table QER field (for SDFDP rev -)
2. Read status registers 1 and 2.
3. Modify status to clear Block Protect bits and leave QE bit unchanged.
4. Write the status register using an atomic {write_enable, write_status} sequence (this happens automatically when hardware sequencing is used.
5. Issue a write_disable instruction using software sequencing.

After global unlock, BIOS has the ability to lock down small sections of the flash as long as they do not involve the ME or GbE region. See 6.1 Unlocking SPI Flash Device Protection for Skylake PCH-LP Platform and 6.2 Locking SPI Flash via Status Register for more information about flash based write/erase protection.



3.1.4 JEDEC ID (Opcode 9Fh)

Since each serial flash device may have unique capabilities and commands, the JEDEC ID is the necessary mechanism for identifying the device so the uniqueness of the device can be comprehended by the controller (master). The JEDEC ID uses the opcode 9Fh and a specified implementation and usage model. This JEDEC Standard Manufacturer and Device ID read method is defined in Standard JESD21-C, PRN03-NV1 and is available on the JEDEC website: www.jedec.org.

3.1.5 Multiple Page Write Usage Model

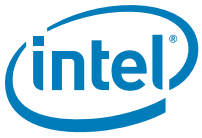
Intel platforms have firmware usage models require that the serial flash device support multiple writes to a page (minimum of 512 writes) without requiring a preceding erase command. BIOS commonly uses capabilities such as counters that are used for error logging and system boot progress logging. These counters are typically implemented by using byte-writes to 'increment' the bits within a page that have been designated as the counter. The Intel firmware usage models require the capability for multiple data updates within any given page. These data updates occur via byte-writes without executing a preceding erase to the given page. Both the BIOS and Intel Management Engine firmware multiple page write usage models apply to sequential and non-sequential data writes.

Flash parts must also support the writing of a single byte 1024 times in a single 256-byte page without erase. There will be 64 pages where this usage model will occur. These 64 pages will be every 16 kilobytes.

3.1.6 Hardware Sequencing Requirements

The following table contains a list of commands and the associated opcodes that a SPI-based serial flash device must support in order to be compatible with hardware sequencing.

Commands	OPCODE	Notes
Write to Status Register	01h	Writes a byte to SPI flash's status register. Enable Write to Status Register command must be run prior to this command
Program Data	02h	Single byte or 64 byte write as determined by flash part capabilities and software
Read Data	03h	
Write Disable	04h	
Read Status	05h	Outputs contents of SPI flash's status register
Write Enable	06h	
Fast Read	0Bh	
Enable Write to Status Register	06h	If write-status 01h requires a write-enable, then 06h must enable write-status.
Erase	Programmable/ Discoverable	4 Kbyte erase. Uses the value from SFDP (if available) else value from VSCCn Erase Opcode register value
Chip Erase	C7h and/or 60	
JEDEC ID	9Fh	See Section 3.1.4 for more information
Dual Output Fast Read	3Bh/ Discoverable	Discoverable opcodes are obtained from each component's SFDP table
Dual I/O Fast Read	Discoverable	Opcode is optained from each component's SFDP table
Quad I/O Fast Read	Discoverable	Opcode is optained from each component's SFDP table



3.2 Skylake PCH-LP SPI AC Electrical Compatibility Guidelines

Table 3-1. SPI Timings (20 MHz)

Sym	Parameter	Min	Max	Units	Notes
t180a	Serial Clock Frequency - 20MHz Operation	17.06	18.73	MHz	1
t183a	Tco of SPI_MOSI with respect to serial clock falling edge at the host	-5	13	ns	
t184a	Setup of SPI_MISO with respect to serial clock falling edge at the host	16	-	ns	
t185a	Hold of SPI_MISO with respect to serial clock falling edge at the host	0	-	ns	
t186a	Setup of SPI_CS[1:0]# assertion with respect to serial clock rising edge at the host	30	-	ns	
t187a	Hold of SPI_CS[1:0]# assertion with respect to serial clock rising edge at the host	30	-	ns	
t188a	SPI_CLK High time	26.37	-	ns	2
t189a	SPI_CLK Low time	26.82	-	ns	2

Notes:
1. Typical clock frequency driven by Skylake PCH-LP Family is 17.86 MHz.
2. Measurement point for low time and high time is taken at.5(VccME3_3).

Table 3-2. SPI Timings (33 MHz)

Sym	Parameter	Min	Max	Units	Notes
t180b	Serial Clock Frequency - 33 MHz Operation	29.83	32.81	MHz	1
t183b	Tco of SPI_MOSI with respect to serial clock falling edge at the host	-5	5	ns	
t184b	Setup of SPI_MISO with respect to serial clock falling edge at the host	8	-	ns	
t185b	Hold of SPI_MISO with respect to serial clock falling edge at the host	0	-	ns	
t186b	Setup of SPI_CS[1:0]# assertion with respect to serial clock rising edge at the host	30	-	ns	
t187b	Hold of SPI_CS[1:0]# assertion with respect to serial clock rising edge at the host	30	-	ns	
t188b	SPI_CLK High time	14.88	-	ns	2
t189b	SPI_CLK Low time	15.18	-	ns	2

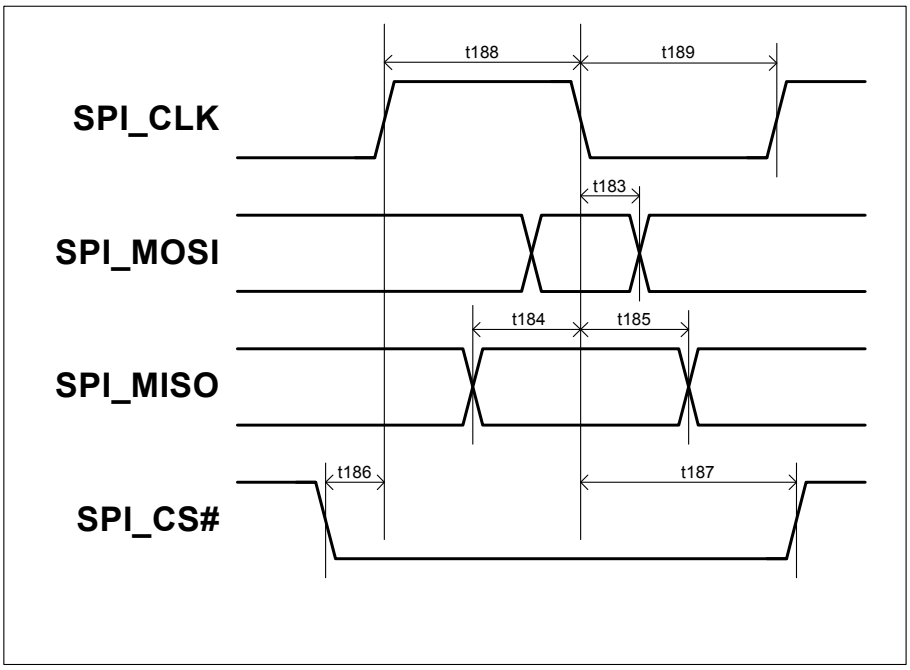
Notes:
1. Typical clock frequency driven by Skylake PCH-LP Family is 31.25 MHz.
2. Measurement point for low time and high time is taken at.5(VccME3_3).

Table 3-3. SPI Timings (50 MHz)

Sym	Parameter	Min	Max	Units	Notes
t180c	Serial Clock Frequency - 50 MHz Operation	46.99	53.40	MHz	1
t183c	Tco of SPI_MOSI with respect to serial clock falling edge at the host	-3	3	ns	
t184c	Setup of SPI_MISO with respect to serial clock falling edge at the host	8	-	ns	
t185c	Hold of SPI_MISO with respect to serial clock falling edge at the host	0	-	ns	
t186c	Setup of SPI_CS[1:0]# assertion with respect to serial clock rising edge at the host	30	-	ns	
t187c	Hold of SPI_CS[1:0]# assertion with respect to serial clock rising edge at the host	30	-	ns	
t188c	SPI_CLK High time	7.84	-	ns	2, 3
t189c	SPI_CLK Low time	11.84	-	ns	2, 3

Notes:
1. Typical clock frequency driven by Skylake PCH-LP Family is 50 MHz.
2. When using 50 MHz mode ensure target flash component can meet t188c and t189c specifications. Recommended to use SPI flash component rated at 66 MHz or faster.
3. Measurement point for low time and high time is taken at.5(VccME3_3).

Figure 3-1. SPI Timing

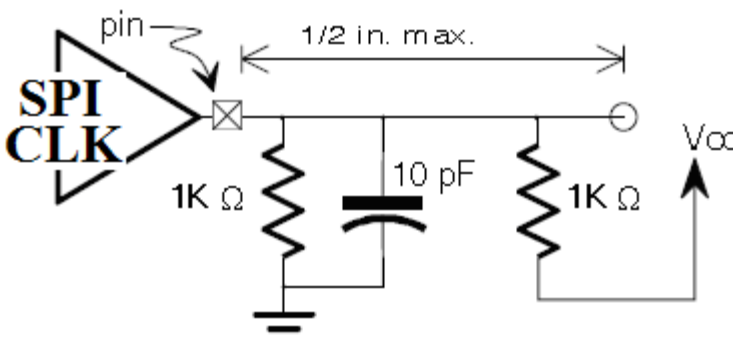


3.3 SPI Flash DC Electrical Compatibility Guidelines

Parameter	Min	Max	Units	Notes
Supply Voltage (Vcc)	3.14	3.7	V	
Input High Voltage	0.5*VCC	VCC+0.5	V	
Input Low Voltage	-0.5	0.3*VCC	V	
Output High Characteristics	0.9*VCC	VCC	V	Ioh = -0.5mA
Output Low Characteristics		0.1*VCC		Iol = 1.5mA
Input Leakage Current	-10	10	uA	
Output Rise Slew Rate (0.2 Vcc - 0.6 Vcc)	1	4	V/ns	1
Output Fall Slew Rate (0.6 Vcc - 0.2 Vcc)	1	4	V/ns	1

Note:
1. Testing condition: 1K pull up to Vcc, 1kohm pull down and 10 pF pull down and 1/2 inch trace. See Figure 3.3 for more detail.

Figure 3-2. PCH Test Load



§ §

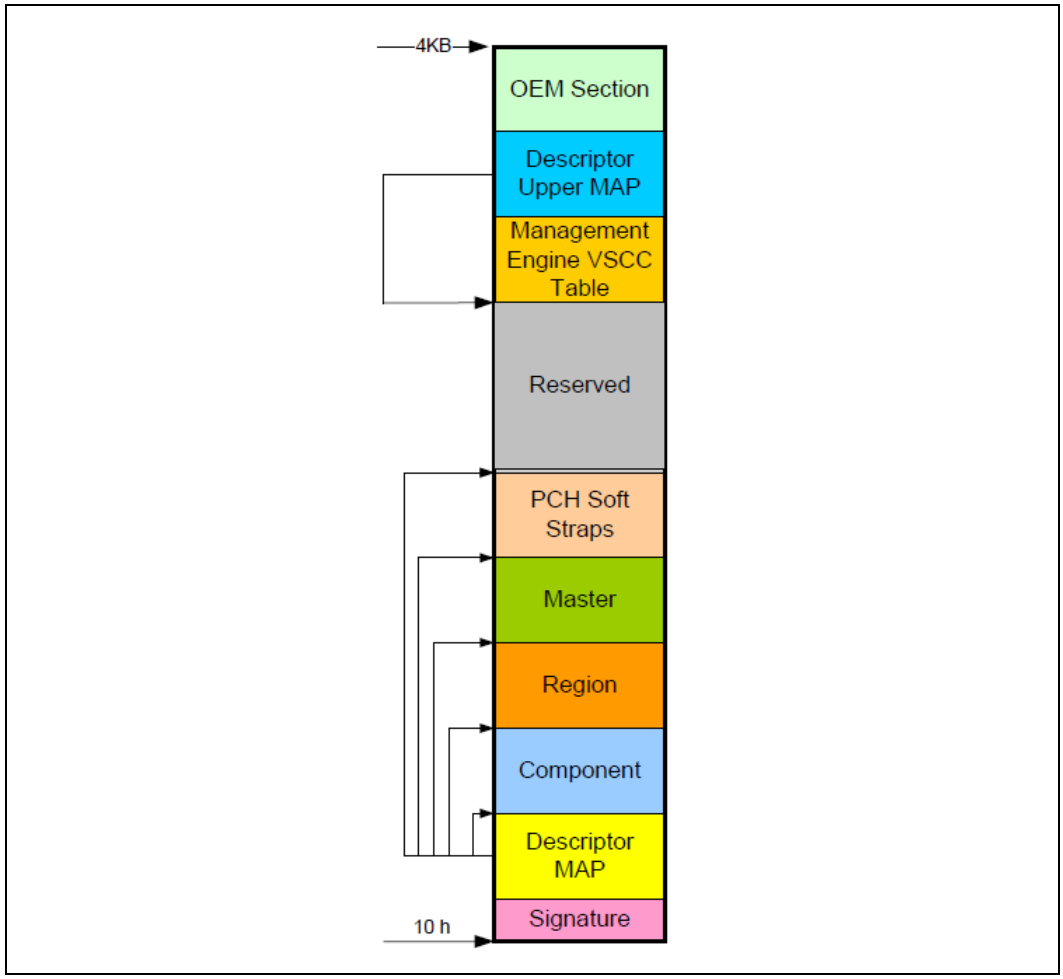
4 Descriptor Overview

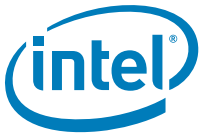
The Flash Descriptor is a data structure that is programmed on the SPI flash part on Skylake PCH-LP based platforms. The Descriptor data structure describes the layout of the flash as well as defining configuration parameters for the PCH. The descriptor is on the SPI flash itself and is not in memory mapped space like PCH programming registers. The maximum size of the Flash Descriptor is 4 KBytes. It requires its own discrete erase block, so it may need greater than 4 KBytes of flash space depending on the flash architecture that is on the target system.

The information stored in the Flash Descriptor can only be written during the manufacturing process as its read/write permissions must be set to Read Only when the computer leaves the manufacturing floor.

The Descriptor has 9 parts:

Figure 4-1. Flash Descriptor (Skylake PCH-LP)





- The Flash signature at the bottom of the flash (offset 10h) must be 0FF0A55Ah in order to be in Descriptor mode.
- The Descriptor map has pointers to the lower five descriptor sections as well as the size of each.
- The Component section has information about the SPI flash part(s) the system. It includes the number of components, density of each component, read, write and erase frequencies and invalid instructions.
- The Region section defines the base and the limit of the BIOS, ME, GbE, PDR (Optional), Embedded Controller (EC) and regions as well as their size.
- The master region contains the hardware security settings for the flash, granting read/write permissions for each region and identifying each master.
- PCH chipset soft strap sections contain PCH configurable parameters.
- The Reserved region is for future chipset usage.
- The Descriptor Upper Map determines the length and base address of the Intel® ME VSCC Table.
- The Intel® ME VSCC Table holds the JEDEC ID and the ME VSCC information for all the SPI Flash part(s) supported by the NVM image. BIOS and GbE write and erase capabilities depend on VSCC0 and VSCC1 registers in SPIBAR memory space.
- OEM Section is 256 Byte section reserved at the top of the Flash Descriptor for use by the OEM.

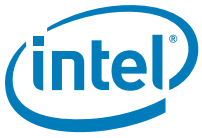
See ***SPI Supported Feature Overview*** and ***Flash Descriptor Records*** in the *Skylake PCH-LPH Family External Design Specification (EDS)*.

4.1 Flash Descriptor Content

The following sections describe the data structure of the Flash Descriptor on the SPI device. These are not registers or memory space within PCH. FDBAR - is address 0x0 on the SPI flash device on chip select 0.

Recommended flash descriptor map:

Region Name	Starting Address
Signature	0x10
Component FCBA	0x30
Regions FRBA	0x40
Masters FMBA	0x80
PCH Straps FPSBA	0x100
CPU Straps FCPUSBA	0x300
Register Init FIBA	0x340



4.1.1 Descriptor Signature and Map

4.1.1.1 FLVALSIG - Flash Valid Signature (Flash Descriptor Records)

Memory Address:FDBAR + 010h Size: 32 bits

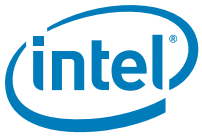
Recommended Value:0FF0A55Ah

Bits	Description
31:0	**Flash Valid Signature.** This field identifies the Flash Descriptor sector as valid. If the contents at this location contain 0FF0A55Ah, then the Flash Descriptor is considered valid and it will operate in Descriptor Mode (**Note:** Non-Descriptor mode is not supported for Skylake).

4.1.1.2 FLMAP0 - Flash Map 0 Register (Flash Descriptor Records)

Memory Address: FDBAR + 014h Size: 32 bits

Bits	Description
31:27	Reserved
26:24	**Reserved**
23:16	**Flash Region Base Address (FRBA).** This identifies address bits [11:4] for the Region portion of the Flash Descriptor. Bits [24:12] and bits [3:0] are 0. Set this value to 04h. This will define FRBA as 40h.
15:13	Reserved
12	**Reserved. Set to '0'**
11	**Reserved. Set to '0'**
10	Reserved
9:8	**Number Of Components (NC)**. This field identifies the total number of Flash Components. Each supported Flash Component requires a separate chip select. 00 = 1 Component 01 = 2 Components All other settings = Reserved
7:0	**Flash Component Base Address (FCBA)**. This identifies address bits [11:4] for the Component portion of the Flash Descriptor. Bits [24:12] and bits [3:0] are 0. set this field to 03h. This will define FCBA as 30h



4.1.1.3 FLMAP1 - Flash Map 1 Register (Flash Descriptor Records)

Memory Address: FDBAR + 018h Size: 32 bits

Recommended Value: 41100208h

Bits	Description
31:24	**PCH Strap Length (PSL).** Identifies the 1s based number of Dwords of PCH Straps to be read, up to 255 DWs (1KB) max. A setting of all 0's indicates there are no PCH DW straps. This field **MUST** be set to 42h
23:16	**Flash PCH Strap Base Address (FPSBA).** This identifies address bits [11:4] for the PCH Strap portion of the Flash Descriptor. Bits [24:12] and bits [3:0] are 0. Set this field to 10h. This will define FPSBA to 100h
15:11	Reserved
10:8	**Number Of Masters (NM).** This field identifies the total number of Flash Masters. Set this field to 10b
7:0	**Flash Master Base Address (FMBA).** This identifies address bits [11:4] for the Master portion of the Flash Descriptor. Bits [24:12] and bits [3:0] are 0. Set this field to 08h. This will define FMBA as 80h

4.1.1.4 FLMAP2—Flash Map 2 Register (Flash Descriptor Records)

Memory Address: FDBAR + 01Ch Size: 32 bits

Bits	Description
31:24	**Register Init Length (RIL):** Identifies the 1's based number of register initialization entries. If this field is set to 0, then there are no Register Init entries to send. Each register init entry is 2DW in length. Set this field to 0h.
23:16	Reserved. Set this field to 31h.
15:08	**CPU Strap Length (CPUSL).** Identifies the 1's based number of Dwords of Processor Straps to be read, up to 255 DWs (1KB) max. A setting of all 0's indicates there are no Processor DW straps. Set this field to 03h.
7:0	**Flash CPU Strap Base Address (FCPUSBA).** This identifies address bits [11:4] for the Processor Strap portion of the Flash Descriptor. Bits [24:12] and bits [3:0] are 0. Set this field to 30h. This will define FCPUSBA as 300h



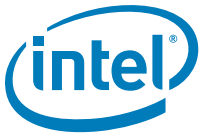
4.1.2 Flash Descriptor Component Section

4.1.2.1 FLCOMP—Flash Components Register (Flash Descriptor Records)

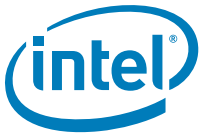
The following section of the Flash Descriptor is used to identify the different SPI Flash Components and their capabilities.

Memory Address: FCBA + 000h Size: 32 bits

Bits	Description
31	Reserved
30	**Dual Output Fast Read Support** 0 : Dual Output Fast Read is not supported 1 : Dual Output Fast Read is supported ***Notes:*** 1. This setting is no longer required and has deprecated in Skylake.
29:27	**Read ID and Read Status Clock Frequency**. 010 = 48 MHz 100 = 30 MHz 110 = 17 MHz All other Settings = Reserved ***Notes:*** 1. If more than one Flash component exists, this field must be set to the lowest common frequency of the different Flash components. 2. If setting to 48 MHz, ensure flash meets timing requirements defined in Table 3-3
26:24	**Write and Erase Clock Frequency**. 010 = 48 MHz 100 = 30 MHz 110 = 17 MHz All other Settings = Reserved ***Notes:*** 1. If more than one Flash component exists, this field must be set to the lowest common frequency of the different Flash components. 2. If setting to 48 MHz, ensure flash meets timing requirements defined in Table 3-3
23:21	**Fast Read Clock Frequency**. This field identifies the frequency that can be used with the Fast Read instruction. This field is undefined if the Fast Read Support field is '0'. 010 = 48 MHz 100 = 30 MHz 110 = 17 MHz All other Settings = Reserved ***Notes:*** 1. If more than one Flash component exists, this field must be set to the lowest common frequency of the different Flash components. 2. If setting to 48 MHz, ensure flash meets timing requirements defined in Table 3-3
20	**Fast Read Support**. 0 = Fast Read is not Supported 1 = Fast Read is supported If the Fast Read Support bit is a '1' and a device issues a Direct Read or issues a read command from the Hardware Sequencer and the length is greater than 4 bytes, then the SPI Flash instruction should be “Fast Read”. If the Fast Read Support is a '0' or the length is 1-4 bytes, then the SPI Flash instruction should be “Read”. Reads to the Flash Descriptor always use the Read command independent of the setting of this bit. ***Notes:*** 1. If more than one Flash component exists, this field can only be set to '1' if both components support Fast Read. 2. It is strongly recommended to set this bit to 1b



Bits	Description
19:17	**Read Clock Frequency**. 110= 17MHz All other Settings = Reserved ***Note:*** 1. If more than one Flash component exists, this field must be set to the lowest common frequency of the different Flash components.
16:8	Reserved
7:4	**Component 1 Density.** (C1DEN) This field identifies the size of the 2nd Flash component connected directly to the PCH. If there is not 2nd Flash component, the contents of this field should be read as "1111b" 0000 = 512 KB 0001 = 1 MB 0010 = 2 MB 0011 = 4 MB 0100 = 8 MB 0101 = 16 MB 0110 = 32 MB 0111 = 64 MB 1000 - 1110 = Reserved ***Note:*** This field is defaulted to "1111b" after reset ***Note:*** C1DEN field will be **ignored** if FLMAP0.NC bit [9:8] is set to 00 i.e. 1 component only.
3:0	**Component 0 Density (C0DEN).** This field identifies the size of the 1st or only Flash component connected directly to the PCH. 0000 = 512 KB 0001 = 1 MB 0010 = 2 MB 0011 = 4 MB 0100 = 8 MB 0101 = 16 MB 0110 = 32 MB 0111 = 64 MB 1000 - 1111 = Reserved ***Note:*** This field is defaulted to "0101b" (16MB) after reset.



4.1.2.2 FLILL—Flash Invalid Instructions Register (Flash Descriptor Records)

Memory Address: FCBA + 004h Size: 32 bits

Bits	Description
31:24	**Invalid Instruction 3**. **Default set to 0xAD** See definition of Invalid Instruction 0
23:16	**Invalid Instruction 2**. **Default set to 0x60** See definition of Invalid Instruction 0
15:8	**Invalid Instruction 1**. **Default set to 0x42** See definition of Invalid Instruction 0
7:0	**Invalid Instruction 0**. **Default set to 0x21** ***Note:*** Opcode for an instruction that the Flash Controller should protect against, such as Chip Erase. This byte should be set to 0 if there are no invalid instructions to protect against for this field. Opcodes programmed in the Software Sequencing Opcode Menu Configuration and Prefix-Opcode Configuration are not allowed to use any of the Invalid Instructions listed in this register.

4.1.2.3 FLILL1—Flash Invalid Instructions Register (Flash Descriptor Records)

Memory Address: FCBA + 008h Size: 32 bits

Bits	Description
31:24	**Invalid Instruction 7**. **Default set to C7** See definition of Invalid Instruction 0
23:16	**Invalid Instruction 6**. **Default set to 0xC4** See definition of Invalid Instruction 0
15:8	**Invalid Instruction 5**. **Default set to 0xB9** See definition of Invalid Instruction 0



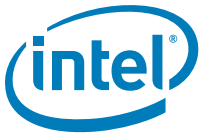
Bits	Description
7:0	**Invalid Instruction 4**. **Default set to 0xB7** See definition of Invalid Instruction 0

4.1.3 Flash Descriptor Region Section

The following section of the Flash Descriptor is used to identify the different Regions of the NVM image on the SPI flash.

Flash Regions:

- If a particular region is not using SPI Flash, the particular region should be disabled by setting the Region Base to all 1's, and the Region Limit to all 0's (base is higher than the limit)
- For each region except FLREG0, the Flash Controller must have a default Region Base of 7FFFh and the Region Limit to 0000h within the Flash Controller in case the Number of Regions specifies that a region is not used.



4.1.3.1 FLREG0—Flash Region 0 (Flash Descriptor) Register (Flash Descriptor Records)

Memory Address: FRBA + 000h Size: 32 bits

Recommended Value: 00000000h

Bits	Description
31	Reserved
30:16	**Region Limit.** This specifies bits 26:12 of the ending address for this Region. ***Notes:*** 1. Set this field to 0b. This defines the ending address of descriptor as being FFFh. 2. Region limit address Bits[11:0] are assumed to be FFFh
15	Reserved
14:0	**Region Base.** This specifies address bits 26:12 for the Region Base. ***Note:*** Set this field to all 0s. This defines the descriptor address beginning at 0h.

4.1.3.2 FLREG1—Flash Region 1 (BIOS) Register (Flash Descriptor Records)

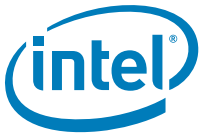
Memory Address: FRBA + 004h Size: 32 bits

Bits	Description
31	Reserved
30:16	**Region Limit.** This specifies bits 26:12 of the ending address for this Region. ***Notes:*** 1. Must be set to 0000h if BIOS region is unused (on Firmware hub) 2. Ensure BIOS region size is a correct reflection of actual BIOS image that will be used in the platform 3. Region limit address Bits[11:0] are assumed to be FFFh
15	Reserved
14:0	**Region Base.** This specifies address bits 26:12 for the Region Base. ***Note:*** If the BIOS region is not used, the Region Base must be programmed to 7FFFh

4.1.3.3 FLREG2—Flash Region 2 (Intel® ME) Register (Flash Descriptor Records)

Memory Address: FRBA + 008h Size: 32 bits

Bits	Description
31	Reserved
30:16	**Region Limit.** This specifies bits 26:12 of the ending address for this Region. ***Notes:*** 1. Ensure size is a correct reflection of actual Intel® ME firmware size that will be used in the platform 2. Region limit address Bits[11:0] are assumed to be FFFh
15	Reserved
14:0	**Region Base.** This specifies address bits 26:12 for the Region Base.



4.1.3.4 FLREG3—Flash Region 3 (GbE) Register (Flash Descriptor Records)

Memory Address: FRBA + 00Ch Size: 32 bits

Bits	Description
31	Reserved
30:16	**Region Limit.** This specifies bits 26:12 of the ending address for this Region. ***Notes:*** 1. The maximum Region Limit is 128KB above the region base. 2. If the GbE region is not used, the Region Limit must be programmed to 0000h 3. Region limit address Bits[11:0] are assumed to be FFFh
15	Reserved
14:0	**Region Base.** This specifies address bits 26:12 for the Region Base. ***Note:*** If the GbE region is not used, the Region Base must be programmed to 7FFFh

4.1.3.5 FLREG4—Flash Region 4 (Platform Data) Register (Flash Descriptor Records)

Memory Address: FRBA + 010h Size: 32 bits

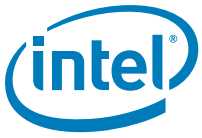
Bits	Description
31	Reserved
30:16	**Region Limit.** This specifies bits 26:12 of the ending address for this Region. ***Notes:*** 1. If PDR Region is not used, the Region Limit must be programmed to 0000h 2. Ensure BIOS region size is a correct reflection of actual BIOS image that will be used in the platform 3. Region limit address Bits[11:0] are assumed to be FFFh
15	Reserved
14:0	**Region Base.** This specifies address bits 26:12 for the Region Base. ***Note:*** If the Platform Data region is not used, the Region Base must be programmed to 7FFFh

4.1.3.6 FLREG8—Flash Region 8(Embeded Controller) Register (Flash Descriptor Records)

Memory Address: FRBA + 020h Size: 32 bits

Bits	Description
31	Reserved
30:16	Region Limit (RL): This specifies address bits 26:12 for the Region n Limit. The value in this register is loaded from the contents in the Flash Descriptor.FLREGn.Region Limit, where 7 <= n <= 11
15	Reserved
14:0	Region Base (RB): This specifies address bits 26:12 for the Region n Base The value in this register is loaded from the contents in the Flash Descriptor. FLREGn.Region Base, where 7 <= n <= 11

Note: Flash Region 5 (FRBA + 014h), Region 6 (FRBA + 018h), Region 7 (FRBA + 01Ch) and Region 9 (FRBA + 024h) are all reserved in client platform and should set to 7FFFh.



4.1.4 Flash Descriptor Master Section

4.1.4.1 FLMSTR1—Flash Master 1 (Host CPU/ BIOS)

Memory Address: FMBA + 000h Size: 32 bits

Bits	Description
31:20	**Master Region Write Access:** Each bit [31:20] corresponds to Regions [11:0]. If the bit is set, this master can erase and write that particular region through register accesses. Note: Bit 21 and 26 are don't care as the primary master always has read/write permission to its primary region
19:8	**Master Region Read Access:** Each bit [19:8] corresponds to Regions [11:0]. If the bit is set, this master can read that particular region through register accesses. Note: Bit 9 and 14 are don't care as the primary master always read/write permission to its primary region.
7:0	Reserved

4.1.4.2 FLMSTR2—Flash Master 2 (Intel® ME)

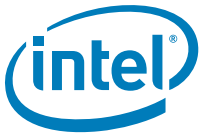
Memory Address: FMBA + 004h Size:32 bits

Bits	Description
31:20	**Master Region Write Access:** Each bit [31:20] corresponds to Regions [11:0]. If the bit is set, this master can erase and write that particular region through register accesses. Note: Bit 22 is a don't care as the primary master always has read/write permission to its primary region
19:8	**Master Region Read Access:** Each bit [19:8] corresponds to Regions [11:0]. If the bit is set, this master can read that particular region through register accesses. Note: Bit 10 is a don't care as the primary master always read/write permission to its primary region.
7:0	Reserved

4.1.4.3 FLMSTR3—Flash Master 3 (GbE)

Memory Address: FMBA + 008h Size:32 bits

Bits	Description
31:20	**Master Region Write Access:** Each bit [31:20] corresponds to Regions [11:0]. If the bit is set, this master can erase and write that particular region through register accesses. Note: Bit 23 is a don't care as the primary master always has read/write permission to its primary region
19:8	**Master Region Read Access:** Each bit [19:8] corresponds to Regions [11:0]. If the bit is set, this master can read that particular region through register accesses. Note: Bit 11 is a don't care as the primary master always read/write permission to its primary region.
7:0	Reserved



4.1.4.4 FLMSTR4—Flash Master 4 (Reserved)

Memory Address: FMBA + 00Ch Size:32 bits

Bits	Description
31:0	Reserved set to '0'

4.1.4.5 FLMSTR5—Flash Master 5 (EC)

Memory Address: FMBA + 010h Size:32 bits

Bits	Description
31:20	**Master Region Write Access:** Each bit [31:20] corresponds to Regions [11:0]. If the bit is set, this master can erase and write that particular region through register accesses. Note: Bit 28 is a don't care as the primary master always has read/write permission to its primary region
19:8	**Master Region Read Access:** Each bit [19:8] corresponds to Regions [11:0]. If the bit is set, this master can read that particular region through register accesses. Note: Bit 16 is a don't care as the primary master always read/write permission to its primary region.
7:0	Reserved

4.1.5 PCH / CPU Softstraps

See Chapter 9, "Flash Descriptor PCH / CPU Configuration Section" for details.

4.1.6 Descriptor Upper Map Section

4.1.6.1 FLUMAP1—Flash Upper Map 1 (Flash Descriptor Records)

Memory Address:FDBAR + EFCh Size: 32 bits

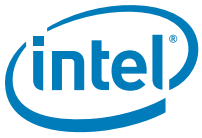
Bits	Default	Description
31:16	0	Reserved
15:8	1	**Intel® ME VSCC Table Length (VTL).** Identifies the 1s based number of DWORDS contained in the VSCC Table. Each SPI component entry in the table is 2 DWORDS long.
7:0	1	**Intel® ME VSCC Table Base Address (VTBA).** This identifies address bits [11:4] for the VSCC Table portion of the Flash Descriptor. Bits [26:12] and bits [3:0] are 0.

4.1.7 Intel® ME Vendor Specific Component Capabilities Table

Entries in this table allow support for a SPI flash part for Intel Management Engine capabilities including Intel® Active Management Technology.

Since Flash Partition Boundary Address (FPBA) has been removed, UVSCC and LVSCC has been replaced with VSCC0 and VSCC1 in Skylake PCH-LP. VSCC0 is for SPI component 0 and VSCC1 is for SPI component 1.

Each VSCC table entry is composed of two 32 bit fields: JEDEC IDn and the corresponding VSCCn value.



See 4.4 Intel® ME Vendor-Specific Component Capabilities (Intel® ME VSCC) Table for information on how to program individual entries.

4.1.7.1 JID0—JEDEC-ID 0 Register (Flash Descriptor Records)

Memory Address: VTBA + 000h Size: 32 bits

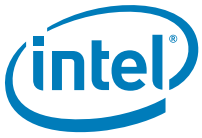
Bits	Description
31:24	Reserved
23:16	**SPI Component Device ID 1.** This field identifies the second byte of the Device ID of the SPI Flash Component. This is the third byte returned by the Read JEDEC-ID command (opcode 9Fh).
15:8	**SPI Component Device ID 0.** This field identifies the first byte of the Device ID of the SPI Flash Component. This is the second byte returned by the Read JEDEC-ID command (opcode 9Fh).
7:0	**SPI Component Vendor ID.** This field identifies the one byte Vendor ID of the SPI Flash Component. This is the first byte returned by the Read JEDEC-ID command (opcode 9Fh).

4.1.7.2 VSCC0—Vendor Specific Component Capabilities 0 (Flash Descriptor Records)

Memory Address: VTBA + 0C4h Size: 32 bits

Note: VSCC0 applies to SPI flash that connected to CS0.

Bits	Description
31:16	Reserved
15:8	**Erase Opcode (EO)**. This field must be programmed with the Flash erase instruction opcode that corresponds to the erase size that is in BES.
7:5	**Quad Enable Requirements (QER)** 000 = Device does not have a QE bit. Device detects 1-1-4 and 1-4-4 reads based on instruction. DQ3 / HOLD# functions as hold during instruction phase. 001 = QE is bit 1 of status register 2. It is set via Write Status with two data bytes where bit 1 of the second byte is one. It is cleared via Write Status with two data bytes where bit 1 of the second byte is zero. Writing only one byte to the status register has the side effect of clearing status register 2, including the QE bit. The 100b code is used if writing one byte to the status register does not modify status register 2. 010 = QE is bit 6 of status register 1. It is set via Write Status with one data byte where bit 6 is one. It is cleared via Write Status with one data byte where bit 6 is zero. 011 = QE is bit 7 of status register 2. It is set via Write status register 2 instruction 3Eh with one data byte where bit 7 is one. It is cleared via Write status register 2 instruction 3Eh with one data byte where bit 7 is zero. The status register 2 is read using instruction 3Fh. 100 = QE is bit 1 of status register 2. It is set via Write Status with two data bytes where bit 1 of the second byte is one. It is cleared via Write Status with two data bytes where bit 1 of the second byte is zero. In contrast to the 001b code, writing one byte to the status register does not modify status register 2. 101 = QE is bit 1 of the status register 2. Status register 1 is read using Read Status instruction 05h. Status register 2 is read using instruction 35h. QE is set via Write Status instruction 01h with two data bytes where bit 1 of the second byte is one. It is cleared via Write Status with two data bytes where bit 1 of the second byte is zero. other = reserved ***Note:*** Please refer to Table note#1 below for details.
4:0	**Reserved set to 00101b**
Notes: 1. The manufacturers information included in the QER list are for guidance purpose. Some manufacturer devices operate as shown in the table above. Check manufacturer's data sheet for exact requirements.	



4.1.7.3 JIDn—JEDEC-ID Register n (Flash Descriptor Records)

Memory Address: VTBA + (n*8)h Size:32 bits

"n" is an integer denoting the index of the Intel® ME VSCC table. See **Table 4.1.7.1** for details.

4.1.7.4 VSCCn—Vendor Specific Component Capabilities n (Flash Descriptor Records)

Memory Address: VTBA + 0C4h + (n*8)h Size: 32 bits

"n" is an integer denoting the index of the Intel® ME VSCC table. See **Table 4.1.7.2** for details.

4.2 OEM Section

Memory Address: F00h Size: 256 Bytes

256 Bytes are reserved at the top of the Flash Descriptor for use by the OEM. The information stored by the OEM can only be written during the manufacturing process as the Flash Descriptor read/write permissions must be set to Read Only when the computer leaves the manufacturing floor. The PCH Flash controller does not read this information. FFh is suggested to reduce programming time.

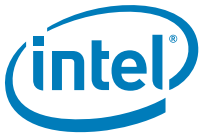
4.3 Region Access Control

Regions of the flash can be defined from read or write access by setting a protection parameter in the Master section of the Descriptor. There are only three masters that have the ability to access other regions: CPU/BIOS, Intel® ME Firmware, and GbE software/driver running on CPU.

Table 4-1. Region Access Control Table Options

Master Read/Write Access				
Region (#)	**CPU and BIOS**	**ME/PCH**	**GbE Controller**	**EC**
Descriptor (0)	Not Accessible	Not Accessible	Not Accessible	Not Accessible
BIOS (1)	CPU and BIOS can always read from and write to BIOS region	Read / Write	Read / Write	Read / Write
ME (2)	Read / Write	ME can always read from and write to ME region	Read / Write	Read / Write
GbE (3)	Read / Write	Read / Write	GbE software can always read from and write to GbE region	Read / Write
PDR (4)	Not Accessible	Not Accessible	Not Accessible	Not Accessible
EC - Embedded Controller (Optional) (8)	Read / Write	Read / Write	Read / Write	EC can always read from and write to EC region

Notes:
1. Descriptor and PDR region is not a master, so they will not have Master R/W access.
2. Descriptor should NOT have write access by any master in production systems.
3. PDR region should only have read and/or write access by CPU/Host. GbE and ME should NOT have access to PDR region.



4.3.1 Intel Recommended Permissions for Region Access

The following Intel recommended read/write permissions are necessary to secure Intel® ME and Intel® ME FW.

The table below shows the values to be inserted into the Flash image tool. The values below will provide the access levels described in the table above.

Table 4-2. Recommended Read/Write Settings for Platforms

	ME	GbE	BIOS	EC
Read	0b 0000 1101 = 0x0d	0b 0000 1000 = 0x08	0b 000‡ 1011 = 0x‡B	0b 0010 0000 = 0x20
Write	0b 0000 1100 = 0x0c	0b 0000 1000 = 0x08	0b 000‡ 1010 = 0x‡A	0b 0010 0000 = 0x20

Note:
1. ‡ = Value dependent on if PDR is implemented and if Host access is desired.

4.3.2 Overriding Region Access

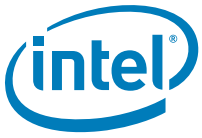
Once access Intel recommended Flash settings have been put into the flash descriptor, it may be necessary to update the ME region with a Host program or write a new Flash descriptor.

Assert HDA_SDO HIGH during the rising edge of PWROK to set the Flash descriptor override strap.

This strap should only be visible and available in manufacturing or during product development.

After this strap has been set you can use a host based flash programming tool like FPT.exe to write/read any area of serial flash that is not protected by Protected Range Registers. Any area of flash protected by Protected range Registers will still NOT be writeable/readable.

See 6.3 SPI Protected Range Register Recommendations for more details.



4.4 Intel® ME Vendor-Specific Component Capabilities (Intel® ME VSCC) Table

The Intel® ME VSCC Table defines how the Intel® ME will communicate with the installed SPI flash if there is no SFDP table found. This table is defined in the descriptor and is the responsibility of who puts together the NVM image. VSCCn registers are defined in memory space and must be set by BIOS. This table must define every flash part that is intended to be used. The size (number of max entries) of the table is defined in 4.1.6.1 FLUMAP1—Flash Upper Map 1 (Flash Descriptor Records). Each Table entry is made of two parts: the JEDEC ID and VSCC setting.

Table 4-3. Jidn - JEDEC ID Portion of Intel® ME VSCC Table

Bits	Description
31:24	Reserved.
23:16	**SPI Component Device ID 1:** This identifies the second byte of the Device ID of the SPI Flash Component. This is the third byte returned by the Read JEDEC-ID command (opcode 9Fh).
15:8	**SPI Component Device ID 0:** This identifies the first byte of the Device ID of the SPI Flash Component. This is the second byte returned by the Read JEDEC-ID command (opcode 9Fh).
7:0	**SPI Component Vendor ID:** This identifies the one byte Vendor ID of the SPI Flash Component. This is the first byte returned by the Read JEDEC-ID command (opcode 9Fh).

If using Flash Image Tool (FIT) refer to System Tools user guide in the Intel® ME FW kit and the respective FW Bring up Guide on how to build the image. If not, refer to 4.1.6.1 FLUMAP1—Flash Upper Map 1 (Flash Descriptor Records) thru 4.2 OEM Section.

4.4.1 How to Set a VSCC Entry in Intel® ME VSCC Table for Skylake PCH-LP Platforms

VSCC0 needs to be programmed in instances where there is only SPI component in the system. When using an asymmetric flash component (part with two different sets of attributes based on address) VCSCC0 and VSCC1 will need to be used. This includes if the system is intended to support both symmetric AND asymmetric SPI flash parts.

Refer to 4.4.2 Intel® ME VSCC Table Settings for Skylake PCH-LP Family Systems.

See text below the table for explanation on how to determine Intel Management Engine VSCC value.

Table 4-4. Vsccn – Vendor-Specific Component Capabilities Portion of the Skylake PCH-LP Platforms (Sheet 1 of 2)

Bits	Description
31:16	Reserved
15:8	**Erase Opcode (EO)**. This field must be programmed with the Flash erase instruction opcode that corresponds to the erase size that is in BES.

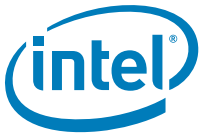
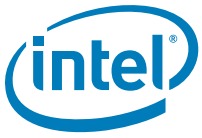


Table 4-4. Vsccn – Vendor-Specific Component Capabilities Portion of the Skylake PCH-LP Platforms (Sheet 2 of 2)

Bits	Description
7:5	**Quad Enable Requirements (QER)** 000 = Part does not require a Quad Enable bit to be set, either because Quad is not supported or because the manufacturer permanently enables Quad capability (e.g. Micron, Numonyx). 001 = Part requires bit 9 in status register 2 to be set to enable quad IO. Writing one byte to status register clears all bits in register 2, therefore status register writes MUST be two bytes. If the status register is unlocked and SFDP bits WSR or VSCC WSR is 1 then SPI controller cannot use the quad output, quad IO features of this part because the hardware will automatically write one byte of zeros to status register with every write/erase. (e.g. Winbond, AMIC, Spansion). 010 = Part requires bit 6 of status register 1 to be set to enable quad IO. If the status register is unlocked and SFDP WSR bit or VSCC WSR is 1 then flash controller cannot use the quad output, quad IO features of this part because the hardware will automatically write one byte of zeros to status register with every write/erase (e.g. Macronix). 011 = Part requires bit 7 of the configuration register to be set to enable Quad (e.g. Atmel). 100 = Part requires bit 9 in status register 2 to be set to enable quad IO. Writing one byte to the status register does not clear the second byte (SST/Microchip, Winbond). ***Note:*** Please refer to Table note#6 below for details.
4	**Write Enable on Write Status (WEWS)** 0 = 50h is the opcode used to unlock the status register on SPI flash if **WSR** (bit 3) is set to 1b. 1 = 06h is the opcode used to unlock the status register on SPI flash if **WSR** (bit 3) is set to 1b. ***Note:*** Please refer to Table Note #4 below for a description how this bit is used.
3	**Write Status Required (WSR)** 0 = No automatic write of 00h will be made to the SPI flash's status register) 1 = A write of 00h to the SPI flash's status register will be sent on EVERY write and erase performed by Intel® ME to the SPI flash. ***Note:*** Please refer to Table Note #5 below for a description how this bit is used.
2	**Write Granularity (WG)**. 0 = 1 Byte 1 = 64 Bytes
1:0	**Block/Sector Erase Size (BES)**. This field identifies the erasable sector size for all Flash components. 00 = 256 Bytes 01 = 4 K Bytes 10 = 8 K Bytes 11 = 64K Bytes

Notes:
1. Bit 3 (**WEWS**) and/or bit 4 (**WSR**) should not be set to '1' if there are non volatile bits in the SPI flash's status register. This may lead to premature flash wear out.
2. This is not an atomic (uninterrupted) sequence. The PCH will not wait for the status write to complete before issuing the next command, potentially causing SPI flash instructions to be disregarded by the SPI flash part. If the SPI flash component's status register is non-volatile, then BIOS should issue an atomic software sequence cycle to unlock the flash part.
3. If both bits 3 (**WSR)** and 4 (**WEWS**) are set to 1b, then sequence of 06h 01h 00h is sent to unlock the SPI flash on EVERY write and erase that Intel Management Engine firmware performs.
4. If bit 3 (**WSR)** is set to 1b and bit 4 (**WEWS**) is set to 0b then sequence of 50h 01h 00h is sent to unlock the SPI flash on EVERY write and erase that Intel Management Engine firmware performs.
5. If bit 3 (**WSR)** is set to 0b and bit 4 (**WEWS**) is set to 0b or 1b then sequence of 60h is sent to unlock the SPI flash on EVERY write and erase that Processor or Intel GbE FW performs.
6. The manufacturers information included in the QER list are for guidance purpose. Some manufacturer devices operate as shown in the table above. Check manufacturer's datasheet for exact requirements.

Erase Opcode (**EO**) and **Block/Sector Erase Size** (**BSES**) should be set based on the flash part and the firmware on the platform. For Intel® ME enabled platforms this should be 4 KB.



Write Status Required (WSR) or Write Enable on Write Status (WEWS) should be set on flash devices that require an opcode to enable a write to the status register. Intel® ME Firmware will write a 00h to status register to unlock the flash part for every erase/write operation. If this bit is set on a flash part that has non-volatile bits in the status register then it may lead to pre-mature wear out of the flash.

- Set the **WSR** bit to 1b and **WEWS** to 0b if the Enable Write Status Register opcode (50h) is needed to unlock the status register. Opcodes sequence sent to SPI flash will bit 50h 01h 00h.
- Set the **WSR** bit to 1b AND **WEWS** bit to 1b if write enable (06h) will unlock the status register. Opcodes sequence sent to SPI flash will bit 06h 01h 00h.
- Set the **WSR** bit to 0b AND **WEWS** bit to 0b or 1b, if write enable (06h) will unlock the status register. Opcodes sequence sent to SPI flash will bit 06h
- **WSR or WEWS should be not be set on devices that use non volatile memory for their status register.** Setting this bit will cause operations to be ignored, which may cause undesired operation. Ask target flash vendor if this is the case for the target flash. See 6.1 Unlocking SPI Flash Device Protection for Skylake PCH-LP Platform and 6.2 Locking SPI Flash via Status Register for more information.

Erase Opcode (**EO**) and Block/Sector Erase Size (**BES**) should be set based on the flash part and the firmware on the platform.

Write Granularity (WG) bit should be set based on the capabilities of the flash device. If the flash part is capable of writing 1 to 64 bytes (or more) with the 02h command you can set this bit 0 or 1. Setting this bit high will result in faster write performance. If flash part only supports single byte write only, then set this bit to 0.

Bit ranges 31:16 and 7:5 are reserved and should set to all zeros.

4.4.2 Intel® ME VSCC Table Settings for Skylake PCH-LP Family Systems

To understand general guidelines for BIOS VSCC settings on different SPI flash devices, please refer to **VSCCommn.bin Content application note** (VSCCommn_bin Content.pdf under Flash Image Tool directory).

§ §

5 Serial Flash Discoverable Parameter (SFDP) Overview

5.1 Introduction

As the feature set of serial flash progresses, there is an increasing amount of divergence as individual vendors find different solution to adding new functionality such as speed and addressing.

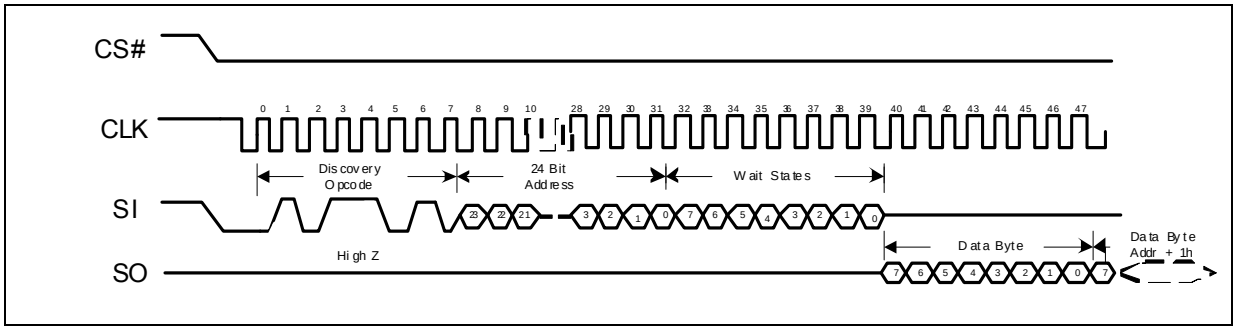
These guidelines are a standard that will allow for individual vendors to have their value add features, but will allow for a controller to discover the attributes needed to operate.

5.2 Discoverable Parameter Opcode and Flash Cycle

The discoverable parameter read opcode behaves like a fast read command. The opcode is 5Ah and the address cycle is 24 bit long. After the opcode 5Ah is clocked in, there are 24 bit of address clocked in. There will then be eight clock (8 wait states) before valid data is clocked out. There is flexibility in the number of wait states, but they must be byte aligned (multiple of 8 wait states).

SFDP read must update at a frequency between 17 MHz and 48 MHz with a single byte of wait state.

Figure 5-1. SFDP Read Instruction Sequence

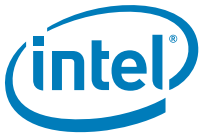


5.3 Parameter Table Supported on PCH

The flash controller first checks for a valid SFDP header. The value of the major and minor revision fields in the SFDP header are don't care. If a valid SFDP header is found, the controller supports auto discovery of the Component Property Parameter Table (CPPT).

The following capabilities are only supported on PCH if CPPT is successfully discovered and parameter values indicate that they are supported. These capabilities are not supported as default.

- Quad I/O Read
- Quad Output Read



- Dual I/O read
- Block /Sector Erase size

Note: If SFDP is valid and advertises 4 Kbyte erase capability, then BES is taken from the SFDP table, otherwise it is taken from the BIOS VCSS table.

PCH will also read the following opcode from parameter table and store to PCH is SFDP is valid and the following function is supported.

- Erase Opcode
- Dual Output Fast Read Opcode
- Dual I/O Fast Read Opcode
- Quad Output Fast Read Opcode
- Quad I/O Fast Read Opcode

5.4 Detailed JEDEC Specification

Please refer to www.jedec.com JESD216 for detailed SFDP specification on SPI.

§ §

6 Configuring BIOS/GbE for SPI Flash Access

6.1 Unlocking SPI Flash Device Protection for Skylake PCH-LP Platform

BIOS must account for any built in protection from the flash device itself. BIOS must ensure that any flash based protection will only apply to BIOS region only. It should not affect the ME or GbE regions.

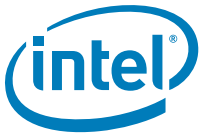
All the SPI flash devices that meet the SPI flash requirements in the *Skylake PCH-LP Family External Design Specification (EDS)* will be unlocked by writing a 00h to the SPI flash's status register. This command must be done via an atomic software sequencing to account for differences in flash architecture. Atomic cycles are uninterrupted in that it does not allow other commands to execute until a read status command returns a 'not busy' result from the flash.

Some flash vendors implement their status registers in NVM flash (non-volatile memory). This takes much more time than a write to volatile memory. During this write, the flash part will ignore all commands but a read to the status register (opcode 05h). The output of the read status register command will tell the PCH when the transaction is done.

Recommended flash unlocking sequence:

- Write enable (06h) command will have to be in the prefix opcode configuration register.
- The "write to status register" opcode (01h) will need to be an opcode menu configuration option.
- Opcode type for write to status register will be '01': a write cycle type with no address needed.
- The FDATA0 register should to be programmed to 0000 0000h.
- Data Byte Count (DBC) in Software Sequencing Flash Control register should be 000000b. Errors may occur if any non zero value is here.
- Set the Cycle Opcode Pointer (COP) to the "write to status register" opcode.
- Set to Sequence Prefix Opcode Pointer (SPOP) to Write Enable.
- Set the Data Cycle (DS) to 1.
- Set the Atomic Cycle Sequence (ACS) bit to 1.
- To execute sequence, set the SPI Cycle Go bit to 1.

Please see the ***Serial Peripheral Interface Memory Mapped Configuration Registers*** in the *Skylake PCH-LP Family External Design Specification (EDS)* for more detailed information.



6.2 Locking SPI Flash via Status Register

Flash vendors that implement their status register with non-volatile memory can be updated a limited number of times. This means that this register may wear out before the desired endurance for the rest of the flash. It is highly recommended that BIOS vendors and customers do NOT use the SPI flash's status register to protect the flash in multiple master systems.

BIOS should try to minimize the number of times that the system is locked and unlocked.

Care should be taken when using status register based SPI flash protection in multiple master systems such as Intel® ME FW and/or integrated GbE. BIOS must ensure that any flash based protection will apply to BIOS region only. It should not affect the ME or GbE regions.

Please contact your desired flash vendor to see if their status register protection bits volatile or non-volatile. Flash parts implemented with volatile systems do not have this concern.

6.3 SPI Protected Range Register Recommendations

The PCH has a mechanism to set up to 5 address ranges from HOST access. These are defined in PR0, PR1, PR2, PR3 and PR4 in the PCH EDS. These address ranges are NOT unlocked by assertion of Flash descriptor Override.

It is strongly recommended to use a protected range register to lock down the factory default portion of Intel® ME FW region. The runtime portion should be left unprotected as to allow BIOS to update it.

It is strongly recommended that if Flash Descriptor Override strap (which can be checked by reading **FDOPSS (0b Flash Descriptor override is set, 1b not set) in PCH memory space (SPIBAR+C4h bit 13))** is set, do not set a Protected range to cover the Intel® ME FW factory defaults. This would allow a flashing of a complete image when the Flash descriptor Override strap is set.

6.4 Recommendations for Flash Configuration Lockdown and Vendor Component Lock Bits

6.4.1 Flash Configuration Lockdown

It is strongly recommended that BIOS sets the Host and GbE **Flash Configuration Lock-Down (FLOCKDN)** bits (located at SPIBAR + 04h and MBAR +04h respectively) to '1' on production platforms. If these bits are not set, it is possible to make register changes that can cause undesired host, integrated GbE and Intel® ME functionality as well as lead to unauthorized flash region access.

Refer to **HSFS— Hardware Sequencing Flash Status Register** in the Serial Peripheral Interface Memory Mapped Configuration Registers section and **HSFS— Hardware Sequencing Flash Status Register** in the GbE SPI Flash Programing Registers section in the Skylake PCH-LP Family External Design Specification (EDS).

6.4.2 Vendor Component Lock

It is strongly recommended that BIOS sets the **Vendor Component Lock (VCL)** bits. These bits are located in the BIOS/GbE VSCC0 registers. VCL applies the lock to both VSCC0 and VSCC1 even if VSCC1 is not used. Without the VCL bits set, it is possible to make Host/GbE VSCC register(s) changes in that can cause undesired host and integrated GbE SPI flash functionality.

Refer to **VSCC— Vendor Specific Component Capabilities Register** in the *Skylake PCH-LP Family External Design Specification (EDS)* for more information.

6.5 Host Vendor Specific Component Control Registers (VSCC)

VSCC are memory mapped registers are used by the PCH when BIOS or Integrate LAN reads, programs or erases the SPI flash via Hardware sequencing.

Flash Partition Boundary Address (FBPBA) has been removed and UVSCC and LVSCC has been replaced with VSCC0 and VSCC1 in Skylake PCH-LP. VSCC0 is for SPI component 0 and VSCC1 is for SPI component 1. SPI controller will determine which VSCC (VCSCC0 or VCSCC1) to be used by comparing Flash Linear Address (FLA) with size of SPI component 0 (C0DEN). When FLA <= C0DEN then VSCC0 will be used; whereas FLA > C0DEN then VSCC1 will be used If one SPI flash component used in the system, VSCC0 needs to be set.

Refer to **VSCC— Lower Vendor Specific Component Capabilities Register** and in the *Skylake PCH-LP Family External Design Specification (EDS)*.

See text below the tables for explanation on how to determine VSCC register values.

Table 6-1. VSCC0 - Vendor-Specific Component Capabilities Register for SPI Component 0 (Sheet 1 of 3)

Bit	Description
31	**Component Property Parameter Table Valid (CPPTV) - RO:** This bit is set to a 1 if the Flash Controller detects a valid SFDP Component Property Parameter Table in SPI Component 0 If CPPTV bit is '0', software must configure the VSCC register appropriately. If CPPTV bit is '1', the corresponding parameter values discovered via SFDP will be used. In most cases, software is not required to configure the VSCC register. However, if the SFDP table indicates an erase size other than 4k byte, then the software is required to program the VSCC.EO register with the correct erase opcode.
30:24	Reserved
23	Vendor Component Lock (VCL): — RW/L: '0': The lock bit is not set '1': The Vendor Component Lock bit is set. This register locks itself when set. This bit applies to both VSCC0 and VSCC1 All bits locked by (**VCL)** will remained locked until a global reset.
22:16	Reserved

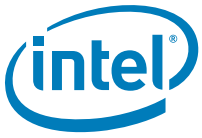


Table 6-1. VSCC0 - Vendor-Specific Component Capabilities Register for SPI Component 0 (Sheet 2 of 3)

Bit	Description
15:8	**Erase Opcode (EO)**— RW: This register is programmed with the Flash erase instruction opcode required by the vendor's Flash component. Software must program this register if the SFDP table for this component does not show 4 kByte erase capability This register is locked by the Vendor Component Lock (**VCL**) bit. ***Note:*** If CPPTV is 1 and the SPDP0 table shows 4k erase capability, the SFDP0 erase code is used instead of this register
7:5	**Quad Enable Requirements (QER)** 000 = Part does not require a Quad Enable bit to be set, either because Quad is not supported or because the manufacturer permanently enables Quad capability (e.g. Micron, Numonyx). 001 = Part requires bit 9 in status register 2 to be set to enable quad IO. Writing one byte to status register clears all bits in register 2, therefore status register writes MUST be two bytes. If the status register is unlocked and SFDP bits WSR or VSCC WSR is 1 then SPI controller cannot use the quad output, quad IO features of this part because the hardware will automatically write one byte of zeros to status register with every write/erase. (e.g. Winbond, AMIC, Spansion). 010 = Part requires bit 6 of status register 1 to be set to enable quad IO. If the status register is unlocked and SFDP WSR bit or VSCC WSR is 1 then flash controller cannot use the quad output, quad IO features of this part because the hardware will automatically write one byte of zeros to status register with every write/erase (e.g. Macronix). 011 = Part requires bit 7 of the configuration register to be set to enable Quad (e.g. Atmel). 100 = Part requires bit 9 in status register 2 to be set to enable quad IO. Writing one byte to the status register does not clear the second byte (SST/Microchip, Winbond). ***Note:*** This register is locked by the Vendor Component Lock (VCL) bit.
4	**Write Enable on Write Status (WEWS)** — RW: '0' = 50h will be the opcode used to unlock the status register on the SPI flash if **WSR** (bit 3) is set to 1b. '1' = 06h will be the opcode used to unlock the status register on the SPI flash if **WSR** (bit 3) is set to 1b. This register is locked by the Vendor Component Lock (VCL) bit. ***Note:*** Please refer to Table 6-3 for a description of how these bits is used.
3	**Write Status Required (WSR)** — RW: '0' = No automatic write of 00h will be made to the SPI flash's status register. '1' = A write of 00h to the SPI flash's status register will be sent on EVERY write and erase to the SPI flash performed by Host and GbE. This register is locked by the Vendor Component Lock (**VCL**) bit. ***Note:*** Please refer to Table 6-3 for a description of how these bits is used.
2	**Write Granularity (WG) — RW:** 0: 1 Byte 1: 64 Byte This register is locked by the Vendor Component Lock (**VCL**) bit. ***Notes:*** 1. If more than one Flash component exists, this field must be set to the lowest common write granularity of the different Flash components 2. If using 64 B write, BIOS must ensure that multiple byte writes do not occur over 256 B boundaries. This will lead to corruption as the write will wrap around the page boundary on the SPI flash part. This is a feature in page writable SPI flash.

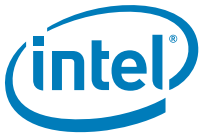


Table 6-1. VSCC0 - Vendor-Specific Component Capabilities Register for SPI Component 0 (Sheet 3 of 3)

Bit	Description
1:0	**Block/Sector Erase Size (BES)—** RW: This field identifies the erasable sector size for Flash components. Valid Bit Settings: 00: 256 Byte 01: 4 KByte 10: 8 KByte 11: 64 K This register is locked by the Vendor Component Lock (**VCL**) bit. Hardware takes no action based on the value of this register. The contents of this register are to be used only by software and can be read in the HSFSTS.BERASE register in both the BIOS and the GbE program registers if FLA is less than FPBA.

Table 6-2. VSCC1 - Vendor Specific Component Capabilities Register for SPI Component 1 (Sheet 1 of 2)

Bit	Description
31	**Component Property Parameter Table Valid (CPPTV) - RO:** This bit is set to a 1 if the Flash Controller detects a valid SFDP Component Property Parameter Table in SPI Component 1 If CPPTV bit is '0', software must configure the VSCC register appropriately. If CPPTV bit is '1', the corresponding parameter values discovered via SFDP will be used. In most cases, software is not required to configure the VSCC register. However, if the SFDP table indicates an erase size other than 4k byte, then the software is required to program the VSCC.EO register with the correct erase opcode.
30:16	Reserved
15:8	**Erase Opcode (EO)**— RW: This register is programmed with the Flash erase instruction opcode required by the vendor's Flash component. This register is locked by the Vendor Component Lock (**VCL**) bit.
7:5	**Quad Enable Requirements (QER)** 000 = Part does not require a Quad Enable bit to be set, either because Quad is not supported or because the manufacturer permanently enables Quad capability (e.g. Micron, Numonyx). 001 = Part requires bit 9 in status register 2 to be set to enable quad IO. Writing one byte to status register clears all bits in register 2, therefore status register writes MUST be two bytes. If the status register is unlocked and SFDP bits WSR or VSCC WSR is 1 then SPI controller cannot use the quad output, quad IO features of this part because the hardware will automatically write one byte of zeros to status register with every write/erase. (e.g. Winbond, AMIC, Spansion). 010 = Part requires bit 6 of status register 1 to be set to enable quad IO. If the status register is unlocked and SFDP WSR bit or VSCC WSR is 1 then flash controller cannot use the quad output, quad IO features of this part because the hardware will automatically write one byte of zeros to status register with every write/erase (e.g. Macronix). 011 = Part requires bit 7 of the configuration register to be set to enable Quad (e.g. Atmel). 100 = Part requires bit 9 in status register 2 to be set to enable quad IO. Writing one byte to the status register does not clear the second byte (SST/Microchip, Winbond). ***Note:*** This register is locked by the Vendor Component Lock (VCL) bit.
4	**Write Enable on Write to Status (WEWS)** — RW: '0' = 50h will be the opcode used to unlock the status register if **WSR** (bit 3) is set to 1b. '1' = 06h will be the opcode used to unlock the status register if **WSR** (bit 3) is set to 1b. This register is locked by the Vendor Component Lock (**VCL**) bit. Please refer to Table 6-3 for a description of how these bits is used.

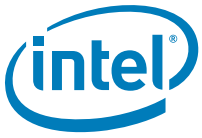


Table 6-2. VSCC1 - Vendor Specific Component Capabilities Register for SPI Component 1 (Sheet 2 of 2)

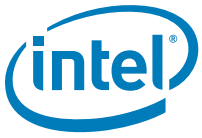
Bit	Description
3	**Write Status Required (WSR)** — RW: '0' = No automatic write of 00h will be made to the SPI flash's status register '1' = A write of 00h to the SPI flash's status register will be sent on EVERY write and erase to the SPI flash performed by Host and GbE. This register is locked by the Vendor Component Lock (**VCL**) bit. ***Note:*** Please refer to Table 6-3 for a description of how these bits is used.
2	**Write Granularity (WG) —** RW**:** 0: 1 Byte 1: 64 Byte This register is locked by the Vendor Component Lock (**VCL**) bit. If more than one Flash component exists, this field must be set to the lowest common write granularity of the different Flash components. If using 64 B write, BIOS must ensure that multiple byte writes do not occur over 256 B boundaries. This will lead to corruption as the write will wrap around the page boundary on the SPI flash part. This is a feature in page writeable SPI flash.
1:0	**Block/Sector Erase Size (BES)—** RW: This field identifies the erasable sector size for all Flash components. Valid Bit Settings: 00: 256 Byte 01: 4 KByte 10: 8 KByte 11: 64 K This register is locked by the Vendor Component Lock (**VCL**) bit. Hardware takes no action based on the value of this register. The contents of this register are to be used only by software and can be read in the HSFSTS.BERASE register in both the BIOS and the GbE program registers if FLA is less than FPBA.

Erase Opcode (**EO**) and **Block/Sector Erase Size** (**BSES**) should be set based on the flash part and the firmware on the platform.

- Either **Write Status Required (WSR) or Write Enable on Write Status (WEWS)** should be set on flash devices that require an opcode to enable a write to the status register. BIOS and GbE will write a 00h to the SPI flash's status register to unlock the flash part for every erase/write operation. If this bit is set on a flash part that has non-volatile bits in the status register then it may lead to pre-mature wear out of the flash and may result in undesired flash operation. Please refer to Table 6-3 for a description of how these bits is set and what is the expected operation from the controller during erase/write operation.

Table 6-3. Description of How WSR and WEWS is Used

WSR	WEWS	Flash Operation
1b	0b	If the Enable Write Status Register opcode (50h) is needed to unlock the status register. Opcodes sequence sent to SPI flash will bit 50h 01h 00h.
1b	1b	If write enable (06h) will unlock the status register. Opcodes sequence sent to SPI flash will bit 06h 01h 00h.
0b	0 or 1b	Sequence of 60h is sent to unlock the SPI flash on EVERY write and erase that Processor or Intel GbE FW performs.



Note: **WSR or WEWS should be not be set on devices that use non volatile memory for their status register.** Setting this bit will cause operations to be ignored, which may cause undesired operation. Ask target flash vendor if this is the case for the target flash. See 6.1 Unlocking SPI Flash Device Protection for Skylake PCH-LP Platform and 6.2 Locking SPI Flash via Status Register for more information.

Write Granularity (WG) bit should be set based on the capabilities of the flash device. If the flash part is capable of writing 1 to 64 bytes (or more) with the 02h command you can set this bit 0 or 1. Setting this bit high will result in faster write performance. If flash part only supports single byte write only, then set this bit to 0. Setting this bit high requires that BIOS ensure that no multiple byte write operation does not cross a 256 Byte page boundary, as it will have unintended results. This is a feature of page programming capable flash parts.

Vendor Component Lock (VCL) should remain unlocked during development, but locked in shipping platforms. When **VCL** and **FLOCKDN** are set, it is possible that you may not be able to use in system programming methodologies including Intel Flash Programming Tool if programmed improperly. It will require a system reset to unlock this register and BIOS not to set this bits. See 6.4 Recommendations for Flash Configuration Lockdown and Vendor Component Lock Bits for more details.

All reserved bits should set to zeros.

6.6 Host VSCC Register Settings

To understand general guidelines for VSCC settings with different SPI flash devices, please refer to **VSCCommn.bin content application note** (VSCCommn_bin Content.pdf under Flash Image Tool directory). VSCCommn.bin contains SPI devices vendor ID, device ID and recommended VSCC values.

§ §

7 Intel® ME Disable for Debug/ Flash Burning Purposes

This section is purely for debug purposes. Intel® ME FW is the only supported configuration for Skylake PCH-LP based system.

7.1 Intel® ME Disable

Here are the ways one can disable the Intel® ME for purposes of in system programming the flash.

1. HDA_SDO (Manufacturing mode jumper or Flash descriptor override jumper) asserted HIGH on the rising edge of PWROK. Power off or cold reset. Note: this is only valid as long as you do not specifically set the variable Flash Descriptor Override Pin-Strap Ignore in the Flash Image Tool to false.
2. Use -disableME command line option through FPT tool.

HECI ME region unlock - There is a HECI command that allows Intel® ME FW to boot up in a temporarily disabled state and allows for a host program to overwrite the ME region.

Note: Removing the DIMM from channel 0 no longer has any effect on Intel® ME functionality.

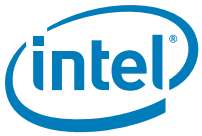
7.1.1 Erasing/Programming Intel® ME Region

If CPU/Host has access to ME region, then one could either erase/program the ME region to all FFh. If there is no access, then one must assert HDA_SDO (Flash descriptor override strap) HIGH during the rising edge of PWROK. If there are Protected Range registers set, then you will not be able to program this w/o a BIOS option to turn off this protected range. (See 6.3 SPI Protected Range Register Recommendations) for more detail.

This depends on the board booting HW defaults for clock configuration. If any clock configuration is required for booting the platform that is not in the HW defaults, then this option may not work for you.

FPT will automatically disable Intel ME when erasing any address in ME region.

§ §



8 Recommendations for SPI Flash Programming in Manufacturing Environments

It is recommended that the Intel® ME be disabled when you are programming the ME region. Intel® ME FW performs regular writes/erases to the ME region. Therefore some bits may be changed after programming. Please note that not all of these options will be optimal for your manufacturing process.

Any method of programming SPI flash where the system is not powered will not result in any interference from Intel® ME FW. The following methods are for Intel® ME FW:

- Program via In Circuit Test – System is not fully powered here.
- Program via external flash burn-in solution.
- Assert HDA_SDO HIGH (Flash Descriptor Override Jumper) on the rising edge of PWROK. Note: this is only valid as long as you do not specifically disable this functionality in fixed offset variable.

§ §

9 Flash Descriptor PCH / CPU Configuration Section

The following section describes functionality and how to set soft strapping for a target platform. Improper setting of soft straps can lead to undesired operation and may lead to returns/recalls.

9.1 PCH Descriptor Record 0 (Flash Descriptor Records)

Flash Address:FPSBA + 000h

Default Flash Address: 100h

Offset from 0	Bits	Description	Usage	FIT Visible
0x100h	32:23	**Reserved, set to '0'**		**No**
	22	**Intel® Platform Trusted Technology Supported (Intel® PTT)** 0 = Intel® PTT Enabled **(default)** 1 = Intel® PTT Disabled		**Yes**
	21	**Intel® Trace Hub - Emergency Mode:** 0 = ROM Tracing Emergency mode disabled **(default)** 1 = ROM Tracing Emergency mode enabled	This option enables ROM Tracing in the base platform image.	**Yes**
	20	**Deep Sx Enable (Deep_SX_EN):** 0 = Deep Sx is not supported on the platform 1 = Deep Sx is supported on the platform **(default)**	This requires the target platform to support Deep Sx state **Note:** When configuring Deep Sx you must also set **DEEPSX_PLT_CFG_SS**.	**Yes**
	19	**Intel® ME Reset Capture on CL_RST#: (MER_CL):** 0 = PCH Signal CL_RST# does NOT assert when Intel® ME performs a reset. **(default)** 1 = PCH Signal CL_RST# asserts when Intel® ME resets.	Notes: Signal CL_RST# is only present on mobile PCH	**Yes**
	18	**Reserved, set to '0'**		**No**
	17	**Direct Connect Interface (DCI) Enabled:** 0 = DCI Disabled 1 = DCI Enabled **(default)**		**Yes**
	16	**Reserved, set to '0'**		**Yes**
	15:7	**Reserved, set to '0'**		**No**

Offset from 0	Bits	Description	Usage	FIT Visible
0x100h (Cont)	6	**RPMC Rebinding Enabled** **Set to '0b'**		**Yes**
	5	**RPMC Supported:** This bit enables RPMC support 0 = RPMC is not supported **(default)** 1 = RPMC is supported		**Yes**
	4:2	**Reserved, set to '0'**		**No**
	1	**Intel® Trace Hub Soft Enable:** 0 = ROM Tracing Soft Disable **(default)** 1 = ROM Tracing Soft Enable	This soft strap enables ROM based tracing in the ME. ***Note:*** Only applicable if Intel® Trace Hub Debug Messages strap is also enabled	**Yes**
	0	**Firmware ROM Bypass Enable Softstrap:** 0 = ROM Bypass disabled **(default)** 1 = ROM Bypass enabled	Firmware ROM Bypass Enable Softstrap.	**Yes**

9.2 PCH Descriptor Record 1 (Flash Descriptor Records)

Flash Address:FPSBA + 004h

Default Flash Address: 104h

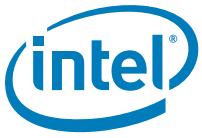
Offset from 0	Bits	Description	Usage	FIT Visible
0x104h	0	**SMBus / SMLink TCO Slave Connection:** 0 = TCO Slave connected to Intel® ME SMBus **(default)** 1 = TCO Slave connected to Intel® ME SMBus and SMLink0	See: Skylake Platform Controller Hub (PCH-LP) EDS for more details.	**Yes**

9.3 PCH Descriptor Record 2 (Flash Descriptor Records)

Flash Address:FPSBA + 005h

Default Flash Address: 105h

Offset from 0	Bits	Description	Usage	FIT Visible
0x105h	0	**Intel® ME SMBus Enable:** This bit must always be set to 1.		**No**



9.4 PCH Descriptor Record 3 (Flash Descriptor Records)

Flash Address:FPSBA + 006h

Default Flash Address: 106h

Offset from 0	Bits	Description	Usage	FIT Visible
0x106h	7:0	**Reserved, set to '0'**		**No**

9.5 PCH Descriptor Record 4 (Flash Descriptor Records)

Flash Address:FPSBA + 007h

Default Flash Address: 107h

Offset from 0	Bits	Description	Usage	FIT Visible
0x107h	6:0	**Intel® ME SMBus I²C Address (MESMI2CA):** Defines 7 bit Intel ME SMBus I2C target address **Default set to '0'** **Note:** This field is only used for testing purposes.	This address is only used by Intel® ME FW for testing purposes. If **MESMI2CEN** (**Offset 0x10A** bit 0) is set to 1 then the address used in this field must be non-zero and not conflict with any other devices on the segment.	**Yes**

9.6 PCH Descriptor Record 5 (Flash Descriptor Records)

Flash Address:FPSBA + 008h

Default Flash Address: 108h

Offset from 0	Bits	Description	Usage	FIT Visible
0x108h	6:0	**Intel® ME SMBus ASD Address (MESMASDA):** Intel® ME SMBus Controller ASD Target Address. ASD: Alert Sending Device **Default set to '0'** ***Note:*** This field is only applicable if there is an ASD attached to SMBus and using Intel® AMT	If **MESMASDEN(PCH Descriptor Record 8 bit 0)** is set to'1' there must be a valid address for ASD. The address must be determined by the BIOS developer based on the requirements below. A valid address must be: • Non-zero value • Must be a unique address on the Host SMBus segment • Be compatible with the master on SMBus - For example, if the ASD address the master that needs write thermal information to an address "xy"h. Then this field must be set to xy"h.	**Yes**

9.7 PCH Descriptor Record 6 (Flash Descriptor Records)

Flash Address:FPSBA + 009h

Default Flash Address: 109h

Offset from 0	Bits	Description	Usage	FIT Visible
0x109h	6:0	**Intel® ME SMBus MCTP Address (MESMMCTPA):** Defines 7 bit Intel ME SMBus MCTP target address **Default set to '0'** ***Note:*** This field is only used for testing purposes.	If **MESMMCTPAEN (PCHSTRP3 bit 8)** is set to 1 then the address used in this field must be non-zero and not conflict with any other devices on the segment.	**Yes**

9.8 PCH Descriptor Record 7 (Flash Descriptor Records)

Flash Address:FPSBA + 00Ah

Default Flash Address: 10Ah

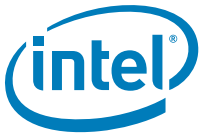
Offset from 0	Bits	Description	Usage	FIT Visible
0x10Ah	0	**Intel® ME SMBus I^2C Address Enable (MESMI2CEN):** 0 = Intel® ME SMBus I^2C Address is disabled **(default)** 1 = Intel® ME SMBus I^2C Address is enabled ***Note:*** This field is only used for testing purposes.	This field should only be set to '1' for testing purposes	**Yes**

9.9 PCH Descriptor Record 8 (Flash Descriptor Records)

Flash Address:FPSBA + 00Bh

Default Flash Address: 10Bh

Offset from 0	Bits	Description	Usage	FIT Visible
0x10Bh	0	**Intel® ME SMBus ASD Address Enable (MESMASDEN):** 0 = Intel® ME SMBus ASD Address is disabled **(default)** 1 = Intel® ME SMBus ASD Address is enabled ***Note:*** This field is only applicable if there is an ASD attached to SMBus and using Intel® AMT	This bit must only be set to '1' when there is an ASD (Alert Sending Device) attached to Host SMBus. This is only applicable in platforms using Intel® AMT. ***Note:*** This setting is not the same for all designs, is dependent on the board design. The setting of this field must be determined by the BIOS developer and the platform hardware designer.	**Yes**



9.10 PCH Descriptor Record 9 (Flash Descriptor Records)

Flash Address:FPSBA + 00Ch

Default Flash Address: 10Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x10Ch	0	**Intel® ME SMBus MCTP Address Enable (MESMMCTPA):** 0 = Intel ME SMBus MCTP Address is disabled **(default)** 1 = Intel ME SMBus MCTP Address is enabled ***Note:*** This field is only used for testing purposes.		**Yes**

9.11 PCH Descriptor Record 10 (Flash Descriptor Records)

Flash Address:FPSBA + 00Dh Size: 8 bit Default value: 00h

Default Flash Address: 10Dh

Offset from 0	Bits	Description	Usage	FIT Visible
0x10Dh	0	**Reserved, set to '0'**		**No**

9.12 PCH Descriptor Record 11 (Flash Descriptor Records)

Flash Address:FPSBA + 00Eh

Default Flash Address: 10Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0x10Eh	15:0	**Intel® ME SMBus Subsystem Vendor ID for ASF (MESMA2UDID):** MESMAUDID[15:0] - **Subsystem Vendor ID** The values contained in MESMAUDID[15:0] is provided as bytes 10-11 of the data payload to an external master when it initiates a Directed GET UDID Block Read Command to the Alert Sending Device ASD's address. **Default set to '0x0000'**		**Yes**
0x110h	15:0	**Intel® ME SMBus Subsystem Device ID for ASF (MESMA2UDID):** MESMAUDID[31:16] - **Subsystem Device ID** The values contained in MESMAUDID[31:16] is provided as bytes 8-9 of the data payload to an external master when it initiates a Directed GET UDID Block Read Command to the Alert Sending Device ASD's address. **Default set to '0'**		**Yes**

9.13 PCH Descriptor Record 12 (Flash Descriptor Records)

Flash Address:FPSBA + 012h

Default Flash Address: 112h

Offset from 0	Bits	Description	Usage	FIT Visible
0x112h	15:0	**Reserved, set to '0'**		**No**

9.14 PCH Descriptor Record 13 (Flash Descriptor Records)

Flash Address:FPSBA + 016h

Default Flash Address: 116h

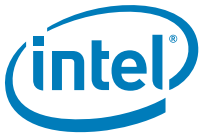
Offset from 0	Bits	Description	Usage	FIT Visible
0x116h	1:0	**Intel® ME SMBus Frequency (SMB0FRQ):** The value of these bits determine the physical bus speed supported by the HW. **Set to '0x1'**	Intel® ME SMBus	**No**

9.15 PCH Descriptor Record 14 (Flash Descriptor Records)

Flash Address:FPSBA + 018h Size: 8 bit Default value: 00h

Default Flash Address: 118h

Offset from 0	Bits	Description	Usage	FIT Visible
0x118h	0	**Reserved, set to '0'**		**No**



9.16 PCH Descriptor Record 15 (Flash Descriptor Records)

Flash Address:FPSBA + 019h

Default Flash Address: 119h

Offset from 0	Bits	Description	Usage	FIT Visible
0x119h	0	**SMLink0 Enable (SML0_EN):** Configures if SMLink0 segment is enabled 0 = Disabled 1 = Enabled **(default)** ***Notes:*** 1. This bit MUST be set to '1' when utilizing integrated LAN controller. 2. This bit MUST be set to '1' when utilizing NFC enabled on the platform. 3. The SMBus TCO Slave controller must be routed to this SMLink 0 Segment. 4. This segment should be set to 0 in one of the following cases: a. Not using Intel NFC solution b. Disabled by the user.	This bit MUST be set to '1' when Intel NFC enabled on the platform. The Intel PHY SMBus controller must be routed to this SMLink 0 Segment. If not using Intel NFC solution or if disabling it, then this segment must be disabled (set to '0'). ***Note:*** This setting is not the same for all designs, is dependent on the board design. The setting of this field must be determined by the BIOS developer and the platform hardware designer.	**Yes**

9.17 PCH Descriptor Record 16 (Flash Descriptor Records)

Flash Address:FPSBA + 01Ah Size: 8 bit Default value: 00h

Default Flash Address: 11Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0x11Ah	7:0	**Reserved, set to '0'**		**No**

9.18 PCH Descriptor Record 17 (Flash Descriptor Records)

Flash Address:FPSBA + 01Bh Size: 8 bit Default value: 00h

Default Flash Address: 11Bh

Offset from 0	Bits	Description	Usage	FIT Visible
0x11Bh	7:0	**Reserved, set to '0'**		**No**

9.19 PCH Descriptor Record 18 (Flash Descriptor Records)

Flash Address:FPSBA + 01Ch

Default Flash Address: 11Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x11Ch	15:0	**Reserved, set to '0'**		**No**

9.20 PCH Descriptor Record 19 (Flash Descriptor Records)

Flash Address:FPSBA + 020h Size: 8 bit Default value: 00h

Default Flash Address: 120h

Offset from 0	Bits	Description	Usage	FIT Visible
0x120h	0	**Reserved, set to '0'**		**No**

9.21 PCH Descriptor Record 20 (Flash Descriptor Records)

Flash Address:FPSBA + 021h Size: 8 bit Default value: 00h

Default Flash Address: 121h

Offset from 0	Bits	Description	Usage	FIT Visible
0x121h	0	**Reserved, set to '0'**		**No**

9.22 PCH Descriptor Record 21 (Flash Descriptor Records)

Flash Address:FPSBA + 022h

Default Flash Address: 122h

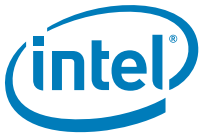
Offset from 0	Bits	Description	Usage	FIT Visible
0x122h	31:0	**Reserved, set to '0'**		**No**

9.23 PCH Descriptor Record 22 (Flash Descriptor Records)

Flash Address:FPSBA + 026h

Default Flash Address: 126h

Offset from 0	Bits	Description	Usage	FIT Visible
0x126h	31:0	**Reserved, set to '0'**		**No**



9.24 PCH Descriptor Record 23 (Flash Descriptor Records)

Flash Address:FPSBA + 02Ah

Default Flash Address: 12Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0x12Ah	1:0	**SMLink0 Frequency (SML0FRQ):** These bits determine the physical bus speed supported by the HW. 00 = Reserved 01 = Standard Mode - up to 100 kHz 10 = Fast Mode - up to 400 kHz 11 = Fast Mode Plus - up to 1 MHz **(default)**	Speed is dependent on board topology and layout.	**Yes**

9.25 PCH Descriptor Record 24 (Flash Descriptor Records)

Flash Address:FPSBA + 02Ch Size: 8 bit Default value: 00h

Default Flash Address: 12Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x12Ch	0	**Reserved, set to '0'**		**No**

9.26 PCH Descriptor Record 25 (Flash Descriptor Records)

Flash Address:FPSBA + 02Dh

Default Flash Address: 12Dh

Offset from 0	Bits	Description	Usage	FIT Visible
0x12Dh	0	**SMLink1 Enable (SML1_EN):** Configures if SMLink1 segment is enabled 0 = Disabled 1 = Enabled **(default)** ***Note:*** This must be set to '1' platforms that use PCH SMBus based thermal reporting.	This bit must be set to '1' if using the PCH's Thermal reporting. If setting this bit to '0', there must be an external solution that gathers temperature information from PCH and processor. ***Note:*** This setting is not the same for all designs, is dependent on the board design. The setting of this field must be determined by the BIOS developer and the platform hardware designer.	**Yes**

9.27 PCH Descriptor Record 26 (Flash Descriptor Records)

Flash Address:FPSBA + 02Eh

Default Flash Address: 12Eh

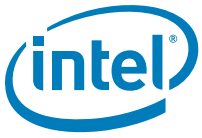
Offset from 0	Bits	Description	Usage	FIT Visible
0x12Eh	7:1	**SMLink1 GP Target Address (SML1GPA):** SMLink1 controller General Purpose Target Address (7:1) ***Notes:*** 1. This field is not active unless SML1GPAEN is set to '1'. 2. This address MUST be set if there is a device on the SMLink1 segment that will use SMBus based PCH thermal reporting. 3. If SML1GPAEN ='1' then this field must be a valid 7 bit, non-zero address that does not conflict with any other devices on SMLink1 segment. **Default set to '0'**	When **SML1GPAEN** ='1', there needs to be a valid GP address in this field. This address used here is design specific. The BIOS developer and / or platform hardware designer must supply an address with the criteria below. A valid address must be: • Non-zero value • Must be a unique address on the SMLink1 segment • Be compatible with the master on SMLink1 - For example if the GP address the master that needs read thermal information from a certain address, then this filed must be set accordingly.	**Yes**
	0	**SMLink1 GP Target Address Enable (SML1GPAEN):** SMLink1 controller General Purpose Target Address Enable 0 = SMLink1 GP Address is disabled **(default)** 1 = SMLink1 GP Address is enabled This bit MUST set to '1' if there is a device on the SMLink1 segment that will use SMBus based PCH thermal reporting. This bit MUST be set to '0' if PCH thermal reporting is not used.	This bit must be set in cases where SMLink1 has a master that requires SMBus based Thermal Reporting that is supplied by the PCH. Some examples of this master could be an Embedded Controller, a BMC, or any other SMBus Capable device that needs Processor or PCH temperature information. If no master on the SMLink1 segment is capable of utilizing thermal reporting, then this field must be set to '0'. ***Note:*** This setting is not the same for all designs, is dependent on the board design. The setting of this field must be determined by the BIOS developer and the platform hardware designer.	**Yes**

9.28 PCH Descriptor Record 27 (Flash Descriptor Records)

Flash Address:FPSBA + 02Fh

Default Flash Address: 12Fh

Offset from 0	Bits	Description	Usage	FIT Visible
0x12Fh	6:0	**SMLink1 I^{2}C* Target Address (SML1I2CA):** Defines the 7 bit I2C target address for PCH Thermal Reporting on SMLink1. ***Notes:*** 1. This field is not active unless SML1I2CAEN is set to '1'. 2. This address MUST be set if there is a device on the SMLink1 segment that will use thermal reporting supplied by PCH. 3. If SML1I2CAEN ='1' then this field must be a valid 7 bit, non-zero address that does not conflict with any other devices on SMLink1 segment. 4. This address can be different for every design, ensure BIOS developer supplies the address. **Default set to '0'**	When **SML1I2CAEN(PCHSTRP11 bit 24)** ='1', there needs to be a valid I2C address in this field. This address used here is design specific. The BIOS developer and/or platform hardware designer must supply an address with the criteria below. **A valid address must be:** • Non-zero value • Must be a unique address on the SMLink1 segment • Be compatible with the master on SMLink1 - For example, if the I^{2}C address the master that needs write thermal information to a address "xy"h. Then this filed must be to "xy"h.	**Yes**



9.29 PCH Descriptor Record 28 (Flash Descriptor Records)

Flash Address:FPSBA + 030h Size: 8 bit Default value: 00h

Default Flash Address: 130h

Offset from 0	Bits	Description	Usage	FIT Visible
0x130h	6:0	**Reserved, set to '0'**		**No**

9.30 PCH Descriptor Record 29 (Flash Descriptor Records)

Flash Address:FPSBA + 031h Size: 8 bit Default value: 00h

Default Flash Address: 131h

Offset from 0	Bits	Description	Usage	FIT Visible
0x131h	6:0	**Reserved, set to '0'**		**No**

9.31 PCH Descriptor Record 30 (Flash Descriptor Records)

Flash Address:FPSBA + 032h

Default Flash Address: 132h

Offset from 0	Bits	Description	Usage	FIT Visible
0x132h	0	**SMLink1 I^{2}C Target Address Enable (SML1I2CAEN):** 0 = SMLink1 I^{2}C Address is disabled **(default)** 1 = SMLink1 I^{2}C Address is enabled ***Notes:*** 1. This bit MUST set to '1' if there is a device on the SMLink1 segment that will use PCH thermal reporting. 2. This bit MUST be set to '0' if PCH thermal reporting is not used.	This bit must be set in cases where SMLink1 has a master that requires SMBus based Thermal Reporting that is supplied by the PCH. Some examples of this master could be an Embedded Controller, a BMC, or any other SMBus Capable device that needs Processor and/or PCH temperature information. If no master on the SMLink1 segment is capable of utilizing thermal reporting, then this field must be set to '0'. ***Note:*** This setting is not the same for all designs, is dependent on the board design. The setting of this field must be determined by the BIOS developer and the platform hardware designer.	**Yes**

9.32 PCH Descriptor Record 31 (Flash Descriptor Records)

Flash Address:FPSBA + 033h Size: 8 bit Default value: 00h

Default Flash Address: 133h

Offset from 0	Bits	Description	Usage	FIT Visible
0x133h	0	**Reserved, set to '0'**		**No**

9.33 PCH Descriptor Record 32 (Flash Descriptor Records)

Flash Address:FPSBA + 034h Size: 8 bit Default value: 00h

Default Flash Address: 134h

Offset from 0	Bits	Description	Usage	FIT Visible
0x134h	0	**Reserved, to '0'**		**No**

9.34 PCH Descriptor Record 33 (Flash Descriptor Records)

Flash Address:FPSBA + 035h Size: 8 bit Default value: 00h

Default Flash Address: 135h

Offset from 0	Bits	Description	Usage	FIT Visible
0x135h	0	**Reserved, set to '0'**		**No**

9.35 PCH Descriptor Record 34 (Flash Descriptor Records)

Flash Address:FPSBA + 036h

Default Flash Address: 136h

Offset from 0	Bits	Description	Usage	FIT Visible
0x136h	31:0	**Reserved, set to '0'**		**No**

9.36 PCH Descriptor Record 35 (Flash Descriptor Records)

Flash Address:FPSBA + 03Ah

Default Flash Address: 13Ah

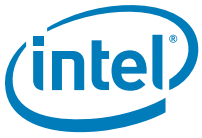
Offset from 0	Bits	Description	Usage	FIT Visible
0x13Ah	15:0	**Reserved, set to '0'**		**No**

9.37 PCH Descriptor Record 36 (Flash Descriptor Records)

Flash Address:FPSBA + 03Eh

Default Flash Address: 13Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0x13Eh	1:0	**SMLink1 Frequency (SML1FRQ) Frequency** 00 = Reserved 01 = Standard Mode - up to 100 kHz **(default)** 10 = Fast Mode - up to 400 kHz 11 = Fast Mode Plus - up to 1 MHz		**Yes**



9.38 PCH Descriptor Record 37 (Flash Descriptor Records)

Flash Address:FPSBA + 040h

Default Flash Address: 140h

Offset from 0	Bits	Description	Usage	FIT Visible
0x140h	0	**Reserved, set to '0'**		**No**

9.39 PCH Descriptor Record 38 (Flash Descriptor Records)

Flash Address:FPSBA + 041h

Default Flash Address: 141h

Offset from 0	Bits	Description	Usage	FIT Visible
0x144h	6:0	**GbE MAC SMBus Address:** This is the 7 bit SMBus address to accept SMBus cycles from the PHY. This field must be programmed to **70h**.	This is the Intel integrated wired MAC's SMBus address. This field must be programmed to 70h. GbE PHY SMBus Address and GbE MAC address have to be programmed to 64h and 70h in order to ensure proper arbitration of SMBus communication between the Intel integrated MAC and PHY.	**Yes**

9.40 PCH Descriptor Record 39 (Flash Descriptor Records)

Flash Address:FPSBA + 045h

Default Flash Address: 145h

Offset from 0	Bits	Description	Usage	FIT Visible
0x145h	6:0	**Reserved, set to '0'**		**No**

9.41 PCH Descriptor Record 40 (Flash Descriptor Records)

Flash Address:FPSBA + 046h Size: 8 bit Default value: 00h

Default Flash Address: 146h

Offset from 0	Bits	Description	Usage	FIT Visible
0x146h	0	**Reserved, set to '0'**		**No**

9.42 PCH Descriptor Record 41 (Flash Descriptor Records)

Flash Address:FPSBA + 047h

Default Flash Address: 147h

Offset from 0	Bits	Description	Usage	FIT Visible
0x147h	0	**Gbe MAC SMBus Address Enable (GBEMAC_SMBUS_ADDR_EN):** 0 = Disabled 1 = Enabled **(default)** ***Notes:*** 1.This bit MUST be set to '1' when utilizing Intel integrated wired LAN. 2.If not using Intel integrated wired LAN solution or if disabling it, then this segment must be set to '0'.	This bit must be set to '1' if Intel integrated wired LAN solution is used. If not using, or if disabling Intel integrated wired LAN solution, then this field must be set to '0'.	**Yes**

9.43 PCH Descriptor Record 42 (Flash Descriptor Records)

Flash Address:FPSBA + 048h Size: 8 bit Default value: 03h

Default Flash Address: 148h

Offset from 0	Bits	Description	Usage	FIT Visible
0x148h	1:0	**Reserved, set to '0x3'**		**No**

9.44 PCH Descriptor Record 43 (Flash Descriptor Records)

Flash Address:FPSBA + 049h Size: 8 bit Default value: 01h

Default Flash Address: 149h

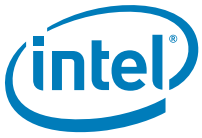
Offset from 0	Bits	Description	Usage	FIT Visible
0x149h	2:0	**Reserved, set to '0x2'**		**No**

9.45 PCH Descriptor Record 44 (Flash Descriptor Records)

Flash Address:FPSBA + 04Ch Size: 8 bit Default value: 64h

Default Flash Address: 14Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x14Ch	6:0	**GbE PHY SMBus Address:** This is the 7 bit SMBus address the PHY uses to accept SMBus cycles from the MAC. This field must be programmed to **64h**.	This is the Intel PHY's SMBus address. This field must be programmed to 64h. GbE PHY SMBus Address and GbE MAC address have to be programmed to 64h and 70h in order to ensure proper arbitration of SMBus communication between the Intel integrated MAC and PHY.	**Yes**



9.46 PCH Descriptor Record 45 (Flash Descriptor Records)

Flash Address:FPSBA + 04Dh Size: 8 bit Default value: 00h

Default Flash Address: 14Dh

Offset from 0	Bits	Description	Usage	FIT Visible
0x14Dh	6:0	**Reserved, set to '0'**		**No**

9.47 PCH Descriptor Record 46 (Flash Descriptor Records)

Flash Address:FPSBA + 04Eh Size: 8 bit Default value: 00h

Default Flash Address: 14Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0x14Eh	0	**Reserved, set to '0'**		**No**

9.48 PCH Descriptor Record 47 (Flash Descriptor Records)

Flash Address:FPSBA + 04Fh Size: 8 bit Default value: 00h

Default Flash Address: 14Fh

Offset from 0	Bits	Description	Usage	FIT Visible
0x14Fh	0	**Reserved, set to '0'**		**No**

9.49 PCH Descriptor Record 48 (Flash Descriptor Records)

Flash Address:FPSBA + 050h Size: 8 bit Default value: 00h

Default Flash Address: 150h

Offset from 0	Bits	Description	Usage	FIT Visible
0x150h	1:0	**Reserved, set to '0'**		**No**

9.50 PCH Descriptor Record 49 (Flash Descriptor Records)

Flash Address:FPSBA + 051h Size: 8 bit Default value: 00h

Default Flash Address: 151h

Offset from 0	Bits	Description	Usage	FIT Visible
0x151h	2:0	**Reserved, set to '0'**		**No**

9.51 PCH Descriptor Record 50 (Flash Descriptor Records)

Flash Address:FPSBA + 054h

Default Flash Address: 154h

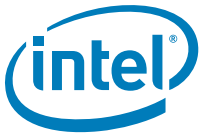
Offset from 0	Bits	Description	Usage	FIT Visible
0x154h	7:6	**Reserved, set to '0'**		**No**
	5:4	**Intel® RST for PCIe-C3 Select x2 or x4:** 00 = Reserved 01 = Intel® RST for PCIe-C3 configured for x2 **(default)** 10 = Intel® RST for PCIe-C3 configured for x4 11 = Reserved	This is used to configure the platform for the Intel® RST for PCIe interface to either x2 or x4 lane operation on **PCIe Controller 3 (Port 9-12).** ***Note:*** 1. Only 2 concurrent SATA Express devices supported for Skylake-LP	**Yes**
	3:2	**Intel® RST for PCIe-C2 Select x2 or x4:** 00 = Reserved 01 = Intel® RST for PCIe-C2 configured for x2 **(default)** 10 = Intel® RST for PCIe-C2 configured for x4 11 = Reserved	This is used to configure the platform for the Intel® RST for PCIe interface to either x2 or x4 lane operation on **PCIe Controller 2 (Port 5-8).** ***Note:*** 1. Only 2 concurrent SATA Express devices supported for Skylake-LP.	**Yes**
	1:0	**Reserved, set to '0x1'**		**No**

9.52 PCH Descriptor Record 51 (Flash Descriptor Records)

Flash Address:FPSBA + 055h Size: 8 bit Default value: 00h

Default Flash Address: 155h

Offset from 0	Bits	Description	Usage	FIT Visible
	5:4	**Intel® RST for PCIe Ctrl 3 Strap:** 00 = Reserved 01 = Reserved 10 = 2x2 **(default)** 11 = 1x4	This is used to configure the platform for the Intel® RST for PCIe interface to either x2 or x4 lane operation on **PCIe Controller 3 (Port 9-12)**. ***Note:*** 1. Only 3 concurrent SATA Express devices supported for Skylake-H. 2. When enabling the Intel® RST for PCIe interface this setting must match the port configuration **PCIe Controller 3 (Port 9-12)** and **Intel® RST for PCIe Controller 3.**	**No**
	3:2	**Intel® RST for PCIe Ctrl 2 Strap:** 00 = Reserved 01 = Reserved 10 = 2x2 **(default)** 11 = 1x4	This is used to configure the platform for the Intel® RST for PCIe interface to either x2 or x4 lane operation on **PCIe Controller 2 (Port 5-8)**. ***Note:*** 1. Only 3 concurrent SATA Express devices supported for Skylake-H 2. When enabling the Intel® RST for PCIe interface this setting must match the port configuration **PCIe Controller 2 (Port 5-8)** and **Intel® RST for PCIe Controller 2.**	**No**
0x155h	1:0	**Reserved, set to '0x2'**		**No**



9.53 PCH Descriptor Record 52 (Flash Descriptor Records)

Flash Address:FPSBA + 058h

Default Flash Address: 158h

Offset from 0	Bits	Description	Usage	FIT Visible
0x158h	5:2	**Reserved, set to '0'**		**No**
	1:0	**Reserved, set to '0x2'**		**No**

9.54 PCH Descriptor Record 53 (Flash Descriptor Records)

Flash Address:FPSBA + 05Ch

Default Flash Address: 15Ch

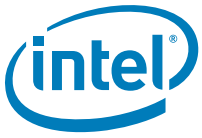
Offset from 0	Bits	Description	Usage	FIT Visible
0x15Ch	5:4	**Reserved, set to '0'**		**No**
	3:2	**Intel® RST for PCIe Controller 2:** 00 = Reserved 01 = Reserved 10 = 2x2 **(default)** 11 = 1x4	This is used to configure the platform for the Intel® RST for PCIe interface to either x2 or x4 lane operation on **PCIe Controller 2 (Port 5-8).** ***Note:*** 1. Only 2 concurrent SATA Express devices supported for Skylake-LP. 2. The x1 is required to meet PCIe specification requirement but is not a supported SATA Express configuration. 3. When enabling the Intel® RST for PCIe interface this setting must match the port configuration **PCIe Controller 2 (Port 5-8)** and **Intel® RST for PCIe Controller 2.**	**Yes**
	1:0	**Reserved, set to '0'**		**No**

9.55 PCH Descriptor Record 54 (Flash Descriptor Records)

Flash Address:FPSBA + 060h

Default Flash Address: 160h

Offset from 0	Bits	Description	Usage	FIT Visible
0x160h	5:4	**Intel® RST for PCIe Controller 3:** 00 = Reserved 01 = Reserved 10 = 2x2 **(default)** 11 = 1x4	This is used to configure the platform for the Intel® RST for PCIe interface to either x2 or x4 lane operation on **PCIe Controller 3 (Port 9-12).** ***Note:*** 1. Only 2 concurrent SATA Express devices supported for Skylake-LP. 2. The x1 is required to meet PCIe specification requirement but is not a supported SATA Express configuration. 3. When enabling the Intel® RST for PCIe interface this setting must match the port configuration **PCIe Controller 3 (Port 9-12)** and **Intel® RST for PCIe Controller 3.** 4. Skylake-Y only supports x2 mode configuration on this controller.	**Yes**
	3:2	**Reserved, set to '0'**		**No**
	1:0	**Reserved, set to '0'**		**No**



9.56 PCH Descriptor Record 55 (Flash Descriptor Records)

Flash Address:FPSBA + 064h

Default Flash Address: 164h

Offset from 0	Bits	Description	Usage	FIT Visible
0x164h	7:6	**LAN PHY Power Control GPD11 Signal Configuration:** 00 = Use as GPD11 01 = Use as LANPHYPC **(default)** **Note:** LANPHYPC can only be driven low if SLP_LAN# is deasserted. Signal can instead be used as GPD11.	**LAN PHY Power Control:** LANPHYPC should be connected to LAN_DISABLE_N on the PHY. PCH will drive LANPHYPC. low to put the PHY into a low power state when functionality is not needed.	**Yes**
	5	**SLP_WLAN# / GPD9 Signal Configuration:** 0 = Use as SLP_WLAN# **(default)** 1 = Use as GPD9	**WLAN Sub-System Sleep Control:** When SLP_WLAN# is de-asserted it indicates that the PHY device must be powered. When SLP_WLAN# is asserted, power can be shut off to the PHY device. SLP_WLAN# will always be deasserted in S0 and anytime SLP_A# is de-asserted.	**Yes**
	4:3	**Reserved, set to '0'**		**No**
	2	**SLP_A# / GPD6 Signal Configuration:** 0 = Use as SLP_A# **(default)** 1 = Use as GPD6		**Yes**
	1	**SLP_S4# / GPD5 Signal Configuration:** 0 = Use as SLP_S4# **(default)** 1 = Use as GPD5		**Yes**
	0	**SLP_S3# / GPD4 Signal Configuration:** 0 = Use as SLP_S3# **(default)** 1 = Use as GPD4		**Yes**

9.57 PCH Descriptor Record 56 (Flash Descriptor Records)

Flash Address:FPSBA + 065h

Default Flash Address: 165h

Offset from 0	Bits	Description	Usage	FIT Visible
0x165h	0	**SLP_S5# / GDP10 Signal Configuration:** 0 = Use as SLP_S5# **(default)** 1 = Use as GPD10		**Yes**

9.58 PCH Descriptor Record 57 (Flash Descriptor Records)

Flash Address:FPSBA + 068h

Default Flash Address: 168h

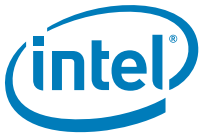
Offset from 0	Bits	Description	Usage	FIT Visible
0x168h	5:4	**SATA / PCIe GP Select for Port 2 (SATA_PCIE_GP2):** 00 = PCIe Port 12 is statically assigned to SATA Port 2 01 = PCIe Port 12 is statically assigned to PCIe (or GbE) **(default)** 10 = Reserved 11 = Assigned based on the polarity for SATAXPCIE2	This strap must also be configured when setting the PCIe/SATA Combo Port 3 Strap (**PCIE_SATA_P3_Flex**) **Note:** This strap and the PCIe/SATA Combo Port 3 Strap (**PCIE_SATA_P3_Flex**) and (**SATA_PCIE_GP2**) must match for proper port function.	**No**
	3:2	**SATA / PCIe GP Select for Port 1 (SATA_PCIE_GP1):** 00 = PCIe Port 8 / PCIe Port 11 is statically assigned to SATA Port 1 01 = PCIe Port 8 / PCIe Port 11 is statically assigned to PCIe (or GbE) 10 = Reserved 11 = Assigned based on the polarity for SATAXPCIE1 **(default)**	This strap must also be configured when setting the PCIe/SATA Combo Port 1 Strap (**PCIE_SATA_P1_Flex**) or PCIe/SATA Combo Port 2 Strap (**PCIE_SATA_P2_Flex**). **Note:** This strap and the PCIe/SATA Combo Port 1 Strap (**PCIE_SATA_P1_Flex**) or PCIe/ SATA Combo Port 2 Strap (**PCIE_SATA_P2_Flex**) and (**SATA_PCIE_SP1**) must match for proper port function.	**No**
	1:0	**SATA / PCIe GP Select for Port 0 (SATA_PCIE_GP0):** 00 = PCIe Port 7 is statically assigned to SATA Port 0 **(default)** 01 = PCIe Port 7 is statically assigned to PCIe (or GbE) 10 = Reserved 11 = Assigned based on the polarity for SATAXPCIE0	This strap must also be configured when setting the PCIe/SATA Combo Port 0 strap (**PCIE_SATA_P0_Flex**). **Note:** This strap and the PCIe/SATA Combo Port 0 strap (**PCIE_SATA_P0_Flex**) and (**SATA_PCIE_SP0)** must match for proper port function.	**No**

9.59 PCH Descriptor Record 58 (Flash Descriptor Records)

Flash Address:FPSBA + 06Ch

Default Flash Address: 16Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x16Ch	7:5	**Reserved, set to '0'**		**No**
	4	**USB3/ SSIC Combo Port 1 Configuration (USB3_SSIC_P1_STRP)** 0 = Statically assigned to USB3 **(default)** 1 = Statically assigned to SSIC	This strap must also be configured when setting the USB3 / SSIC Combo Port 1 strap (**USB3_SSIC_P1_Flex**). **Note:** This strap and the USB3 / SSIC Combo Port 1 strap (**USB3_SSIC_P1_Flex**) must match forproper port function.	**No**
	3:0	**Reserved, set to '0'**		**No**



9.60 PCH Descriptor Record 59 (Flash Descriptor Records)

Flash Address:FPSBA + 06Dh

Default Flash Address: 16Dh

Offset from 0	Bits	Description	Usage	FIT Visible
0x16Dh	7:0	**Reserved, set to '0'**		**No**

9.61 PCH Descriptor Record 60 (Flash Descriptor Records)

Flash Address:FPSBA + 06Eh

Default Flash Address: 16Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0x16Eh	7:6	**Reserved, set to '0'**		**No**
	5:4	**Reserved, set to '0'**		**No**
	3:2	**USB3 / PCIe Combo Port 1 Strap (PCIE_USB3_P1_STRP)** 00 = Statically assigned to USB3 (default prior to strap pull) 01 = Statically assigned to PCI Express (or GbE) (**default)** 10 = Reserved 11 = Reserved	This strap must also be configured when setting the USB3 / PCIe Combo Port 1 strap (**PCIE_USB3_P1_Flex**). **Note:** This strap and the USB3 / PCIe Combo Port 1 strap (**PCIE_USB3_P1_Flex**) must match forproper port function.	**No**
	1:0	**USB3 / PCIe Combo Port 0 Strap (PCIE_USB3_P0_STRP)** 00 = Statically assigned to USB3 (default prior to strap pull) 01 = Statically assigned to PCI Express (or GbE) (**default**) 10 = Reserved 11 = Reserved	This strap must also be configured when setting the USB3 / PCIe Combo Port 0 strap (**PCIE_USB3_P0_Flex**). **Note:** This strap and the USB3 / PCIe Combo Port 0 strap (**PCIE_USB3_P0_Flex**) must match forproper port function.	**No**

9.62 PCH Descriptor Record 61 (Flash Descriptor Records)

Flash Address:FPSBA + 070h

Default Flash Address: 170h

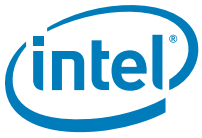
Offset from 0	Bits	Description	Usage	FIT Visible
0x170h	31:0	**Reserved, set to '0'**		**No**

9.63 PCH Descriptor Record 62 (Flash Descriptor Records)

Flash Address:FPSBA + 074h Size: 8 bit Default value: 0Eh

Default Flash Address: 174h

Offset from 0	Bits	Description	Usage	FIT Visible
0x174h	3:1	**Reserved, set to '111b'**		**No**
	0	**Reserved, set to '0'**		**No**



9.64 PCH Descriptor Record 63 (Flash Descriptor Records)

Flash Address:FPSBA + 078h

Default Flash Address: 178h

Offset from 0	Bits	Description	Usage	FIT Visible
0x178h	1	**Reserved, set to '0'**		**No**
	0	**TPM Over SPI Bus Enable (TOS):** 0 = TPM is not on SPI **(default)** 1 = TPM is on SPI		**Yes**

9.65 PCH Descriptor Record 64 (Flash Descriptor Records)

Flash Address:FPSBA + 07Ch

Default Flash Address: 17Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x17Ch	7	**Reserved, set to '0'**		**No**
	6	**Intel® PHY Over PCIe Enable (PHY_PCIE_EN):** 0 = Intel integrated wired MAC/PHY communication is not enabled over PCI Express*. 1 = The PCI Express* port selected by the **PHY_PCIEPORT_SEL** soft strap to be used by Intel® PHY **(default)** ***Notes:*** This bit must be "1" if using Intel integrated wired LAN solution.	This bit MUST be set to '1' if using Intel® integrated wired LAN solution. If not using, or if disabling Intel® integrated wired LAN solution then set this to '0'.	**Yes**
	5:3	**GBE PCIe* Port Select (GBE_PCIEPORTSEL):** This strap defines the GbE port. 000 = PORT3 001 = PORT4 010 = PORT5 **(default)** 011 = PORT9 100 = PORT10 101-111b = Reserved	This field tells the PCH which PCI Express* port an Intel® PHY is connected. If PHY_PCIE_EN is ='0', then this field is ignored. ***Notes:*** This setting is not the same for all designs, is dependent on the board design. The platform hardware designer or schematic review can determine what PCIe Port the Intel wired PHY is routed.	**Yes**
	2	**DMI / PCIe Port Staggering Enable:** 0 = Disabled 1 = Enabled **(default)**		**Yes**
	1:0	**Reserved, set to '0'**		**No**

9.66 PCH Descriptor Record 65 (Flash Descriptor Records)

Flash Address:FPSBA + 07Dh

Default Flash Address: 17Dh

Offset from 0	Bits	Description	Usage	FIT Visible
0x17Dh	7:6	**Reserved, set to '0'**		**No**
	5:4	**SATA / PCIe Combo Port 2 Strap (PCIE_SATA_P2_Flex):** 00 = PCIe Port 11 is statically assigned to SATA Port 1 01 = PCIe Port 11 is statically assigned to PCIe (or GbE) **(default)** 10 = Reserved 11 = Assigned based on the polarity of SATAXPCIE1 determined by PSCPSP_P2_STRP	This setting determine if PCIe/SATA Comb Port 2 is configured natively for SATA or PCIe. If the strap setting is configured to '11' the Combo Port behavior is determined by the Combo Port2 Select Polarity strap (**PSCPSP_P2_STRP**). **Note:** The settings for this strap and the SATA / PCIe Select for Port 1(**SATA_PCIE_SP1**) and (**SATA_PCIE_GP1**) strap must match for proper port function.	**Yes**
	3:2	**SATA / PCIe Combo Port 1 Strap (PCIE_SATA_P1_Flex):** 00 = PCIe Port 8 is statically assigned to SATA Port 1 01 = PCIe Port 8 is statically assigned to PCIe (or GbE) 10 = Reserved 11 = Assigned based on the polarity of SATAXPCIE1 determined by PSCPSP_P1_STRP **(default)**	This setting determine if PCIe/SATA Comb Port 1 is configured natively for SATA or PCIe. If the strap setting is configured to '11' the Combo Port behavior is determined by the Combo Port1 Select Polarity strap (**PSCPSP_P1_STRP**). **Note:** The settings for this strap and the SATA / PCIe Select for Port 1 (**SATA_PCIE_SP1**) and (**SATA_PCIE_GP1**) strap must match for proper port function.	**Yes**
	1:0	**SATA / PCIe Combo Port 0 Strap (PCIE_SATA_P0_Flex):** 00 = PCIe Port 7 is statically assigned to SATA Port 0 **(default)** 01 = PCIe Port 7 is statically assigned to PCIe (or GbE) 10 = Reserved 11 = Assigned based on the polarity of SATAXPCIE0 determined by PSCPSP_P0_STRP	This setting determine if PCIe/SATA Comb Port 0 is configured natively for SATA or PCIe. If the strap setting is configured to '11' the Combo Port behavior is determined by the Combo Port0 Select Polarity strap (**PSCPSP_P0_STRP**). **Note:** The settings for this strap and the SATA / PCIe Select for Port 0 (**SATA_PCIE_SP0**) and (**SATA_PCIE_GP0**) must match for proper port function.	**Yes**

9.67 PCH Descriptor Record 66 (Flash Descriptor Records)

Flash Address:FPSBA + 07Eh

Default Flash Address: 17Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0x17Eh	7:5	**Reserved, set to '0'**		**No**
	4	**USB3 / SSIC Combo Port 1 (USB3_SSIC_P1_Flex):** 0x0 = USB3 Port 2 **(default)** 0x1 = SSIC Port 1 ***Note:*** For SSIC **USB3_SSIC_CFG** needs to be set to 0x0. ***Note:*** For USB3 **USB3_SSIC_CFG** needs to be set to 0x1	This setting determine if USB3 / SSIC Combo Port 1 is configured natively for USB3 or SSIC. **Note:** The settings for this strap and the USB3 / SSIC Select for Port 1 (**USB3_SSIC_P1_STRP**) strap must match for proper port function.	**Yes**
	3:0	**Reserved, set to '0'**		**No**

9.68 PCH Descriptor Record 67 (Flash Descriptor Records)

Flash Address:FPSBA + 07Fh

Default Flash Address: 17Fh

Offset from 0	Bits	Description	Usage	FIT Visible
0x17Fh	7:0	**Reserved, set to '0'**		**No**

9.69 PCH Descriptor Record 68 (Flash Descriptor Records)

Flash Address:FPSBA + 80h

Default Flash Address: 180h

Offset from 0	Bits	Description	Usage	FIT Visible
0x180h	7:2	Reserved, set to '0'		**No**
	1:0	**SATA / PCIe Combo Port 3 Strap (PCIE_SATA_P3_Flex):** 00 = PCIe Port 12 is statically assigned to SATA Port 2 01 = PCIe Port 12 is statically assigned to PCIe (or GbE) **(default)** 10 = Reserved 11 = Assigned based on the polarity of SATAXPCIE2 determined by PSCPSP_P3_STRP	This setting determines if PCIe/SATA Comb Port 3 is configured natively for SATA or PCIe. If the strap setting is configured to '11' the Combo Port behavior is determined by the Combo Port Select Polarity strap (**PSCPSP_P3_STRP**). **Note:** The settings for this strap and the SATA / PCIe Select for Port 2(**SATA_PCIE_SP2**) and (**SATA_PCIE_GP2**) must match for proper port function.	**Yes**

9.70 PCH Descriptor Record 69 (Flash Descriptor Records)

Flash Address:FPSBA + 81h

Default Flash Address: 181h

Offset from 0	Bits	Description	Usage	FIT Visible
0x181h	7:0	**Reserved, set to '0'**		**No**

9.71 PCH Descriptor Record 70 (Flash Descriptor Records)

Flash Address:FPSBA + 82h

Default Flash Address: 182h

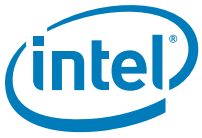
Offset from 0	Bits	Description	Usage	FIT Visible
0x182h	7:4	**Reserved, set to '0'**		**No**
	3:2	**USB3 / PCIe Combo Port 1 (PCIE_USB3_P1_Flex):** 00 = Statically assigned to USB3 Port 6 01 = Statically assigned to PCIe Port 2 (or GbE) **(default)** 10 = Reserved. 11 = Reserved.	This setting determine if USB3 / PCIe Combo Port 1 is configured natively for USB3 or PCIe. **Note:** The settings for this strap and the USB3 / PCIe Select for Port 1 (**PCIE_USB3_P1_STRP**) strap must match for proper port function.	**Yes**
	1:0	**USB3 / PCIe Combo Port 0 (PCIE_USB3_P0_Flex):** 00 = Statically assigned to USB3 Port 5 01 = Statically assigned to PCIe Port1 (or GbE) **(default)** 10 = Reserved. 11 = Reserved.	This setting determine if USB3 / PCIe Combo Port 0 is configured natively for USB3 or PCIe. **Note:** The settings for this strap and the USB3 / PCIe Select for Port 0 (**PCIE_USB3_P0_STRP**) strap must match for proper port function.	**Yes**

9.72 PCH Descriptor Record 71 (Flash Descriptor Records)

Flash Address:FPSBA + 83h

Default Flash Address: 183h

Offset from 0	Bits	Description	Usage	FIT Visible
0x183h	7:0	**Reserved, set to '0'**		**No**



9.73 PCH Descriptor Record 72 (Flash Descriptor Records)

Flash Address:FPSBA + 84h

Default Flash Address: 184h

Offset from 0	Bits	Description	Usage	FIT Visible
0x184h	7:4	**Reserved, set to '0'**		**No**
	3	**Polarity Select SATA / PCIe Combo Port 3 (PSCPSP_P3_STRP):** 0x0 = Combo Port 3 is set to PCIe mode when the Combo Port Select pin is '0' and SATA when Combo Port Select pin is '1' **(default)** 0x1 = Combo Port 3 is set to SATA mode when the Combo Port Select pin is '0' and PCIe when Combo Port Select pin is '1' **Note:** This strap is expected to be set to '0x1' when the combo port is mapped to NGFF M.2 or eSATA connector and set to '0x0' when the combo port is mapped to mSATA connector.	This strap is used to determine the configuration the native mode configuration for PCIe/SATA Combo Port 3. Note: This setting only has effect when PCIe/ SATA Combo Port 3 (**PCIE_SATA_P3_STRP**) is configured to '11' When configuring this strap you must also configure SATA / PCIe GPIO Polarity Port 2 (**SPS2**) to the same setting.	**Yes**
	2	**Polarity Select SATA / PCIe Combo Port 2 (PSCPSP_P2_STRP):** 0x0 = Combo Port 2 is set to PCIe mode when the Combo Port Select pin is '0' and SATA when Combo Port Select pin is '1' **(default)** 0x1 = Combo Port 2 is set to SATA mode when the Combo Port Select pin is '0' and PCIe when Combo Port Select pin is '1' **Note:** This strap is expected to be set to '0x1' when the combo port is mapped to NGFF M.2 or eSATA connector and set to '0x0' when the combo port is mapped to mSATA connector.	This strap is used to determine the configuration the native mode configuration for PCIe/SATA Combo Port 2. Note: This setting only has effect when PCIe/ SATA Combo Port 2 (**PCIE_SATA_P2_STRP**) is configured to '11' When configuring this strap you must also configure SATA / PCIe GPIO Polarity Port 1 (**SPS1**) to the same setting.	**Yes**
	1	**Polarity Select SATA / PCIe Combo Port 1 (PSCPSP_P1_STRP):** 0x0 = Combo Port 1 is set to PCIe mode when the Combo Port Select pin is '0' and SATA when Combo Port Select pin is '1' **(default)** 0x1 = Combo Port 1 is set to SATA mode when the Combo Port Select pin is '0' and PCIe when Combo Port Select pin is '1' **Note:** This strap is expected to be set to '0x1' when the combo port is mapped to NGFF M.2 or eSATA connector and set to '0x0' when the combo port is mapped to mSATA connector.	This strap is used to determine the configuration the native mode configuration for PCIe/SATA Combo Port 1. Note: This setting only has effect when PCIe/ SATA Combo Port 1 (**PCIE_SATA_P1_STRP**)is configured to '11' When configuring this strap you must also configure SATA / PCIe GPIO Polarity Port 1 (**SPS1**) to the same setting.	**Yes**
	0	**Polarity Select SATA / PCIe Combo Port 0 (PSCPSP_P0_STRP):** 0x0 = Combo Port 0 is set to PCIe mode when the Combo Port Select pin is '0' and SATA when Combo Port Select pin is '1' **(default)** 0x1 = Combo Port 0 is set to SATA mode when the Combo Port Select pin is '0' and PCIe when Combo Port Select pin is '1' **Note:** This strap is expected to be set to '0x1' when the combo port is mapped to NGFF M.2 or eSATA connector and set to '0x0' when the combo port is mapped to mSATA connector.	This strap is used to determine the configuration the native mode configuration for PCIe/SATA Combo Port 0. Note: This setting only has effect when PCIe/ SATA Combo Port 0 (**PCIE_SATA_P0_STRP**) is configured to '11' When configuring this strap you must also configure SATA / PCIe GPIO Polarity Port 0 (**SPS0**)to the same setting.	**Yes**

9.74 PCH Descriptor Record 73 (Flash Descriptor Records)

Flash Address:FPSBA + 85h

Default Flash Address: 185h

Offset from 0	Bits	Description	Usage	FIT Visible
0x185h	7:0	**Reserved, set to '0'**		**No**

9.75 PCH Descriptor Record 74 (Flash Descriptor Records)

Flash Address:FPSBA + 86h

Default Flash Address: 186h

Offset from 0	Bits	Description	Usage	FIT Visible
0x186h	7:0	**Reserved, set to '0'**		**No**

9.76 PCH Descriptor Record 75 (Flash Descriptor Records)

Flash Address:FPSBA + 87h

Default Flash Address: 187h

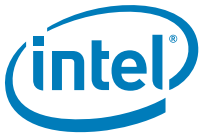
Offset from 0	Bits	Description	Usage	FIT Visible
0x187h	7:0	**Reserved, set to '0'**		**No**

9.77 PCH Descriptor Record 76 (Flash Descriptor Records)

Flash Address:FPSBA + 88h Size: 8 bit Default value: 00h

Default Flash Address: 188h

Offset from 0	Bits	Description	Usage	FIT Visible
0x188h	0	**Reserved, set to '0'**		**No**



9.78 PCH Descriptor Record 77 (Flash Descriptor Records)

Flash Address:FPSBA + 8Ch

Default Flash Address: 18Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x18Ch	7:6	**Reserved. Set to 0x1**		**No**
	5:4	**SATA / PCIe Select for Port 2 (SATA_PCIE_SP2):** 00 = PCIe Port 12 is statically assigned to SATA Port 1 01 = PCIe Port 12 is statically assigned to PCIe (or GbE) **(default)** 10 = Reserved 11 = Assigned based on the polarity for SATAXPCIE2	This strap must also be configured when setting the PCIe/SATA Combo Port 3 Strap (**PCIE_SATA_P3_Flex**) **Note:** This strap and the PCIe/SATA Combo Port 3 Strap (**PCIE_SATA_P3_Flex**) and (**SATA_PCIE_GP2)** must match for proper port function.	**No**
	3:2	**SATA / PCIe Select for Port 1 (SATA_PCIE_SP1):** 00 = PCIe Port 8 / PCIe Port 11 is statically assigned to SATA Port 1 01 = PCIe Port 8 / PCIe Port 11 is statically assigned to PCIe (or GbE) 10 = Reserved 11 = Assigned based on the polarity for SATAXPCIE1 **(default)**	This strap must also be configured when setting the PCIe/SATA Combo Port 1 Strap (**PCIE_SATA_P1_Flex**) or PCIe/SATA Combo Port 2 Strap (**PCIE_SATA_P2_Flex**). **Note:** This strap and the PCIe/SATA Combo Port 1 Strap (**PCIE_SATA_P1_Flex**) or PCIe/ SATA Combo Port 2 Strap (**PCIE_SATA_P2_Flex**) and (**SATA_PCIE_GP1)** must match for proper port function.	**No**
	1:0	**SATA / PCIe Select for Port 0 (SATA_PCIE_SP0):** 00 = PCIe Port 7 is statically assigned to SATA Port 0 **(default)** 01 = PCIe Port 7 is statically assigned to PCIe (or GbE) 10 = Reserved 11 = Assigned based on the polarity for SATAXPCIE0	This strap must also be configured when setting the PCIe/SATA Combo Port 0 strap (**PCIE_SATA_P0_Flex**). **Note:** This strap and the PCIe/SATA Combo Port 0 strap (**PCIE_SATA_P0_Flex**) and (**SATA_PCIE_GP0**) must match for proper port function.	**No**

9.79 PCH Descriptor Record 78 (Flash Descriptor Records)

Flash Address:FPSBA + 8Dh

Default Flash Address: 18Dh

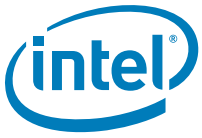
Offset from 0	Bits	Description	Usage	FIT Visible
0x18Dh	7	**Reserved. Set to 0x0**		**No**
	6	**SATA / PCIe GPIO Polarity Port 2 (SPS2):** 0x0 = GPIO Polarity Port 2 is set to PCIe mode when the SATAXPCIE2 pin is '0' and SATA when SATAXPCIE2 pin is '1' **(default)** 0x1 = GPIO Polarity Port 2 is set to SATA mode when the SATAXPCIE2 pin is '0' and PCIe when SATAXPCIE2 pin is '1'	This strap must also be configured if **PCIe/ SATA Combo Port 3 Strap (PCIE_SATA_P3_Flex)** is configured to '11' **Note:** This setting only has effect when SATA / PCIe Select for Port 3 (**SATA_PCIE_SP2**) is configured to '11' **Note:** This strap and the Polarity Select SATA / PCIe Combo Port 3 (**PSCPSP_P3_STRP**) must match for proper port function.	**No**
	5	**SATA / PCIe GPIO Polarity Port 1 (SPS1):** 0x0 = GPIO Polarity Port 1 is set to PCIe mode when the SATAXPCIE1 pin is '0' and SATA when SATAXPCIE1 pin is '1' **(default)** 0x1 = GPIO Polarity Port 1 is set to SATA mode when the SATAXPCIE1 pin is '0' and PCIe when SATAXPCIE1 pin is '1'	This strap must also be configured if **PCIe/ SATA Combo Port 1 Strap (PCIE_SATA_P1_Flex) or PCIe/SATA Combo Port 2 Strap (PCIE_SATA_P2_Flex)** is configured to '11' **Note:** This setting only has effect when SATA / PCIe Select for Port 1 (**SATA_PCIE_SP2**) is configured to '11' **Note:** This strap and the Polarity Select SATA / PCIe Combo Port 1 (**PSCPSP_P2_STRP**) must match for proper port function.	**No**
	4	**SATA / PCIe GPIO Polarity Port 0 (SPS0):** 0x0 = GPIO Polarity Port 0 is set to PCIe mode when the SATAXPCIE0 pin is '0' and SATA when SATAXPCIE0 pin is '1' **(default)** 0x1 = GPIO Polarity Port 0 is set to SATA mode when the SATAXPCIE0 pin is '0' and PCIe when SATAXPCIE0 pin is '1'	This strap must also be configured if **PCIe/ SATA** Combo Port 0 strap (**PCIE_SATA_P0_Flex**) is configured to '11' **Note:** This setting only has effect when SATA / PCIe Select for Port 0 (**SATA_PCIE_SP0**) is configured to '11' **Note:** This strap and the Polarity Select SATA / PCIe Combo Port 0 (**PSCPSP_P0_STRP**) must match for proper port function.	**No**
	3:0	**Reserved, set to '0x5'**		**No**

9.80 PCH Descriptor Record 79 (Flash Descriptor Records)

Flash Address:FPSBA + 8Eh Size: 8 bit Default value: 00h

Default Flash Address: 18Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0x18Eh	1:0	**Reserved, set to '0'**		**No**



9.81 PCH Descriptor Record 80 (Flash Descriptor Records)

Flash Address:FPSBA + 90h

Default Flash Address: 190h

Offset from 0	Bits	Description	Usage	FIT Visible
0x190h	7:2	**Reserved set to '0x24'**		**No**
	1:0	**Reserved, set to '0x1'**		**No**

9.82 PCH Descriptor Record 81 (Flash Descriptor Records)

Flash Address:FPSBA + 91h

Default Flash Address: 191h

Offset from 0	Bits	Description	Usage	FIT Visible
0x191h	7	**Reserved, set to '0x1'**		**No**
	6:0	**Reserved, set to '0x70'**		**No**

9.83 PCH Descriptor Record 82 (Flash Descriptor Records)

Flash Address:FPSBA + 92h

Default Flash Address: 192h

Offset from 0	Bits	Description	Usage	FIT Visible
0x192h	7:3	**Reserved set to '0x01'**		**No**
	2:0	**PHY Connection (PHYCON):** This field determines if Intel® wired PHY is connected. 000 = No PHY connected 001= PHY on SMBus 010 = PHY on SMLink0 **(default)** 011 = PHY on SMLink1	This field must be set to "10" if Intel® integrated wired LAN solution is used. If not using, or if disabling Intel® integrated wired LAN solution, then field must be set to "00".	**Yes**

9.84 PCH Descriptor Record 83 (Flash Descriptor Records)

Flash Address:FPSBA + 93h

Default Flash Address: 193h

Offset from 0	Bits	Description	Usage	FIT Visible
0x193h	7:4	**Reserved, set to '0xf'**		**No**
	3:2	**Reserved, set to '0x3'**		**No**
	1:0	**Reserved, set to '0x3'**		**No**

9.85 PCH Descriptor Record 84 (Flash Descriptor Records)

Flash Address:FPSBA + 94h

Default Flash Address: 194h

Offset from 0	Bits	Description	Usage	FIT Visible
0x194h	7:4	**Reserved, set to '0xf'**		**No**
	3	**Reserved, set to '0'**		**No**
	2	**Reserved set to '0x1'**		**No**
	1:0	**Reserved, set to '0x3'**		**No**

9.86 PCH Descriptor Record 85 (Flash Descriptor Records)

Flash Address:FPSBA + 95h

Default Flash Address: 195h

Offset from 0	Bits	Description	Usage	FIT Visible
0x195h	7:2	**Reserved, set to '0x3f'**		**No**
	1:0	**Reserved, set to '0'**		**No**

9.87 PCH Descriptor Record 86 (Flash Descriptor Records)

Flash Address:FPSBA + 96h

Default Flash Address: 196h

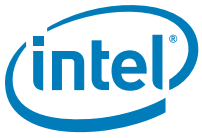
Offset from 0	Bits	Description	Usage	FIT Visible
0x196h	7:2	**Reserved, set to '0x3f'**		**No**
	1:0	**Reserved, set to '0'**		**No**

9.88 PCH Descriptor Record 87 (Flash Descriptor Records)

Flash Address:FPSBA + 97h

Default Flash Address: 197h

Offset from 0	Bits	Description	Usage	FIT Visible
0x197h	7:2	**Reserved, set to '0x3f'**		**No**
	1:0	**Reserved, set to '0'**		**No**



9.89 PCH Descriptor Record 88 (Flash Descriptor Records)

Flash Address:FPSBA + 98h

Default Flash Address: 198h

Offset from 0	Bits	Description	Usage	FIT Visible
0x198h	31:0	**Reserved, set to '0'**		**No**

9.90 PCH Descriptor Record 89 (Flash Descriptor Records)

Flash Address:FPSBA + 9Ch

Default Flash Address: 19Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x19Ch	7:0	**Reserved, set to '0'**		**No**

9.91 PCH Descriptor Record 90 (Flash Descriptor Records)

Flash Address:FPSBA + 9Dh

Default Flash Address: 19Dh

Offset from 0	Bits	Description	Usage	FIT Visible
0x19Dh	7:5	**Reserved, set to '0x0'**		**No**
	4:3	**PCIe Controller 1 (Port 1-4):** Straps to set the default value of the PCI Express Port Configuration 1 register covering PCIe ports 1-4. 00 = 4x1 01 = 1x2, 2x1 10 = 2x2 11 = 1x4 **(default)** ***Note:*** Refer to EDS for PCIe supported port configurations.	Setting of this field depend on what PCIe ports 1-4 configurations are desired by the board manufacturer. ***Note:*** This field must be determined by the PCI Express port requirements of the design. The platform hardware designer must determine this setting.	**Yes**
	2	**PCIe Controller 1 Lane Reversal:** 0 = PCIe Lanes are not reversed. **(default)** 1 = PCIe Lanes are reversed. ***Note:*** Refer to EDS supported Lane reversal configuration.	This bit controls lane reversal behavior for PCIe Controller 1. PCI Express port lane reversal can be done to aid in the laying out of the board. **Note:** This setting is dependent on the board design. The platform hardware designer must determine if this port needs lane reversal.	**Yes**
	1:0	**Reserved, set to '0'**		**No**

9.92 PCH Descriptor Record 91 (Flash Descriptor Records)

Flash Address:FPSBA + 9Eh

Default Flash Address: 19Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0x19Eh	7:0	Reserved, set to '0'		No

9.93 PCH Descriptor Record 92 (Flash Descriptor Records)

Flash Address:FPSBA + 9Fh

Default Flash Address: 19Fh

Offset from 0	Bits	Description	Usage	FIT Visible
0x19Fh	7:0	Reserved, set to '0'		No

9.94 PCH Descriptor Record 93 (Flash Descriptor Records)

Flash Address:FPSBA + A0h

Default Flash Address: 1A0h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1A0h	7:0	Reserved, set to '0'		No

9.95 PCH Descriptor Record 94 (Flash Descriptor Records)

Flash Address:FPSBA + A1h

Default Flash Address: 1A1h

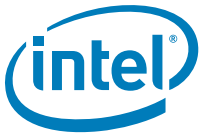
Offset from 0	Bits	Description	Usage	FIT Visible
0x1A1h	7:0	Reserved, set to '0'		No

9.96 PCH Descriptor Record 95 (Flash Descriptor Records)

Flash Address:FPSBA + A2h

Default Flash Address: 1A2h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1A2h	7:0	Reserved, set to '0'		No



9.97 PCH Descriptor Record 96 (Flash Descriptor Records)

Flash Address:FPSBA + A3h

Default Flash Address: 1A3h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1A3h	7:0	**Reserved, set to '0'**		**No**

9.98 PCH Descriptor Record 97 (Flash Descriptor Records)

Flash Address:FPSBA + A4h

Default Flash Address: 1A4h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1A4h	7:0	**Reserved, set to '0'**		**No**

9.99 PCH Descriptor Record 98 (Flash Descriptor Records)

Flash Address:FPSBA + A5h

Default Flash Address: 1A5h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1A5h	7:5	**Reserved, set to '0'**		**No**
	4:3	**PCIe Controller 2 (Port 5-8):** Straps to set the default value of the PCI Express Port Configuration 2 register covering PCIe ports 5-8. 00 = 4x1 **(default)** 01 = 1x2, 2x1 10 = 2x2 11 = 1x4 ***Note:*** Refer to EDS for PCIe supported port configurations.	Setting of this field depend on what PCIe ports 5-8 configurations are desired by the board manufacturer. ***Note:*** This field must be determined by the PCI Express port requirements of the design. The platform hardware designer must determine this setting.	**Yes**
	2	**PCIe Controller 2 Lane Reversal:** 0 = PCIe Lanes are not reversed. **(default)** 1 = PCIe Lanes are reversed. **Note**: Refer to EDS supported Lane reversal configuration.	This bit controls lane reversal behavior for PCIe Controller 2. PCI Express port lane reversal can be done to aid in the laying out of the board. ***Note:*** This setting is dependent on the board design. The platform hardware designer must determine if this port needs lane reversal.	**Yes**
	1:0	**Reserved, set to '0'**		**No**

9.100 PCH Descriptor Record 99 (Flash Descriptor Records)

Flash Address:FPSBA + A6h

Default Flash Address: 1A6h

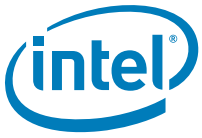
Offset from 0	Bits	Description	Usage	FIT Visible
0x1A6h	7:0	**Reserved, set to '0'**		**No**

9.101 PCH Descriptor Record 100 (Flash Descriptor Records)

Flash Address:FPSBA + A7h

Default Flash Address: 1A7h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1A7h	7	**PCIe Controller 2 Port 4 SRIS:** 0x0 = Disabled **(default)** 0x1 = Enabled	This is used to configures the platform Intel® RST for PCIe (SATA Express) interface on **PCIe Controller 2**. ***Note:*** 1. Only 2 concurrent SATA Express devices supported for Skylake-LP. 2. The x1 is required to meet PCIe specification requirement but is not a supported SATA Express configuration.	**Yes**
	6	**PCIe Controller 2 Port 3 SRIS:** 0x0 = Disabled **(default)** 0x1 = Enabled	This is used to configures the platform Intel® RST for PCIe (SATA Express) interface on **PCIe Controller 2**. ***Note:*** 1. Only 2 concurrent SATA Express devices supported for Skylake-LP. 2. The x1 is required to meet PCIe specification requirement but is not a supported SATA Express configuration.	**Yes**
	5	**PCIe Controller 2 Port 2 SRIS:** 0x0 = Disabled **(default)** 0x1 = Enabled	This is used to configures the platform Intel® RST for PCIe (SATA Express) interface on **PCIe Controller 2**. ***Note:*** 1. Only 2 concurrent SATA Express devices supported for Skylake-LP. 2. The x1 is required to meet PCIe specification requirement but is not a supported SATA Express configuration.	**Yes**
	4	**PCIe Controller 2 Port 1 SRIS:** 0x0 = Disabled **(default)** 0x1 = Enabled	This is used to configures the platform Intel® RST for PCIe (SATA Express) interface on **PCIe Controller 2**. ***Note:*** 1. Only 2 concurrent SATA Express devices supported for Skylake-LP. 2. The x1 is required to meet PCIe specification requirement but is not a supported SATA Express configuration.	**Yes**
	3:0	**Reserved, set to '0'**		**No**



9.102 PCH Descriptor Record 101 (Flash Descriptor Records)

Flash Address:FPSBA + A8h

Default Flash Address: 1A8h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1A8h	7:0	**Reserved, set to '0'**		**No**

9.103 PCH Descriptor Record 102 (Flash Descriptor Records)

Flash Address:FPSBA + A9h

Default Flash Address: 1A9h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1A9h	7:0	**Reserved, set to '0'**		**No**

9.104 PCH Descriptor Record 103 (Flash Descriptor Records)

Flash Address:FPSBA + AAh

Default Flash Address: 1AAh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1AAh	7:0	**Reserved, set to '0'**		**No**

9.105 PCH Descriptor Record 104 (Flash Descriptor Records)

Flash Address:FPSBA + ABh

Default Flash Address: 1ABh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1ABh	7:0	**Reserved, set to '0'**		**No**

9.106 PCH Descriptor Record 105 (Flash Descriptor Records)

Flash Address:FPSBA + ACh

Default Flash Address: 1ACh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1ACh	7:0	**Reserved, set to '0'**		**No**

9.107 PCH Descriptor Record 106 (Flash Descriptor Records)

Flash Address:FPSBA + ADh

Default Flash Address: 1ADh

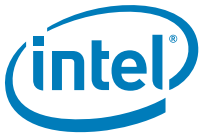
Offset from 0	Bits	Description	Usage	FIT Visible
0x1ADh	7:5	**Reserved, set to '0'**		**No**
	4:3	**PCIe Controller 3 (Port 9-12):** Straps to set the default value of the PCI Express Port Configuration 3 register covering PCIe ports 9-12. 00 = 4x1 **(default)** 01 = 1x2, 2x1 10 = 2x2 11 = 1x4 ***Note:*** Refer to EDS for PCIe supported port configurations. ***Note:*** For Skylake-LP Base U and Premium Y PCIe Controller 3 has only Port 9-10 and is limited to 1x2, 2x1 port configuration only.	Setting of this field depend on what PCIe ports 9-12 configurations are desired by the board manufacturer. ***Note:*** This field must be determined by the PCI Express port requirements of the design. The platform hardware designer must determine this setting.	**Yes**
	2	**PCIe Controller 3 Lane Reversal:** 0 = PCIe Lanes are not reversed. **(default)** 1 = PCIe Lanes are reversed. **Note**: Refer to EDS supported Lane reversal configuration.	This bit controls lane reversal behavior for PCIe Controller 3. PCI Express port lane reversal can be done to aid in the laying out of the board. **Note:** This setting is dependent on the board design. The platform hardware designer must determine if this port needs lane reversal.	**Yes**
	1:0	**Reserved, set to '0'**		**No**

9.108 PCH Descriptor Record 107 (Flash Descriptor Records)

Flash Address:FPSBA + AEh

Default Flash Address: 1AEh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1AEh	7:0	**Reserved, set to '0'**		**No**



9.109 PCH Descriptor Record 108 (Flash Descriptor Records)

Flash Address:FPSBA + AFh

Default Flash Address: 1AFh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1AFh	7	**PCIe Controller 3 Port 4 SRIS Enable:** 0x0 = Disabled **(default)** 0x1 = Enabled	This is used to configures the platform Intel® RST for PCIe (SATA Express) interface on **PCIe Controller 3**. ***Note:*** 1. Only 2 concurrent SATA Express devices supported for Skylake-LP. 2. The x1 is required to meet PCIe specification requirement but is not a supported SATA Express configuration.	**Yes**
	6	**PCIe Controller 3 Port 3 SRIS Enable:** 0x0 = Disabled **(default)** 0x1 = Enabled	This is used to configures the platform Intel® RST for PCIe (SATA Express) interface on **PCIe Controller 3**. ***Note:*** 1. Only 2 concurrent SATA Express devices supported for Skylake-LP. 2. The x1 is required to meet PCIe specification requirement but is not a supported SATA Express configuration.	**Yes**
	5	**PCIe Controller 3 Port 2 SRIS Enable:** 0x0 = Disabled **(default)** 0x1 = Enabled	This is used to configures the platform Intel® RST for PCIe (SATA Express) interface on **PCIe Controller 3**. ***Note:*** 1. Only 2 concurrent SATA Express devices supported for Skylake-LP. 2. The x1 is required to meet PCIe specification requirement but is not a supported SATA Express configuration.	**Yes**
	4	**PCIe Controller 3 Port 1 SRIS Enable:** 0x0 = Disabled **(default)** 0x1 = Enabled	This is used to configures the platform Intel® RST for PCIe (SATA Express) interface on **PCIe Controller 3**. ***Note:*** 1. Only 2 concurrent SATA Express devices supported for Skylake-LP. 2. The x1 is required to meet PCIe specification requirement but is not a supported SATA Express configuration.	**Yes**
	3:0	**Reserved, set to '0'**		**No**

9.110 PCH Descriptor Record 109 (Flash Descriptor Records)

Flash Address:FPSBA + B0h

Default Flash Address: 1B0h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1B0h	7:0	**Reserved, set to '0'**		**No**

9.111 PCH Descriptor Record 110 (Flash Descriptor Records)

Flash Address:FPSBA + B1h

Default Flash Address: 1B1h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1B1h	7:0	**Reserved, set to '0'**		**No**

9.112 PCH Descriptor Record 111 (Flash Descriptor Records)

Flash Address:FPSBA + B2h

Default Flash Address: 1B2h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1B2h	7:0	**Reserved, set to '0'**		**No**

9.113 PCH Descriptor Record 112 (Flash Descriptor Records)

Flash Address:FPSBA + B3h

Default Flash Address: 1B3h

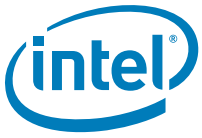
Offset from 0	Bits	Description	Usage	FIT Visible
0x1B3h	7:0	**Reserved, set to '0'**		**No**

9.114 PCH Descriptor Record 113 (Flash Descriptor Records)

Flash Address:FPSBA + B4h

Default Flash Address: 1B4h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1B4h	31:7	**Reserved, set to '0'**		**No**
	6	**Reserved, set to '0x1'**		**No**
	5:0	**Reserved, set to '0x7'**		**No**



9.115 PCH Descriptor Record 114 (Flash Descriptor Records)

Flash Address:FPSBA + B8h

Default Flash Address: 1B8h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1B8h	7:6	**Reserved, set to '0'**		**No**
	5	**XHCI Port 5 Ownership (XHCI_PORT5_OWNERSHIP_STRAP):** Strap to decide XHCI Port 6 Ownership between XHCI/PCIe/CSI. 0x0 = XHCI Port 6 configured as XHCI 0x1 = XHCI Port 6 configures as Non-XHCI **(default)**		**Yes**
	4	**XHCI Port 4 Ownership (XHCI_PORT4_OWNERSHIP_STRAP):** Strap to decide XHCI Port 5 Ownership between XHCI/PCIe/CSI. 0x0 = XHCI Port 5 configured as XHCI 0x1 = XHCI Port 5 configures as Non-XHCI **(default)**		**Yes**
	3	**XHCI Port 3 Ownership (XHCI_PORT3_OWNERSHIP_STRAP):** Strap to decide XHCI Port 4 Ownership between XHCI/PCIe/CSI. 0x0 = XHCI Port 4 configured as XHCI **(default)** 0x1 = XHCI Port 4 configures as Non-XHCI		**Yes**
	2	**XHCI Port 2 Ownership (XHCI_PORT2_OWNERSHIP_STRAP):** Strap to decide XHCI Port 3 Ownership between XHCI/PCIe/CSI. 0x0 = XHCI Port 3 configured as XHCI **(default)** 0x1 = XHCI Port 3 configures as Non-XHCI		**Yes**
	1	**XHCI Port 1 Ownership (XHCI_PORT1_OWNERSHIP_STRAP):** Strap to decide XHCI Port 2 Ownership between XHCI/PCIe/CSI. 0x0 = XHCI Port 2 configured as XHCI **(default)** 0x1 = XHCI Port 2 configures as Non-XHCI		**Yes**
	0	**XHCI Port 0 Ownership (XHCI_PORT0_OWNERSHIP_STRAP):** Strap to decide XHCI Port 1 Ownership between XHCI/PCIe/CSI. 0x0 = XHCI Port 1 configured as XHCI **(default)** 0x1 = XHCI Port 1 configures as Non-XHCI		**Yes**

9.116 PCH Descriptor Record 115 (Flash Descriptor Records)

Flash Address:FPSBA + B9h

Default Flash Address: 1B9h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1B9h	7:2	**Reserved, set to '0'**		**No**
	1	**USB3 / SSIC Port 1 Configuration (USB3_SSIC_PORT1_STRAP):** Strap to decide Port 1 Ownership between USB3/ SSIC. 0x0 = Port 1 configured for USB3 **(default)** 0x1 = Port 1 configured for SSIC	This strap must be configured when setting USB3 / SSIC Combo Port 1 strap (**USB3_SSIC_P1_Flex**). **Note:** This strap and the USB3 / SSIC Combo Port 1 strap (**USB3_SSIC_P1_Flex**) must match for proper port function.	**No**
	0	**Reserved, set to '0'**		**Yes**

9.117 PCH Descriptor Record 116 (Flash Descriptor Records)

Flash Address:FPSBA + BAh

Default Flash Address: 1BAh

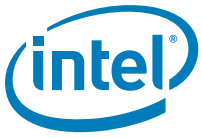
Offset from 0	Bits	Description	Usage	FIT Visible
0x1BAh	7:0	**Reserved, set to '0'**		**No**

9.118 PCH Descriptor Record 117 (Flash Descriptor Records)

Flash Address:FPSBA + BCh

Default Flash Address: 1BCh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1BCh	7:6	**Reserved, set to '0'**		**No**
	5:4	**Reserved, set to '0x3'**		**No**
	3:0	**Reserved, set to '0xf'**		**No**



9.119 PCH Descriptor Record 118 (Flash Descriptor Records)

Flash Address:FPSBA + BDh

Default Flash Address: 1BDh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1BDh	7:4	**Reserved, set to '0'**		**No**
	3:2	**PROCPWRGD and SYS_PWROK high to SUS_STAT# de-assertion (tPCH46)**: 00 = 1 ms **(default)** 01 = Reserved 10 = 5 ms 11 = 2 ms	tPCH46: PROCPWRGD and SYS_PWROK high to SUS_STAT# deassertion. Refer to EDS for details.	**Yes**
	1:0	**PCH clock output stable to PROCPWRGD high (tPCH45):** 00 = 100 ms 01 = 50 ms 10 = 5 ms 11 = 1 ms **(default)**	tPCH45: PCH clock output stable to PROCPWRGD high. Refer to EDS for details.	**Yes**

9.120 PCH Descriptor Record 119 (Flash Descriptor Records)

Flash Address:FPSBA + BEh

Default Flash Address: 1BEh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1BEh	7:5	**Reserved, set to '0'**		**No**
	6:5	**APWROK Timing (APWROK_TIMING):** 00 = 2 ms **(default)** 01 = 4 ms 10 = 8 ms 11 = 16 ms	This soft strap determines the time between the SLP_A# pin de-asserting and the APWROK timer expiration.	**Yes**
	4	**Deep Sx Enable (DEEPSX_PLT_CFG_SS):** 0 =The platform does not support DeepSx. 1 =The platform supports DeepSx **(default)**	This requires the target platform to support Deep SX state **Note:** When configuring Deep Sx you must also set **Deep_SX_EN**.	**Yes**
	3	**LAN PHY Power Up Time (LAN_PHY_PU_TIME):** 0 =100ms **(default)** 1 =50ms	This bit determines how long the delay for LAN PHY to power up after de-assertion of SLP_LAN#.	**Yes**
	2:0	**Reserved, set to '0'**		**No**

9.121 PCH Descriptor Record 120 (Flash Descriptor Records)

Flash Address:FPSBA + BFh

Default Flash Address: 1BFh

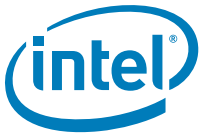
Offset from 0	Bits	Description	Usage	FIT Visible
0x1BFh	7:4	**Reserved, set to '0'**		**No**
	3	**Intel® Trace Hub Debug Messages Enable:** 0 = PCH Tracing debug messages Disabled **(default)** 1 = PCH Tracing debug messages Enabled	This setting enables debug messages on the Intel® Trace Hub. **Note:** You will also need to set the Intel® Trace Hub Soft Enable to "Enabled"	**Yes**
	2	**Reserved, set to '0'**		**No**
	1	**Reserved** **Set to '1' for A-Step PCH** **Set to '0' for B-Step PCH**		**No**
	0	**PCIe Power Stable Timer (tPCH33):** 0 = tPCH33 timer is disabled **(default)** 1 = PCH will count 99ms from PWROK assertion before PLTRST# is de-asserted.	Board dependent. Default is disabled, Platform is required to ensure timing of PWROK and SYS_PWROK in such a way that it satisfies the PCIe timing requirement of power stable to reset de-assertion.	**Yes**

9.122 PCH Descriptor Record 121 (Flash Descriptor Records)

Flash Address:FPSBA + C0h

Default Flash Address: 1C0h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1C0h	7	**Integrated Sensor Hub Supported:** 0 = Enable Integrated Sensor Hub 1 = Disable Integrated Sensor Hub **(default)**		**Yes**
	6:1	**Reserved, set to '0'**		**No**
	0	**Intel® Integrated wired LAN Enable (IWL_EN):** 0 = Enabled Intel® Integrated wired LAN Solution **(default)** 1 = Disabled Intel® Integrated wired LAN Solution ***Note:*** This must be set to '0' if the platform is using Intel's integrated wired LAN solution. Set to '1' if not using Intel integrated wired LAN solution or if disabling it.	This must be set to '0' if the platform is using the Intel® Integrated wired LAN solution. This must be set to '1' if not using the Intel® Integrated wired LAN solution or if disabling it.	**Yes**



9.123 PCH Descriptor Record 122 (Flash Descriptor Records)

Flash Address:FPSBA + C1h

Default Flash Address: 1C1h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1C1h	7:0	**Reserved, set to '0'**		**No**

9.124 PCH Descriptor Record 123 (Flash Descriptor Records)

Flash Address:FPSBA + C2h

Default Flash Address: 1C2h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1C2h	7:0	**Reserved, set to '0'**		**No**

9.125 PCH Descriptor Record 124 (Flash Descriptor Records)

Flash Address:FPSBA + C3h

Default Flash Address: 1C3h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1C3h	7:0	**Reserved, set to '0'**		**No**

9.126 PCH Descriptor Record 125 (Flash Descriptor Records)

Flash Address:FPSBA + C4h

Default Flash Address: 1C4h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1C4h	31:5	**Reserved, set to '0'**		**No**
	4	**USB3 / SSIC Configuration (USB3_SSIC_CFG)** 0 = SSIC Enabled 1 = USB3 Enabled **(default)**	This strap must be configured when setting USB3 / SSIC Combo Port 1 strap **(USB3_SSIC_P1_Flex).**	**No**
	3	**Reserved, set to '0'**		**No**
	2:1	**OPI Link Voltage Strap (OPD_LVO_STRP):** 0 = 0.85 Volts 1 = 0.95 Volts **(default)**	This strap must be configured when setting OPI Link Speed strap (**OPD_LVO**). **Note:** This strap and the OPI Link Speed strap (**OPD_LVO**) must match the same voltage configuration setting for proper platform operation function.	**No**
	0	**OPI Link Speed Strap (OPDMI_STRP):** 0 = GT2 Link Speed **(default)** 1 = GT4 Link Speed	This strap must be configured when setting OPI Link Speed strap (**OPDMI_TLS**). **Note:** This strap and the OPI Link Speed strap (**OPDMI_TLS**) must match the same GT configuration setting for proper platform operation function.	**No**

9.127 PCH Descriptor Record 126 (Flash Descriptor Records)

Flash Address:FPSBA + C7h

Default Flash Address: 1C7h

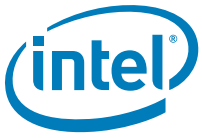
Offset from 0	Bits	Description	Usage	FIT Visible
0x1C7h	7:0	**Reserved, set to '0'**		**No**

9.128 PCH Descriptor Record 127 (Flash Descriptor Records)

Flash Address:FPSBA + C8h

Default Flash Address: 1C8h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1C8h	7:0	**Reserved, set to '0'**		**No**



9.129 PCH Descriptor Record 128 (Flash Descriptor Records)

Flash Address:FPSBA + C9h

Default Flash Address: 1C9h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1C9h	7:0	Reserved, set to '0'		No

9.130 PCH Descriptor Record 129 (Flash Descriptor Records)

Flash Address:FPSBA + CAh

Default Flash Address: 1CAh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1CAh	7	Reserved, set to '0'		No
	6:0	Reserved, set to '0x64'		No

9.131 PCH Descriptor Record 130 (Flash Descriptor Records)

Flash Address:FPSBA + CBh

Default Flash Address: 1CBh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1CBh	7:3	Reserved, set to '0'		No
	2:0	Reserved, set to '0x2'		No

9.132 PCH Descriptor Record 131 (Flash Descriptor Records)

Flash Address:FPSBA + CCh

Default Flash Address: 1CCh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1CCh	31:0	Reserved, set to '0x0'		No

9.133 PCH Descriptor Record 132 (Flash Descriptor Records)

Flash Address:FPSBA + D0h

Default Flash Address: 1D0h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1D0h	7:0	Reserved, set to '0'		No

9.134 PCH Descriptor Record 133 (Flash Descriptor Records)

Flash Address:FPSBA + D1h

Default Flash Address: 1D1h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1D1h	7:0	**Reserved, set to '0xf4'**		**No**

9.135 PCH Descriptor Record 134 (Flash Descriptor Records)

Flash Address:FPSBA + D2h

Default Flash Address: 1D2h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1D2h	7:4	**Reserved, set to '0x6'**		**No**
	3:0	**Reserved, set to '0x1'**		**No**

9.136 PCH Descriptor Record 135 (Flash Descriptor Records)

Flash Address:FPSBA + D3h

Default Flash Address: 1D3h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1D3h	7:0	**Reserved, set to '0x9'**		**No**

9.137 PCH Descriptor Record 136 (Flash Descriptor Records)

Flash Address:FPSBA + D4h

Default Flash Address: 1D4h

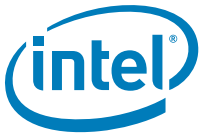
Offset from 0	Bits	Description	Usage	FIT Visible
0x1D4h	7:0	**Reserved, set to '0x19'**		**No**

9.138 PCH Descriptor Record 137 (Flash Descriptor Records)

Flash Address:FPSBA + D8h

Default Flash Address: 1D8h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1D8h	7:0	**Reserved, set to '0x79'**		**No**



9.139 PCH Descriptor Record 138 (Flash Descriptor Records)

Flash Address:FPSBA + D9h

Default Flash Address: 1D9h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1D9h	7:0	**Reserved, set to '0x55'**		**No**

9.140 PCH Descriptor Record 139 (Flash Descriptor Records)

Flash Address:FPSBA + DAh

Default Flash Address: 1DAh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1DAh	7:0	**Reserved, set to '0x55'**		**No**

9.141 PCH Descriptor Record 140 (Flash Descriptor Records)

Flash Address:FPSBA + DBh

Default Flash Address: 1DBh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1DBh	6:0	**Reserved, set to '0x55'**		**No**

9.142 PCH Descriptor Record 141 (Flash Descriptor Records)

Flash Address:FPSBA + DCh

Default Flash Address: 1DCh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1DCh	7:0	**Reserved, set to '0x1f'**		**No**

9.143 PCH Descriptor Record 142 (Flash Descriptor Records)

Flash Address:FPSBA + DDh

Default Flash Address: 1DDh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1DDh	1:0	**Reserved, set to '0x1'**		**No**

9.144 PCH Descriptor Record 143 (Flash Descriptor Records)

Flash Address:FPSBA + DEh

Default Flash Address: 1DEh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1DEh	7:0	**Reserved, set to '0'**		**No**

9.145 PCH Descriptor Record 144 (Flash Descriptor Records)

Flash Address:FPSBA + DFh

Default Flash Address: 1DFh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1DFh	1:0	**Reserved, set to '0'**		**No**

9.146 PCH Descriptor Record 145 (Flash Descriptor Records)

Flash Address:FPSBA + E0h

Default Flash Address: 1E0h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1E0h	3:0	**Reserved, set to '0x3'**		**No**

9.147 PCH Descriptor Record 146 (Flash Descriptor Records)

Flash Address:FPSBA + E1h

Default Flash Address: 1E1h

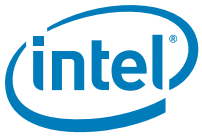
Offset from 0	Bits	Description	Usage	FIT Visible
0x1E1h	4:0	**Reserved, set to '0x07'**		**No**

9.148 PCH Descriptor Record 147 (Flash Descriptor Records)

Flash Address:FPSBA + E2h

Default Flash Address: 1E2h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1E2h	2:0	**Reserved, set to '0x1'**		**No**



9.149 PCH Descriptor Record 148 (Flash Descriptor Records)

Flash Address:FPSBA + E3h

Default Flash Address: 1E3h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1E3h	6:3	**Reserved, set to '0x1'**		**No**
	2:0	**Reserved, set to '0x2'**		**No**

9.150 PCH Descriptor Record 149 (Flash Descriptor Records)

Flash Address:FPSBA + E4h

Default Flash Address: 1E4h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1E4h	2:0	**Reserved, set to '0'**		**No**

9.151 PCH Descriptor Record 150 (Flash Descriptor Records)

Flash Address:FPSBA + E5h

Default Flash Address: 1E5h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1E5h	1:0	**Reserved, set to '0x2'**		**No**

9.152 PCH Descriptor Record 151 (Flash Descriptor Records)

Flash Address:FPSBA + E6h

Default Flash Address: 1E6h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1E6h	7:0	**Reserved, set to '0'**		**No**

9.153 PCH Descriptor Record 152 (Flash Descriptor Records)

Flash Address:FPSBA + E7h

Default Flash Address: 1E7h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1E7h	1:0	**Reserved, set to '0'**		**No**

9.154 PCH Descriptor Record 153 (Flash Descriptor Records)

Flash Address:FPSBA + E8h

Default Flash Address: 1E8h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1E8h	7:0	**Reserved, set to '0x09'**		**No**

9.155 PCH Descriptor Record 154 (Flash Descriptor Records)

Flash Address:FPSBA + E9h

Default Flash Address: 1E9h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1E9h	1:0	**Reserved, set to '0'**		**No**

9.156 PCH Descriptor Record 155 (Flash Descriptor Records)

Flash Address:FPSBA + EAh Size: 8 bit Default value: 01h

Default Flash Address: 1EAh

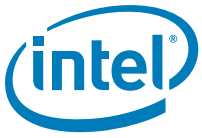
Offset from 0	Bits	Description	Usage	FIT Visible
0x1EAh	7:6	**Reserved, set to '0'**		**No**
	5:3	**Reserved, set to '0x1'**		**No**
	2	**Reserved, set to '0x1'**		**No**
	1:0	**Reserved, set to '0x3'**		**No**

9.157 PCH Descriptor Record 156 (Flash Descriptor Records)

Flash Address:FPSBA + EBh

Default Flash Address: 1EBh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1EBh	7:2	**Reserved, set to '0'**		**No**
	1	**Reserved, set to '0x1'**		**No**
	0	**Reserved, set to '0'**		**No**



9.158 PCH Descriptor Record 157 (Flash Descriptor Records)

Flash Address:FPSBA + ECh

Default Flash Address: 1ECh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1ECh	15:0	**Reserved, set to '0'**		**No**

9.159 PCH Descriptor Record 158 (Flash Descriptor Records)

Flash Address:FPSBA + EEh

Default Flash Address: 1EEh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1EEh	7:0	**Reserved, set to '0xff'**		**No**

9.160 PCH Descriptor Record 159 (Flash Descriptor Records)

Flash Address:FPSBA + EFh

Default Flash Address: 1EFh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1EFh	7:0	**Reserved, set to '0'**		**No**

9.161 PCH Descriptor Record 160 (Flash Descriptor Records)

Flash Address:FPSBA + F0h

Default Flash Address: 1F0h

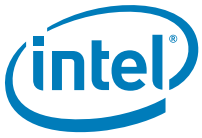
Offset from 0	Bits	Description	Usage	FIT Visible
0x1F0h	7	**Reserved, set to '0'**		**No**
	6:4	**Top Swap Block size (TSBS):** 000 = 64 KB. Invert A16 if Top Swap is enabled **(Default)** 001 = 128 KB. Invert A17 if Top Swap is enabled 010 = 256 KB. Invert A18 if Top Swap is enabled 011 = 512 KB. Invert A19 if Top Swap is enabled 100 = 1 MB. Invert A20 if Top Swap is enabled 101 - 111: Reserved. ***Note:*** This setting is dependent on BIOS architecture and can be different per design. The BIOS developer for the target platform has to determine this value. ***Note:*** If FWH is set as Boot BIOS destination then PCH only supports 64 KB Top Swap block size. This value has to be determined by how BIOS implements Boot-Block.	his allows for the system to use alternate code in order to boot a platform based upon the **Top Swap** (GPIO66/SDIO_D0 pulled low during the rising edge of **PWROK**.) strap being asserted. **Top Swap** inverts an address on access to SPI and firmware hub, so the processor fetches the alternate Top Swap block instead of the original boot-block. The size of the Top Swap block and setting of this field must be determined by the BIOS developer. If this is not set correctly, then BIOS boot-block recovery mechanism will not work. ***Note:*** This setting is not the same for all designs, is dependent on the architecture of BIOS. The setting of this field must be determined by the BIOS developer.	**Yes**
	3	**Quad I/O Read Enable (QIORE):** 0 = Quad I/O Read is disabled **(default)** 1 = Quad I/O Read is enabled	This soft strap only has effect if Quad Output Read is discovered as supported via the SFDP If parameter table is not detected via SFDP, this bit has no effect and Quad I/O Read is controlled via the Flash Descriptor Component Section. Dual Output Fast Read Support Bit	**Yes**
	2	**Quad Output Read Enable (QORE):** 0 = Quad Output Read is disabled **(default)** 1 = Quad Output Read is enabled	This soft strap only has effect if Quad Output Read is discovered as supported via the SFDP If parameter table is not detected via SFDP, this bit has no effect and Quad Output Read is controlled via the Flash Descriptor Component Section. Dual Output Fast Read Support Bit	**Yes**
	1	**Dual I/O Read Enable (DIORE):** 0 = Dual I/O Read is disabled **(Default)** 1 = Dual I/O Read is enabled	this soft strap only has effect if Dual I/O Read is discovered as supported via the SFDP If parameter table is not detected via SFDP, this bit has no effect and Dual Output I/O Read is controlled via the Flash Descriptor Component Section. Dual Output Fast Read Support Bit	**Yes**
	0	**Dual Output Read Enable (DORE):** 0 = Dual Output Read is disabled **(Default)** 1 = Dual Output Read is enabled	This soft strap only has effect if Dual Output read is discovered as supported via the SFDP. If parameter table is not detected via SFDP, this bit has no effect and Dual Output Read is controlled via the Flash Descriptor Component Section. Dual Output Fast Read Support Bit	**Yes**

9.162 PCH Descriptor Record 161 (Flash Descriptor Records)

Flash Address:FPSBA + F1h

Default Flash Address: 1F1h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1F1h	7:0	**Reserved, set to '0'**		**No**



9.163 PCH Descriptor Record 162 (Flash Descriptor Records)

Flash Address:FPSBA + F2h

Default Flash Address: 1F2h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1F2h	7	**SPI Voltage Select (SPI_1p8volt_sel):** 0 = SPI supply voltage set to 3.3 volts **(default)** 1 = SPI supply voltage set to 1.8 volts	This strap sets the internal control signal on the pad for either 1.8 or 3.3 V operation. ***Note:*** The strap defaults to 1.8V mode before the soft straps are loaded, i.e. before the actual supply voltage is known. This is because the pad performance is slightly better when assuming 1.8V when the actual is 3.3V than vice-versa.	**Yes**
	6:0	**Reserved, set to '0'**		**No**

9.164 PCH Descriptor Record 163 (Flash Descriptor Records)

Flash Address:FPSBA + F3h

Default Flash Address: 1F3h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1F3h	7:0	**Reserved, set to '0'**		**No**

9.165 PCH Descriptor Record 164 (Flash Descriptor Records)

Flash Address:FPSBA + F4h

Default Flash Address: 1F4h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1F4h	7	**Reserved, set to '0'**		**No**
	6:4	**Reserved, default to 100b**		**No**
	3:0	**Reserved, set to '0x5'**		**No**

9.166 PCH Descriptor Record 165 (Flash Descriptor Records)

Flash Address:FPSBA + F5h

Default Flash Address: 1F5h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1F5h	7:3	**Reserved, set to '0x10'**		**No**
	2:0	**TPM Clock Frequency (STCF):** This field is defined with a broad range to support both SOC and PCH implementations. The listed frequencies are approximate. 000 = Reserved 001 = Reserved 010 = 48MHz 011 = Reserved 100 = 30 MHz 101 = Reserved 110 = 17 MHz **(default)** 111 = reserved ***Notes:*** This field identifies the serial clock frequency for TPM on SPI. This field is undefined if the TPM on SPI is disabled either by soft-strap or fuse.	This field identifies the frequency that should be used with the TPM on SPI. This field is undefined if the TPM on SPI is disabled by softstrap	**Yes**

9.167 PCH Descriptor Record 166 (Flash Descriptor Records)

Flash Address:FPSBA + F6h

Default Flash Address: 1F6h

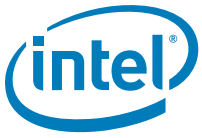
Offset from 0	Bits	Description	Usage	FIT Visible
0x1F6h	7:0	**Reserved, set to '0'**		**No**

9.168 PCH Descriptor Record 167 (Flash Descriptor Records)

Flash Address:FPSBA + F7h

Default Flash Address: 1F7h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1F7h	7:0	**Reserved, set to '0'**		**No**



9.169 PCH Descriptor Record 168 (Flash Descriptor Records)

Flash Address:FPSBA + F8h

Default Flash Address: 1F8h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1F8h	31:0	**Reserved, set to '0'**		**No**

9.170 PCH Descriptor Record 169 (Flash Descriptor Records)

Flash Address:FPSBA + FCh

Default Flash Address: 1FCh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1FCh	7:6	**Reserved, set to '0'**		**No**
	5:3	**eSPI / EC Bus Frequency:** For Slave 0 (EC/BMC): Indicates the maximum frequency of the eSPI bus that is supported by the eSPI Master and platform configuration (trace length, number of Slaves, etc.). The actual frequency of the eSPI bus will be the minimum of this field and the Slave's maximum frequency advertised in its General Capabilities register. 0x0 = 20MHz 0x1 = 24MHz 0x2 = 30 MHz 0x3 = 48MHz 0x4 = 60MHz **(default)** 05x = Reserved 0x6 = Reserved 0x7 = Reserved		**Yes**
	2	**eSPI / EC Boot Enable:** 0 = PCH will wait for EC (Slave 0) to load its boot code via MAFS 1 = PCH will not wait for EC (Slave 0) to load its boot code via MASF **(default)**	For setting '0' the PCH (eSPI) will wait for SLAVE_BOOT_LOAD_DONE Virtual Wire to be asserted before proceeding with the rest of the boot flow; EC is required to assert this VW whether or not it loads its code from PCH Flash. For setting '1' PCH (eSPI) will not gate its boot flow for EC to boot its code; EC_BOOT_LOAD_DONE is internally forced asserted immediately.	**Yes**
	1	**eSPI / EC OOB Channel Enable:** 0 = OOB Channel is enabled if EC (Slave 0) supports it **(default)** 1 = OOB Channel is disabled		**Yes**
	0	**eSPI / EC Peripheral Channel Enable:** 0 = Peripheral / LPC channel enabled if EC (Slave 0) supports it **(default)** 1 = Peripheral / LPC channel is disabled		**Yes**

9.171 PCH Descriptor Record 170 (Flash Descriptor Records)

Flash Address:FPSBA + FDh

Default Flash Address: 1FDh

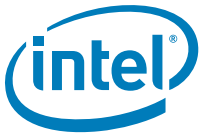
Offset from 0	Bits	Description	Usage	FIT Visible
0x1FDh	23:4	**Reserved, set to '0'**		**No**
	3:2	**eSPI / EC Maximum I/O Mode:** Indicates the maximum IO Mode (Single/Dual/Quad) of the eSPI bus that is supported by the eSPI Master and specific platform configuration. The actual IO Mode of the eSPI bus will be the minimum of this field and the Slave's maximum IO Mode advertised in its General Capabilities register. 0x0 = Single IO Mode 0x1 = Single and Dual IO Mode 0x2 = Single and Quad IO Mode 0x3 = Single, Dual and Quad I/O **(default)**		**Yes**
	1	**Reserved, set to '1'**		**No**
	0	**eSPI / EC CRC Check Enable:** **For Slave 0 (EC/BMC)** 0 = CRC Checking enabled 1 = CRC checking disabled **(default)**		**Yes**

9.172 PCH Descriptor Record 171 (Flash Descriptor Records)

Flash Address:FPSBA + 100h

Default Flash Address: 200h

Offset from 0	Bits	Description	Usage	FIT Visible
0x200h	7:0	**Reserved, set to '0'**		**No**



9.173 PCH Descriptor Record 172 (Flash Descriptor Records)

Flash Address:FPSBA + 101h

Default Flash Address: 201h

Offset from 0	Bits	Description	Usage	FIT Visible
0x201h	7	**Reserved, set to '0'**		**No**
	6:4	**eSPI / EC Max Read Request Payload size for OOB Channel:** This setting allows the eSPI / EC HW maximum read request OOB payload size (128 bytes) to be overridden for debug or other usage. All sizes below are address aligned. 0x0 = Max Read Request size 64 bytes **(default)** 0x1 = Max Read Request size 128 bytes 0x2 = Max Read Request size 256 bytes 0x3 = Max Read Request size 512 bytes 0x4 = Max Read Request size 1024 bytes 0x5 = Max Read Request size 2048 bytes 0x6 = Max Read Request size 4096 0x7 = Reserved ***Note:*** This encoding does NOT match the eSPI Specifications.		**Yes**
	3:1	**eSPI / EC Max Read Request Payload size for Master Attached Flash Channel:** This setting allows the eSPI / EC HW maximum read request Master Attach Flash Channel payload size (64 bytes) to be overridden for debug or other usage. All sizes below are address aligned. 0x0 = Max Read Request size 64 bytes **(default)** 0x1 = Max Read Request size 128 bytes 0x2 = Max Read Request size 256 bytes 0x3 = Max Read Request size 512 bytes 0x4 = Max Read Request size 1024 bytes 0x5 = Max Read Request size 2048 bytes 0x6 = Max Read Request size 4096 0x7 = Reserved ***Note:*** This encoding does NOT match the eSPI Specifications.		**Yes**
	0	**eSPI / EC Max Outstanding Request for Master Attached Flash Channel:** 0 = Maximum of 2 outstanding requests allowed **(default)** 1 = Maximum of 1 outstanding requests allowed		**Yes**

9.174 PCH Descriptor Record 173 (Flash Descriptor Records)

Flash Address:FPSBA + 102h

Default Flash Address: 202h

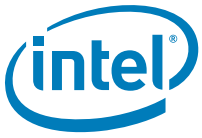
Offset from 0	Bits	Description	Usage	FIT Visible
0x202h	7:3	**Reserved, set to '0'**		**No**
	2:0	**eSPI / EC Max Read Request Payload size for Peripheral Channel:** This setting allows the eSPI / EC HW maximum read request payload size (64 bytes) to be overridden for debug or other usage. All sizes below are address aligned. 0x0 = Max Read Request size 64 bytes **(default)** 0x1 = Max Read Request size 128 bytes 0x2 = Max Read Request size 256 bytes 0x3 = Max Read Request size 512 bytes 0x4 = Max Read Request size 1024 bytes 0x5 = Max Read Request size 2048 bytes 0x6 = Max Read Request size 4096 0x7 = Reserved ***Note:*** This encoding does NOT match the eSPI Specifications.		**Yes**

9.175 PCH Descriptor Record 174 (Flash Descriptor Records)

Flash Address:FPSBA + 103h

Default Flash Address: 203h

Offset from 0	Bits	Description	Usage	FIT Visible
0x203h	7:3	**Reserved, set to '0'**		**No**
	2:0	**eSPI / EC Max Virtual Wire Channels:** Max Virtual Wire (WV) / IRQ Channel Count; HW max is 8, however soft-strap can force it down for debug or other usage. 0x0 = eSPI / EC set to 8 VW Channels **(default)** 0x1 = eSPI / EC set to 4 VW Channels 0x2 = eSPI / EC set to 2 VW Channels 0x3 = eSPI / EC set to 1 VW Channel 0x4 = Reserved 0x5 = Reserved 0x6 = Reserved 0x7 = Reserved		**Yes**



9.176 PCH Descriptor Record 175 (Flash Descriptor Records)

Flash Address:FPSBA + 104h

Default Flash Address: 204h

Offset from 0	Bits	Description	Usage	FIT Visible
0x204h	7:4	**Reserved, set to '0xf'**		**No**
	3	**Reserved, set to '0'**		**No**
	2	**Reserved, set to '0x1'**		**No**
	1:0	**Reserved, set to '0'**		**No**

9.177 PCH Descriptor Record 176 (Flash Descriptor Records)

Flash Address:FPSBA + 105h

Default Flash Address: 205h

Offset from 0	Bits	Description	Usage	FIT Visible
0x205h	7	**Reserved, set to '0'**		**No**
	6:4	**OPI Link Width (OPDMI_LW):** 000 = 1 Lane 001 = 2 Lanes 010 = 4 Lanes 011 = 8 Lanes **(default)**	This setting configures the OPI Link Width. For further details see the Skylake PCH EDS.	**Yes**
	3:0	**OPI Link Speed (OPDMI_TLS):** 0x2 = GT2 Link Speed **(default)** 0x3 = GT4 Link Speed	This strap must be configured when setting OPI Link Speed Strap **(OPDMI_STRP)**. **Note:** This strap and the OPI Link Speed Strap **(OPDMI_STRP)** must match the same GT configuration setting for proper platform operation function. This setting configures the OPI Link Width. For further details see the Skylake PCH EDS.	**Yes**

9.178 PCH Descriptor Record 177 (Flash Descriptor Records)

Flash Address:FPSBA + 106h

Default Flash Address: 206h

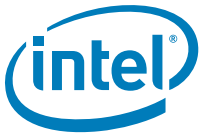
Offset from 0	Bits	Description	Usage	FIT Visible
0x206h	7:6	**Reserved, set to '0'**		**No**
	5	**DMI Lane Reversal (DMILR):** 0 = DMI Lanes are not reversed.**(default)** 1 = DMI Lanes are reversed.	This field is used only when DMI Lanes are reversed on the layout. This usually only is done on layout constrained boards where reversing lanes help routing. **Note:** This setting is dependent on the board design. The platform hardware designer must determine if DMI needs lane reversal.	**Yes**
	4	**Reserved, set to '0'**		**No**
	3:2	**Reserved, set to '0x1'**		**No**
	1:0	**Reserved, set to '0'**		**No**

9.179 PCH Descriptor Record 178 (Flash Descriptor Records)

Flash Address:FPSBA + 107h

Default Flash Address: 207h

Offset from 0	Bits	Description	Usage	FIT Visible
0x207h	7:1	**Reserved, set to '0'**		**No**
	0	**OPI Link Voltage (OPD_LVO):** 0 = 0.95 Volts **(default)** 1 = 0.85 Volts	This strap must be configured when setting OPI Link Speed strap (**OPD_LVO_STRP**). **Note:** This strap and the OPI Link Speed strap (**OPD_LVO_STRP**) must match the same voltage configuration setting for proper platform operation function. This setting configures the OPI Link Voltage. For further details see Skylake PCH EDS.	**Yes**



9.180 CPU Descriptor Record 0 (Flash Descriptor Records)

Flash Address:FCPUSBA + 000h

Default Flash Address: 300h

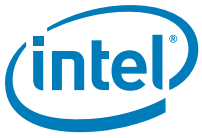
Offset from 0	Bits	Description	Usage	FIT Visible
0x300h	31:14	**Reserved, set to '0x0'**		**No**
	13	**JTAG Power Disable:** 0 = Disable JTAG Power for C10 and deeper states **(Default)** 1 = Enable JTAG Power for C10 and deeper states	This setting determines if JTAG power will be maintained on C10 or lower power states. **Note:** This strap is intended for debugging purposed only.	**Yes**
	12	**Processor Boot Max Frequency:** 0 = Disable Boot Max Frequency 1 = Enable Boot Max Frequency **(Default)**	This setting determines if the processor will operate at maximum frequency at power-on and boot. **Note:** This strap is intended for debugging purposed only.	**Yes**
	11:6	**Flex Ratio:** '0x0' **(Default)**	This setting controls the maximum processor non-turbo ratio. **Note:** This strap is intended for debugging purposed only. See BIOS Spec for more details on maximum processor non-turbo ratio configuration.	**Yes**
	5	**BIST Initialization:** 0 = Disable BIST at Reset **(Default)** 1 = Enable BIST at Reset	This setting determines if BIST will be run at platform reset after BIOS requested actions. **Note:** This strap is intended for debugging purposed only.	**Yes**
	4	**Reserved, set to '0x0'**		**No**
	3:1	**Number of Active Cores:** 0 = All Cores active **(Default)** 1 = One core active 2 = Two cores active 3 = Three cores active 4 = Four cores active	This setting controls the number of active processor cores. **Note:** This strap is intended for debugging purposed only. See BIOS Spec for more details on enabling / disabling processor cores.	**Yes**
	0	**Disable Hyper threading:** 0 = Enable Hyper Threading **(Default)** 1 = Disable Hyper Threading	This setting control enabling / disabling of Hyper threading. **Note:** This strap is intended for debugging purposed only. See BIOS Spec for more details on enabling / disabling Hyper threading	**Yes**

9.181 CPU Descriptor Record 1 (Flash Descriptor Records)

Flash Address:FCPUSBA + 004h

Default Flash Address: 304h

Offset from 0	Bits	Description	Usage	FIT Visible
0x304h	31	**Platform IMON Disable:** '0x0' **(Default)**	**Note:** This strap should be left at the recommended default setting.	**Yes**
	30	**SVID Presence:** 0 = SVID is present **(Default)** 1 = No SVID is present	This setting determine if SVID rails are present on the platform. See Processor EDS for details.	**Yes**
	29:25	**Reserved, set to '0'**		**No**
	24	**GT_S VR Type:** 0 = GT slice domain VR type SVID **(Default)** 1 = GT slice domain VR type is fixed VR	This setting determines the GT slice domain VR type. See Processor EDS for details.	**Yes**
	23:20	**GT_S Power Plane Topology:** '0x1' **(Default)**	This setting determines the GT slice power plane topology. See Processor EDS for details. **Note:** This strap should be left at the recommended default setting.	**Yes**
	19	**GT_US VR Type:** 0 = GT Unslice domain VR type SVID **(Default)** 1 = GT Unslice domain VR type is fixed VR	This setting determines the GT Unslice domain VR type. See Processor EDS for details.	**Yes**
	18:15	**GT_US Power Plane Topology:** '0x1' **(Default)**	This setting determines the GT Unslice power plane topology. See Processor EDS for details. **Note:** This strap should be left at the recommended default setting.	**Yes**
	14	**Ring VR Type:** 0 = Ring domain VR Type SVID **(Default)** 1 = Ring domain VR type is fixed VR	This setting determines the Ring domain VR type. See Processor EDS for details.	**Yes**
	13:10	**Ring Power Plane Topology:** '0x0' **(Default)**	This setting determines the Ring power plane topology. See Processor EDS for details. **Note:** This strap should be left at the recommended default setting.	**Yes**
	9	**IA Power Plane VR:** 0 = IA core domain VR Type SVID **(Default)** 1 = IA core domain VR type is fixed VR	This setting determines the IA core domain VR type. See Processor EDS for details.	**Yes**
	8:5	**IA Power Plane Topology:** '0x0' **(Default)**	This setting determines the IA power plane topology. See Processor EDS for details. **Note:** This strap should be left at the recommended default setting.	**Yes**



Offset from 0	Bits	Description	Usage	FIT Visible
0x304h (Cont)	4	**SA VR Type:** 0 = SA core domain VR Type SVID **(Default)** 1 = SA core domain VR type is fixed VR	This setting determines the SA core domain VR type. See Processor EDS for details.	**Yes**
	3:0	**SA Power Plane Topology:** '0x2' **(Default)**	This setting determines the SA power plane topology. See Processor EDS for details. **Note:** This strap should be left at the recommended default setting.	**Yes**

9.182 CPU Descriptor Record 2 (Flash Descriptor Records)

Flash Address:FCPUSBA + 008h

Default Flash Address: 308h

Offset from 0	Bits	Description	Usage	FIT Visible
0x308h	31:28	**SE Key Mode:** '0x0' **(Default)**	**Note:** This strap should be left at the recommended default setting.	**Yes**
	27:10	**Reserved set to '0'**		**No**
	9	**EDRAM VR Type:** 0 = EDRAM core domain VR Type SVID 1 = EDRAM core domain VR type is fixed VR **(Default)**	This setting determines the eOPIO domain VR type. See Processor EDS for details.	**Yes**
	8:5	**EDRAM Power Plane Topology:** '0x0' **(Default)**	This setting determines the EDRAM power plane topology. See Processor EDS for details. **Note:** This strap should be left at the recommended default setting.	**Yes**
	4	**eOPIO VR Type:** 0 = eOPIO domain VR Type SVID 1 = eOPIO core domain VR type is fixed VR **(Default)**	This setting determines the eOPIO domain VR type. See Processor EDS for details.	**Yes**
	3:0	**eOPIO Power Plane Topology:** '0x0' **(Default)**	This setting determines the eOPIO power plane topology. See Processor EDS for details. **Note:** This strap should be left at the recommended default setting.	**Yes**

§ §

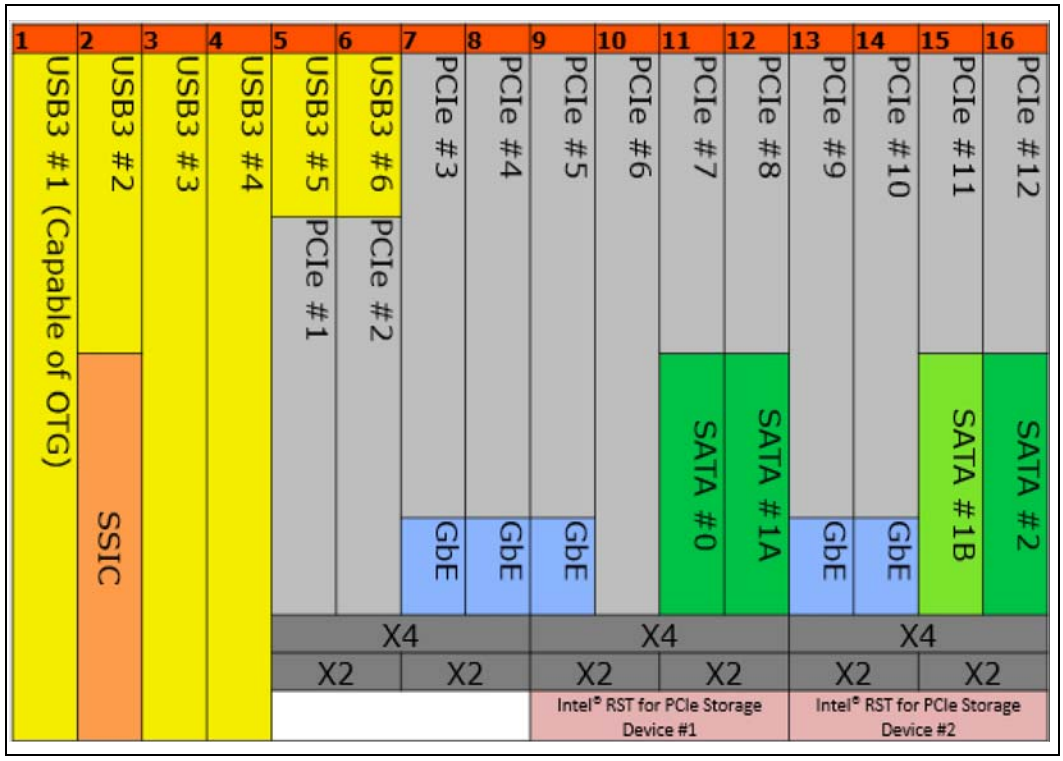
10 Configuration Dependencies

10.1 Descriptor Configuration Setting Enabling Dependencies

This chapter outlines the descriptor configuration dependencies for enabling Skylake Hardware I/O, Bus and GPIO components.

10.1.1 High Speed IO (HSIO) Port Enabling

Below diagram provides better illustration on HSIO muxing and next table shows how to enable each mux functionality on HSIO lane.



Note: Refer to EDS for exact number HSIO lane# supported. Some SKUs may have less HSIO lane. Get full understanding on HSIO lane muxing architecture from EDS.

Note: GbE enabling only allow at the HSIO lanes shown in the diagram one at a time.

Note: SATA#1 only allow at HSIO Lanes shown in the diagram one at a time.

The table below gives examples of how to enable each mux functionality on the HSIO lanes:

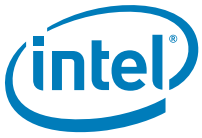


Table 10-1. HSIO Lane Muxing Selection (Sheet 1 of 3)

HSIO Lane (Port#)	Strap Offset (value)	Description
Lane 1 (USB P1)	FPSBA + 0b8h[0] = 0x0	Straps to decide XHCI Port 0 Ownership between XHCI/PCIe/CSI
	FPSBA + 0b9h[0] = 0x0	Straps to decide Port 0 Ownership between USB3/SSIC
Lane 2 (USB P2)	FPSBA + 06ch[4] = 0x0	USB3/SSIC Combo Port 1 Strap (USB3_SSIC_P1_STRP)
	FPSBA + 07eh[4] = 0x0	USB3/ SSIC Combo Port 1 Strap
	FPSBA + 0b8h[1] = 0x0	Straps to decide XHCI Port 1 Ownership between XHCI/PCIe/CSI
	FPSBA + 0b9h[1] = 0x0	Straps to decide Port 1 Ownership between USB3/SSIC
Lane 2 (SSIC P1)	FPSBA + 06ch[4] = 0x1	USB3/SSIC Combo Port 1 Strap (USB3_SSIC_P1_STRP)
	FPSBA + 07eh[4] = 0x1	USB3/ SSIC Combo Port 1 Strap
	FPSBA + 0b8h[1] = 0x0	Straps to decide XHCI Port 1 Ownership between XHCI/PCIe/CSI
	FPSBA + 0b9h[1] = 0x1	Straps to decide Port 1 Ownership between USB3/SSIC
Lane 3 (USB P3)	FPSBA + 06ch[5] = 0x0	USB3/SSIC Combo Port 2 Strap (USB3_SSIC_P2_STRP)
	FPSBA + 07eh[5] = 0x0	USB3/ SSIC Combo Port 2 Strap
	FPSBA + 0b8h[2] = 0x0	Straps to decide XHCI Port 2 Ownership between XHCI/PCIe/CSI
	FPSBA + 0b9h[2] = 0x0	Straps to decide Port 2 Ownership between USB3/SSIC
Lane 3 (SSIC P2)		
Lane 4 (USB P4)	FPSBA + 0b8h[3] = 0x0	Straps to decide XHCI Port 3 Ownership between XHCI/PCIe/CSI
	FPSBA + 0b9h[3] = 0x0	Straps to decide Port 3 Ownership between USB3/SSIC
Lane 5 (USB P5)	FPSBA + 06eh[1:0] = 0x0	PCIe/USB3 Combo Port 0 Strap (PCIE_USB3_P0_STRP)
	FPSBA + 082h[1:0] = 0x0	PCIe/USB3 Combo Port 0 Strap
	FPSBA + 0b8h[4] = 0x0	Straps to decide XHCI Port 4 Ownership between XHCI/PCIe/CSI
	FPSBA + 0b9h[4]=0x0	Straps to decide Port 4 Ownership to USB3
Lane 5 (PCIe P1)	FPSBA + 06eh[1:0] = 0x1	PCIe/USB3 Combo Port 0 Strap (PCIE_USB3_P0_STRP)
	FPSBA + 082h[1:0] = 0x1	PCIe/USB3 Combo Port 0 Strap
	FPSBA + 0b8h[4] = 0x1	Straps to decide XHCI Port 4 Ownership between XHCI/PCIe/CSI

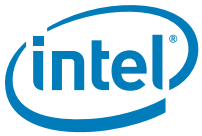


Table 10-1. HSIO Lane Muxing Selection (Sheet 2 of 3)

HSIO Lane (Port#)	Strap Offset (value)	Description
Lane 6 (USB P6)	FPSBA + 06eh[3:2] = 0x0	PCIe/USB3 Combo Port 1 Strap (PCIE_USB3_P0_STRP)
	FPSBA + 082h[3:2] = 0x0	PCIe/USB3 Combo Port 1 Strap
	FPSBA + 0b8h[5] = 0x0	Straps to decide XHCI Port 5 Ownership between XHCI/PCIe/CSI
	FPSBA + 0b9h[5] = 0x0	Straps to decide Port 5 Ownership to USB3
Lane 6 (PCIe P2)	FPSBA + 06eh[3:2] = 0x1	PCIe/USB3 Combo Port 1 Strap (PCIE_USB3_P0_STRP)
	FPSBA + 082h[3:2] = 0x1	PCIe/USB3 Combo Port 1 Strap
	FPSBA + 0b8h[5] = 0x1	Straps to decide XHCI Port 5 Ownership between XHCI/PCIe/CSI
Lane 7 (PCIe P3)	No muxing	
Lane 8 (PCIe P4)	No muxing	
Lane 9 (PCIe P5)	No muxing	
Lane 10 (PCIe P6)	No muxing	
Lane 11 (SATA P0)	FPSBA + 068h[1:0] = 0x0	SATA / PCIe GP Select for Port 0
	FPSBA + 07dh[1:0] = 0x0	PCIe/SATA Combo Port 0 Strap
	FPSBA + 08ch[1:0] = 0x0	SATA_PCIE_Select_for_Port_0
Lane 11 (PCIe P7)	FPSBA + 068h[1:0] = 0x1	SATA / PCIe GP Select for Port 0
	FPSBA + 07dh[1:0] = 0x1	PCIe/SATA Combo Port 0 Strap
	FPSBA + 08ch[1:0] = 0x1	SATA_PCIE_Select_for_Port_0
Lane 12 (SATA P1) Note: SATA mode only choose between Lane12 or Lane15 at one time	FPSBA + 068h[3:2] = 0x0	SATA / PCIe GP Select for Port 1
	FPSBA + 07dh[3:2] = 0x0	PCIe/SATA Combo Port 1 Strap
	FPSBA + 08ch[3:2] = 0x0	SATA_PCIE_Select_for_Port_1
Lane 12 (PCIe P8)	FPSBA + 068h[3:2] = 0x1	SATA / PCIe GP Select for Port 1
	FPSBA + 07dh[3:2] = 0x1	PCIe/SATA Combo Port 1 Strap
	FPSBA + 08ch[3:2] = 0x1	SATA_PCIE_Select_for_Port_1
Lane 13 (PCIe P9)	No strap for muxing	
Lane 14 (PCIe P10)	No strap for muxing	
Lane 15 (SATA P1) (Only SKL-U) Note: SATA mode only choose between Lane12 or Lane15 at one time	FPSBA + 068h[3:2] = 0x0	SATA / PCIe GP Select for Port 1
	FPSBA + 07dh[5:4] = 0x0	PCIe/SATA Combo Port 2 Strap
	FPSBA + 08ch[3:2] = 0x0	SATA_PCIE_Select_for_Port_1
Lane 15 (PCIe P11) (Only SKL-U)	FPSBA + 068h[3:2] = 0x1	SATA / PCIe GP Select for Port 1
	FPSBA + 07dh[5:4] = 0x1	PCIe/SATA Combo Port 2 Strap
	FPSBA + 08ch[3:2] = 0x1	SATA_PCIE_Select_for_Port_1
Lane 16 (SATA P2) (Only SKL-U)	FPSBA + 068h[5:4] = 0x0	SATA / PCIe GP Select for Port 2
	FPSBA + 080h[1:0] = 0x0	PCIE/SATA Combo Port 3 Strap
	FPSBA + 08ch[5:4] = 0x0	SATA_PCIE_Select_for_Port_2

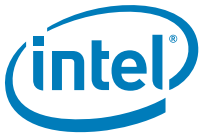


Table 10-1. HSIO Lane Muxing Selection (Sheet 3 of 3)

HSIO Lane (Port#)	Strap Offset (value)	Description
Lane 16 (PCIe P12) (Only SKL-U)	FPSBA + 068h[5:4] = 0x1	SATA / PCIe GP Select for Port 2
	FPSBA + 080h[1:0] = 0x1	PCIE/SATA Combo Port 3 Strap
	FPSBA + 08ch[5:4] = 0x1	SATA_PCIE_Select_for_Port_2

10.1.1.1 Configuring PCIe on HSIO

For PCIe Controller #1:

Recommended Steps	Straps	
1. Configure HSIO lane to be PCIe.	Refer HSIO Muxing Table	
2. Configure PCIe lane, x1, x2 or x4	FPSBA + 09dh[4:3]	

For PCIe Controller #2:

Recommended Steps	Straps	
1. Configure HSIO lane to be PCIe.	Refer HSIO Muxing Table	
2. Configure PCIe lane, x1, x2 or x4	FPSBA + 0a5h[4:3]	

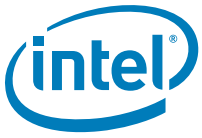
For PCIe Controller #3:

Recommended Steps	Straps	
1. Configure HSIO lane to be PCIe.	Refer HSIO Muxing Table	
2. Configure PCIe lane, x1, x2 or x4	FPSBA + 0adh[4:3]	

10.1.1.2 Configure Intel® RST on PCIe

Configure Intel RST on PCIe Controller #2:

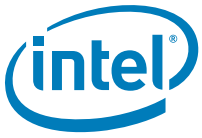
Recommended Steps	Straps	
1. Configure HSIO lane to be PCIe.	Refer HSIO Muxing Table	
2. Configure PCIe lane, to Intel RST supported lane x2 or x4	FPSBA + 054h[3:2]	00 - NAND Cycle Router A1 configured for PCIe NAND x1 01 - NAND Cycle Router A1 configured for PCIe NAND x2 10 - NAND Cycle Router A1 configured for PCIe NAND x4



Recommended Steps	Straps	
	FPSBA + 055h[3:2]	CFG1x4, 2'b11 CFG2x2, 2'b10 CFG1x22x1, 2'b01 CFG4x1, 2'b00
	FPSBA + 05Ch[3:2]	CFG1x4, 2'b11 CFG2x2, 2'b10 CFG1x22x1, 2'b01 CFG4x1, 2'b00

Configure Intel RST on PCIe Controller #3:

Recommended Steps	Straps	
1. Configure HSIO lane to be PCIe.	Refer HSIO Muxing Table	
2. Configure PCIe lane, to Intel RST supported lane x2 or x4	FPSBA + 054h[5:4]	00 - NAND Cycle Router A1 configured for PCIe NAND x1 01 - NAND Cycle Router A1 configured for PCIe NAND x2 10 - NAND Cycle Router A1 configured for PCIe NAND x4
	FPSBA + 055h[5:4]	CFG1x4, 2'b11 CFG2x2, 2'b10 CFG1x22x1, 2'b01 CFG4x1, 2'b00
	FPSBA + 060h[5:4]	CFG1x4, 2'b11 CFG2x2, 2'b10 CFG1x22x1, 2'b01 CFG4x1, 2'b00



10.1.2 Intel® Integrated LAN Controller Enabling

If Yes:

Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
0x144h	6:0	**0x70h**	GbE MAC SMBus Address
0x147h	0	**1b**	Gbe MAC SMBus Address Enable
0x149h	2:0	**0x2h**	Reserved
0x148h	1:0	**0x3h**	Reserved
0x17Ch	6	**1b**	Intel Phy Over PCIe Enable
0x17Ch	5:3	**Design dependent**	GBE PCIe* Port Select 000 = PORT3 001 = PORT4 010 = PORT5 011 = PORT9 100 = PORT10
0x193h	3	**1b**	LC SMBus add enable GbE_ADDREN
0x193h	2	**1b**	LCD SMBus add enable PHY_ADDREN
0x192h	7:3	**0x01h**	Reserved
0x192h	2:0	**0x3h**	PHY Connection
0x191h	7	**0x1h**	Reserved
0x191h	6:0	**0x70h**	Reserved
0x190h	7:2	**0x24h**	Reserved
0x190h	1:0	**0x3h**	Reserved
0x194h	2	**0x1h**	Reserved
0x1C0h	0	**0b**	Intel® Integrated wired LAN Enable
0x164h	7:6	**01b**	LAN PHY Power Control GDP11 Signal Configuration Note: For non-Intel Wired LAN, set to 00b

10.1.3 Intel® Wireless LAN Controller Enabling

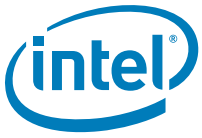
If Yes:

First step, follow HSIO mux table to enable PCIe port that connect to Wireless LAN.

Set PCIe config accordingly, x1

Then set below straps.

Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
0x164h	5	**0b**	SLP_WLAN# / GDP9 Signal Configuration



10.1.4 Deep Sx Enabling Dependencies

To enable:

Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
0x100h	20	**1b**	Deep Sx Enable
0x1BEh	4	**1b**	DEEPSX_PLT_CFG_SS [See Descriptor Configuration Chapter Section 9.1 for details]

To disable:

Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
0x100h	20	**0b**	Deep Sx Enable
0x1BEh	4	**0b**	DEEPSX_PLT_CFG_SS [See Descriptor Configuration Chapter Section 9.1 for details]

10.1.5 RPMC Enabling Dependencies

If Yes:

Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
0x100h	5	**1b**	RPMC Supported
0x100h	6	**1b**	RPMC Rebinding Enabled

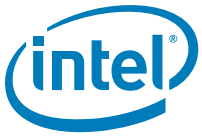
If No:

Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
0x100h	5	**0b**	RPMC Supported
0x100h	6	**0b**	RPMC Rebinding Enabled

10.1.6 Intel® SMBus Enabling

To enable SMBus:

Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
0x105h	0	**1b**	Intel® ME SMBus Enable
0x107h	6:0	**User input**	Intel® ME SMBus I^2C Address
0x108h	6:0	**User Input**	Intel® ME SMBus ASD Address [See Descriptor Configuration Chapter Section 9.6 for details]
0x109h	6:0	**User Input**	Intel® ME SMBus MCTP Address
0x10Ah	0	**1b**	Intel® ME SMBus I^2C Address Enable. To enable = 1b
0x10Bh	0	**1b**	Intel® ME SMBus ASD Address Enable
0x10Ch	0	**1b**	Intel® ME SMBus MCTP Address Enable
0x10Eh	15:0	**User input**	Intel® ME SMBus Subsystem Vendor & Device ID for ASF [31:16] [See Descriptor Configuration Chapter Section 9.12 for details]
0x116h	1:0	**11b**	Intel® ME SMBus Frequency



10.1.7 SMLink0 Enabling Dependencies

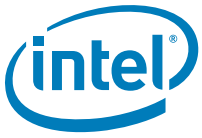
To enable SMLink0:

Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
0x119h	0	**1b**	Intel® ME SMLink0 Enable
0x11Bh	6:0	**User input**	Intel® ME SMBus I²C Address
0x11Ch	6:0	**User Input**	Intel® ME SMBus ASD Address [See Descriptor Configuration Chapter Section 9.6 for details]
0x11Dh	6:0	**User Input**	Intel® ME SMBus MCTP Address
0x11Eh	0	**1b**	Intel® ME SMBus I²C Address Enable. To enable = 1b
0x11Fh	0	**1b**	Intel® ME SMBus ASD Address Enable
0x120h	0	**1b**	Intel® ME SMBus MCTP Address Enable
0x123h	15:0	**User input**	Intel® ME SMBus Subsystem Vendor & Device ID for ASF [31:16] [See Descriptor Configuration Chapter Section 9.12 for details]
0x12Ah	1:0	**11b**	Intel® ME SMBus Frequency

10.1.8 SMLink1 Enabling Dependencies

To enable SMLink1:

Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
0x12Dh	0	**1b**	Intel® ME SMLink1 Enable
0x12Fh	6:0	**User input**	Intel® ME SMBus I²C Address
0x130h	6:0	**User Input**	Intel® ME SMBus ASD Address [See Descriptor Configuration Chapter Section 9.6 for details]
0x131h	6:0	**User Input**	Intel® ME SMBus MCTP Address
0x132h	0	**1b**	Intel® ME SMBus I²C Address Enable. To enable = 1b
0x133h	0	**1b**	Intel® ME SMBus ASD Address Enable
0x134h	0	**1b**	Intel® ME SMBus MCTP Address Enable
0x13Bh	15:0	**User input**	Intel® ME SMBus Subsystem Vendor & Device ID for ASF [31:16] [See Descriptor Configuration Chapter Section 9.12 for details]
0x13Eh	1:0	**11b**	Intel® ME SMBus Frequency



10.1.9 TPM over SPI Enabling Dependencies

To enable TPM over SPI,

Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
0x178h	0	**1b**	TPM Over SPI Bus Enable
0x1F5h	2:0	**User select**	TPM Clock Frequency [See Descriptor Configuration Chapter Section 9.166 for details]

To disable TPM over SPI,

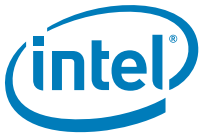
Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
0x178h	0	**0b**	TPM Over SPI Bus Enable

10.1.10 mSATA/M.2 / SATA Express Enabling

10.1.10.1 SATA0 / PCIe7 mSATA /M.2 / SATA Express Enabling HSIO

Port 0 if to run on configurable mode by SATAXPCIE0 (e.g. mSATA/M.2 / SATA Express)

Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
0x168h	1:0	**11b**	SATA / PCIe GP Select for Port 0
0x17Dh	1:0	**11b**	PCIe / SATA Combo Port 0 Strap
0x18Ch	1:0	**11b**	SATA / PCIe Select for Port 0
0x184h	0	**0b**	Polarity Select SATA / PCIe Combo Port 0 (PSCPSP_P0_STRP) When SATAXPCIE0 /SATAGP0 ='0' - PCIe Mode When SATAXPCIE0 /SATAGP0='1' -SATA Mode
0x18Dh	4	**0b**	SATA / PCIe GPIO Polarity Port 0 (SPS0) When SATAXPCIE0 /SATAGP0 ='0' - PCIe Mode When SATAXPCIE0 /SATAGP0='1' - SATA Mode
Or			
0x184h	0	**1b**	Polarity Select SATA / PCIe Combo Port 0 (PSCPSP_P0_STRP) When SATAXPCIE0 /SATAGP0 ='0' - SATA Mode When SATAXPCIE0 /SATAGP0 ='1' - PCIe Mode
0x18Dh	4	**1b**	SATA / PCIe GPIO Polarity Port 0 (SPS0) When SATAXPCIE0 /SATAGP0 ='0' - SATA Mode When SATAXPCIE0 /SATAGP0 ='1' - PCIe Mode



10.1.10.2 SATA1A / PCIe8 mSATA /M.2 / SATA Express Enabling

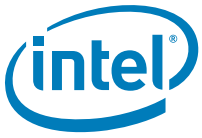
Port 1, if to run on configurable mode by SATAXPCIE1 (e.g. mSATA /M.2 / SATA Express)

Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
0x168h	3:2	**11b**	SATA / PCIe GP Select for Port 1
0x17Dh	3:2	**11b**	PCIe / SATA Combo Port 1 Strap
0x18Ch	3:2	**11b**	SATA / PCIe Select for Port 1
0x184h	1	**0b**	Polarity Select SATA / PCIe Combo Port 1 (PSCPSP_P1_STRP) When SATAXPCIE1 /SATAGP1 ='0' - PCIe Mode When SATAXPCIE1 /SATAGP1 ='1' -SATA Mode
0x18Dh	5	**0b**	SATA / PCIe GPIO Polarity Port 1 (SPS1) When SATAXPCIE1 /SATAGP1 ='0' - PCIe Mode When SATAXPCIE1 /SATAGP1 ='1' -SATA Mode
Or			
0x184h	1	**1b**	Polarity Select SATA / PCIe Combo Port 1 (PSCPSP_P1_STRP) When SATAXPCIE1 /SATAGP1 ='0' - SATA Mode When SATAXPCIE1 /SATAGP1 ='1' -PCIe Mode
0x18Dh	5	**1b**	SATA / PCIe GPIO Polarity Port 1 (SPS1) When SATAXPCIE1 /SATAGP1 ='0' - SATA Mode When SATAXPCIE1 /SATAGP1 ='1' -PCIe Mode

10.1.10.3 SATA1B / PCIe11 mSATA /M.2 / SATA Express Enabling

Port2, if to run on configurable mode by SATAXPCIE1 (e.g. mSATA /M.2 / SATA Express)

Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
0x168h	3:2	**11b**	SATA / PCIe GP Select for Port 1
0x17Dh	5:4	**11b**	PCIe / SATA Combo Port 2 Strap
0x18Ch	3:2	**11b**	SATA / PCIe Select for Port 1
0x184h	2	**0b**	Polarity Select SATA / PCIe Combo Port 2 (PSCPSP_P2_STRP) When SATAXPCIE1 /SATAGP1 ='0' - PCIe Mode When SATAXPCIE1 /SATAGP1 ='1' -SATA Mode
0x18Dh	5	**0b**	SATA / PCIe GPIO Polarity Port 1 (SPS1) When SATAXPCIE1 /SATAGP1 ='0' - PCIe Mode When SATAXPCIE1 /SATAGP1 ='1' -SATA Mode
Or			
0x184h	2	**1b**	Polarity Select SATA / PCIe Combo Port 2 (PSCPSP_P2_STRP) When SATAXPCIE1 /SATAGP1 ='0' - SATA Mode When SATAXPCIE1 /SATAGP1 ='1' -PCIe Mode
0x18Dh	5	**1b**	SATA / PCIe GPIO Polarity Port 1 (SPS1) When SATAXPCIE1 /SATAGP1 ='0' - SATA Mode When SATAXPCIE1 /SATAGP1 ='1' -PCIe Mode



10.1.10.4 SATA2 / PCIe12 mSATA /M.2 / SATA Express Enabling

Port 3, if to run on configurable mode by SATAXPCIE2 (e.g. mSATA /M.2 / SATA Express)

Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
0x168h	5:4	**11b**	SATA / PCIe GP Select for Port 2
0x180h	1:0	**11b**	PCIe / SATA Combo Port 3 Strap
0x18Ch	5:4	**11b**	SATA / PCIe Select for Port 3
0x184h	3	**0b**	Polarity Select SATA / PCIe Combo Port 3 (PSCPSP_P3_STRP) When SATAXPCIE2 /SATAGP2 ='0' - PCIe Mode When SATAXPCIE2 /SATAGP2 ='1' -SATA Mode
0x18Dh	6	**0b**	SATA / PCIe GPIO Polarity Port 3 (SPS3) When SATAXPCIE2 /SATAGP2 ='0' - PCIe Mode When SATAXPCIE2 /SATAGP2 ='1' -SATA Mode
Or			
0x184h	3	**1b**	Polarity Select SATA / PCIe Combo Port 3 (PSCPSP_P3_STRP) When SATAXPCIE2 /SATAGP2='0' - SATA Mode When SATAXPCIE2 /SATAGP2 ='1' -PCIe Mode
0x18Dh	6	**1b**	SATA / PCIe GPIO Polarity Port 3 (SPS3) When SATAXPCIE2 /SATAGP2='0' - SATA Mode When SATAXPCIE2 /SATAGP2='1' - PCIe Mode

§ §

A FAQ and Troubleshooting

A.1 FAQ

Q: How do I find the Flash Programming Tool (FPT) and Flash Image Tool (FIT) for my platform?

A: The aforementioned flash tools are included in the system tools directory in Intel® ME FW kit. Please ensure that you download the appropriate kit for the target platform.

Target	Platform Name In VIP	Kit Name
Skylake	Skylake Platform	Intel® Management Engine 11.X (use latest version)

Q: How do I build an Image for my Intel PCH based platform?

A: Skylake PCH-LPH family based platforms, you can follow the appropriate instructions in the FW Bringup Guide which is located in the root directory of the appropriate Intel® ME KIT.

Q: Is my flash part supported by the Flash Programming Tool (FPT)? How can I add support for a new flash to FPT?

A: Look at fparts.txt to see if the intended flash part is present. If the intended flash part meets the guidelines defined in the *Skylake PCH-LP Family External Design Specification (EDS), Intel®* Management Engine (Intel® ME) Firmware SPI Flash Requirements *and* support may be added to FPT by adding an entry for the part into the Fparts.txt file.

Q: Is my flash part supported by Intel® ME Firmware? How can I add support for a new flash to Intel® ME Firmware?

A: As long as the SPI flash devices meets the requirements defined in the *Skylake PCH-LP Family External Design Specification (EDS)*, support may be added for the device. BIOS will have to set up the Host VSCC registers. The Intel Management Engine VSCC table in the descriptor will also have to be set up in order to get Intel® ME firmware to work.

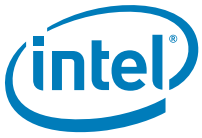
Adding support does not imply validation or guarantee a flash part will work. Platform designers/integrators will have to validate all flash parts with their platforms to ensure full functionality and reliability.

Q: Do I have to use SFDP enabled SPI flash parts?

A: Yes you will need to use SFDP enabled SPI flash parts regardless of using the VSCC table entries Skylake does not support VSCC only SPI flash parts.

Q: Why does FPT/verify fail for my system even when I wrote nothing to flash?

A: Intel® ME Firmware performs periodic writes to SPI flash when it is active. Due to this the ME region may not match the source file. There are also other system activities beside the Intel® ME that can change the data on the flash vs the original image. For example, the GbE check sum is updated on flash part whenever the value is incorrect.



Q: How can I overwrite the descriptor when FPT does not have write access? How can I overwrite a region that is locked down by descriptor protections? How do I write to flash space that is not defined by the descriptor?

A: By asserting HDA_SDO (flash descriptor override strap) low on the rising edge of PWROK, you can read, write and erase all of SPI flash space regardless of descriptor protections. Any protections imposed by BIOS or directly to the SPI flash part still apply. This should only be used in debug or manufacturing environments. End customers should **NOT** receive systems with this strap engaged.

Q: I have two flash parts installed on the board. Why does fpt /i only show one flash part?

A: Skylake PCH-*LP* will not recognize the second SPI flash part unless it is in descriptor mode and the Component section of the descriptor properly describes the flash. Another possibility is that you have two different flash parts and the second flash part is not defined in fparts.txt.

A.2 Troubleshooting

Q: I'm seeing the following error:

```
Intel(R) Flash Programming Tool. Version:  x.x.x.xxxx
Copyright (c) 2007-2015, Intel Corporation. All rights reserved.
Platform: Intel(R) Qxx Express Chipset
Reading HSFSTS register... Flash Descriptor: Invalid

--- Flash Devices Found ---

Error: Timedout waiting for hardware to complete read operation!
    SSFSTS register: 0x00

Error: Timedout waiting for hardware to complete read operation!
    SSFSTS register: 0x00

Error: Timedout waiting for hardware to complete read operation!
    SSFSTS register: 0x00

Error: Failed to read the device ID from the flash part!
```

A: You may be using the wrong version of FPT. Please ensure that you are using the flash tools that were provided in the kit for the target systems.

Q: What does following FPT error message mean?

Error: The host does not have write access to the target flash memory!

A: In order for FPT to read or write to a given region, BIOS/Host must have read/write permissions to that target region. This access is set in the descriptor. Look closely at all the addresses defined in the output of FPT /i. If there are any gaps in flash space defined you cannot perform a full flash write. You have to update region by region. Refer to 4.3 Region Access Control for more information. You may have to reflash the descriptor to get the proper access.

Q: What does following FPT error message mean?

Error: Flash program registers are locked! HSFSTS[15] (FLOCKDN).

A: The Flash Configuration Lock-Down (FLCOKDN) bit was set HSFS (hardware sequencing flash status register). This locks down all the program registers in the ICH. If your BIOS and descriptor do not set up Hardware Sequencing, you will have to leave this bit unset in order to use FPT. You may have to upgrade the latest version of FPT as older versions do not support Hardware Sequencing. Please refer to **Hardware Sequencing Flash Status Register** in the *Skylake PCH-LP Family External Design Specification (EDS)* for the location for the HSFS. Try reflashing the SPI device with a 3rd Party programmer. If you still see this error message, please contact your BIOS vendor to ensure that they are not setting this bit.

Q: What does following FPT error message mean?

Error: There is no supported SPI flash device installed.

A: See the answer to the question above: ***Is my flash part supported by the Flash Programming Tool (FPT)? How can I add support for a new flash to FPT?***

If the tool correctly identifies the flash part installed and still gives an error message like:

--- Flash Devices Found ---
SPI1234 ID:0x123456 Size: 4096KB (32768Kb)
Device ID: 0xFFFF not supported.

Error 405: There is no supported SPI flash device installed

This error will result when the descriptor has two flash parts defined. Edit the image via FIT/FITC and set the number of flash components to 1.

See 6.4 Recommendations for Flash Configuration Lockdown and Vendor Component Lock Bits for Opcodes required for FPT operation.

§ §