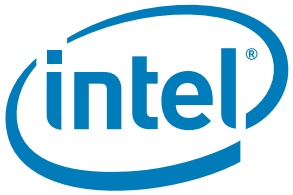


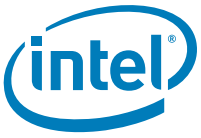
Ice lake-N Client Platform

SPI Programming Guide

August 2019

Revision 1.1

Intel Confidential



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.

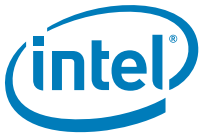
Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families. Go to: http://www.intel.com/products/processor_number.

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.



Contents

1 Introduction 11
1.1 Overview 11
1.2 Terminology 12
1.3 Reference Documents 12

2 PCH SPI Flash Architecture 14
2.1 Descriptor Mode 14
2.2 Serial Flash Discoverable Parameter (SFDP) 14
2.3 SPI Fast Read 14
2.4 Intel® Trusted Platform Module (Intel® TPM) on SPI Bus 14
2.5 Boot Flow for Ice Lake PCH-LP Family 14
2.6 Flash Regions 15
2.6.1 Flash Region Layout 15
2.6.2 Flash Region Sizes 17
2.7 Hardware Sequencing 17

3 PCH SPI Flash Compatibility Requirement 18
3.1 Ice Lake PCH SPI Flash Requirements 18
3.1.1 General Requirements 18
3.1.2 Bios Requirement 19
3.1.3 Software / Firmware Requirements 19
3.1.4 JEDEC ID (Opcode 9Fh) 20
3.1.5 Multiple Page Write Usage Model 20
3.1.6 Hardware Sequencing Requirements 20
3.2 Ice Lake PCH SPI AC Electrical Compatibility Guidelines 21
3.3 SPI Flash DC Electrical Compatibility Guidelines 23

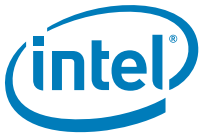
4 Descriptor Overview 24
4.1 Flash Descriptor Content 25
4.1.1 Descriptor Signature and Map 26
4.1.1.1 FLVALSIG - Flash Valid Signature (Flash Descriptor Records) 26
4.1.1.2 FLMAP0 - Flash Map 0 Register (Flash Descriptor Records) 26
4.1.1.3 FLMAP1 - Flash Map 1 Register (Flash Descriptor Records) 28
4.1.1.4 FLMAP2—Flash Map 2 Register (Flash Descriptor Records) 28
4.1.1.5 FLMAP3—Flash Map 3 Register (Flash Descriptor Records) 28
4.1.2 Flash Descriptor Component Section 29
4.1.2.1 FLCOMP—Flash Components Register (Flash Descriptor Records) 29
4.1.2.2 FLILL—Flash Invalid Instructions Register (Flash Descriptor Records) 32
4.1.2.3 FLILL1—Flash Invalid Instructions Register (Flash Descriptor Records) 32
4.1.3 Flash Descriptor Region Section 33
4.1.3.1 FLREG0—Flash Region 0 (Flash Descriptor) Register ..... (Flash Descriptor Records) 34
4.1.3.2 FLREG1—Flash Region 1 (BIOS) Register (Flash Descriptor Records) 34

4.1.3.3 FLREG2—Flash Region 2 (IFWI / Intel® ME ROM Bypass) Register (Flash Descriptor Records) 34
4.1.3.4 FLREG3—Flash Region 3 (GbE) Register (Flash Descriptor Records) 35
4.1.3.5 FLREG4—Flash Region 4 (Platform Data) Register (Flash Descriptor Records) 35
4.1.3.6 FLREG8—Flash Region 8 (Embedded Controller) Register (Flash Descriptor Records) 35
4.1.4 Flash Descriptor Master Section 37
4.1.4.1 FLMSTR1—Flash Master 1 (Host CPU/ BIOS) 37
4.1.4.2 FLMSTR2—Flash Master 2 (Intel® ME) 37
4.1.4.3 FLMSTR3—Flash Master 3 (GbE) 37
4.1.4.4 FLMSTR4—Flash Master 4 (Reserved) 38
4.1.4.5 FLMSTR5—Flash Master 5 (EC) 38
4.1.5 PCH / CPU Softstraps 39
4.1.6 Descriptor Upper Map Section 39
4.1.6.1 FLUMAP1—Flash Upper Map 1 (Flash Descriptor Records) 39
4.1.6.2 IFWI / Intel® ME ROM Bypass Size 39
4.1.6.3 MIP - Descriptor Table 39
4.1.7 Intel® ME Vendor Specific Component Capabilities Table 40
4.1.7.1 JID0—JEDEC-ID 0 Register (Flash Descriptor Records) 40
4.1.7.2 VSCC0—Vendor Specific Component Capabilities 0 (Flash Descriptor Records) 41
4.1.7.3 JIDn—JEDEC-ID Register n (Flash Descriptor Records) 41
4.1.7.4 VSCCn—Vendor Specific Component Capabilities n (Flash Descriptor Records) 41
4.2 OEM Section 42
4.3 Region Access Control 42
4.3.1 Intel Recommended Permissions for Region Access 43
4.3.2 Overriding Region Access 43
4.4 Intel® ME Vendor-Specific Component Capabilities (Intel® ME VSCC) Table 44
4.4.1 How to Set a VSCC Entry in Intel® ME VSCC Table for Ice Lake PCH-LP Platforms 44
4.4.2 Intel® ME VSCC Table Settings for Ice Lake PCH-LP Family Systems 46
5 Serial Flash Discoverable Parameter (SFDP) Overview 47
5.1 Introduction 47
5.2 Discoverable Parameter Opcode and Flash Cycle 47
5.3 Parameter Table Supported on PCH 47
5.4 Detailed JEDEC Specification 48
6 Configuring BIOS/GbE for SPI Flash Access 49
6.1 Unlocking SPI Flash Device Protection for Ice Lake PCH-LP Platform 49
6.2 Locking SPI Flash via Status Register 50
6.3 SPI Protected Range Register Recommendations 50
6.4 Recommendations for Flash Configuration Lockdown and Vendor Component Lock Bits 50
6.4.1 Flash Configuration Lockdown 50
6.4.2 Vendor Component Lock 51
6.5 Host Vendor Specific Component Control Registers (VSCC) 51
6.6 Host VSCC Register Settings 55
7 IFWI / Intel® ME Disable for Debug/Flash Burning Purposes 56
7.1 IFWI / Intel® ME Disable 56
7.1.1 Erasing/Programming Intel® ME Region 56
8 Recommendations for SPI Flash Programming in Manufacturing Environments 57

9 Flash Descriptor PCH / PMC / CPU and Intel® CSME Configuration Section 58

9.1 PCH Descriptor Record 0 (Flash Descriptor Records) 58
9.2 PCH Descriptor Record 1 (Flash Descriptor Records) 58
9.3 PCH Descriptor Record 2 (Flash Descriptor Records) 58
9.4 PCH Descriptor Record 3 (Flash Descriptor Records) 58
9.5 PCH Descriptor Record 4 (Flash Descriptor Records) 59
9.6 PCH Descriptor Record 5 (Flash Descriptor Records) 59
9.7 PCH Descriptor Record 6 (Flash Descriptor Records) 59
9.8 PCH Descriptor Record 7 (Flash Descriptor Records) 59
9.9 PCH Descriptor Record 8 (Flash Descriptor Records) 60
9.10 PCH Descriptor Record 9 (Flash Descriptor Records) 60
9.11 PCH Descriptor Record 10 (Flash Descriptor Records) 61
9.12 PCH Descriptor Record 11 (Flash Descriptor Records) 61
9.13 PCH Descriptor Record 12 (Flash Descriptor Records) 61
9.14 PCH Descriptor Record 13 (Flash Descriptor Records) 62
9.15 PCH Descriptor Record 14 (Flash Descriptor Records) 62
9.16 PCH Descriptor Record 15 (Flash Descriptor Records) 63
9.17 PCH Descriptor Record 16 (Flash Descriptor Records) 64
9.18 PCH Descriptor Record 17 (Flash Descriptor Records) 65
9.19 PCH Descriptor Record 18 (Flash Descriptor Records) 65
9.20 PCH Descriptor Record 19 (Flash Descriptor Records) 65
9.21 PCH Descriptor Record 20 (Flash Descriptor Records) 66
9.22 PCH Descriptor Record 21 (Flash Descriptor Records) 66
9.23 PCH Descriptor Record 22 (Flash Descriptor Records) 67
9.24 PCH Descriptor Record 23 (Flash Descriptor Records) 67
9.25 PCH Descriptor Record 24 (Flash Descriptor Records) 67
9.26 PCH Descriptor Record 25 (Flash Descriptor Records) 67
9.27 PCH Descriptor Record 26 (Flash Descriptor Records) 68
9.28 PCH Descriptor Record 27 (Flash Descriptor Records) 69
9.29 PCH Descriptor Record 28 (Flash Descriptor Records) 70
9.30 PCH Descriptor Record 29 (Flash Descriptor Records) 71
9.31 PCH Descriptor Record 30 (Flash Descriptor Records) 72
9.32 PCH Descriptor Record 31 (Flash Descriptor Records) 73
9.33 PCH Descriptor Record 32 (Flash Descriptor Records) 74
9.34 PCH Descriptor Record 33 (Flash Descriptor Records) 75
9.35 PCH Descriptor Record 34 (Flash Descriptor Records) 76
9.36 PCH Descriptor Record 35 (Flash Descriptor Records) 76
9.37 PCH Descriptor Record 36 (Flash Descriptor Records) 76
9.38 PCH Descriptor Record 37 (Flash Descriptor Records) 77
9.39 PCH Descriptor Record 38 (Flash Descriptor Records) 78
9.40 PCH Descriptor Record 39 (Flash Descriptor Records) 79
9.41 PCH Descriptor Record 40 (Flash Descriptor Records) 80
9.42 PCH Descriptor Record 41 (Flash Descriptor Records) 81
9.43 PCH Descriptor Record 42 (Flash Descriptor Records) 82
9.44 PCH Descriptor Record 43 (Flash Descriptor Records) 83
9.45 PCH Descriptor Record 44 (Flash Descriptor Records) 83
9.46 PCH Descriptor Record 45 (Flash Descriptor Records) 84
9.47 PCH Descriptor Record 46 (Flash Descriptor Records) 85
9.48 PCH Descriptor Record 47 (Flash Descriptor Records) 85
9.49 PCH Descriptor Record 48 (Flash Descriptor Records) 86
9.50 PCH Descriptor Record 49 (Flash Descriptor Records) 87
9.51 PCH Descriptor Record 50 (Flash Descriptor Records) 87
9.52 PCH Descriptor Record 51 (Flash Descriptor Records) 88
9.53 PCH Descriptor Record 52 (Flash Descriptor Records) 88
9.54 PCH Descriptor Record 53 (Flash Descriptor Records) 89

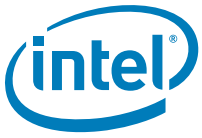
9.55 PCH Descriptor Record 54 (Flash Descriptor Records) 89
9.56 PCH Descriptor Record 55 (Flash Descriptor Records) 89
9.57 PCH Descriptor Record 56 (Flash Descriptor Records) 90
9.58 PCH Descriptor Record 57 (Flash Descriptor Records) 90
9.59 PCH Descriptor Record 58 (Flash Descriptor Records) 90
9.60 PCH Descriptor Record 59 (Flash Descriptor Records) 90
9.61 PCH Descriptor Record 60 (Flash Descriptor Records) 90
9.62 PCH Descriptor Record 61 (Flash Descriptor Records) 91
9.63 PCH Descriptor Record 62 (Flash Descriptor Records) 91
9.64 PCH Descriptor Record 63 (Flash Descriptor Records) 91
9.65 PCH Descriptor Record 64 (Flash Descriptor Records) 92
9.66 PCH Descriptor Record 65 (Flash Descriptor Records) 93
9.67 PCH Descriptor Record 66 (Flash Descriptor Records) 93
9.68 PCH Descriptor Record 67 (Flash Descriptor Records) 94
9.69 PCH Descriptor Record 68 (Flash Descriptor Records) 94
9.70 PCH Descriptor Record 69 (Flash Descriptor Records) 94
9.71 PCH Descriptor Record 70 (Flash Descriptor Records) 94
9.72 PCH Descriptor Record 71 (Flash Descriptor Records) 95
9.73 PCH Descriptor Record 72 (Flash Descriptor Records) 95
9.74 PCH Descriptor Record 73 (Flash Descriptor Records) 95
9.75 PCH Descriptor Record 74 (Flash Descriptor Records) 95
9.76 PCH Descriptor Record 75 (Flash Descriptor Records) 96
9.77 PCH Descriptor Record 76 (Flash Descriptor Records) 96
9.78 PCH Descriptor Record 77 (Flash Descriptor Records) 96
9.79 PCH Descriptor Record 78 (Flash Descriptor Records) 96
9.80 PCH Descriptor Record 79 (Flash Descriptor Records) 97
9.81 PCH Descriptor Record 80 (Flash Descriptor Records) 97
9.82 PCH Descriptor Record 81 (Flash Descriptor Records) 97
9.83 PCH Descriptor Record 82 (Flash Descriptor Records) 98
9.84 PCH Descriptor Record 83 (Flash Descriptor Records) 98
9.85 PCH Descriptor Record 84 (Flash Descriptor Records) 98
9.86 PCH Descriptor Record 85 (Flash Descriptor Records) 98
9.87 PCH Descriptor Record 86 (Flash Descriptor Records) 98
9.88 PCH Descriptor Record 87 (Flash Descriptor Records) 99
9.89 PCH Descriptor Record 88 (Flash Descriptor Records) 99
9.90 PCH Descriptor Record 89 (Flash Descriptor Records) 99
9.91 PCH Descriptor Record 90 (Flash Descriptor Records) 100
9.92 PCH Descriptor Record 91 (Flash Descriptor Records) 100
9.93 PCH Descriptor Record 92 (Flash Descriptor Records) 100
9.94 PCH Descriptor Record 93 (Flash Descriptor Records) 100
9.95 PCH Descriptor Record 94 (Flash Descriptor Records) 100
9.96 PCH Descriptor Record 95 (Flash Descriptor Records) 101
9.97 PCH Descriptor Record 96 (Flash Descriptor Records) 101
9.98 PCH Descriptor Record 97 (Flash Descriptor Records) 102
9.99 PCH Descriptor Record 98 (Flash Descriptor Records) 102
9.100 PCH Descriptor Record 99 (Flash Descriptor Records) 103
9.101 PCH Descriptor Record 100 (Flash Descriptor Records) 103
9.102 PCH Descriptor Record 101 (Flash Descriptor Records) 103
9.103 PCH Descriptor Record 102 (Flash Descriptor Records) 104
9.104 PCH Descriptor Record 103 (Flash Descriptor Records) 104
9.105 PCH Descriptor Record 104 (Flash Descriptor Records) 104
9.106 PCH Descriptor Record 105 (Flash Descriptor Records) 104
9.107 PCH Descriptor Record 106 (Flash Descriptor Records) 104
9.108 PCH Descriptor Record 107 (Flash Descriptor Records) 105
9.109 PCH Descriptor Record 108 (Flash Descriptor Records) 105



9.110 PCH Descriptor Record 109 (Flash Descriptor Records) 105
9.111 PCH Descriptor Record 110 (Flash Descriptor Records) 106
9.112 PCH Descriptor Record 111 (Flash Descriptor Records) 106
9.113 PCH Descriptor Record 112 (Flash Descriptor Records) 107
9.114 PCH Descriptor Record 113 (Flash Descriptor Records) 107
9.115 PCH Descriptor Record 114 (Flash Descriptor Records) 107
9.116 PCH Descriptor Record 115 (Flash Descriptor Records) 107
9.117 PCH Descriptor Record 116 (Flash Descriptor Records) 107
9.118 PCH Descriptor Record 117 (Flash Descriptor Records) 108
9.119 PCH Descriptor Record 118 (Flash Descriptor Records) 108
9.120 PCH Descriptor Record 119 (Flash Descriptor Records) 108
9.121 PCH Descriptor Record 120 (Flash Descriptor Records) 108
9.122 PCH Descriptor Record 121 (Flash Descriptor Records) 108
9.123 PCH Descriptor Record 122 (Flash Descriptor Records) 109
9.124 PCH Descriptor Record 123 (Flash Descriptor Records) 109
9.125 PCH Descriptor Record 124 (Flash Descriptor Records) 109
9.126 PCH Descriptor Record 125 (Flash Descriptor Records) 109
9.127 PCH Descriptor Record 126 (Flash Descriptor Records) 110
9.128 PCH Descriptor Record 127 (Flash Descriptor Records) 110
9.129 PCH Descriptor Record 128 (Flash Descriptor Records) 110
9.130 PCH Descriptor Record 129 (Flash Descriptor Records) 111
9.131 PCH Descriptor Record 130 (Flash Descriptor Records) 111
9.132 PCH Descriptor Record 131 (Flash Descriptor Records) 111
9.133 PCH Descriptor Record 132 (Flash Descriptor Records) 111
9.134 PCH Descriptor Record 133 (Flash Descriptor Records) 112
9.135 PCH Descriptor Record 134 (Flash Descriptor Records) 112
9.136 PCH Descriptor Record 135 (Flash Descriptor Records) 112
9.137 PCH Descriptor Record 136 (Flash Descriptor Records) 112
9.138 PCH Descriptor Record 137 (Flash Descriptor Records) 112
9.139 PCH Descriptor Record 138 (Flash Descriptor Records) 113
9.140 PCH Descriptor Record 139 (Flash Descriptor Records) 113
9.141 PCH Descriptor Record 140 (Flash Descriptor Records) 113
9.142 PCH Descriptor Record 141 (Flash Descriptor Records) 113
9.143 PCH Descriptor Record 142 (Flash Descriptor Records) 113
9.144 PCH Descriptor Record 143 (Flash Descriptor Records) 114
9.145 PCH Descriptor Record 144 (Flash Descriptor Records) 114
9.146 PCH Descriptor Record 145 (Flash Descriptor Records) 114
9.147 PCH Descriptor Record 146 (Flash Descriptor Records) 114
9.148 PCH Descriptor Record 147 (Flash Descriptor Records) 114
9.149 PCH Descriptor Record 148 (Flash Descriptor Records) 115
9.150 PCH Descriptor Record 149 (Flash Descriptor Records) 115
9.151 PCH Descriptor Record 150 (Flash Descriptor Records) 115
9.152 PCH Descriptor Record 151 (Flash Descriptor Records) 115
9.153 PCH Descriptor Record 152 (Flash Descriptor Records) 115
9.154 PCH Descriptor Record 153 (Flash Descriptor Records) 116
9.155 PCH Descriptor Record 154 (Flash Descriptor Records) 116
9.156 PCH Descriptor Record 155 (Flash Descriptor Records) 116
9.157 PCH Descriptor Record 156 (Flash Descriptor Records) 116
9.158 PCH Descriptor Record 157 (Flash Descriptor Records) 116
9.159 PCH Descriptor Record 158 (Flash Descriptor Records) 117
9.160 PCH Descriptor Record 159 (Flash Descriptor Records) 117
9.161 PCH Descriptor Record 160 (Flash Descriptor Records) 117
9.162 MIP Table Descriptor Record 0 (Flash Descriptor Records) 118
9.163 MIP Table Descriptor Record 1 (Flash Descriptor Records) 118
9.164 MIP Table Descriptor Record 2 (Flash Descriptor Records) 118

9.165 MIP Table Descriptor Record 3 (Flash Descriptor Records) 118
9.166 MIP Table Descriptor Record 4 (Flash Descriptor Records) 119
9.167 MIP Table Descriptor Record 5 (Flash Descriptor Records) 119
9.168 MIP Table Descriptor Record 6 (Flash Descriptor Records) 119
9.169 MIP Table Descriptor Record 7 (Flash Descriptor Records) 119
9.170 MIP Table Descriptor Record 8 (Flash Descriptor Records) 120
9.171 MIP Table Descriptor Record 9 (Flash Descriptor Records) 120
9.172 PMC Descriptor Record 0 (Flash Descriptor Records) 121
9.173 PMC Descriptor Record 1 (Flash Descriptor Records) 122
9.174 PMC Descriptor Record 2 (Flash Descriptor Records) 123
9.175 PMC Descriptor Record 3 (Flash Descriptor Records) 123
9.176 PMC Descriptor Record 4 (Flash Descriptor Records) 123
9.177 PMC Descriptor Record 5 (Flash Descriptor Records) 124
9.178 PMC Descriptor Record 6 (Flash Descriptor Records) 124
9.179 PMC Descriptor Record 7 (Flash Descriptor Records) 124
9.180 PMC Descriptor Record 8 (Flash Descriptor Records) 125
9.181 PMC Descriptor Record 9 (Flash Descriptor Records) 125
9.182 PMC Descriptor Record 10 (Flash Descriptor Records) 126
9.183 PMC Descriptor Record 11 (Flash Descriptor Records) 127
9.184 PMC Descriptor Record 12 (Flash Descriptor Records) 128
9.185 PMC Descriptor Record 13 (Flash Descriptor Records) 129
9.186 PMC Descriptor Record 14 (Flash Descriptor Records) 130
9.187 PMC Descriptor Record 15 (Flash Descriptor Records) 130
9.188 PMC Descriptor Record 16 (Flash Descriptor Records) 130
9.189 PMC Descriptor Record 17 (Flash Descriptor Records) 130
9.190 PMC Descriptor Record 18 (Flash Descriptor Records) 130
9.191 PMC Descriptor Record 19 (Flash Descriptor Records) 131
9.192 PMC Descriptor Record 20 (Flash Descriptor Records) 131
9.193 CPU Descriptor Record 0 (Flash Descriptor Records) 132
9.194 CPU Descriptor Record 1 (Flash Descriptor Records) 133
9.195 CPU Descriptor Record 2 (Flash Descriptor Records) 134
9.196 CPU Descriptor Record 3 (Flash Descriptor Records) 135
9.197 CPU Descriptor Record 4 (Flash Descriptor Records) 136
9.198 CPU Descriptor Record 5 (Flash Descriptor Records) 137
9.199 CPU Descriptor Record 6 (Flash Descriptor Records) 138
9.200 CPU Descriptor Record 7 (Flash Descriptor Records) 139
9.201 CPU Descriptor Record 8 (Flash Descriptor Records) 141
9.202 CPU Descriptor Record 9 (Flash Descriptor Records) 142
9.203 CPU Descriptor Record 10 (Flash Descriptor Records) 143
9.204 CPU Descriptor Record 11 (Flash Descriptor Records) 144
9.205 Intel® CSME Descriptor Record 0 (Flash Descriptor Records) 145
9.206 Intel® CSME Descriptor Record 1 (Flash Descriptor Records) 146

A FAQ and Troubleshooting 148

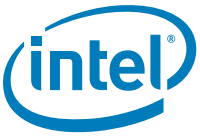


Figures

2-1 SPI Flash Region Layout 16
3-1 SPI Timing 22
3-2 PCH Test Load 23
4-1 Flash Descriptor (Ice Lake PCH-LP) 24
5-1 SFDP Read Instruction Sequence 47

Tables

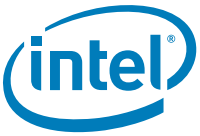
1-1 Terminology 12
1-2 Reference Documents 12
3-1 SPI Timings (17 MHz) 21
3-2 SPI Timings (30 MHz) 21
3-3 SPI Timings (48 MHz) 22
4-1 Region Access Control Table Options 42
4-2 Recommended Read/Write Permissions 43
4-3 Recommended Read/Write Settings for Platforms 43
4-4 Jidn - JEDEC ID Portion of Intel® ME VSCC Table 44
4-5 Vsccn – Vendor-Specific Component Capabilities Portion of the Ice Lake PCH-LP Platforms 44
6-1 VSCC0 - Vendor-Specific Component Capabilities Register for SPI Component 0 51
6-2 VSCC1 - Vendor Specific Component Capabilities Register for SPI Component 1 53
6-3 Description of How WSR and WEWS is Used 54



Revision History

Document Number	Revision Number	Description	Revision Date
	0.6	• Initial Release	October 2017
	0.61	• Added PMC USB2 DbC port enable strap setting offset 0xC24	November 2017
	0.62	• CPU and Intel® CSME strap setting offsets	January 2018
	0.7	• Updated to latest Harness v102	June 2018
	0.8	• Updated to latest Harness v119	December 2018
	0.81	• Corrected encoding descriptions for VCC SFR OC PG Present, VCC ST PG Present and VCC STG PG Present	January 2019
	1.0‘	• Updated to Rev 1.0	July 2019
	1.1	• Added SPI Software Re-Binding setting information	August 2019

§ §



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 Ice Lake 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 Ice Lake 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, “IFWI / 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 / PMC / CPU and Intel® CSME Configuration Section”

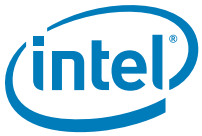
- Flash Descriptor PCH / CPU Soft Strap Section.

Chapter 10, “Configuration Dependencies”

- Descriptor configuration dependencies for enabling Ice Lake 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
Intel® FPT	Intel® Flash Programming Tool - programs the SPI flash
FIT	Intel® 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
IFWI	Integrated Firmware Image Layout
Intel® AMT	Intel® Active Management Technology
Ice Lake PCH-LP	Ice Lake 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
MCP	Multi-Chip package
MDTBA	MIP Descriptor Table Base Address
MIP	Master Image Profile
PCH	Platform Controller Hub
PCH–LP	Platform Controller Hub – Low Power
PMC	Power Management Controller (PCH)
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
Ice Lake 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.

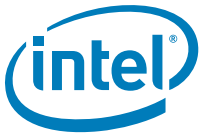
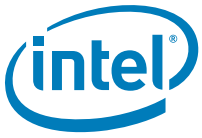


Table 1-2. Reference Documents

Document	Document # / Location
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 Ice Lake 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: **Ice Lake only supports Descriptor mode.**

See ***SPI Supported Feature Overview*** of the latest Intel Platform Controller Hub Family External Design Specification (EDS) for Ice Lake PCH 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.

Ice Lake PCH 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 Ice Lake PCH Family for more detailed information 60-MHz support requires SPI component that meet 66-MHz timing.

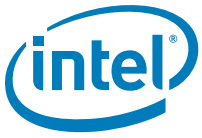
2.4 Intel® Trusted Platform Module (Intel® TPM) on SPI Bus

Ice Lake 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 Ice Lake PCH Family for more detailed information.

2.5 Boot Flow for Ice Lake PCH-LP Family

See Boot BIOS strap in the **Functional Straps** of the latest Intel Platform Controller Hub Family External Design Specification (EDS) for Ice Lake PCH 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	IFWI (Integrated Firmware Image)[1]
3	GbE – Location for Integrated LAN firmware and MAC address
4	PDR – Platform Data Region (Optional)[2]
8	EC - Embedded Controller (Optional)[3]

Notes:

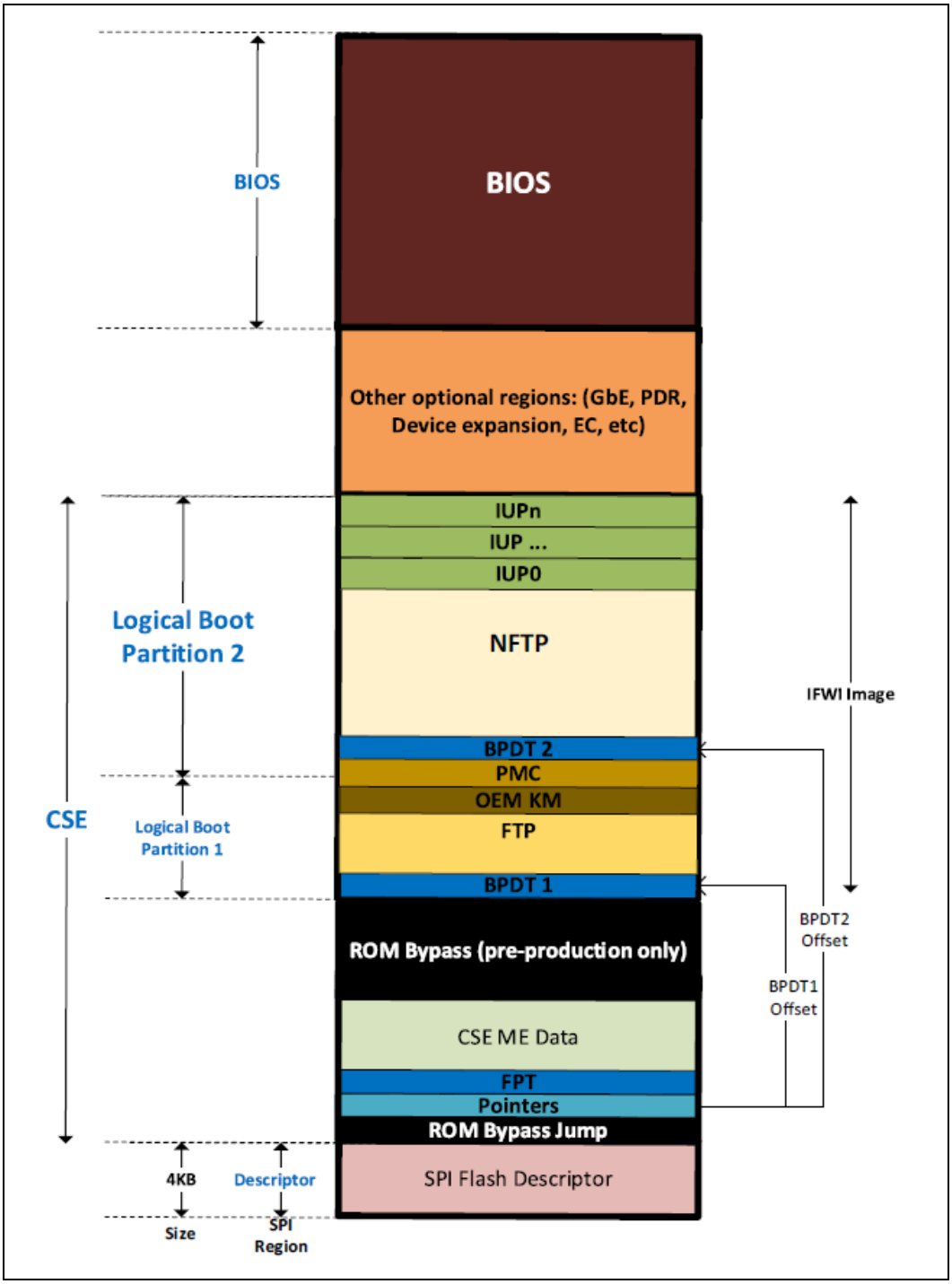
1. Also include as a part of IFWI in some instances is Intel® Management Engine (Intel® ME FW) ROM Bypass
2. The PDR region is optional and is not applicable for Ice Lake PCH-LP or not required for proper platform operation.
3. The EC region is optional and is not required for proper platform operation.

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

2.6.1 Flash Region Layout

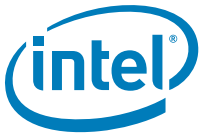
In the SPI Controller; a 4K descriptor at the base of the SPI device splits the device into regions and defines the access control to each region.

Figure 2-1. SPI Flash Region Layout



As seen in Figure 2-1, the descriptor defines at least the following device regions:

1. **Intel® ME ROM Bypass Region:** Starting from offset 4K. This regions is used for Intel® ME ROM Bypass. When Intel® ME ROM Bypass does not exist, this region size is 0.
2. **IFWI Region:** This region starts after the Intel® ME ROM Bypass region.
3. **BIOS Region:** This region starts after the IFWI region.



2.6.2 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 Ice Lake 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.

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

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

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 *Ice Lake PCH-LP Family External Design Specification (EDS)* for more details.

§ §

3 PCH SPI Flash Compatibility Requirement

3.1 Ice Lake PCH SPI Flash Requirements

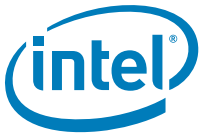
- Ice Lake PCH Family allows for up to two SPI flash devices to store BIOS, Intel® ME FW and integrated LAN information.
  - **— Intel® ME FW is required for Ice Lake PCH Family-based platforms**
  - — Each SPI component can support up to 64 MB (128 MB total addressable) using 26-bit addressing
- 3.3V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

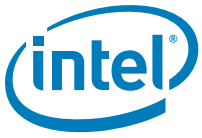
BIOS must ensure there is no SPI flash based read/write/erase protection on the GbE region. GbE firmware and drivers for the integrated LAN need to be able to read, write and erase the GbE region at all times.

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 Ice Lake 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

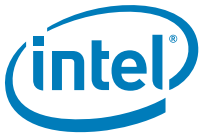
Intel platforms have firmware usage models which require that the serial flash device support multiple writes to a page (minimum of 512 writes) without requiring a preceding erase command. BIOS commonly uses capabilities such as counters that are used for error logging and system boot progress logging. 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 Ice Lake PCH SPI AC Electrical Compatibility Guidelines

Table 3-1. SPI Timings (17 MHz)

Sym	Parameter	Min	Max	Units	Notes
t180a	Serial Clock Frequency - 17MHz 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 Ice Lake PCH Family is 17.86 MHz.
2. Measurement point for low time and high time is taken at 0.5(VccSPI).

Table 3-2. SPI Timings (30 MHz)

Sym	Parameter	Min	Max	Units	Notes
t180b	Serial Clock Frequency - 30MHz 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

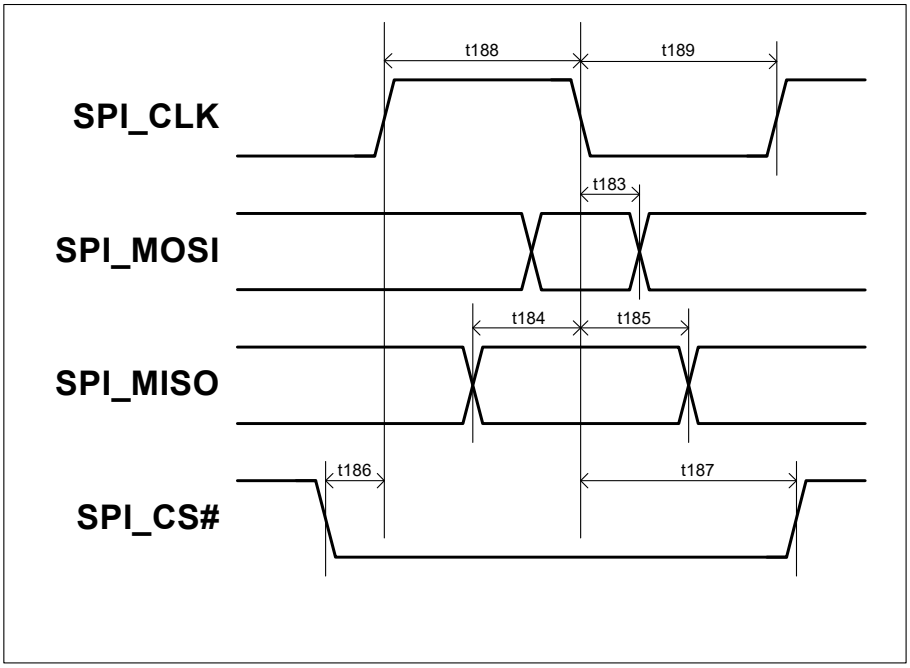
Notes:
1. Typical clock frequency driven by Ice Lake PCH Family is 30 MHz.
2. Measurement point for low time and high time is taken at 0.5(VccSPI).

Table 3-3. SPI Timings (48 MHz)

Sym	Parameter	Min	Max	Units	Notes
t180c	Serial Clock Frequency - 48 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 Ice Lake PCH Family is 48 MHz.
2. When using 48 MHz mode ensure target flash component can meet t188c and t189c specifications. Measurement should be taken at a point as close as possible to the package pin.
3. Measurement point for low time and high time is taken at 0.5(VccSPI).

Figure 3-1. SPI Timing

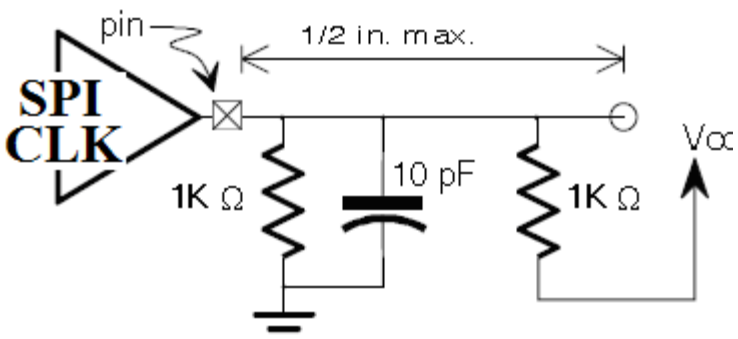


3.3 SPI Flash DC Electrical Compatibility Guidelines

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



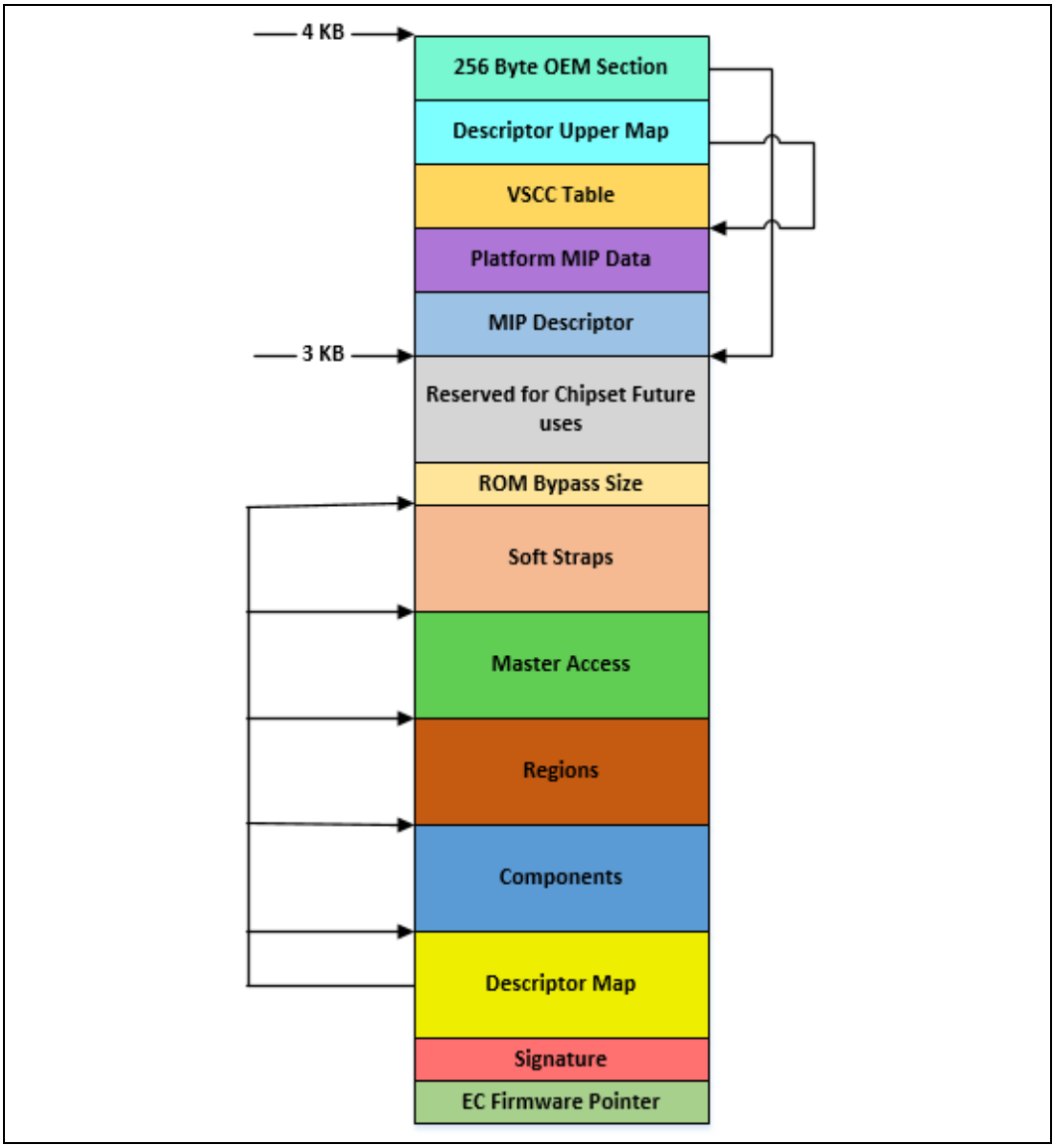
§ §

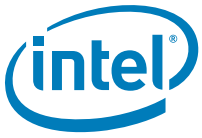
4 Descriptor Overview

The Flash Descriptor is a data structure that is programmed on the SPI flash part on Ice Lake PCH 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.

Figure 4-1. Flash Descriptor (Ice Lake PCH-LP)





- EC Firmware Pointer is located in the first 16 bytes of the Descriptor and contains the address location for EC flash region. The format for the EC Firmware Pointer address is dependent on EC vendors/OEM implementation of this field.
- 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, IFWI, GbE, PDR (Optional), Embedded Controller (EC), and Device Expansion (Intel® ME Data) 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 *Ice Lake PCH-LP 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
EC Firmware Pointer	0x0
Signature	0x10
Component FCBA	0x30
Regions FRBA	0x40
Masters FMBA	0x80
PCH Straps FPSBA	0x100
Legacy CPU Straps[1]	0x300
MDTBA	0xC00
PMC Straps	0xC14
CPU Straps	0xC60
Intel® ME Straps	0xC90
Register Init FIBA	0x340

1. The Legacy CPU Straps are for BIOS compatibility and are a duplication of the CPU Straps located 0xC64.

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

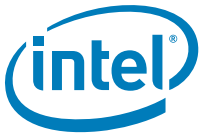
Recommended Value:0FF0A55Ah

Bits	Description	FIT Visible
31:0	**Flash Valid Signature.** This field identifies the Flash Descriptor sector as valid. If the contents at this location contains 0FF0A55Ah, then the Flash Descriptor is considered valid and it will operate in Descriptor Mode (**Note:** Non-Descriptor mode is not supported).	**No**

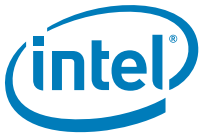
4.1.1.2 FLMAP0 - Flash Map 0 Register (Flash Descriptor Records)

Memory Address: FDBAR + 014h Size: 32 bits

Bits	Description	FIT Visible
31:27	**Reserved**	**No**
26:24	**Reserved**	**No**
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.	**No**
15:13	**Reserved**	**No**
12	**Fingerprint sensor on shared flash / TPM SPI bus** 0 = No fingerprint sensor is connected to CS1 1 = Fingerprint sensor is connected to CS1 and acting as a flash device ***Note:*** Hardware does not use this field. This value must be read directly from flash. It's not available via Host FDOC/FDOD registers.	**Yes**
11	**Touch on dedicated SPI bus** 0 = No Touch device is connected to the dedicated Touch SPI bus 1 = Touch device is connected to the dedicated Touch SPI bus ***Note:*** Hardware does not use this field. This value must be read directly from flash. It's not available via Host FDOC/FDOD registers.	**Yes**
10	**Touch on shared flash / TPM SPI bus** 0 = No Touch device is connected to CS1 1 = Touch device is connected to CS1 and acting as a flash device ***Note:*** Hardware does not use this field. This value must be read directly from flash. It's not available via Host FDOC/FDOD registers.	**Yes**



Bits	Description	FIT Visible
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 **Note:** With the introduction of DnX mode support, the flash controller ignores this descriptor field. It determines the number of attached flash components by virtue of SFDP discovery. Software may still use this field, therefore it must be properly initialized.	**Yes**
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	**No**



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

Memory Address: FDBAR + 018h Size: 32 bits

Bits	Description	FIT Visible
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 49h	**No**
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	**No**
15:11	Reserved	**No**
10:8	**Number Of Masters (NM).** This field identifies the total number of Flash Masters. **Note:** This field is not used by the Flash Controller.	**No**
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	**No**

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

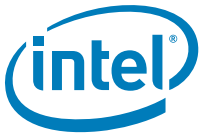
Memory Address: FDBAR + 01Ch Size: 32 bits

Bits	Description	FIT Visible
31:0	Reserved	**No**

4.1.1.5 FLMAP3—Flash Map 3 Register (Flash Descriptor Records)

Memory Address: FDBAR + 020h Size: 32 bits

Bits	Description	FIT Visible
31:21	Major Version	**No**
20:14	Minor Version	**No**
13:0	Reserved	**No**



4.1.2 Flash Descriptor Component Section

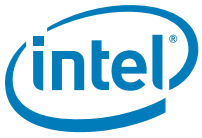
4.1.2.1 FLCOMP—Flash Components Register (Flash Descriptor Records)

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

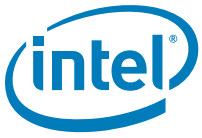
Memory Address: FCBA + 000h Size: 32 bits

Bits	Description	FIT Visible
31	Reserved	**No**
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.	**No**
29:27	**Read ID and Read Status Clock Frequency**. 001 = Reserved 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, ensure flash meets timing requirements defined in Table 3-3	**Yes**
26:24	**Write and Erase Clock Frequency**. 001 = Reserved 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, ensure flash meets timing requirements defined in Table 3-3	**Yes**
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'. 001 = Reserved 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 48MHz, ensure flash meets timing requirements defined in Table 3-3	**Yes**

Bits	Description	FIT Visible
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	**Yes**
19:17	**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 05x = Reserved 0x6 = Reserved 0x7 = Reserved	**Yes**
16	Reserved	**No**
15	**Quad I/O Read Enable (QIORE):** 0 = Quad I/O Read is disabled 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.	**Yes**
14	**Quad Output Read Enable (QORE):** 0 = Quad Output Read is disabled 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.	**Yes**
13	**Dual I/O Read Enable (DIORE):** 0 = Dual I/O Read is disabled 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.	**Yes**



Bits	Description	FIT Visible
12	**Dual Output Read Enable (DORE):** 0 = Dual Output Read is disabled 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.	**Yes**
11:10	**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	**Yes**
9	**SPI Voltage Select (SPI_1p8volt_sel):** 0 = SPI supply voltage set to 3.3 volts 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.	**No**
8	Reserved	**No**
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.	**Yes**
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.	**Yes**



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

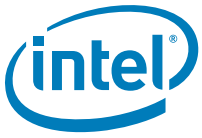
Memory Address: FCBA + 004h Size: 32 bits

Bits	Description	FIT Visible
31:24	**Invalid Instruction 3**. **Default set to 0xAD** See definition of Invalid Instruction 0	**Yes**
23:16	**Invalid Instruction 2**. **Default set to 0x60** See definition of Invalid Instruction 0	**Yes**
15:8	**Invalid Instruction 1**. **Default set to 0x42** See definition of Invalid Instruction 0	**Yes**
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.	**Yes**

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

Memory Address: FCBA + 008h Size: 32 bits

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



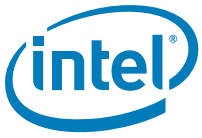
Bits	Description	FIT Visible
7:0	**Invalid Instruction 4**. **Default set to 0xB7** See definition of Invalid Instruction 0	**Yes**

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	FIT Visible
31	Reserved	**No**
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	**No**
15	Reserved	**No**
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.	**No**

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

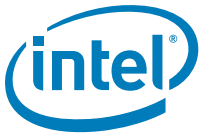
Memory Address: FRBA + 004h Size: 32 bits

Bits	Description	FIT Visible
31	Reserved	**No**
30:16	**Region Limit.** This specifies bits 26:12 of the ending address for this Region. ***Notes:*** 1. Must be set to 0000h if Intel® ME ROM Bypass 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	**No**
15	Reserved	**No**
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	**No**

4.1.3.3 FLREG2—Flash Region 2 (IFWI / Intel® ME ROM Bypass) Register (Flash Descriptor Records)

Memory Address: FRBA + 008h Size: 32 bits

Bits	Description	FIT Visible
31	Reserved	**No**
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 IFWI size that will be used in the platform 2. Region limit address Bits[11:0] are assumed to be FFFh	**No**
15	Reserved	**No**
14:0	**Region Base.** This specifies address bits 26:12 for the Region Base.	**No**



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

Memory Address: FRBA + 00Ch Size: 32 bits

Bits	Description	FIT Visible
31	Reserved	**No**
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	**No**
15	Reserved	**No**
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	**No**

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

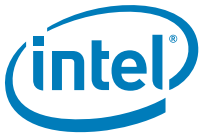
Memory Address: FRBA + 010h Size: 32 bits

Bits	Description	FIT Visible
31	Reserved	**No**
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	**No**
15	Reserved	**No**
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	**No**

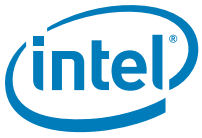
4.1.3.6 FLREG8—Flash Region 8 (Embedded Controller) Register (Flash Descriptor Records)

Memory Address: FRBA + 020h Size: 32 bits

Bits	Description	FIT Visible
31	Reserved	**No**
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	**No**
15	Reserved	**No**
14:0	**Region Base.** This specifies address bits 26:12 for the Region Base. The value in this register is loaded from the contents in the Flash Descriptor. FLREGn.Region Base, where 7 <= n <= 11	**No**



Note: Region 6 (FRBA + 018h), Region 7 (FRBA + 01Ch) and Region 9 (FRBA + 024h), Region 10 (FRBA + 28h), Region 11 (FRBA + 2Ch), Region 12 (FRBA + 30h), Region 13 (FRBA + 34h), Region 14 (FRBA + 38h) and Region 15 (FRBA + 03Ch) 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	FIT Visible
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	**Yes**
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.	**Yes**
7:4	**Extended Region Write Access:** Each bit [7:4] corresponds to Regions [15:12]. If the bit is set, this master can erase and write that particular region through register accesses.	**Yes**
3:0	**Extended Region Read Access:** Each bit [3:0] corresponds to Regions [15:12]. If the bit is set, this master can erase and write that particular region through register accesses.	**Yes**

4.1.4.2 FLMSTR2—Flash Master 2 (Intel® ME)

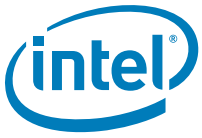
Memory Address: FMBA + 004h Size:32 bits

Bits	Description	FIT Visible
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	**Yes**
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.	**Yes**
7:4	**Extended Region Write Access:** Each bit [7:4] corresponds to Regions [15:12]. If the bit is set, this master can erase and write that particular region through register accesses.	**Yes**
3:0	**Extended Region Read Access:** Each bit [3:0] corresponds to Regions [15:12]. If the bit is set, this master can erase and write that particular region through register accesses.	**Yes**

4.1.4.3 FLMSTR3—Flash Master 3 (GbE)

Memory Address: FMBA + 008h Size:32 bits

Bits	Description	FIT Visible
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	**Yes**
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.	**Yes**



Bits	Description	FIT Visible
7:4	**Extended Region Write Access:** Each bit [7:4] corresponds to Regions [15:12]. If the bit is set, this master can erase and write that particular region through register accesses.	**Yes**
3:0	**Extended Region Read Access:** Each bit [3:0] corresponds to Regions [15:12]. If the bit is set, this master can erase and write that particular region through register accesses.	**Yes**

4.1.4.4 FLMSTR4—Flash Master 4 (Reserved)

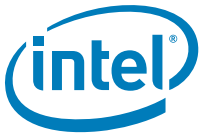
Memory Address: FMBA + 00Ch Size:32 bits

Bits	Description	FIT Visible
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 17 is a don't care as the primary master always has read/write permission to its primary region	**No**
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 13 is a don't care as the primary master always read/write permission to its primary region.	**No**
7:4	**Extended Region Write Access:** Each bit [7:4] corresponds to Regions [15:12]. If the bit is set, this master can erase and write that particular region through register accesses.	**No**
3:0	**Extended Region Read Access:** Each bit [3:0] corresponds to Regions [15:12]. If the bit is set, this master can erase and write that particular region through register accesses.	**No**

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	**Yes**
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.	**Yes**
7:4	**Extended Region Write Access:** Each bit [7:4] corresponds to Regions [15:12]. If the bit is set, this master can erase and write that particular region through register accesses.	**Yes**
3:0	**Extended Region Read Access:** Each bit [3:0] corresponds to Regions [15:12]. If the bit is set, this master can erase and write that particular region through register accesses.	**Yes**



4.1.5 PCH / CPU Softstraps

See Chapter 9, "Flash Descriptor PCH / PMC / CPU and Intel® CSME Configuration Section" for details.

4.1.6 Descriptor Upper Map Section

This section of the flash descriptor is used by ME to find SPI VSCC information and MIP data.

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

Memory Address:FDBAR + EFCh Size: 32 bits

Bits	Default	Description	FIT Visible
31:16	0xC1	**MIP Descriptor Table Base Address (MDTBA).** This identifies base address bits [11:4] for the Platform Configuration Data Structure in the Flash Descriptor Bits [26:12] and bits [3:0] are 0.	**No**
23:16	0xFF	Reserved	**No**
15:8	0x1	**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. Max recommended is 10 entries to allow for room for Platform Configuration Data (MIP)	**No**
7:0	0x1	**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.	**No**

4.1.6.2 IFWI / Intel® ME ROM Bypass Size

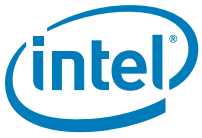
Memory Address:FDBAR + C00h Size: 32 bits

Bits	Default	Description	FIT Visible
31:0	0xFF	**ROM BYPASS Size.** ROM reads this value to determine the size of the region. **Only applicable for A0 stepping.**	**No**

4.1.6.3 MIP - Descriptor Table

Memory Address:FDBAR + MDTBA

Name	Offset	Size (bytes)	Description	FIT Visible
Number of Descriptors	0x0	2	Number of MIP blocks ('n') inside this MIP structure	**Yes**
Size of MIP	0x2	2	Size, in bytes, of this MIP structure (including the MDT structure)	**Yes**
Block 0 Type	0x4	2	Type of block 0. Can be one of the following: 0 = CSE (USB 2 PHY Configuration) 1 = PMC Soft Straps 2 = Reserved ***Note:*** In order to simplify handling a new block type can be defined for each usage	**Yes**



Name	Offset	Size (bytes)	Description	FIT Visible
Block 0 Offset	0x6	2	Offset of block 0	**Yes**
Block 0 Length	0x8	2	Length of block 0 in bytes	**Yes**
Block 0 Reserved	0xA	2	Must be 0	**Yes**
Block 1 Type	0xC	2	See Block 0 type	**Yes**
Block 1 Offset	0xE	2	Offset of block 1	**Yes**
Block 1 Length	0x10	2	Length of block 1 in bytes	**Yes**
Block 1 Reserved	0x12	2	Must be 0	**Yes**
.....				**Yes**
Block ‘n’ Type		2	See Block 0 type	**Yes**
Block ‘n’ Offset		2	Offset of block ‘n’	**Yes**
Block ‘n’ Length		2	Length of block ‘n’ in bytes	**Yes**
Block ‘n’ Reserved		2	Must be 0	**Yes**

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 Ice Lake 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	FIT Visible
31:24	Reserved	**No**
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).	**Yes**
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).	**Yes**
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).	**Yes**

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

Memory Address: VTBA + 004h Size: 32 bits

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

Bits	Description	FIT Visible
31:16	Reserved	**No**
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.	**No**
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.	**No**
4:0	**Reserved set to 00101b**	**No**

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)

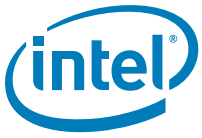
Memory Address: VTBA + (n*8)h Size:32 bits

"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.

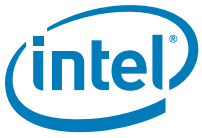
4.3 Region Access Control

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 four masters that have the ability to access other regions: CPU/BIOS, Intel® ME Firmware, GbE software/driver running on CPU and EC.

Table 4-1. Region Access Control Table Options

Master Read/Write Access				
Region (#)	**CPU / BIOS**	**IFWI (Intel® ME)**	**GbE Controller**	**EC**
Descriptor (0)	Read Only	Read Only	Not Accessible	Not Accessible
BIOS (1)	CPU / BIOS can always read from and write to BIOS region prior to EOP	Not Accessible	Not Accessible	Not Accessible
IFWI / Intel® Management Engine ROM Bypass (2)	Read / Write (BIOS Only)	Intel®ME can always read from and write to IFWI region	Not Accessible	Not Accessible
GbE (3)	Not Accessible	Read / Write	GbE software can always read from and write to GbE region	Not Accessible
PDR (4)	Not Accessible	Not Accessible	Not Accessible	Not Accessible
EC - Embedded Controller (Optional) (8)	Read / Write	Not Accessible	Not Accessible	EC can always read from and write to EC region

Notes:
1. The Region Access values listed above represent post manufacturing configuration only.
2. Descriptor and PDR region is not a master, so they will not have Master R/W access.
3. Descriptor should NOT have write access by any master in production systems.
4. 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.

Table 4-2. Recommended Read/Write Permissions

Master Access	Descriptor Region Bit 0	BIOS Region Bit1	IFWI / Intel® ME ROM Bypass Region Bit2	GbE Region Bit3	PDR Region Bit4	EC Region Bit8
ME read access	Y	N	Y	Y	N	N
ME write access	N	N	Y	N	N	N
GbE read access	Y	N	N	Y	N	N
GbE write access	N	N	N	Y	N	N
BIOS read access	Y	Y	Y	Y	‡	†
BIOS write access	N	Y	N	Y	‡	†
EC read access	Y	*	N	N	N	Y
EC write access	N	N	N	N	N	Y

Note:
1. ‡ = Host access to PDR is the discretion of the customer. Implementation of PDR is optional.
2. † = Optional BIOS access to the EC region.
3. * = Optional EC Read access to BIOS.

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.

Warning: Pre-configuring the flash image to Intel recommended read / write permission through the Intel® FIT tool and then flashing the resulting image will cause the platform to enter into end-of-manufacturing flow which will result in the FPFs being permanently set in the PCH if the platform is using production silicon and production Intel® ME firmware with the PV bit set.

Table 4-3. Recommended Read/Write Settings for Platforms

	ME	GbE	BIOS	EC
Read	0b 0000 0000 0000 1101 = 0x000D	0b 0000 0000 0000 1001 = 0x0009	0b 0000 000† 000‡ 1011 = 0x0†‡F	0b 0000 0001 0000 00*1 = 0x0101 or 0x0103
Write	0b 0000 0000 0000 0100 = 0x0004	0b 0000 0000 0000 1000 = 0x0008	0b 0000 000† 000‡ 1010 = 0x0†‡A	0b 0000 0001 0000 0000 = 0x0100

Note:
1. ‡ = Value dependent on if PDR is implemented and if Host access is desired.
2. † = Optional BIOS access to the EC region.
3. * = Optional EC Read access to BIOS.

4.3.2 Overriding Region Access

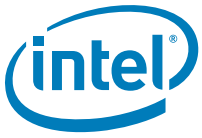
Once access Intel recommended Flash settings have been put into the flash descriptor, it may be necessary to update the ME region with a Host program or write a new Flash descriptor.

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

Bits	Description	FIT Visible
31:24	Reserved.	**No**
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).	**Yes**
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).	**Yes**
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).	**Yes**

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 Ice Lake 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 Ice Lake PCH-LP Family Systems.

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

Table 4-5. Vsccn – Vendor-Specific Component Capabilities Portion of the Ice Lake PCH-LP Platforms (Sheet 1 of 2)

Bits	Description	FIT Visible
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.	

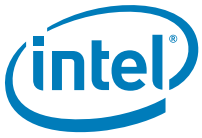


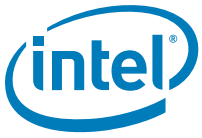
Table 4-5. Vsccn – Vendor-Specific Component Capabilities Portion of the Ice Lake PCH-LP Platforms (Sheet 2 of 2)

Bits	Description	FIT Visible
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.	**No**
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.	**No**
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.	**No**
2	**Write Granularity (WG)**. 0 = 1 Byte 1 = 64 Bytes	**No**
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	**No**

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 Ice Lake 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 Ice Lake 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.

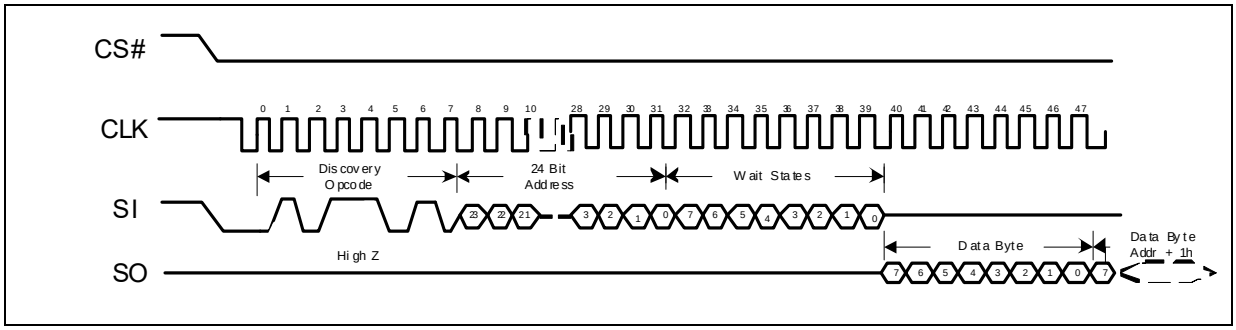
These guidelines are a standard that will allow for individual vendors to have their value add features, but will allow for a controller to discover the attributes needed to operate.

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

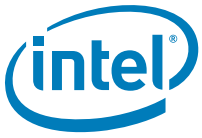


5.3 Parameter Table Supported on PCH

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
- Dual Output 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 if 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 Ice Lake 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.

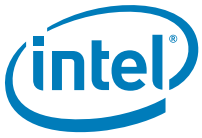
All the SPI flash devices that meet the SPI flash requirements in the *Ice Lake PCH-LP Family External Design Specification (EDS)* will be unlocked by writing a 00h to the SPI flash's status register. This command must be done via an atomic software sequencing to account for differences in flash architecture. 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 *Ice Lake 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.

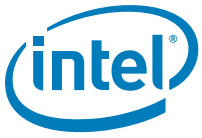
It is strongly recommended that if Flash Descriptor Override strap (which can be checked by reading **FDOPSS (0b Flash Descriptor override is set, 1b not set) in PCH memory space (SPIBAR+C4h bit 13))** is set, do not set a Protected range to cover the Intel® ME FW factory defaults. This would allow a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

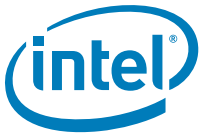


Table 6-1. VSCC0 - Vendor-Specific Component Capabilities Register for SPI Component 0 (Sheet 2 of 3)

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.

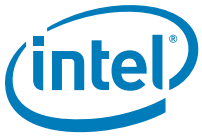


Table 6-1. VSCC0 - Vendor-Specific Component Capabilities Register for SPI Component 0 (Sheet 3 of 3)

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.

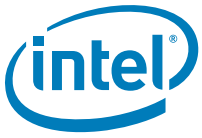


Table 6-2. VSCC1 - Vendor Specific Component Capabilities Register for SPI Component 1 (Sheet 2 of 2)

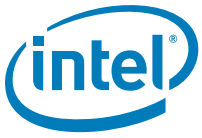
Bit	Description
3	**Write Status Required (WSR)** — RW: '0' = No automatic write of 00h will be made to the SPI flash's status register '1' = A write of 00h to the SPI flash's status register will be sent on EVERY write and erase to the SPI flash performed by Host and GbE. This register is locked by 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 Ice Lake 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.

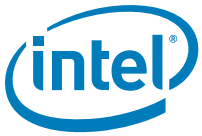
Vendor Component Lock (VCL) should remain unlocked during development, but locked in shipping platforms. When **VCL** and **FLOCKDN** are set, it is possible that you may not be able to use in system programming methodologies including Intel Flash Programming Tool if programmed improperly. It will require 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 IFWI / Intel® ME Disable for Debug/Flash Burning Purposes

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

7.1 IFWI / 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. 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.

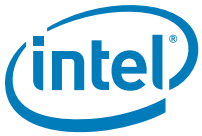
7.1.1 Erasing/Programming Intel® ME Region

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 SPI writing by the Intel ME when erasing any address in IFWI and ME Data regions.

§ §



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 / PMC / CPU and Intel® CSME 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	7:0	**Reserved, set to '0'**		**No**

9.2 PCH Descriptor Record 1 (Flash Descriptor Records)

Flash Address:FPSBA + 001h

Default Flash Address: 101h

Offset from 0	Bits	Description	Usage	FIT Visible
0x101h	7:0	**Reserved, set to '0'**		**No**

9.3 PCH Descriptor Record 2 (Flash Descriptor Records)

Flash Address:FPSBA + 002h

Default Flash Address: 102h

Offset from 0	Bits	Description	Usage	FIT Visible
0x102h	7:0	**Reserved, set to '0'**		**No**

9.4 PCH Descriptor Record 3 (Flash Descriptor Records)

Flash Address:FPSBA + 003h

Default Flash Address: 103h

Offset from 0	Bits	Description	Usage	FIT Visible
0x103h	7:0	**Reserved, set to '0'**		**No**

9.5 PCH Descriptor Record 4 (Flash Descriptor Records)

Flash Address:FPSBA + 004h

Default Flash Address: 104h

Offset from 0	Bits	Description	Usage	FIT Visible
0x104h	7:0	**Reserved, set to '0'**		**No**

9.6 PCH Descriptor Record 5 (Flash Descriptor Records)

Flash Address:FPSBA + 005h

Default Flash Address: 105h

Offset from 0	Bits	Description	Usage	FIT Visible
0x105h	7:0	**Reserved, set to '0'**		**No**

9.7 PCH Descriptor Record 6 (Flash Descriptor Records)

Flash Address:FPSBA + 006h

Default Flash Address: 106h

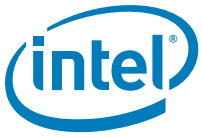
Offset from 0	Bits	Description	Usage	FIT Visible
0x106h	7:0	**Reserved, set to '0'**		**No**

9.8 PCH Descriptor Record 7 (Flash Descriptor Records)

Flash Address:FPSBA + 007h

Default Flash Address: 107h

Offset from 0	Bits	Description	Usage	FIT Visible
0x107h	7:0	**Reserved, set to '0'**		**No**



9.9 PCH Descriptor Record 8 (Flash Descriptor Records)

Flash Address:FPSBA + 008h

Default Flash Address: 108h

Offset from 0	Bits	Description	Usage	FIT Visible
0x108h	7:0	**Reserved, set to '0'**		**No**

9.10 PCH Descriptor Record 9 (Flash Descriptor Records)

Flash Address:FPSBA + 009h

Default Flash Address: 109h

Offset from 0	Bits	Description	Usage	FIT Visible
0x109h	7	**GPP_G7 Individual Voltage Select (GPPC_G7_VCCIO):** 0 = GPP_H7 Voltage set to 3.3v 1 = GPP_H7 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_G7 GPIO pin.	**Yes**
	6	**GPP_G6 Individual Voltage Select (GPPC_G6_VCCIO):** 0 = GPP_G6 Voltage set to 3.3v 1 = GPP_G6 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_G6 GPIO pin.	**Yes**
	5	**GPP_G5 Individual Voltage Select (GPPC_G5_VCCIO):** 0 = GPP_G5 Voltage set to 3.3v 1 = GPP_G5 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_G5 GPIO pin.	**Yes**
	4	**GPP_G4 Individual Voltage Select (GPPC_G4_VCCIO):** 0 = GPP_G4 Voltage set to 3.3v 1 = GPP_G4 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_G4 GPIO pin.	**Yes**
	3	**GPP_G3 Individual Voltage Select (GPPC_G3_VCCIO):** 0 = GPP_G3 Voltage set to 3.3v 1 = GPP_G3 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_G3 GPIO pin.	**Yes**
	2	**GPP_G2 Individual Voltage Select (GPPC_G2_VCCIO):** 0 = GPP_G2 Voltage set to 3.3v 1 = GPP_G2 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_G2 GPIO pin.	**Yes**
	1	**GPP_G1 Individual Voltage Select (GPPC_G1_VCCIO):** 0 = GPP_G1 Voltage set to 3.3v 1 = GPP_G1 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_G1 GPIO pin.	**Yes**

Offset from 0	Bits	Description	Usage	FIT Visible
0x109h (Cont)	0	**GPP_G0 Individual Voltage Select (GPPC_G0_VCCIO):** 0 = GPP_G0 Voltage set to 3.3v 1 = GPP_G0 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_G0 GPIO pin.	**Yes**

9.11 PCH Descriptor Record 10 (Flash Descriptor Records)

Flash Address:FPSBA + 00Ah

Default Flash Address: 10Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0x10Ah	7:0	**Reserved, set to '0'**		**No**

9.12 PCH Descriptor Record 11 (Flash Descriptor Records)

Flash Address:FPSBA + 00Bh

Default Flash Address: 10Bh

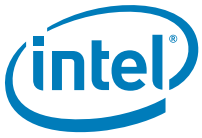
Offset from 0	Bits	Description	Usage	FIT Visible
0x10Bh	7:0	**Reserved, set to '0'**		**No**

9.13 PCH Descriptor Record 12 (Flash Descriptor Records)

Flash Address:FPSBA + 00Ch

Default Flash Address: 10Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x10Ch	7:3	**Reserved, set to '0'**		**No**
	2	**Thunderbolt™ LSx/BSSB-LS #2 Select (TBT_VCCIO_CFG_SRC2):** 0 = Thunderbolt™ LSx/BSSB-LS #2 configured based on Tx pin strap 1 = Thunderbolt™ LSx/BSSB-LS #2 VCCIO configured based on Legacy fuse / soft strap.	This setting determines how VCCIO is configured for Thunderbolt™ LSx/BSSB-LS #2.	**Yes**
	1	**Thunderbolt™ LSx/BSSB-LS #1 Select (TBT_VCCIO_CFG_SRC1):** 0 = Thunderbolt™ LSx/BSSB-LS #1 configured based on Tx pin strap 1 = Thunderbolt™ LSx/BSSB-LS #1 VCCIO configured based on Legacy fuse / soft strap.	This setting determines how VCCIO is configured for Thunderbolt™ LSx/BSSB-LS #1.	**Yes**



Offset from 0	Bits	Description	Usage	FIT Visible
0x10Ch (Cont)	0	**Thunderbolt™ LSx/BSSB-LS #0 Select (TBT_VCCIO_CFG_SRC0):** 0 = Thunderbolt™ LSx/BSSB-LS #0 configured based on Tx pin strap 1 = Thunderbolt™ LSx/BSSB-LS #0 VCCIO configured based on Legacy fuse / soft strap.	This setting determines how VCCIO is configured for Thunderbolt™ LSx/BSSB-LS #0.	**Yes**

9.14 PCH Descriptor Record 13 (Flash Descriptor Records)

Flash Address:FPSBA + 00Dh

Default Flash Address: 10Dh

Offset from 0	Bits	Description	Usage	FIT Visible
0x10Dh	7:0	**Reserved, set to '0'**		**No**

9.15 PCH Descriptor Record 14 (Flash Descriptor Records)

Flash Address:FPSBA + 00Eh

Default Flash Address: 10Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0x10Eh	7	**GPP_E7 Individual Voltage Select (GPPC_E7_VCCIO):** 0 = GPP_C16 Voltage set to 3.3v 1 = GPP_C16 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_E7 GPIO pin.	**Yes**
	6	**GPP_E6 Individual Voltage Select (GPPC_E6_VCCIO):** 0 = GPP_E6 Voltage set to 3.3v 1 = GPP_E6 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_E6 GPIO pin.	**Yes**
	5	**GPP_E5 Individual Voltage Select (GPPC_E5_VCCIO):** 0 = GPP_E5 Voltage set to 3.3v 1 = GPP_E5 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_E5 GPIO pin.	**Yes**
	4	**GPP_E4 Individual Voltage Select (GPPC_E4_VCCIO):** 0 = GPP_E4 Voltage set to 3.3v 1 = GPP_E4 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_E4 GPIO pin.	**Yes**
	3	**GPP_E3 Individual Voltage Select (GPPC_E3_VCCIO):** 0 = GPP_E3 Voltage set to 3.3v 1 = GPP_E3 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_E3 GPIO pin.	**Yes**

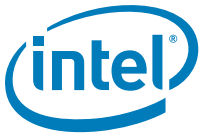
Offset from 0	Bits	Description	Usage	FIT Visible
0x10Eh (Cont)	2	**GPP_E2 Individual Voltage Select (GPPC_E2_VCCIO):** 0 = GPP_E2 Voltage set to 3.3v 1 = GPP_E2 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_E2 GPIO pin.	**Yes**
	1	**GPP_E1 Individual Voltage Select (GPPC_E1_VCCIO):** 0 = GPP_E1 Voltage set to 3.3v 1 = GPP_E1 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_E1 GPIO pin.	**Yes**
	0	**GPP_E0 Individual Voltage Select (GPPC_E0_VCCIO):** 0 = GPP_E0 Voltage set to 3.3v 1 = GPP_E0 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_E0 GPIO pin.	**Yes**

9.16 PCH Descriptor Record 15 (Flash Descriptor Records)

Flash Address:FPSBA + 00Fh

Default Flash Address: 10Fh

Offset from 0	Bits	Description	Usage	FIT Visible
0x10Fh	7	**GPP_E15 Individual Voltage Select (GPPC_E15_VCCIO):** 0 = GPP_E15 Voltage set to 3.3v 1 = GPP_E15 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_E15 GPIO pin.	**Yes**
	6	**GPP_E14 Individual Voltage Select (GPPC_E14_VCCIO):** 0 = GPP_E14 Voltage set to 3.3v 1 = GPP_E14 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_E14 GPIO pin.	**Yes**
	5	**GPP_E13 Individual Voltage Select (GPPC_E13_VCCIO):** 0 = GPP_E13 Voltage set to 3.3v 1 = GPP_E13 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_E13 GPIO pin.	**Yes**
	4	**GPP_E12 Individual Voltage Select (GPPC_E12_VCCIO):** 0 = GPP_E12 Voltage set to 3.3v 1 = GPP_E12 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_E12 GPIO pin.	**Yes**
	3	**GPP_E11 Individual Voltage Select (GPPC_E11_VCCIO):** 0 = GPP_E11 Voltage set to 3.3v 1 = GPP_E11 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_E11 GPIO pin.	**Yes**
	2	**GPP_E10 Individual Voltage Select (GPPC_E10_VCCIO):** 0 = GPP_E10 Voltage set to 3.3v 1 = GPP_E10 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_E10 GPIO pin.	**Yes**



Offset from 0	Bits	Description	Usage	FIT Visible
0x10Fh (Cont)	1	**GPP_E9 Individual Voltage Select (GPPC_E9_VCCIO):** 0 = GPP_E9 Voltage set to 3.3v 1 = GPP_E9 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_E9 GPIO pin.	**Yes**
	0	**GPP_E8 Individual Voltage Select (GPPC_E8_VCCIO):** 0 = GPP_E8 Voltage set to 3.3v 1 = GPP_E8 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_E8 GPIO pin.	**Yes**

9.17 PCH Descriptor Record 16 (Flash Descriptor Records)

Flash Address:FPSBA + 010h

Default Flash Address: 110h

Offset from 0	Bits	Description	Usage	FIT Visible
0x110h	7	**GPP_E23 Individual Voltage Select (GPPC_E23_VCCIO):** 0 = GPP_E23 Voltage set to 3.3v 1 = GPP_E23 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_E23 GPIO pin.	**Yes**
	6	**GPP_E22 Individual Voltage Select (GPPC_E22_VCCIO):** 0 = GPP_E22 Voltage set to 3.3v 1 = GPP_E22 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_E22 GPIO pin.	**Yes**
	5	**GPP_E21 Individual Voltage Select (GPPC_E21_VCCIO):** 0 = GPP_E21 Voltage set to 3.3v 1 = GPP_E21 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_E21 GPIO pin.	**Yes**
	4	**GPP_E20 Individual Voltage Select (GPPC_E20_VCCIO):** 0 = GPP_E20 Voltage set to 3.3v 1 = GPP_E20 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_E20 GPIO pin.	**Yes**
	3	**GPP_E19 Individual Voltage Select (GPPC_E19_VCCIO):** 0 = GPP_E19 Voltage set to 3.3v 1 = GPP_E19 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_E19 GPIO pin.	**Yes**
	2	**GPP_E18 Individual Voltage Select (GPPC_E18_VCCIO):** 0 = GPP_E18 Voltage set to 3.3v 1 = GPP_E18 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_E18 GPIO pin.	**Yes**
	1	**GPP_E17 Individual Voltage Select (GPPC_E17_VCCIO):** 0 = GPP_E17 Voltage set to 3.3v 1 = GPP_E17 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_E17 GPIO pin.	**Yes**

Offset from 0	Bits	Description	Usage	FIT Visible
0x110h (Cont)	0	**GPP_E16 Individual Voltage Select (GPPC_E16_VCCIO):** 0 = GPP_E16 Voltage set to 3.3v 1 = GPP_E16 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_E16 GPIO pin.	**Yes**

9.18 PCH Descriptor Record 17 (Flash Descriptor Records)

Flash Address:FPSBA + 011h

Default Flash Address: 111h

Offset from 0	Bits	Description	Usage	FIT Visible
0x111h	7:0	**Reserved, set to '0'**		**No**

9.19 PCH Descriptor Record 18 (Flash Descriptor Records)

Flash Address:FPSBA + 012h

Default Flash Address: 112h

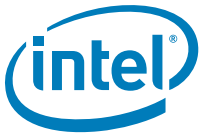
Offset from 0	Bits	Description	Usage	FIT Visible
0x112h	7:0	**Reserved, set to '0'**		**No**

9.20 PCH Descriptor Record 19 (Flash Descriptor Records)

Flash Address:FPSBA + 013h

Default Flash Address: 113h

Offset from 0	Bits	Description	Usage	FIT Visible
0x113h	7:0	**Reserved, set to '0'**		**No**



9.21 PCH Descriptor Record 20 (Flash Descriptor Records)

Flash Address:FPSBA + 014h

Default Flash Address: 114h

Offset from 0	Bits	Description	Usage	FIT Visible
0x114h	7:6	**Reserved, set to '0'**		**No**
	5	**SLP_S5# / GPD10 Signal Configuration:** 0b = Use as SLP_S5# 1b = Use as GPD10		**Yes**
	4	**LAN PHY Power Control GPD11 Signal Configuration:** 0b = Use as LANPHYPC 1b = Use as GPD11 **Note:** 4. LANPHYPC can only be driven low if SLP_LAN# is deasserted. 5. 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**
	3	**SLP_WLAN# / GPD9 Signal Configuration:** 0b = Use as SLP_WLAN# 1b = Use as GPD9	**LAN Sub-System Sleep Control:** When SLP_LAN# is de-asserted it indicates that the PHY device must be powered. When SLP_LAN# is asserted, power can be shut off to the PHY device. SLP_LAN# will always be deasserted in S0 and anytime SLP_A# is de-asserted.	**Yes**
	2	**SLP_A# / GPD6 Signal Configuration:** 0b = Use as SLP_A# 1b = Use as GPD6		**Yes**
	1	**SLP_S4# / GPD5 Signal Configuration:** 0b = Use as SLP_S4# 1b = Use as GPD5		**Yes**
	0	**SLP_S3# / GPD4 Signal Configuration:** 0b = Use as SLP_S3# 1b = Use as GPD4		**Yes**

9.22 PCH Descriptor Record 21 (Flash Descriptor Records)

Flash Address:FPSBA + 015h

Default Flash Address: 115h

Offset from 0	Bits	Description	Usage	FIT Visible
0x115h	7:0	**Reserved, set to '0'**		**No**

9.23 PCH Descriptor Record 22 (Flash Descriptor Records)

Flash Address:FPSBA + 016h

Default Flash Address: 116h

Offset from 0	Bits	Description	Usage	FIT Visible
0x116h	7:0	**Reserved, set to '0'**		**No**

9.24 PCH Descriptor Record 23 (Flash Descriptor Records)

Flash Address:FPSBA + 017h

Default Flash Address: 117h

Offset from 0	Bits	Description	Usage	FIT Visible
0x117h	7:0	**Reserved, set to '0'**		**No**

9.25 PCH Descriptor Record 24 (Flash Descriptor Records)

Flash Address:FPSBA + 018h

Default Flash Address: 118h

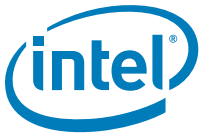
Offset from 0	Bits	Description	Usage	FIT Visible
0x118h	7:4	**Reserved, set to '0'**		**No**
	3	**Intel® SMBus ASD Mode Configuration (SMBALERTB):** 0 = Configured as GPP_C2 1 = Configured as Intel® SMBus ASD	This setting determines the native mode for the SMBAlert signal.	**Yes**
	2:0	**Reserved, set to '0'**		**No**

9.26 PCH Descriptor Record 25 (Flash Descriptor Records)

Flash Address:FPSBA + 019h

Default Flash Address: 119h

Offset from 0	Bits	Description	Usage	FIT Visible
0x119h	7	**GPP_D7 Individual Voltage Select (GPPC_D7_VCCIO):** 0 = GPP_D7 Voltage set to 3.3v 1 = GPP_D7 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_D7 GPIO pin.	**Yes**
	6	**GPP_D6 Individual Voltage Select (GPPC_D6_VCCIO):** 0 = GPP_D6 Voltage set to 3.3v 1 = GPP_D6 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_D6 GPIO pin.	**Yes**



Offset from 0	Bits	Description	Usage	FIT Visible
0x119h (Cont)	5	**GPP_D5 Individual Voltage Select (GPPC_D5_VCCIO):** 0 = GPP_D5 Voltage set to 3.3v 1 = GPP_D5 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_D5 GPIO pin.	**Yes**
	4	**GPP_D4 Individual Voltage Select (GPPC_D4_VCCIO):** 0 = GPP_D4 Voltage set to 3.3v 1 = GPP_D4 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_D4 GPIO pin.	**Yes**
	3	**GPP_D3 Individual Voltage Select (GPPC_D3_VCCIO):** 0 = GPP_D3 Voltage set to 3.3v 1 = GPP_D3 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_D3 GPIO pin.	**Yes**
	2	**GPP_D2 Individual Voltage Select (GPPC_D2_VCCIO):** 0 = GPP_D2 Voltage set to 3.3v 1 = GPP_D2 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_D2 GPIO pin.	**Yes**
	1	**GPP_D1 Individual Voltage Select (GPPC_D1_VCCIO):** 0 = GPP_D1 Voltage set to 3.3v 1 = GPP_D1 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_D1 GPIO pin.	**Yes**
	0	**GPP_D0 Individual Voltage Select (GPPC_D0_VCCIO):** 0 = GPP_D0 Voltage set to 3.3v 1 = GPP_D0 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_D0 GPIO pin.	**Yes**

9.27 PCH Descriptor Record 26 (Flash Descriptor Records)

Flash Address:FPSBA + 01Ah

Default Flash Address: 11Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0x11Ah	7	**GPP_D15 Individual Voltage Select (GPPC_D15_VCCIO):** 0 = GPP_D15 Voltage set to 3.3v 1 = GPP_D15 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_D15 GPIO pin.	**Yes**
	6	**GPP_D14 Individual Voltage Select (GPPC_D14_VCCIO):** 0 = GPP_D14 Voltage set to 3.3v 1 = GPP_D14 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_D14 GPIO pin.	**Yes**
	5	**GPP_D13 Individual Voltage Select (GPPC_D13_VCCIO):** 0 = GPP_D13 Voltage set to 3.3v 1 = GPP_D13 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_D13 GPIO pin.	**Yes**

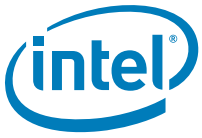
Offset from 0	Bits	Description	Usage	FIT Visible
0x11Ah (Cont)	4	**GPP_D12 Individual Voltage Select (GPPC_D12_VCCIO):** 0 = GPP_D12 Voltage set to 3.3v 1 = GPP_D12 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_D12 GPIO pin.	**Yes**
	3	**GPP_D11 Individual Voltage Select (GPPC_D11_VCCIO):** 0 = GPP_D11 Voltage set to 3.3v 1 = GPP_D11 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_D11 GPIO pin.	**Yes**
	2	**GPP_D10 Individual Voltage Select (GPPC_D10_VCCIO):** 0 = GPP_D10 Voltage set to 3.3v 1 = GPP_D10 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_D10 GPIO pin.	**Yes**
	1	**GPP_D9 Individual Voltage Select (GPPC_D9_VCCIO):** 0 = GPP_D9 Voltage set to 3.3v 1 = GPP_D9 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_D9 GPIO pin.	**Yes**
	0	**GPP_D8 Individual Voltage Select (GPPC_D8_VCCIO):** 0 = GPP_D8 Voltage set to 3.3v 1 = GPP_D8 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_D8 GPIO pin.	**Yes**

9.28 PCH Descriptor Record 27 (Flash Descriptor Records)

Flash Address:FPSBA + 01Bh

Default Flash Address: 11Bh

Offset from 0	Bits	Description	Usage	FIT Visible
0x11Bh	7	**GPP_D23 Individual Voltage Select (GPPC_D23_VCCIO):** 0 = GPP_D23 Voltage set to 3.3v 1 = GPP_D23 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_D23 GPIO pin.	**Yes**
	6	**GPP_D22 Individual Voltage Select (GPPC_D22_VCCIO):** 0 = GPP_D22 Voltage set to 3.3v 1 = GPP_D22 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_D22 GPIO pin.	**Yes**
	5	**GPP_D21 Individual Voltage Select (GPPC_D21_VCCIO):** 0 = GPP_D21 Voltage set to 3.3v 1 = GPP_D21 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_D21 GPIO pin.	**Yes**
	4	**GPP_D20 Individual Voltage Select (GPPC_D20_VCCIO):** 0 = GPP_D20 Voltage set to 3.3v 1 = GPP_D20 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_D20 GPIO pin.	**Yes**



Offset from 0	Bits	Description	Usage	FIT Visible
0x11Bh (Cont)	3	**GPP_D19 Individual Voltage Select (GPPC_D19_VCCIO):** 0 = GPP_D19 Voltage set to 3.3v 1 = GPP_D19 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_D19 GPIO pin.	**Yes**
	2	**GPP_D18 Individual Voltage Select (GPPC_D18_VCCIO):** 0 = GPP_D18 Voltage set to 3.3v 1 = GPP_D18 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_D18 GPIO pin.	**Yes**
	1	**GPP_D17 Individual Voltage Select (GPPC_D17_VCCIO):** 0 = GPP_D17 Voltage set to 3.3v 1 = GPP_D17 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_D17 GPIO pin.	**Yes**
	0	**GPP_D16 Individual Voltage Select (GPPC_D16_VCCIO):** 0 = GPP_D16 Voltage set to 3.3v 1 = GPP_D16 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_D16 GPIO pin.	**Yes**

9.29 PCH Descriptor Record 28 (Flash Descriptor Records)

Flash Address:FPSBA + 01Ch

Default Flash Address: 11Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x11Ch	7	**GPP_H7 Individual Voltage Select (GPPC_H7_VCCIO):** 0 = GPP_H7 Voltage set to 3.3v 1 = GPP_H7 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_H7 GPIO pin.	**Yes**
	6	**GPP_H6 Individual Voltage Select (GPPC_H6_VCCIO):** 0 = GPP_H6 Voltage set to 3.3v 1 = GPP_H6 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_H6 GPIO pin.	**Yes**
	5	**GPP_H5 Individual Voltage Select (GPPC_H5_VCCIO):** 0 = GPP_H5 Voltage set to 3.3v 1 = GPP_H5 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_H5 GPIO pin.	**Yes**
	4	**GPP_H4 Individual Voltage Select (GPPC_H4_VCCIO):** 0 = GPP_H4 Voltage set to 3.3v 1 = GPP_H4 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_H4 GPIO pin.	**Yes**
	3	**GPP_H3 Individual Voltage Select (GPPC_H3_VCCIO):** 0 = GPP_H3 Voltage set to 3.3v 1 = GPP_H3 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_H3 GPIO pin.	**Yes**

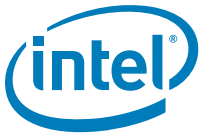
Offset from 0	Bits	Description	Usage	FIT Visible
0x11Ch (Cont)	2	**GPP_H2 Individual Voltage Select (GPPC_H2_VCCIO):** 0 = GPP_H2 Voltage set to 3.3v 1 = GPP_H2 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_H2 GPIO pin.	**Yes**
	1	**GPP_H1 Individual Voltage Select (GPPC_H1_VCCIO):** 0 = GPP_H1 Voltage set to 3.3v 1 = GPP_H1 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_H1 GPIO pin.	**Yes**
	0	**GPP_H0 Individual Voltage Select (GPPC_H0_VCCIO):** 0 = GPP_H0 Voltage set to 3.3v 1 = GPP_H0 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_H0 GPIO pin.	**Yes**

9.30 PCH Descriptor Record 29 (Flash Descriptor Records)

Flash Address:FPSBA + 01Dh

Default Flash Address: 11Dh

Offset from 0	Bits	Description	Usage	FIT Visible
0x11Dh	7	**GPP_H15 Individual Voltage Select (GPPC_H15_VCCIO):** 0 = GPP_H15 Voltage set to 3.3v 1 = GPP_H15 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_H15 GPIO pin.	**Yes**
	6	**GPP_H14 Individual Voltage Select (GPPC_H14_VCCIO):** 0 = GPP_H14 Voltage set to 3.3v 1 = GPP_H14 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_H14 GPIO pin.	**Yes**
	5	**GPP_H13 Individual Voltage Select (GPPC_H13_VCCIO):** 0 = GPP_H13 Voltage set to 3.3v 1 = GPP_H13 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_H13 GPIO pin.	**Yes**
	4	**GPP_H12 Individual Voltage Select (GPPC_H12_VCCIO):** 0 = GPP_H12 Voltage set to 3.3v 1 = GPP_H12 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_H12 GPIO pin.	**Yes**
	3	**GPP_H11 Individual Voltage Select (GPPC_H11_VCCIO):** 0 = GPP_H11 Voltage set to 3.3v 1 = GPP_H11 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_H11 GPIO pin.	**Yes**
	2	**GPP_H10 Individual Voltage Select (GPPC_H10_VCCIO):** 0 = GPP_H10 Voltage set to 3.3v 1 = GPP_H10 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_H10 GPIO pin.	**Yes**



Offset from 0	Bits	Description	Usage	FIT Visible
0x11Dh (Cont)	1	**GPP_H9 Individual Voltage Select (GPPC_H9_VCCIO):** 0 = GPP_H9 Voltage set to 3.3v 1 = GPP_H9 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_H9 GPIO pin.	**Yes**
	0	**GPP_H8 Individual Voltage Select (GPPC_H8_VCCIO):** 0 = GPP_H8 Voltage set to 3.3v 1 = GPP_H8 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_H8 GPIO pin.	**Yes**

9.31 PCH Descriptor Record 30 (Flash Descriptor Records)

Flash Address:FPSBA + 01Eh

Default Flash Address: 11Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0x11Eh	7	**GPP_H23 Individual Voltage Select (GPPC_H23_VCCIO):** 0 = GPP_H23 Voltage set to 3.3v 1 = GPP_H23 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_H23 GPIO pin.	**Yes**
	6	**GPP_H22 Individual Voltage Select (GPPC_H22_VCCIO):** 0 = GPP_H22 Voltage set to 3.3v 1 = GPP_H22 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_H22 GPIO pin.	**Yes**
	5	**GPP_H21 Individual Voltage Select (GPPC_H21_VCCIO):** 0 = GPP_H21 Voltage set to 3.3v 1 = GPP_H21 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_H21 GPIO pin.	**Yes**
	4	**GPP_H20 Individual Voltage Select (GPPC_H20_VCCIO):** 0 = GPP_H20 Voltage set to 3.3v 1 = GPP_H20 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_H20 GPIO pin.	**Yes**
	3	**GPP_H19 Individual Voltage Select (GPPC_H19_VCCIO):** 0 = GPP_H19 Voltage set to 3.3v 1 = GPP_H19 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_H19 GPIO pin.	**Yes**
	2	**GPP_H18 Individual Voltage Select (GPPC_H18_VCCIO):** 0 = GPP_H18 Voltage set to 3.3v 1 = GPP_H18 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_H18 GPIO pin.	**Yes**
	1	**GPP_H17 Individual Voltage Select (GPPC_H17_VCCIO):** 0 = GPP_H17 Voltage set to 3.3v 1 = GPP_H17 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_H17 GPIO pin.	**Yes**

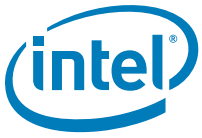
Offset from 0	Bits	Description	Usage	FIT Visible
0x11Eh (Cont)	0	**GPP_H16 Individual Voltage Select (GPPC_H16_VCCIO):** 0 = GPP_H16 Voltage set to 3.3v 1 = GPP_H16 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_H16 GPIO pin.	**Yes**

9.32 PCH Descriptor Record 31 (Flash Descriptor Records)

Flash Address:FPSBA + 01Fh

Default Flash Address: 11Fh

Offset from 0	Bits	Description	Usage	FIT Visible
0x11Fh	7	**GPP_C7 Individual Voltage Select (GPPC_C7_VCCIO):** 0 = GPP_C7 Voltage set to 3.3v 1 = GPP_C7 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_C7 GPIO pin.	**Yes**
	6	**GPP_C6 Individual Voltage Select (GPPC_C6_VCCIO):** 0 = GPP_C6 Voltage set to 3.3v 1 = GPP_C6 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_C6 GPIO pin.	**Yes**
	5	**GPP_C5 Individual Voltage Select (GPPC_C5_VCCIO):** 0 = GPP_C5 Voltage set to 3.3v 1 = GPP_C5 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_C5 GPIO pin.	**Yes**
	4	**GPP_C4 Individual Voltage Select (GPPC_C4_VCCIO):** 0 = GPP_C4 Voltage set to 3.3v 1 = GPP_C4 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_C4 GPIO pin.	**Yes**
	3	**GPP_C3 Individual Voltage Select (GPPC_C3_VCCIO):** 0 = GPP_C3 Voltage set to 3.3v 1 = GPP_C3 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_C3 GPIO pin.	**Yes**
	2	**GPP_C2 Individual Voltage Select (GPPC_C2_VCCIO):** 0 = GPP_C2 Voltage set to 3.3v 1 = GPP_C2 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_C2 GPIO pin.	**Yes**
	1	**GPP_C1 Individual Voltage Select (GPPC_C1_VCCIO):** 0 = GPP_C1 Voltage set to 3.3v 1 = GPP_C1 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_C1 GPIO pin.	**Yes**
	0	**GPP_C0 Individual Voltage Select (GPPC_C0_VCCIO):** 0 = GPP_C0 Voltage set to 3.3v 1 = GPP_C0 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_C0 GPIO pin.	**Yes**



9.33 PCH Descriptor Record 32 (Flash Descriptor Records)

Flash Address:FPSBA + 020h

Default Flash Address: 120h

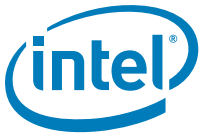
Offset from 0	Bits	Description	Usage	FIT Visible
0x120h	7	**GPP_C15 Individual Voltage Select (GPPC_C15_VCCIO):** 0 = GPP_C15 Voltage set to 3.3v 1 = GPP_C15 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_C15 GPIO pin.	**Yes**
	6	**GPP_C14 Individual Voltage Select (GPPC_C14_VCCIO):** 0 = GPP_C14 Voltage set to 3.3v 1 = GPP_C14 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_C14 GPIO pin.	**Yes**
	5	**GPP_C13 Individual Voltage Select (GPPC_C13_VCCIO):** 0 = GPP_C13 Voltage set to 3.3v 1 = GPP_C13 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_C13 GPIO pin.	**Yes**
	4	**GPP_C12 Individual Voltage Select (GPPC_C12_VCCIO):** 0 = GPP_C12 Voltage set to 3.3v 1 = GPP_C12 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_C12 GPIO pin.	**Yes**
	3	**GPP_C11 Individual Voltage Select (GPPC_C11_VCCIO):** 0 = GPP_C11 Voltage set to 3.3v 1 = GPP_C11 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_C11 GPIO pin.	**Yes**
	2	**GPP_C10 Individual Voltage Select (GPPC_C10_VCCIO):** 0 = GPP_C10 Voltage set to 3.3v 1 = GPP_C10 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_C10 GPIO pin.	**Yes**
	1	**GPP_C9 Individual Voltage Select (GPPC_C9_VCCIO):** 0 = GPP_C9 Voltage set to 3.3v 1 = GPP_C9 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_C9 GPIO pin.	**Yes**
	0	**GPP_C8 Individual Voltage Select (GPPC_C8_VCCIO):** 0 = GPP_C8 Voltage set to 3.3v 1 = GPP_C8 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_C8 GPIO pin.	**Yes**

9.34 PCH Descriptor Record 33 (Flash Descriptor Records)

Flash Address:FPSBA + 021h

Default Flash Address: 121h

Offset from 0	Bits	Description	Usage	FIT Visible
0x121h	7	**GPP_C23 Individual Voltage Select (GPPC_C23_VCCIO):** 0 = GPP_C23 Voltage set to 3.3v 1 = GPP_C23 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_C23 GPIO pin.	**Yes**
	6	**GPP_C22 Individual Voltage Select (GPPC_C22_VCCIO):** 0 = GPP_C22 Voltage set to 3.3v 1 = GPP_C22 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_C22 GPIO pin.	**Yes**
	5	**GPP_C21 Individual Voltage Select (GPPC_C21_VCCIO):** 0 = GPP_C21 Voltage set to 3.3v 1 = GPP_C21 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_C21 GPIO pin.	**Yes**
	4	**GPP_C20 Individual Voltage Select (GPPC_C20_VCCIO):** 0 = GPP_C20 Voltage set to 3.3v 1 = GPP_C20 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_C20 GPIO pin.	**Yes**
	3	**GPP_C19 Individual Voltage Select (GPPC_C19_VCCIO):** 0 = GPP_C16 Voltage set to 3.3v 1 = GPP_C16 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_C19 GPIO pin.	**Yes**
	2	**GPP_C18 Individual Voltage Select (GPPC_C18_VCCIO):** 0 = GPP_C16 Voltage set to 3.3v 1 = GPP_C16 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_C18 GPIO pin.	**Yes**
	1	**GPP_C17 Individual Voltage Select (GPPC_C17_VCCIO):** 0 = GPP_C16 Voltage set to 3.3v 1 = GPP_C16 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_C17 GPIO pin.	**Yes**
	0	**GPP_C16 Individual Voltage Select (GPPC_C16_VCCIO):** 0 = GPP_C16 Voltage set to 3.3v 1 = GPP_C16 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_C16 GPIO pin.	**Yes**



9.35 PCH Descriptor Record 34 (Flash Descriptor Records)

Flash Address:FPSBA + 022h

Default Flash Address: 122h

Offset from 0	Bits	Description	Usage	FIT Visible
0x122h	7:0	**Reserved, set to '0x40'**		**No**

9.36 PCH Descriptor Record 35 (Flash Descriptor Records)

Flash Address:FPSBA + 023h

Default Flash Address: 123h

Offset from 0	Bits	Description	Usage	FIT Visible
0x123h	7:0	**Reserved, set to '0'**		**No**

9.37 PCH Descriptor Record 36 (Flash Descriptor Records)

Flash Address:FPSBA + 024h

Default Flash Address: 124h

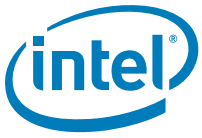
Offset from 0	Bits	Description	Usage	FIT Visible
0x124h	7:5	**Reserved, set to '0'**		**No**
	4	**Thunderbolt™ LSx/BSSB-LS #3 Select (TBT_VCCIO_CFG_SRC3):** 0 = Thunderbolt™ LSx/BSSB-LS #3 configured based on Tx pin strap 1 = Thunderbolt™ LSx/BSSB-LS #3 VCCIO configured based on Legacy fuse / soft strap.	This setting determines how VCCIO is configured for Thunderbolt™ LSx/BSSB-LS #3.	**Yes**
	3	**Intel® HD Audio Voltage Select (GPPR_VCCIO):** 0 = Intel® HD Audio Voltage Select to 3.3v 1 = Intel® HD Audio Voltage Select set to 1.8v	This setting controls configures the VCCIO voltage for all of the Intel® HD Audio GPIO pins.	**Yes**
	2	**SPI Voltage Select (GPP_SPI_Select):** 0 = SPI Voltage set to 3.3v 1 = SPI Voltage set to 1.8v	This setting controls the VCCIO voltage for the SPI.	**Yes**
	1:0	**Reserved, set to '0'**		**No**

9.38 PCH Descriptor Record 37 (Flash Descriptor Records)

Flash Address:FPSBA + 025h

Default Flash Address: 125h

Offset from 0	Bits	Description	Usage	FIT Visible
0x125h	7	**GPP_A7 Individual Voltage Select (GPPC_A7_VCCIO):** 0 = GPP_A7 Voltage set to 3.3v 1 = GPP_A7 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_A7 GPIO pin.	**Yes**
	6	**GPP_A6 Individual Voltage Select (GPPC_A6_VCCIO):** 0 = GPP_A6 Voltage set to 3.3v 1 = GPP_A6 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_A6 GPIO pin.	**Yes**
	5	**GPP_A5 Individual Voltage Select (GPPC_A5_VCCIO):** 0 = GPP_A5 Voltage set to 3.3v 1 = GPP_A5 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_A5 GPIO pin.	**Yes**
	4	**GPP_A4 Individual Voltage Select (GPPC_A4_VCCIO):** 0 = GPP_A4 Voltage set to 3.3v 1 = GPP_A4 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_A4 GPIO pin.	**Yes**
	3	**GPP_A3 Individual Voltage Select (GPPC_A3_VCCIO):** 0 = GPP_A3 Voltage set to 3.3v 1 = GPP_A3 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_A3 GPIO pin.	**Yes**
	2	**GPP_A2 Individual Voltage Select (GPPC_A2_VCCIO):** 0 = GPP_A2 Voltage set to 3.3v 1 = GPP_A2 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_A2 GPIO pin.	**Yes**
	1	**GPP_A1 Individual Voltage Select (GPPC_A1_VCCIO):** 0 = GPP_A1 Voltage set to 3.3v 1 = GPP_A1 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_A1 GPIO pin.	**Yes**
	0	**GPP_A0 Individual Voltage Select (GPPC_A0_VCCIO):** 0 = GPP_A0 Voltage set to 3.3v 1 = GPP_A0 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_A0 GPIO pin.	**Yes**



9.39 PCH Descriptor Record 38 (Flash Descriptor Records)

Flash Address:FPSBA + 026h

Default Flash Address: 126h

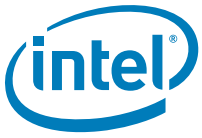
Offset from 0	Bits	Description	Usage	FIT Visible
0x126h	7	**GPP_A15 Individual Voltage Select (GPPC_A15 VCCIO):** 0 = GPP_A15 Voltage set to 3.3v 1 = GPP_A15 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_A15 GPIO pin.	**Yes**
	6	**GPP_A14 Individual Voltage Select (GPPC_A14 VCCIO):** 0 = GPP_A14 Voltage set to 3.3v 1 = GPP_A14 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_A14 GPIO pin.	**Yes**
	5	**GPP_A13 Individual Voltage Select (GPPC_A13_VCCIO):** 0 = GPP_A13 Voltage set to 3.3v 1 = GPP_A13 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_A13 GPIO pin.	**Yes**
	4	**GPP_A12 Individual Voltage Select (GPPC_A12_VCCIO):** 0 = GPP_A12 Voltage set to 3.3v 1 = GPP_A12 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_A12 GPIO pin.	**Yes**
	3	**GPP_A11 Individual Voltage Select (GPPC_A11_VCCIO):** 0 = GPP_A11 Voltage set to 3.3v 1 = GPP_A11 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_A11 GPIO pin.	**Yes**
	2	**GPP_A10 Individual Voltage Select (GPPC_A10_VCCIO):** 0 = GPP_A10 Voltage set to 3.3v 1 = GPP_A10 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_A10 GPIO pin.	**Yes**
	1	**GPP_A9 Individual Voltage Select (GPPC_A9_VCCIO):** 0 = GPP_A9 Voltage set to 3.3v 1 = GPP_A9 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_A9 GPIO pin.	**Yes**
	0	**GPP_A8 Individual Voltage Select (GPPC_A8_VCCIO):** 0 = GPP_A8 Voltage set to 3.3v 1 = GPP_A8 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_A8 GPIO pin.	**Yes**

9.40 PCH Descriptor Record 39 (Flash Descriptor Records)

Flash Address:FPSBA + 027h

Default Flash Address: 127h

Offset from 0	Bits	Description	Usage	FIT Visible
0x127h	7	**GPP_A23 Individual Voltage Select (GPPC_A23 VCCIO):** 0 = GPP_A23 Voltage set to 3.3v 1 = GPP_A23 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_A23 GPIO pin.	**Yes**
	6	**GPP_A22 Individual Voltage Select (GPPC_A22 VCCIO):** 0 = GPP_A22 Voltage set to 3.3v 1 = GPP_A22 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_A22 GPIO pin.	**Yes**
	5	**GPP_A21 Individual Voltage Select (GPPC_A21 VCCIO):** 0 = GPP_A21 Voltage set to 3.3v 1 = GPP_A21 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_A21 GPIO pin.	**Yes**
	4	**GPP_A20 Individual Voltage Select (GPPC_A20 VCCIO):** 0 = GPP_A20 Voltage set to 3.3v 1 = GPP_A20 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_A20 GPIO pin.	**Yes**
	3	**GPP_A19 Individual Voltage Select (GPPC_A19 VCCIO):** 0 = GPP_A19 Voltage set to 3.3v 1 = GPP_A19 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_A19 GPIO pin.	**Yes**
	2	**GPP_A18 Individual Voltage Select (GPPC_A18 VCCIO):** 0 = GPP_A18 Voltage set to 3.3v 1 = GPP_A18 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_A18 GPIO pin.	**Yes**
	1	**GPP_A17 Individual Voltage Select (GPPC_A17 VCCIO):** 0 = GPP_A17 Voltage set to 3.3v 1 = GPP_A17 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_A17 GPIO pin.	**Yes**
	0	**GPP_A16 Individual Voltage Select (GPPC_A16 VCCIO):** 0 = GPP_A16 Voltage set to 3.3v 1 = GPP_A16 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_A16 GPIO pin.	**Yes**



9.41 PCH Descriptor Record 40 (Flash Descriptor Records)

Flash Address:FPSBA + 028h

Default Flash Address: 128h

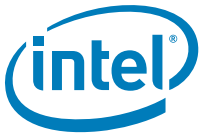
Offset from 0	Bits	Description	Usage	FIT Visible
0x128h	7	**GPP_B7 Individual Voltage Select (GPPC_B7 VCCIO):** 0 = GPP_B7 Voltage set to 3.3v 1 = GPP_B7 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_B7 GPIO pin.	**Yes**
	6	**GPP_B6 Individual Voltage Select (GPPC_B6 VCCIO):** 0 = GPP_B6 Voltage set to 3.3v 1 = GPP_B6 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_B6 GPIO pin.	**Yes**
	5	**GPP_B5 Individual Voltage Select (GPPC_B5 VCCIO):** 0 = GPP_B5 Voltage set to 3.3v 1 = GPP_B5 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_B5 GPIO pin.	**Yes**
	4	**GPP_B4 Individual Voltage Select (GPPC_B4 VCCIO):** 0 = GPP_B4 Voltage set to 3.3v 1 = GPP_B4 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_B4 GPIO pin.	**Yes**
	3	**GPP_B3 Individual Voltage Select (GPPC_B3 VCCIO):** 0 = GPP_B3 Voltage set to 3.3v 1 = GPP_B3 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_B3 GPIO pin.	**Yes**
	2	**GPP_B2 Individual Voltage Select (GPPC_B2 VCCIO):** 0 = GPP_B2 Voltage set to 3.3v 1 = GPP_B2 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_B2 GPIO pin.	**Yes**
	1	**GPP_B1 Individual Voltage Select (GPPC_B1 VCCIO):** 0 = GPP_B1 Voltage set to 3.3v 1 = GPP_B1 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_B1 GPIO pin.	**Yes**
	0	**GPP_B0 Individual Voltage Select (GPPC_B0 VCCIO):** 0 = GPP_B0 Voltage set to 3.3v 1 = GPP_B0 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_B0 GPIO pin.	**Yes**

9.42 PCH Descriptor Record 41 (Flash Descriptor Records)

Flash Address:FPSBA + 029h

Default Flash Address: 129h

Offset from 0	Bits	Description	Usage	FIT Visible
0x129h	7	**GPP_B15 Individual Voltage Select (GPPC_B15 VCCIO):** 0 = GPP_B15 Voltage set to 3.3v 1 = GPP_B15 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_B15 GPIO pin.	**Yes**
	6	**GPP_B14 Individual Voltage Select (GPPC_B14 VCCIO):** 0 = GPP_B14 Voltage set to 3.3v 1 = GPP_B14 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_B14 GPIO pin.	**Yes**
	5	**GPP_B13 Individual Voltage Select (GPPC_B13 VCCIO):** 0 = GPP_B13 Voltage set to 3.3v 1 = GPP_B13 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_B13 GPIO pin.	**Yes**
	4	**GPP_B12 Individual Voltage Select (GPPC_B12 VCCIO):** 0 = GPP_B12 Voltage set to 3.3v 1 = GPP_B12 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_B12 GPIO pin.	**Yes**
	3	**GPP_B11 Individual Voltage Select (GPPC_B11 VCCIO):** 0 = GPP_B11 Voltage set to 3.3v 1 = GPP_B11 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_B11 GPIO pin.	**Yes**
	2	**GPP_B10 Individual Voltage Select (GPPC_B10 VCCIO):** 0 = GPP_B10 Voltage set to 3.3v 1 = GPP_B10 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_B10 GPIO pin.	**Yes**
	1	**GPP_B9 Individual Voltage Select (GPPC_B9 VCCIO):** 0 = GPP_B9 Voltage set to 3.3v 1 = GPP_B9 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_B9 GPIO pin.	**Yes**
	0	**GPP_B8 Individual Voltage Select (GPPC_B8 VCCIO):** 0 = GPP_B8 Voltage set to 3.3v 1 = GPP_B8 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_B8 GPIO pin.	**Yes**



9.43 PCH Descriptor Record 42 (Flash Descriptor Records)

Flash Address:FPSBA + 02Ah

Default Flash Address: 12Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0x12Ah	7	**GPP_B23 Individual Voltage Select (GPPC_B23 VCCIO):** 0 = GPP_B23 Voltage set to 3.3v 1 = GPP_B23 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_B23 GPIO pin.	**Yes**
	6	**GPP_B22 Individual Voltage Select (GPPC_B22 VCCIO):** 0 = GPP_B22 Voltage set to 3.3v 1 = GPP_B22 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_B22 GPIO pin.	**Yes**
	5	**GPP_B21 Individual Voltage Select (GPPC_B21 VCCIO):** 0 = GPP_B21 Voltage set to 3.3v 1 = GPP_B21 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_B21 GPIO pin.	**Yes**
	4	**GPP_B20 Individual Voltage Select (GPPC_B20 VCCIO):** 0 = GPP_B20 Voltage set to 3.3v 1 = GPP_B20 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_B20 GPIO pin.	**Yes**
	3	**GPP_B19 Individual Voltage Select (GPPC_B19 VCCIO):** 0 = GPP_B19 Voltage set to 3.3v 1 = GPP_B19 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_B19 GPIO pin.	**Yes**
	2	**GPP_B18 Individual Voltage Select (GPPC_B18 VCCIO):** 0 = GPP_B18 Voltage set to 3.3v 1 = GPP_B18 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_B18 GPIO pin.	**Yes**
	1	**GPP_B17 Individual Voltage Select (GPPC_B17 VCCIO):** 0 = GPP_B17 Voltage set to 3.3v 1 = GPP_B17 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_B17 GPIO pin.	**Yes**
	0	**GPP_B16 Individual Voltage Select (GPPC_B16 VCCIO):** 0 = GPP_B16 Voltage set to 3.3v 1 = GPP_B16 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GPP_B16 GPIO pin.	**Yes**

9.44 PCH Descriptor Record 43 (Flash Descriptor Records)

Flash Address:FPSBA + 02Bh

Default Flash Address: 12Bh

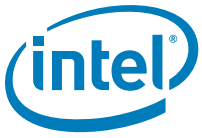
Offset from 0	Bits	Description	Usage	FIT Visible
0x12Bh	7:0	**Reserved, set to '0'**		**No**

9.45 PCH Descriptor Record 44 (Flash Descriptor Records)

Flash Address:FPSBA + 02Ch

Default Flash Address: 12Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x12Ch	7:6	**Reserved, set to '0'**		**No**
	5	**XHCI Port 6 Ownership Strap (XHC_PORT6_OWNERSHIP_STRAP):** Strap to decide XHCI Port 6 Ownership between XHCI/PCIe/CSI. 0x0 = XHC Port 6 configured as XHC **(default)** 0x1 = XHC Port 6 configures as Non-XHC	This strap must also be configured when setting the **USB3 / PCIe Combo Port 5 (FIA/LOSL5)**. **Note:** When **USB3 / PCIe Combo Port 4 (FIA/LOSL5)** configured as USB3 this setting needs to be set to 0x0. When **USB3 / PCIe Combo Port 4 (FIA/LOSL5)** is configured as PCIe this setting needs to be set to 0x1.	**No**
	4	**XHCI Port 5 Ownership Strap (XHC_PORT5_OWNERSHIP_STRAP):** Strap to decide XHCI Port 5 Ownership between XHCI/PCIe/CSI. 0x0 = XHC Port 5 configured as XHC 0x1 = XHC Port 5 configures as Non-XHC **(default)**	This strap must also be configured when setting the **USB3 / PCIe Combo Port 4 (FIA/LOSL4)**. **Note:** When **USB3 / PCIe Combo Port 4 (FIA/LOSL4)** configured as USB3 this setting needs to be set to 0x0. When **USB3 / PCIe Combo Port 4 (FIA/LOSL4)** is configured as PCIe this setting needs to be set to 0x1.	**No**



Offset from 0	Bits	Description	Usage	FIT Visible
0x12Ch (Cont)	3	**XHCI Port 4 Ownership Strap (XHC_PORT4_OWNERSHIP_STRAP):** Strap to decide XHCI Port 4 Ownership between XHCI/PCIe/CSI. 0x0 = XHC Port 4 configured as XHC 0x1 = XHC Port 4 configures as Non-XHC **(default)**	This strap must also be configured when setting the **USB3 / PCIe Combo Port 3 (FIA/LOSL3)**. **Note:** When **USB3 / PCIe Combo Port 3 (FIA/ LOSL3)** configured as USB3 this setting needs to be set to 0x0. When **USB3 / PCIe Combo Port 3 (FIA/ LOSL3)** is configured as PCIe this setting needs to be set to 0x1.	**No**
	2	**XHCI Port 3 Ownership Strap (XHC_PORT3_OWNERSHIP_STRAP):** Strap to decide XHCI Port 3 Ownership between XHCI/PCIe/CSI. 0x0 = XHC Port 3 configured as XHC **(default)** 0x1 = XHC Port 3 configures as Non-XHC	This strap must also be configured when setting the **USB3 / PCIe Combo Port 2 (FIA/LOSL2)**. **Note:** When **USB3 / PCIe Combo Port 2 (FIA/ LOSL2)** configured as USB3 this setting needs to be set to 0x0. When **USB3 / PCIe Combo Port 2 (FIA/ LOSL2)** is configured as PCIe this setting needs to be set to 0x1.	**No**
	1	**XHCI Port 2 Ownership Strap (XHC_PORT2_OWNERSHIP_STRAP):** Strap to decide XHCI Port 2 Ownership between XHCI/PCIe/CSI. 0x0 = XHC Port 2 configured as XHC 0x1 = XHC Port 2 configures as Non-XHC **(default)**	This strap must also be configured when setting the **USB3 / PCIe Combo Port 1 (FIA/LOSL1)**. **Note:** When **USB3 / PCIe Combo Port 1 (FIA/ LOSL1)** configured as USB3 this setting needs to be set to 0x0. When **USB3 / PCIe Combo Port 1 (FIA/ LOSL1)** is configured as PCIe this setting needs to be set to 0x1.	**No**
	0	**XHCI Port 1 Ownership Strap (XHC_PORT1_OWNERSHIP_STRAP):** Strap to decide XHCI Port 1 Ownership between XHCI/PCIe/CSI. 0x0 = XHC Port 1 configured as XHC **(default)** 0x1 = XHC Port 1 configures as Non-XHC	This strap must also be configured when setting the USB3 / PCIe Combo Port 0 (FIA/ LOSL0). **Note:** When **USB3 / PCIe Combo Port 0 (FIA/ LOSL0)** configured as USB3 this setting needs to be set to 0x0. When **USB3 / PCIe Combo Port 0 (FIA/ LOSL0)** is configured as PCIe this setting needs to be set to 0x1.	**No**

9.46 PCH Descriptor Record 45 (Flash Descriptor Records)

Flash Address:FPSBA + 02Dh

Default Flash Address: 12Dh

Offset from 0	Bits	Description	Usage	FIT Visible
0x12Dh	7:0	**Reserved, set to '0'**		**No**

9.47 PCH Descriptor Record 46 (Flash Descriptor Records)

Flash Address:FPSBA + 02Eh

Default Flash Address: 12Eh

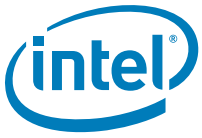
Offset from 0	Bits	Description	Usage	FIT Visible
0x12Eh	7:6	**Reserved, set to '0'**		**No**
	5	**USB3 Port 6 Speed Select:** 0 = Port 6 is configured as USB3.1 Gen2 1 = Port 6 is configured as USB3.1 Gen1	This setting determines the USB3 Port 6 speed capabilities.	**Yes**
	4	**USB3 Port 5 Speed Select:** 0 = Port 5 is configured as USB3.1 Gen2 1 = Port 5 is configured as USB3.1 Gen1	This setting determines the USB3 Port 5 speed capabilities.	**Yes**
	3	**USB3 Port 4 Speed Select:** 0 = Port 4 is configured as USB3.1 Gen2 1 = Port 4 is configured as USB3.1 Gen1	This setting determines the USB3 Port 4 speed capabilities.	**Yes**
	2	**USB3 Port 3 Speed Select:** 0 = Port 3 is configured as USB3.1 Gen2 1 = Port 3 is configured as USB3.1 Gen1	This setting determines the USB3 Port 3 speed capabilities.	**Yes**
	1	**USB3 Port 2 Speed Select:** 0 = Port 2 is configured as USB3.1 Gen2 1 = Port 2 is configured as USB3.1 Gen1	This setting determines the USB3 Port 2 speed capabilities.	**Yes**
	0	**USB3 Port 1 Speed Select:** 0 = Port 1 is configured as USB3.1 Gen2 1 = Port 1 is configured as USB3.1 Gen1	This setting determines the USB3 Port 1 speed capabilities.	**Yes**

9.48 PCH Descriptor Record 47 (Flash Descriptor Records)

Flash Address:FPSBA + 02Fh

Default Flash Address: 12Fh

Offset from 0	Bits	Description	Usage	FIT Visible
0x12Fh	7:6	**Reserved, set to '0'**		**No**
	5	**USB3 Port 6 Initialization Speed Select:** 0 = Port 6 will boot as USB 3.1 Gen1 and carry on LBPM if USB 3.1 Gen2 is enabled 1 = Port 6 will boot as USB 3.1 Gen2 and skip LBPM	This setting determines USB3 Port 6 speed during platform power-up.	**Yes**
	4	**USB3 Port 5 Initialization Speed Select:** 0 = Port 5 will boot as USB 3.1 Gen1 and carry on LBPM if USB 3.1 Gen2 is enabled 1 = Port 5 will boot as USB 3.1 Gen2 and skip LBPM	This setting determines USB3 Port 5 speed during platform power-up.	**Yes**



Offset from 0	Bits	Description	Usage	FIT Visible
0x12Fh (Cont)	3	**USB3 Port 4 Initialization Speed Select:** 0 = Port 4 will boot as USB 3.1 Gen1 and carry on LBPM if USB 3.1 Gen2 is enabled 1 = Port 4 will boot as USB 3.1 Gen2 and skip LBPM	This setting determines USB3 Port 4 speed during platform power-up.	**Yes**
	2	**USB3 Port 3 Initialization Speed Select:** 0 = Port 3 will boot as USB 3.1 Gen1 and carry on LBPM if USB 3.1 Gen2 is enabled 1 = Port 3 will boot as USB 3.1 Gen2 and skip LBPM	This setting determines USB3 Port 3 speed during platform power-up.	**Yes**
	1	**USB3 Port 2 Initialization Speed Select:** 0 = Port 2 will boot as USB 3.1 Gen1 and carry on LBPM if USB 3.1 Gen2 is enabled 1 = Port 2 will boot as USB 3.1 Gen2 and skip LBPM	This setting determines USB3 Port 2 speed during platform power-up.	**Yes**
	0	**USB3 Port 1 Initialization Speed Select:** 0 = Port 1 will boot as USB 3.1 Gen1 and carry on LBPM if USB 3.1 Gen2 is enabled 1 = Port 1 will boot as USB 3.1 Gen2 and skip LBPM	This setting determines USB3 Port 1 speed during platform power-up.	**Yes**

9.49 PCH Descriptor Record 48 (Flash Descriptor Records)

Flash Address:FPSBA + 030h

Default Flash Address: 130h

Offset from 0	Bits	Description	Usage	FIT Visible
0x130h	7:4	**USB3 Port 2 Connector Type Select:** 0x0 = USB Port 2 connector set to Type C 0x2 = USB Port 2 connector set to Type A 0x4 = USB Port 2 connector set to Express Card / M.2 S2	This setting configures the physical connector type for where the USB port [Super Speed / Enhanced Super Speed] is routed. ***Note:*** This Strap and USB3 Port 2 Connector Type Select Aux must match for proper operation.	**Yes**
	3:0	**USB3 Port 1 Connector Type Select:** 0x0 = USB Port 1 connector set to Type C 0x2 = USB Port 1 connector set to Type A 0x4 = USB Port 1 connector set to Express Card / M.2 S2	This setting configures the physical connector type for where the USB port [Super Speed / Enhanced Super Speed] is routed. ***Note:*** This Strap and USB3 Port 1 Connector Type Select Aux must match for proper operation.	**Yes**

9.50 PCH Descriptor Record 49 (Flash Descriptor Records)

Flash Address:FPSBA + 031h

Default Flash Address: 131h

Offset from 0	Bits	Description	Usage	FIT Visible
0x131h	7:4	**USB3 Port 4 Connector Type Select:** 0x0 = USB Port 4 connector set to Type C 0x2 = USB Port 4 connector set to Type A 0x4 = USB Port 4 connector set to Express Card / M.2 S2	This setting configures the physical connector type for where the USB port [Super Speed / Enhanced Super Speed] is routed. ***Note:*** This Strap and USB3 Port 4 Connector Type Select Aux must match for proper operation.	**Yes**
	3:0	**USB3 Port 3 Connector Type Select:** 0x0 = USB Port 3 connector set to Type C 0x2 = USB Port 3 connector set to Type A 0x4 = USB Port 3 connector set to Express Card / M.2 S2	This setting configures the physical connector type for where the USB port [Super Speed / Enhanced Super Speed] is routed. ***Note:*** This Strap and USB3 Port 3 Connector Type Select Aux must match for proper operation.	**Yes**

9.51 PCH Descriptor Record 50 (Flash Descriptor Records)

Flash Address:FPSBA + 032h

Default Flash Address: 132h

Offset from 0	Bits	Description	Usage	FIT Visible
0x132h	7:4	**USB3 Port 6 Connector Type Select:** 0x0 = USB Port 6 connector set to Type C 0x2 = USB Port 6 connector set to Type A 0x4 = USB Port 6 connector set to Express Card / M.2 S2	This setting configures the physical connector type for where the USB port [Super Speed / Enhanced Super Speed] is routed. ***Note:*** This Strap and USB3 Port 6 Connector Type Select Aux must match for proper operation.	**Yes**
	3:0	**USB3 Port 5 Connector Type Select:** 0x0 = USB Port 5 connector set to Type C 0x2 = USB Port 5 connector set to Type A 0x4 = USB Port 5 connector set to Express Card / M.2 S2	This setting configures the physical connector type for where the USB port [Super Speed / Enhanced Super Speed] is routed. ***Note:*** This Strap and USB3 Port 5 Connector Type Select Aux must match for proper operation.	**Yes**

9.52 PCH Descriptor Record 51 (Flash Descriptor Records)

Flash Address:FPSBA + 033h

Default Flash Address: 133h

Offset from 0	Bits	Description	Usage	FIT Visible
0x133h	7:4	**USB2 Port 2 Connector Type Select:** 0x0 = USB Port 2 connector set to Type C 0x2 = USB Port 2 connector set to Type A 0x4 = USB Port 2 connector set to Express Card / M.2 S2	This setting configures the USB2 Port 2 physical connector type for where the USB port is routed.	**Yes**
	3:0	**USB2 Port 1 Connector Type Select:** 0x0 = USB Port 1 connector set to Type C 0x2 = USB Port 1 connector set to Type A 0x4 = USB Port 1 connector set to Express Card / M.2 S2	This setting configures the USB2 Port 1 physical connector type for where the USB port is routed.	**Yes**

9.53 PCH Descriptor Record 52 (Flash Descriptor Records)

Flash Address:FPSBA + 034h

Default Flash Address: 134h

Offset from 0	Bits	Description	Usage	FIT Visible
0x134h	7:4	**USB2 Port 4 Connector Type Select:** 0x0 = USB Port 4 connector set to Type C 0x2 = USB Port 4 connector set to Type A 0x4 = USB Port 4 connector set to Express Card / M.2 S2	This setting configures the USB2 Port 4 physical connector type for where the USB port is routed.	**Yes**
	3:0	**USB2 Port 3 Connector Type Select:** 0x0 = USB Port 3 connector set to Type C 0x2 = USB Port 3 connector set to Type A 0x4 = USB Port 3 connector set to Express Card / M.2 S2	This setting configures the USB2 Port 3 physical connector type for where the USB port is routed.	**Yes**

9.54 PCH Descriptor Record 53 (Flash Descriptor Records)

Flash Address:FPSBA + 035h

Default Flash Address: 135h

Offset from 0	Bits	Description	Usage	FIT Visible
0x135h	7:4	**USB2 Port 6 Connector Type Select:** 0x0 = USB Port 6 connector set to Type C 0x2 = USB Port 6 connector set to Type A 0x4 = USB Port 6 connector set to Express Card / M.2 S2	This setting configures the USB2 Port 6 physical connector type for where the USB port is routed.	**Yes**
	3:0	**USB2 Port 5 Connector Type Select:** 0x0 = USB Port 5 connector set to Type C 0x2 = USB Port 5 connector set to Type A 0x4 = USB Port 5 connector set to Express Card / M.2 S2	This setting configures the USB2 Port 5 physical connector type for where the USB port is routed.	**Yes**

9.55 PCH Descriptor Record 54 (Flash Descriptor Records)

Flash Address:FPSBA + 036h

Default Flash Address: 136h

Offset from 0	Bits	Description	Usage	FIT Visible
0x136h	7:4	**USB2 Port 8 Connector Type Select:** 0x0 = USB Port 8 connector set to Type C 0x2 = USB Port 8 connector set to Type A 0x4 = USB Port 8connector set to Express Card / M.2 S2	This setting configures the USB2 Port 8 physical connector type for where the USB port is routed.	**Yes**
	3:0	**USB2 Port 7 Connector Type Select:** 0x0 = USB Port 7 connector set to Type C 0x2 = USB Port 7 connector set to Type A 0x4 = USB Port 7 connector set to Express Card / M.2 S2	This setting configures the USB2 Port 7 physical connector type for where the USB port is routed.	**Yes**

9.56 PCH Descriptor Record 55 (Flash Descriptor Records)

Flash Address:FPSBA + 037h

Default Flash Address: 137h

Offset from 0	Bits	Description	Usage	FIT Visible
0x137h	7:1	**Reserved, set to '0'**		**No**
	0	**USB Type AB mode Select:** 0 = USB Type AB connector switches based on SW event 1 = USB Type AB connector switches based on HW event	This setting configures the mode for the USB Type AB connector.	**Yes**

9.57 PCH Descriptor Record 56 (Flash Descriptor Records)

Flash Address:FPSBA + 038h

Default Flash Address: 138h

Offset from 0	Bits	Description	Usage	FIT Visible
0x138h	31	**Reserved, set to '0'**		**No**
	1	**Reserved, set to '0x1'**		**No**
	0	**Reserved, set to '0'**		**No**

9.58 PCH Descriptor Record 57 (Flash Descriptor Records)

Flash Address:FPSBA + 03Ch

Default Flash Address: 13Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x13Ch	7:0	**Reserved, set to '0'**		**No**

9.59 PCH Descriptor Record 58 (Flash Descriptor Records)

Flash Address:FPSBA + 03Dh

Default Flash Address: 13Dh

Offset from 0	Bits	Description	Usage	FIT Visible
0x13Dh	7:0	**Reserved, set to '0'**		**No**

9.60 PCH Descriptor Record 59 (Flash Descriptor Records)

Flash Address:FPSBA + 03Eh

Default Flash Address: 13Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0x13Eh	7:0	**Reserved, set to '0xff'**		**No**

9.61 PCH Descriptor Record 60 (Flash Descriptor Records)

Flash Address:FPSBA + 03Fh

Default Flash Address: 13Fh

Offset from 0	Bits	Description	Usage	FIT Visible
0x13Fh	7:0	**Reserved, set to '0'**		**No**

9.62 PCH Descriptor Record 61 (Flash Descriptor Records)

Flash Address:FPSBA + 040h

Default Flash Address: 140h

Offset from 0	Bits	Description	Usage	FIT Visible
0x140h	7	**Reserved, set to '0'**		**No**
	6:4	**Top Swap Block size (TSBS):** 000 = 64 KB. Invert A16 if Top Swap is enabled 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. ***Notes:*** 1. 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. 2. 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. 3. Intel Client chipset supports top swap block size of up to 256 KB. TS block sizes of greater than 256KB are not supported.	This 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**
	3:0	**Reserved, set to '0'**		**No**

9.63 PCH Descriptor Record 62 (Flash Descriptor Records)

Flash Address:FPSBA + 041h

Default Flash Address: 141h

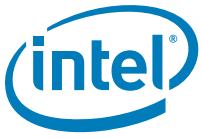
Offset from 0	Bits	Description	Usage	FIT Visible
0x141h	15:0	**Reserved, set to '0'**		**No**

9.64 PCH Descriptor Record 63 (Flash Descriptor Records)

Flash Address:FPSBA + 042h

Default Flash Address: 142h

Offset from 0	Bits	Description	Usage	FIT Visible
0x142h	7:0	**Reserved, set to '0x80'**		**No**



9.65 PCH Descriptor Record 64 (Flash Descriptor Records)

Flash Address:FPSBA + 043h

Default Flash Address: 143h

Offset from 0	Bits	Description	Usage	FIT Visible
0x143h	7:6	**SPI Maximum write and erase Resume to Suspend intervals:** 00 = 128us 01 = 256us 10 = 512us 11 = No Ceiling	This setting specifies the maximum value for the write and erase Resume to Suspend intervals.	**Yes**
	5	**SPI Out of Order operation Enable:** 0 = Out or Order operation Enabled 1 = Out of Order operation Disabled	When this setting is enabled priority operations may be issued while waiting for write / erase operations to complete on the flash device. When this setting is disabled all write / erase type operations in order.	**Yes**
	4	**SPI Suspend / Resume Enable:** 0 = Enable suspend / resume 1 = Disable suspend / resume	When this setting is enabled writes and erases may be suspended to allow a read to be issued on the flash device. When this setting is disabled no transaction will be allowed to the busy flash device.	**Yes**
	3:1	**SPI Resume Holdoff Delay:** 0x0 = 0us 0x1 = 2us 0x2 = 4us 0x3 = 6us 0x4 = 8us 0x5 = 10us 0x6 = 12us 0x7 = 14us	Specifies the time after the completion of a pri_op before the flash controller sends the resume instruction. If a new pri_op is eligible to be issued prior to the end of this delay time then the pri_op is issued and the timer is re-initialized to tRHD. 3-bit field encodes count with range 0-7. tRHD = count * 2us.	**Yes**
	0	**Reserved, set to '0'**		**No**

9.66 PCH Descriptor Record 65 (Flash Descriptor Records)

Flash Address:FPSBA + 044h

Default Flash Address: 144h

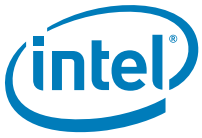
Offset from 0	Bits	Description	Usage	FIT Visible
0x144h	7	**Reserved, set to '0'**		**No**
	6:4	**Intel® Precise Touch and Stylus Controller 1 Maximum Frequency (TMF):** 000 = 120MHz 001 = 60MHz 010 = 48MHz 011 = Reserved 100 = 30 MHz 101 = Reserved 110 = 17 MHz 111 = Reserved ***Note:*** The listed frequencies are approximate.	This field allows the OEM to set an upper limit on the frequency for Touch transactions on Intel® Precise Touch and Stylus Controller 1. Intel® CSME firmware will use the value in this field along with data from the Touch device's capability register to program the Intel® Precise Touch and Stylus Controller 1 Configuration Register.	**Yes**
	3:0	**SPI Idle to Deep Power Down Timeout:** **Set to '0x5'**	SPI Idle to Deep Power Down Timeout Default Specifies the time in microseconds that the Flash Controller waits after all activity is idle before commanding the flash devices to Deep Powerdown, time = 2^N microseconds	**Yes**

9.67 PCH Descriptor Record 66 (Flash Descriptor Records)

Flash Address:FPSBA + 045h

Default Flash Address: 145h

Offset from 0	Bits	Description	Usage	FIT Visible
0x145h	7	**Reserved, set to '0x1'**		**No**
	6:3	**Reserved, set to '0'**		**No**
0x145h (Cont)	2:0	**SPI 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 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.		**Yes**



9.68 PCH Descriptor Record 67 (Flash Descriptor Records)

Flash Address:FPSBA + 046h

Default Flash Address: 146h

Offset from 0	Bits	Description	Usage	FIT Visible
0x146h	7:0	**Reserved, set to '0'**		**No**

9.69 PCH Descriptor Record 68 (Flash Descriptor Records)

Flash Address:FPSBA + 047h

Default Flash Address: 147h

Offset from 0	Bits	Description	Usage	FIT Visible
0x147h	7:3	**Reserved, set to '0'**		**No**
	2:0	**Reserved, set to '0x6'**		**No**

9.70 PCH Descriptor Record 69 (Flash Descriptor Records)

Flash Address:FPSBA + 048h

Default Flash Address: 148h

Offset from 0	Bits	Description	Usage	FIT Visible
0x148h	31:0	**Global Protected Range Default (GPRD):** **Set to '0x0'**	Sets the default value of the GPR0 register in the SPI Flash Controller.	**Yes**

9.71 PCH Descriptor Record 70 (Flash Descriptor Records)

Flash Address:FPSBA + 04Ch

Default Flash Address: 14Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x14Ch	7:0	**Reserved, set to '0x4'**		**No**

9.72 PCH Descriptor Record 71 (Flash Descriptor Records)

Flash Address:FPSBA + 04Dh

Default Flash Address: 14Dh

Offset from 0	Bits	Description	Usage	FIT Visible
0x14Dh	7:4	**Reserved, set to '0'**		**No**
	3:1	**Reserved, set to '0x1'**		**No**
	0	**Reserved, set to '0'**		**No**

9.73 PCH Descriptor Record 72 (Flash Descriptor Records)

Flash Address:FPSBA + 04Eh

Default Flash Address: 14Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0x14Eh	7	**Reserved, set to '0'**		**No**
	6	**Reserved, set to '0x1'**		**No**
	5:0	**Reserved, set to '0x18'**		**No**

9.74 PCH Descriptor Record 73 (Flash Descriptor Records)

Flash Address:FPSBA + 04Fh

Default Flash Address: 14Fh

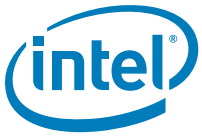
Offset from 0	Bits	Description	Usage	FIT Visible
0x14Fh	7:0	**Reserved, set to '0'**		**No**

9.75 PCH Descriptor Record 74 (Flash Descriptor Records)

Flash Address:FPSBA + 050h

Default Flash Address: 150h

Offset from 0	Bits	Description	Usage	FIT Visible
0x150h	7:2	**Reserved, set to '0'**		**No**
	1	**eSPI / EC Slave Attached Flash Channel OOO Enable:** 0 = In-Order SAF Requests 1 = Out-of-Order SAF Requests		**Yes**
	0	**eSPI / EC Slave Attached Flash Multiple Outstanding Requests Enable:** 0 = Single Outstanding SAF Request 1 = Multiple Outstanding SAF Requests		**Yes**



9.76 PCH Descriptor Record 75 (Flash Descriptor Records)

Flash Address:FPSBA + 051h

Default Flash Address: 151h

Offset from 0	Bits	Description	Usage	FIT Visible
0x151h	7:1	**Reserved, set to '0'**		**No**
	0	**eSPI / EC Max Outstanding Request for Master Attached Flash Channel:** 0 = Maximum of 2 outstanding requests allowed 1 = Maximum of 1 outstanding requests allowed		**Yes**

9.77 PCH Descriptor Record 76 (Flash Descriptor Records)

Flash Address:FPSBA + 052h

Default Flash Address: 152h

Offset from 0	Bits	Description	Usage	FIT Visible
0x152h	7	**Reserved, set to '0'**		**No**
	6	**eSPI Low Frequency Debug Override:** 0 = eSPI Low Frequency Debug Override Enabled 1 = eSPI Low Frequency Debug Override Disabled	When enabled this setting will divide eSPI clock frequency by 8. ***Note:*** This setting should only be used for debugging purposes. Leaving this setting enable will impact eSPI performance.	**Yes**
	5:4	**Reserved, set to '0x1'**		**No**
	3:0	**Reserved, set to '0'**		**No**

9.78 PCH Descriptor Record 77 (Flash Descriptor Records)

Flash Address:FPSBA + 053h

Default Flash Address: 153h

Offset from 0	Bits	Description	Usage	FIT Visible
0x153h	7:0	**Reserved, set to '0'**		**No**

9.79 PCH Descriptor Record 78 (Flash Descriptor Records)

Flash Address:FPSBA + 054h

Default Flash Address: 154h

Offset from 0	Bits	Description	Usage	FIT Visible
0x154h	7:0	**Reserved, set to '0'**		**No**

9.80 PCH Descriptor Record 79 (Flash Descriptor Records)

Flash Address:FPSBA + 055h

Default Flash Address: 155h

Offset from 0	Bits	Description	Usage	FIT Visible
0x155h	7:5	**Reserved, set to '0'**		**No**
	4:3	**PCIe Controller A:** Straps to set the default value of the PCI Express Port Configuration 1 register covering PCIe ports 5, 6 and 7, 8. 00 = 4x1 01 = 1x2, 2x1 10 = 2x2 11 = Reserved **NOTE**: Refer to EDS for PCIe supported port configurations.	Setting of this field depend on what PCIe ports 5, 6 and 7, 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 A Lane Reversal:** 0 = PCIe Lanes are not reversed. 1 = PCIe Lanes are reversed. **Note**: Refer to EDS supported Lane reversal configuration.	This bit controls lane reversal behavior for PCIe Controller A for PCIe. 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**

9.81 PCH Descriptor Record 80 (Flash Descriptor Records)

Flash Address:FPSBA + 056h

Default Flash Address: 156h

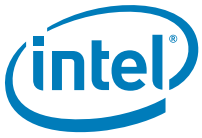
Offset from 0	Bits	Description	Usage	FIT Visible
0x156h	7:0	**Reserved, set to '0'**		**No**

9.82 PCH Descriptor Record 81 (Flash Descriptor Records)

Flash Address:FPSBA + 057h

Default Flash Address: 157h

Offset from 0	Bits	Description	Usage	FIT Visible
0x157h	7:0	**Reserved, set to '0'**		**No**



9.83 PCH Descriptor Record 82 (Flash Descriptor Records)

Flash Address:FPSBA + 058h

Default Flash Address: 158h

Offset from 0	Bits	Description	Usage	FIT Visible
0x158h	7:0	**Reserved, set to '0'**		**No**

9.84 PCH Descriptor Record 83 (Flash Descriptor Records)

Flash Address:FPSBA + 059h

Default Flash Address: 159h

Offset from 0	Bits	Description	Usage	FIT Visible
0x159h	7:0	**Reserved, set to '0'**		**No**

9.85 PCH Descriptor Record 84 (Flash Descriptor Records)

Flash Address:FPSBA + 05Ah

Default Flash Address: 15Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0x15Ah	7:0	**Reserved, set to '0'**		**No**

9.86 PCH Descriptor Record 85 (Flash Descriptor Records)

Flash Address:FPSBA + 05Bh

Default Flash Address: 15Bh

Offset from 0	Bits	Description	Usage	FIT Visible
0x15Bh	7:0	**Reserved, set to '0'**		**No**

9.87 PCH Descriptor Record 86 (Flash Descriptor Records)

Flash Address:FPSBA + 05Ch

Default Flash Address: 15Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x15Ch	0	**Reserved, set to '0'**		**No**

9.88 PCH Descriptor Record 87 (Flash Descriptor Records)

Flash Address:FPSBA + 05Dh

Default Flash Address: 15Dh

Offset from 0	Bits	Description	Usage	FIT Visible
0x15Dh	7:5	**Reserved, set to '0'**		**No**
	4:3	**PCIe Controller B (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 **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 B Lane Reversal:** 0 = PCIe Lanes are not reversed. 1 = PCIe Lanes are reversed. **Note**: Refer to EDS supported Lane reversal configuration.	This bit controls lane reversal behavior for PCIe Controller B. 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**

9.89 PCH Descriptor Record 88 (Flash Descriptor Records)

Flash Address:FPSBA + 05Eh

Default Flash Address: 15Eh

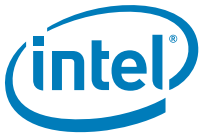
Offset from 0	Bits	Description	Usage	FIT Visible
0x15Eh	7:0	**Reserved, set to '0'**		**No**

9.90 PCH Descriptor Record 89 (Flash Descriptor Records)

Flash Address:FPSBA + 05Fh

Default Flash Address: 15Fh

Offset from 0	Bits	Description	Usage	FIT Visible
0x15Fh	7:0	**Reserved, set to '0'**		**No**



9.91 PCH Descriptor Record 90 (Flash Descriptor Records)

Flash Address:FPSBA + 060h

Default Flash Address: 160h

Offset from 0	Bits	Description	Usage	FIT Visible
0x160h	7:0	**Reserved, set to '0'**		**No**

9.92 PCH Descriptor Record 91 (Flash Descriptor Records)

Flash Address:FPSBA + 061h

Default Flash Address: 161h

Offset from 0	Bits	Description	Usage	FIT Visible
0x161h	7:0	**Reserved, set to '0'**		**No**

9.93 PCH Descriptor Record 92 (Flash Descriptor Records)

Flash Address:FPSBA + 062h

Default Flash Address: 162h

Offset from 0	Bits	Description	Usage	FIT Visible
0x162h	7:0	**Reserved, set to '0'**		**No**

9.94 PCH Descriptor Record 93 (Flash Descriptor Records)

Flash Address:FPSBA + 063h

Default Flash Address: 163h

Offset from 0	Bits	Description	Usage	FIT Visible
0x163h	7:0	**Reserved, set to '0'**		**No**

9.95 PCH Descriptor Record 94 (Flash Descriptor Records)

Flash Address:FPSBA + 064h

Default Flash Address: 164h

Offset from 0	Bits	Description	Usage	FIT Visible
0x164h	7:0	**Reserved, set to '0x14'**		**No**

9.96 PCH Descriptor Record 95 (Flash Descriptor Records)

Flash Address:FPSBA + 065h

Default Flash Address: 165h

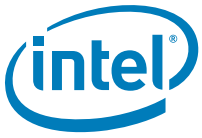
Offset from 0	Bits	Description	Usage	FIT Visible
0x165h	7	**Reserved, set to '0'**		**No**
	6:4	**OPI Link Width (OPDMI_LW):** 0x0 = 1 Lane 0x1 = 2 Lanes 0x2 = 4 Lanes 0x3 = 8 Lanes	This setting configures the OPI Link Width. For further details see the Ice Lake PCH EDS.	**Yes**
	3:0	**OPI Link Speed (OPDMI_TLS):** 0x2 = 2 GT/s Link Speed 0x3 = 4 GT/s 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 Ice Lake PCH EDS.	**Yes**

9.97 PCH Descriptor Record 96 (Flash Descriptor Records)

Flash Address:FPSBA + 066h

Default Flash Address: 166h

Offset from 0	Bits	Description	Usage	FIT Visible
0x166h	7	**Reserved, set to '0'**		**No**
	6	**DMI Lane Reversal (DMILR):** 0 = DMI Lanes are not reversed. 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**
	5	**Reserved, set to '0'**		**No**
	4:2	**Reserved, set to '0x1'**		**No**
	1:0	**Reserved, set to '0'**		**No**



9.98 PCH Descriptor Record 97 (Flash Descriptor Records)

Flash Address:FPSBA + 067h

Default Flash Address: 167h

Offset from 0	Bits	Description	Usage	FIT Visible
0x167h	7:6	**Reserved, set to '0'**		**No**
	5	**Reserved, set to '0x1'**		**No**
	3:4	**Reserved, set to '0'**		**No**
	2:1	**OPI Link Voltage (OPD_LVO):** 0 = 0.85 Volts 1 = 0.95 Volts 2 = 1.05 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 Ice Lake PCH EDS.	**Yes**
	0	**Reserved, set to '0'**		**No**

9.99 PCH Descriptor Record 98 (Flash Descriptor Records)

Flash Address:FPSBA + 068h

Default Flash Address: 168h

Offset from 0	Bits	Description	Usage	FIT Visible
0x168h	31:22	**Reserved, set to '0'**		**No**
	21	**Intel® Trace Hub - Emergency Mode:** 0 = ROM Tracing Emergency mode disabled 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	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	**SPI Software Re-Binding Enable:** 0 = SPI software re-binding disabled 1 = SPI software re-binding enabled	When enabled this settings will allows for SPI rebinding to a new PCH during manufacturing and re-manufacturing flows prior to platform EOM. ***Note:*** Re-binding to a replacement PCH can only be done a maximum of 5 times before the SPI part needs to be re-flashed.	**Yes**
	18	**Reserved, set to '0'**		**No**
	17	**Direct Connect Interface (DCI) Enabled:** 0 = DCI Disabled 1 = DCI Enabled		**Yes**
	16	**Reserved, set to '0'**		**Yes**
	15:12	**Reserved, set to '0'**		**No**

Offset from 0	Bits	Description	Usage	FIT Visible
0x168h (Cont)	11	**Intel® CSME AFS Flash Idle Reclaim Enable:** 0 = AFS Flash Reclaim enabled 1 = AFS Flash Reclaim disabled	This controls enabling / disabling of Intel® CSME AFS Idle flash reclaim capabilities. Note: This setting should be used for debug purposes only	**Yes**
	10	**Intel® CSME Reset Behavior:** 0 = Intel® CSME shall attempt to boot from the next available image, if exists. 1 = Intel® CSME will halt		**Yes**
	9	**Reserved, set to '0'**		**No**
	8:1	**Reserved, set to '0x98'**		**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 Intel® CSME. ***Note:*** Only applicable if Intel® Trace Hub Debug Messages strap is also enabled	**Yes**
	0	**Firmware ROM Bypass Enable Softstrap:** 0 = ROM Bypass disabled 1 = ROM Bypass enabled	Firmware ROM Bypass Enable Softstrap.	**Yes**

9.100 PCH Descriptor Record 99 (Flash Descriptor Records)

Flash Address:FPSBA + 069h

Default Flash Address: 169h

Offset from 0	Bits	Description	Usage	FIT Visible
0x169h	7:0	**Reserved, set to '0'**		**No**

9.101 PCH Descriptor Record 100 (Flash Descriptor Records)

Flash Address:FPSBA + 06Ah

Default Flash Address: 16Ah

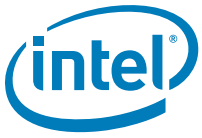
Offset from 0	Bits	Description	Usage	FIT Visible
0x16Ah	7:0	**Reserved, set to '0'**		**No**

9.102 PCH Descriptor Record 101 (Flash Descriptor Records)

Flash Address:FPSBA + 06Bh

Default Flash Address: 16Bh

Offset from 0	Bits	Description	Usage	FIT Visible
0x16Bh	7:0	**Reserved, set to '0'**		**No**



9.103 PCH Descriptor Record 102 (Flash Descriptor Records)

Flash Address:FPSBA + 06Ch

Default Flash Address: 16Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x16Ch	7:0	**Reserved, set to '0x70'**		**No**

9.104 PCH Descriptor Record 103 (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**

9.105 PCH Descriptor Record 104 (Flash Descriptor Records)

Flash Address:FPSBA + 06Eh

Default Flash Address: 16Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0x16Eh	7:0	**Reserved, set to '0'**		**No**

9.106 PCH Descriptor Record 105 (Flash Descriptor Records)

Flash Address:FPSBA + 06Fh

Default Flash Address: 16Fh

Offset from 0	Bits	Description	Usage	FIT Visible
0x16Fh	7:0	**Reserved, set to '0'**		**No**

9.107 PCH Descriptor Record 106 (Flash Descriptor Records)

Flash Address:FPSBA + 070h

Default Flash Address: 170h

Offset from 0	Bits	Description	Usage	FIT Visible
0x170h	7:0	**Reserved, set to '0x3'**		**No**

9.108 PCH Descriptor Record 107 (Flash Descriptor Records)

Flash Address:FPSBA + 071h

Default Flash Address: 171h

Offset from 0	Bits	Description	Usage	FIT Visible
0x171h	7:0	**Reserved, set to '0x2'**		**No**

9.109 PCH Descriptor Record 108 (Flash Descriptor Records)

Flash Address:FPSBA + 072h

Default Flash Address: 172h

Offset from 0	Bits	Description	Usage	FIT Visible
0x172h	7:0	**Reserved, set to '0'**		**No**

9.110 PCH Descriptor Record 109 (Flash Descriptor Records)

Flash Address:FPSBA + 073h

Default Flash Address: 173h

Offset from 0	Bits	Description	Usage	FIT Visible
0x173h	7:0	**Reserved, set to '0'**		**No**

9.111 PCH Descriptor Record 110 (Flash Descriptor Records)

Flash Address:FPSBA + 074h

Default Flash Address: 174h

Offset from 0	Bits	Description	Usage	FIT Visible
0x174h	7	**DCI BSSB over USB3 Port5 Configuration (EXI_PTSS_PORT7):** 0 = BSSB is enabled on USB3 Port5 1 = BSSB is disabled on USB3 Port5	This setting determines if the USB port being used for **DCI** operations has BSSB (Boundary Scan Side Band) enabled. ***Note:*** For S0ix and reset flows BSSB should be enabled.	**Yes**
	6	**DCI BSSB over USB3 Port4 Configuration (EXI_PTSS_PORT6):** 0 = BSSB is enabled on USB3 Port4 1 = BSSB is disabled on USB3 Port4	This setting determines if the USB port being used for **DCI** operations has BSSB (Boundary Scan Side Band) enabled. ***Note:*** For S0ix and reset flows BSSB should be enabled.	**Yes**
	5	**DCI BSSB over USB3 Port3 Configuration (EXI_PTSS_PORT5):** 0 = BSSB is enabled on USB3 Port3 1 = BSSB is disabled on USB3 Port3	This setting determines if the USB port being used for **DCI** operations has BSSB (Boundary Scan Side Band) enabled. ***Note:*** For S0ix and reset flows BSSB should be enabled.	**Yes**
	4	**DCI BSSB over USB3 Port2 Configuration (EXI_PTSS_PORT4):** 0 = BSSB is enabled on USB3 Port2 1 = BSSB is disabled on USB3 Port2	This setting determines if the USB port being used for **DCI** operations has BSSB (Boundary Scan Side Band) enabled. ***Note:*** For S0ix and reset flows BSSB should be enabled.	**Yes**
	3:1	**Reserved, set to '0x6'**		**No**
	0	**DCI BSSB over USB3 Port1 Configuration (EXI_PTSS_PORT0):** 0 = BSSB is enabled on USB3 Port1 1 = BSSB is disabled on USB3 Port1	This setting determines if the USB port being used for **DCI** operations has BSSB (Boundary Scan Side Band) enabled. ***Note:*** For S0ix and reset flows BSSB should be enabled.	**Yes**

9.112 PCH Descriptor Record 111 (Flash Descriptor Records)

Flash Address:FPSBA + 075h

Default Flash Address: 175h

Offset from 0	Bits	Description	Usage	FIT Visible
0x175h	7:1	**Reserved, set to '0'**		**No**
	0	**DCI BSSB over USB3 Port6 Configuration (EXI_PTSS_PORT8):** 0 = BSSB is enabled on USB3 Port6 1 = BSSB is disabled on USB3 Port6	This setting determines if the USB port being used for **DCI** operations has BSSB (Boundary Scan Side Band) enabled. ***Note:*** For S0ix and reset flows BSSB should be enabled.	**Yes**

9.113 PCH Descriptor Record 112 (Flash Descriptor Records)

Flash Address:FPSBA + 076h

Default Flash Address: 176h

Offset from 0	Bits	Description	Usage	FIT Visible
0x176h	7:0	**Reserved, set to '0'**		**No**

9.114 PCH Descriptor Record 113 (Flash Descriptor Records)

Flash Address:FPSBA + 077h

Default Flash Address: 177h

Offset from 0	Bits	Description	Usage	FIT Visible
0x177h	7:0	**Reserved, set to '0'**		**No**

9.115 PCH Descriptor Record 114 (Flash Descriptor Records)

Flash Address:FPSBA + 078h

Default Flash Address: 178h

Offset from 0	Bits	Description	Usage	FIT Visible
0x178h	7:0	**Reserved, set to '0'**		**No**

9.116 PCH Descriptor Record 115 (Flash Descriptor Records)

Flash Address:FPSBA + 079h

Default Flash Address: 179h

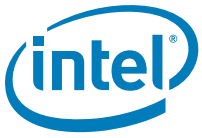
Offset from 0	Bits	Description	Usage	FIT Visible
0x179h	7:0	**Reserved, set to '0'**		**No**

9.117 PCH Descriptor Record 116 (Flash Descriptor Records)

Flash Address:FPSBA + 07Ah

Default Flash Address: 17Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0x17Ah	7:0	**Reserved, set to '0x7'**		**No**



9.118 PCH Descriptor Record 117 (Flash Descriptor Records)

Flash Address:FPSBA + 07Bh

Default Flash Address: 17Bh

Offset from 0	Bits	Description	Usage	FIT Visible
0x17Bh	7:0	**Reserved, set to '0x68'**		**No**

9.119 PCH Descriptor Record 118 (Flash Descriptor Records)

Flash Address:FPSBA + 07Ch

Default Flash Address: 17Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x17Ch	7:0	**Reserved, set to '0x6'**		**No**

9.120 PCH Descriptor Record 119 (Flash Descriptor Records)

Flash Address:FPSBA + 07Dh

Default Flash Address: 17Dh

Offset from 0	Bits	Description	Usage	FIT Visible
0x17Dh	7:0	**Reserved, set to '0'**		**No**

9.121 PCH Descriptor Record 120 (Flash Descriptor Records)

Flash Address:FPSBA + 07Eh

Default Flash Address: 17Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0x17Eh	7:0	**Reserved, set to '0'**		**No**

9.122 PCH Descriptor Record 121 (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**

9.123 PCH Descriptor Record 122 (Flash Descriptor Records)

Flash Address:FPSBA + 080h

Default Flash Address: 180h

Offset from 0	Bits	Description	Usage	FIT Visible
0x180h	7:2	**Reserved, set to '0'**		**No**
	1	**BIOS Guard protection override enable (LPC/ spi_strap_prr_ts_ovr):** 0 = BIOS Guard Fault Tolerant Update Capability is disabled 1 = BIOS guard Fault Tolerant Update Capability is enabled	This setting allows BIOS Guard to bypass the SPI Flash controller protections such as protected range registers and top swap. ***Note:*** For further details please review Intel® Platform Protection Technology with BIOS Guard 2.0 BIOS Specification regarding Fault Tolerant Update (FTU).	**Yes**
	0	**TPM Over SPI Bus Enabled (TOS):** 0 = TPM is not on SPI 1 = TPM is on SPI	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**

9.124 PCH Descriptor Record 123 (Flash Descriptor Records)

Flash Address:FPSBA + 081h

Default Flash Address: 181h

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

9.125 PCH Descriptor Record 124 (Flash Descriptor Records)

Flash Address:FPSBA + 082h

Default Flash Address: 182h

Offset from 0	Bits	Description	Usage	FIT Visible
0x182h	7:0	**Reserved, set to '0'**		**No**

9.126 PCH Descriptor Record 125 (Flash Descriptor Records)

Flash Address:FPSBA + 083h

Default Flash Address: 183h

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

9.127 PCH Descriptor Record 126 (Flash Descriptor Records)

Flash Address:FPSBA + 084h

Default Flash Address: 184h

Offset from 0	Bits	Description	Usage	FIT Visible
0x184h	7:3	**Reserved, set to '0'**		**No**
	2	**DMI / PCIe Port Staggering Enable:** 0 = Disabled 1 = Enabled		**Yes**
	1:0	**Reserved, set to '0x1'**		**No**

9.128 PCH Descriptor Record 127 (Flash Descriptor Records)

Flash Address:FPSBA + 085h

Default Flash Address: 185h

Offset from 0	Bits	Description	Usage	FIT Visible
0x185h	7:0	**Reserved, set to '0x3'**		**No**

9.129 PCH Descriptor Record 128 (Flash Descriptor Records)

Flash Address:FPSBA + 086h

Default Flash Address: 186h

Offset from 0	Bits	Description	Usage	FIT Visible
0x186h	7:4	**USB3 / PCIe Combo Port 1 (FIA/LOSL3):** 0x1 = statically assigned as USB Port 4 0x5 = statically assigned as PCIe Port 5	This setting determine if USB3 / PCIe Combo Port 1 is configured natively for USB3 or PCIe. **Note:** When configuring this setting you must also configure **XHCI Port 4 Ownership Strap (XHC_PORT4_OWNERSHIP_STRAP).**	**Yes**
	3:0	**USB3 / PCIe Combo Port 0 (FIA/LOSL2):** 0x1 = statically assigned as USB Port 3 0x5 = statically assigned as PCIe Port 6	This setting determine if USB3 / PCIe Combo Port 0 is configured natively for USB3 or PCIe. **Note:** When configuring this setting you must also configure **XHCI Port 3 Ownership Strap (XHC_PORT4_OWNERSHIP_STRAP).**	**Yes**

9.130 PCH Descriptor Record 129 (Flash Descriptor Records)

Flash Address:FPSBA + 087h

Default Flash Address: 187h

Offset from 0	Bits	Description	Usage	FIT Visible
0x187h	7:4	**Reserved, set to '0x5'**		**No**
	3:0	**USB3 / PCIe Combo Port 2 (FIA/LOSL4):** 0x1 = statically assigned as USB Port 5 0x5 = statically assigned as PCIe Port 4	This setting determine if USB3 / PCIe Combo Port 2 is configured natively for USB3 or PCIe. **Note:** When configuring this setting you must also configure **XHCI Port 5 Ownership Strap (XHC_PORT5_OWNERSHIP_STRAP).**	**Yes**

9.131 PCH Descriptor Record 130 (Flash Descriptor Records)

Flash Address:FPSBA + 088h

Default Flash Address: 188h

Offset from 0	Bits	Description	Usage	FIT Visible
0x188h	7:0	**Reserved, set to '0x55'**		**No**

9.132 PCH Descriptor Record 131 (Flash Descriptor Records)

Flash Address:FPSBA + 089h

Default Flash Address: 189h

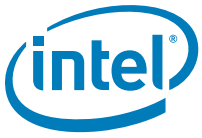
Offset from 0	Bits	Description	Usage	FIT Visible
0x189h	7:4	**Reserved, set to '0x5'**		**No**
	3:0	**Multi Flex Combo Port 0 (FIA/LOSL8):** 0x1 = USB3 Port 6 0x5 = PCIe 8	This setting configures Multi Flex Combo Port 0 to operates as either USB3 Port 6, PCIe Port 8.	**Yes**

9.133 PCH Descriptor Record 132 (Flash Descriptor Records)

Flash Address:FPSBA + 08Ah

Default Flash Address: 18Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0x18Ah	7:0	**Reserved, set to '0'**		**No**



9.134 PCH Descriptor Record 133 (Flash Descriptor Records)

Flash Address:FPSBA + 08Bh

Default Flash Address: 18Bh

Offset from 0	Bits	Description	Usage	FIT Visible
0x18Bh	7:0	**Reserved, set to '0'**		**No**

9.135 PCH Descriptor Record 134 (Flash Descriptor Records)

Flash Address:FPSBA + 08Ch

Default Flash Address: 18Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x18Ch	7:0	**Reserved, set to '0'**		**No**

9.136 PCH Descriptor Record 135 (Flash Descriptor Records)

Flash Address:FPSBA + 08Dh

Default Flash Address: 18Dh

Offset from 0	Bits	Description	Usage	FIT Visible
0x18Dh	7:0	**Reserved, set to '0'**		**No**

9.137 PCH Descriptor Record 136 (Flash Descriptor Records)

Flash Address:FPSBA + 08Eh

Default Flash Address: 18Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0x18Eh	7:0	**Reserved, set to '0'**		**No**

9.138 PCH Descriptor Record 137 (Flash Descriptor Records)

Flash Address:FPSBA + 08Fh

Default Flash Address: 18Fh

Offset from 0	Bits	Description	Usage	FIT Visible
0x18Fh	7:0	**Reserved, set to '0'**		**No**

9.139 PCH Descriptor Record 138 (Flash Descriptor Records)

Flash Address:FPSBA + 090h

Default Flash Address: 190h

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

9.140 PCH Descriptor Record 139 (Flash Descriptor Records)

Flash Address:FPSBA + 091h

Default Flash Address: 191h

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

9.141 PCH Descriptor Record 140 (Flash Descriptor Records)

Flash Address:FPSBA + 092h

Default Flash Address: 192h

Offset from 0	Bits	Description	Usage	FIT Visible
0x192h	7:0	**Reserved, set to '0'**		**No**

9.142 PCH Descriptor Record 141 (Flash Descriptor Records)

Flash Address:FPSBA + 093h

Default Flash Address: 193h

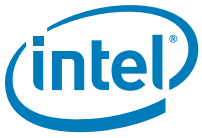
Offset from 0	Bits	Description	Usage	FIT Visible
0x193h	31:0	7:0	**Reserved, set to '0'**	

9.143 PCH Descriptor Record 142 (Flash Descriptor Records)

Flash Address:FPSBA + 094h

Default Flash Address: 194h

Offset from 0	Bits	Description	Usage	FIT Visible
0x194h	7:0	**Reserved, set to '0'**		**No**



9.144 PCH Descriptor Record 143 (Flash Descriptor Records)

Flash Address:FPSBA + 095h

Default Flash Address: 195h

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

9.145 PCH Descriptor Record 144 (Flash Descriptor Records)

Flash Address:FPSBA + 096h

Default Flash Address: 196h

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

9.146 PCH Descriptor Record 145 (Flash Descriptor Records)

Flash Address:FPSBA + 097h

Default Flash Address: 197h

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

9.147 PCH Descriptor Record 146 (Flash Descriptor Records)

Flash Address:FPSBA + 098h

Default Flash Address: 198h

Offset from 0	Bits	Description	Usage	FIT Visible
0x198h	7:0	**Reserved, set to '0'**		**No**

9.148 PCH Descriptor Record 147 (Flash Descriptor Records)

Flash Address:FPSBA + 099h

Default Flash Address: 199h

Offset from 0	Bits	Description	Usage	FIT Visible
0x199h	7:0	**Reserved, set to '0'**		**No**

9.149 PCH Descriptor Record 148 (Flash Descriptor Records)

Flash Address:FPSBA + 09Ah

Default Flash Address: 19Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0x19Ah	7:0	**Reserved, set to '0'**		**No**

9.150 PCH Descriptor Record 149 (Flash Descriptor Records)

Flash Address:FPSBA + 09Bh

Default Flash Address: 19Bh

Offset from 0	Bits	Description	Usage	FIT Visible
0x19Bh	7:0	**Reserved, set to '0'**		**No**

9.151 PCH Descriptor Record 150 (Flash Descriptor Records)

Flash Address:FPSBA + 09Ch

Default Flash Address: 19Ch

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

9.152 PCH Descriptor Record 151 (Flash Descriptor Records)

Flash Address:FPSBA + 09Dh

Default Flash Address: 19Dh

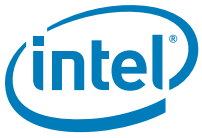
Offset from 0	Bits	Description	Usage	FIT Visible
0x19Dh	7:0	**Reserved, set to '0'**		**No**

9.153 PCH Descriptor Record 152 (Flash Descriptor Records)

Flash Address:FPSBA + 09Eh

Default Flash Address: 19Eh

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



9.154 PCH Descriptor Record 153 (Flash Descriptor Records)

Flash Address:FPSBA + 09Fh

Default Flash Address: 19Fh

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

9.155 PCH Descriptor Record 154 (Flash Descriptor Records)

Flash Address:FPSBA + 0A0h

Default Flash Address: 1A0h

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

9.156 PCH Descriptor Record 155 (Flash Descriptor Records)

Flash Address:FPSBA + 0A1h

Default Flash Address: 1A1h

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

9.157 PCH Descriptor Record 156 (Flash Descriptor Records)

Flash Address:FPSBA + 0A2h

Default Flash Address: 1A2h

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

9.158 PCH Descriptor Record 157 (Flash Descriptor Records)

Flash Address:FPSBA + 0A3h

Default Flash Address: 1A3h

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

9.159 PCH Descriptor Record 158 (Flash Descriptor Records)

Flash Address:FPSBA + 0A4h

Default Flash Address: 1A4h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1A4h	7:0	**Reserved, set to '0x15'**		**No**

9.160 PCH Descriptor Record 159 (Flash Descriptor Records)

Flash Address:FPSBA + 0A5h

Default Flash Address: 1A5h

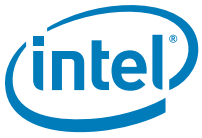
Offset from 0	Bits	Description	Usage	FIT Visible
0x1A5h	7:0	**Reserved, set to '0xAA'**		**No**

9.161 PCH Descriptor Record 160 (Flash Descriptor Records)

Flash Address:FPSBA + 0A6h

Default Flash Address: 1A6h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1A6h	7:0	**Reserved, set to '0x2'**		**No**



9.162 MIP Table Descriptor Record 0 (Flash Descriptor Records)

Flash Address:MDTBA + 000h

Default Flash Address: C00h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC00h	15:0	**Number of MIP Table Descriptor Entries:** **Set to '0x2'**	This setting determines the total number of MIP Table Descriptor entries present in the SPI image.	**Yes**

9.163 MIP Table Descriptor Record 1 (Flash Descriptor Records)

Flash Address:MDTBA + 002h

Default Flash Address: C02h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC02h	15:0	**Size of MIP Descriptor Entry:** **Set to '0xA0'**	This setting determines the size in bytes of the MIP Descriptor Entry structure.	**Yes**

9.164 MIP Table Descriptor Record 2 (Flash Descriptor Records)

Flash Address:MDTBA + 004h

Default Flash Address: C04h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC04h	15:0	**MIP Descriptor Block 0:** **Set to '0x1'**	This setting determines what the data type is for the MIP Descriptor.	**Yes**

9.165 MIP Table Descriptor Record 3 (Flash Descriptor Records)

Flash Address:MDTBA + 006h

Default Flash Address: C06h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC06h	15:0	**MIP Descriptor Block 0 Offset:** **Set to '0x14h'**	This setting determines the offset location of the MIP Descriptor Table Entries.	**Yes**

9.166 MIP Table Descriptor Record 4 (Flash Descriptor Records)

Flash Address:MDTBA + 008h

Default Flash Address: C08h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC08h	15:0	**MIP Descriptor Block 0 Length:** **Set to '0x84h'**	This setting determine the length of the MIP Descriptor Block 0.	**Yes**

9.167 MIP Table Descriptor Record 5 (Flash Descriptor Records)

Flash Address:MDTBA + 00Ah

Default Flash Address: C0Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0xC0Ah	15:0	**Reserved, set to '0'**		**No**

9.168 MIP Table Descriptor Record 6 (Flash Descriptor Records)

Flash Address:MDTBA + 00Ch

Default Flash Address: C0Ch

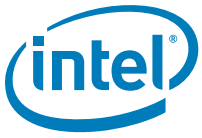
Offset from 0	Bits	Description	Usage	FIT Visible
0xC0Ch	15:0	**MIP Descriptor Block 1 Type:** **Set to '0'**	This setting determines what the data type is for the MIP Descriptor.	**Yes**

9.169 MIP Table Descriptor Record 7 (Flash Descriptor Records)

Flash Address:MDTBA + 00Eh

Default Flash Address: C0Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0xC0Eh	15:0	**MIP Descriptor Block 1 Offset:** **Set to '0x98h'**	This setting determines the offset location of the MIP Descriptor Table Entries.	**Yes**



9.170 MIP Table Descriptor Record 8 (Flash Descriptor Records)

Flash Address:MDTBA + 010h

Default Flash Address: C10h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC10h	15:0	**MIP Descriptor Block 1 Length:** **Set to '0x8h'**	This setting determine the length of the MIP Descriptor Block 0.	**Yes**

9.171 MIP Table Descriptor Record 9 (Flash Descriptor Records)

Flash Address:MDTBA + 012h

Default Flash Address: C12h

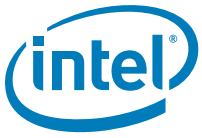
Offset from 0	Bits	Description	Usage	FIT Visible
0xC12h	15:0	**Reserved, set to '0'**		**No**

9.172 PMC Descriptor Record 0 (Flash Descriptor Records)

Flash Address:MDTBA + 014h

Default Flash Address: C14h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC14h	31:28	**Reserved, set to '0'**		**No**
	27	**Intel® Trace Hub Debug Messages Enable:** 0 = PCH Tracing debug messages Disabled 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**
	26	**Reserved, set to '0'**		**No**
	25	**Power Reporting Enable (THERM_PWR_REP_DIS):** 0 = Power Reporting is enabled. 1 = Power Reporting is completely disabled, regardless of the settings in the Thermal Power Reporting configuration registers. ***Note:*** When this setting is disabled the once-per-second timer interrupt associated with this feature must not be turned on.	This bit, when set, causes the PMC FW to completely turn off the Power Reporting feature. ***Note:*** A once-per-second timer interrupt is enabled which triggers firmware to report power and temperature information as enabled by configuration registers.	**Yes**
	24	**PCIe* Power Stable Timer (tPCH33 timer):** 0 = tPCH33 timer is disabled 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**
	23	**Reserved, set to '0'**		**No**
	22:21	**APWROK Timing (APWROK_TIMING):** 00 = 2 ms 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**
	20	**DeepSx Platform Configuration (DEEPSX_PLT_CFG_SS):** 0 =The platform does not support DeepSx. 1 =The platform supports DeepSx		**Yes**
	19	**LAN PHY Power Up Time (LAN_PHY_PU_TIME):** 0 =100ms 1 =50ms	This bit determines how long the delay for LAN PHY to power up after de-assertion of SLP_LAN#.	**Yes**



Offset from 0	Bits	Description	Usage	FIT Visible
0xC14h (cont)	18:16	**Over-Clocking WDT Self-Start Enable (OC_WDT_SS_EN):** 0x0 = Over-Clocking WDT disabled 0x1 = Over-Clocking WDT 3 second timeout 0x2 = Over-Clocking WDT 5 second timeout 0x3 = Over-Clocking WDT 10 second timeout 0x4 = Over-Clocking WDT 15 second timeout 0x5 = Over-Clocking WDT 30 second timeout 0x6 = Over-Clocking WDT 45 second timeout 0x7 = Over-Clocking WDT 60 second timeout	This setting affects whether the Over-Clocking WDT is enabled to automatically start on Host power cycle.	**Yes**
	15:12	**Reserved, set to '0'**		**No**
	11:10	**tPCH46 Timing:** 00 = 1 ms 01 = Reserved 10 = 5 ms 11 = 2 ms	tPCh46: PROCPWRGD and SYS_PWROK high to SUS_STAT# deassertion. Refer to EDS for details.	**Yes**
	9:8	**tPCH45 Timing:** 00 = 100 ms 01 = 50 ms 10 = 5 ms 11 = 1 ms	tPCH45: PCH clock output stable to PROCPWRGD high. Refer to EDS for details.	**Yes**
	7:0	**Reserved, set to '0x7E'**		**No**

9.173 PMC Descriptor Record 1 (Flash Descriptor Records)

Flash Address:MDTBA + 018h

Default Flash Address: C18h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC18h	31:8	**Reserved, set to '0xFE0000'**		**No**
	7	**Integrated Sensor Hub Supported:** 0 = Enable Integrated Sensor Hub 1 = Disable Integrated Sensor Hub		**Yes**
	6:1	**Reserved, set to '0'**		**No**
	0	**Intel® Integrated wired LAN Enable (IWL_EN):** 0 = Enabled Intel® Integrated wired LAN Solution 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**

9.174 PMC Descriptor Record 2 (Flash Descriptor Records)

Flash Address:MDTBA + 01Ch

Default Flash Address: C1Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0xC1Ch	31:0	**Reserved, set to '0x5178810'**		**No**

9.175 PMC Descriptor Record 3 (Flash Descriptor Records)

Flash Address:MDTBA + 020h

Default Flash Address: C20h

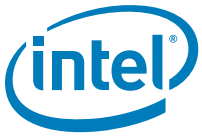
Offset from 0	Bits	Description	Usage	FIT Visible
0xC20h	31:0	**Reserved, set to '0x3BFB0'**		**No**

9.176 PMC Descriptor Record 4 (Flash Descriptor Records)

Flash Address:MDTBA + 024h

Default Flash Address: C24h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC24h	31:18	**Reserved, set to '0x480'**		**No**
	17	**SLP_S0# Tunnel (SLP_S0_TUNNEL_DIS):** 0 = SLP_S0# Tunnel enabled 1 = SLP_S0# Tunnel disabled	This setting enables / disabled the SLP_S0# tunneling over the eSPI to EC interface. ***Note:*** On eSPI enabled platforms this should be set to disabled for proper Sleep S0 operation.	**Yes**
	16:11	**Reserved, set to '0'**		**No**
	10:9	**OPI Link Voltage Strap (OPD_LVO_STRP):** 0x0 = 0.85 Volts 0x1 = 0.95 Volts 0x2 = 1.05 Volts	This strap must be configured when setting OPI Link Voltage strap (**OPD_LVO**). ***Note:*** This strap and the OPI Link Voltage strap (**OPD_LVO**) must match the same voltage configuration setting for proper platform operation function.	**Yes**
	8	**OPI Link Speed Strap (OPDMI_STRP):** 0x0 = 2 / GT/s Link Speed 0x1 = 4 / GT/s 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.	**Yes**



Offset from 0	Bits	Description	Usage	FIT Visible
0xC24h (Cont)	7:3	**USB2 DbC port enable:** 0x00 = No USB2 ports are assigned to DbC 0x80 = USB2 Port 1 DbC enabled 0x88 = USB2 Port 2 DbC enabled 0x90 = USB2 Port 3 DbC enabled 0x98 = USB2 Port 4 DbC enabled 0xA0 = USB2 Port 5 DbC enabled 0xA8 = USB2 Port 6 DbC enabled 0xB0 = USB2 Port 7 DbC enabled 0xB8 = USB2 Port 8 DbC enabled 0xC0 = USB2 Port 9 DbC enabled 0xC8 = USB2 Port 10 DbC enabled All other values are Reserved	This setting determines which USB2 ports are enabled for Early DbC debugging.	**No**
	2:0	**Reserved, set to '0'**		**No**

9.177 PMC Descriptor Record 5 (Flash Descriptor Records)

Flash Address:MDTBA + 028h

Default Flash Address: C28h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC28h	31:0	**Reserved, set to '0x2'**		**No**

9.178 PMC Descriptor Record 6 (Flash Descriptor Records)

Flash Address:MDTBA + 02Ch

Default Flash Address: C2Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0xC2Ch	31:0	**Reserved, set to '0'**		**No**

9.179 PMC Descriptor Record 7 (Flash Descriptor Records)

Flash Address:MDTBA + 030h

Default Flash Address: C30h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC30h	31:0	**Reserved, set to '0'**		**No**

9.180 PMC Descriptor Record 8 (Flash Descriptor Records)

Flash Address:MDTBA + 034h

Default Flash Address: C34h

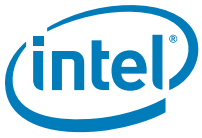
Offset from 0	Bits	Description	Usage	FIT Visible
0xC34h	31:15	**Reserved, set to '0'**		**No**
	14:8	**Reserved, set to '0x64'**		**No**
	7:0	**Reserved, set to '0'**		**No**

9.181 PMC Descriptor Record 9 (Flash Descriptor Records)

Flash Address:MDTBA + 038h

Default Flash Address: C38h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC38h	31:2	**Reserved, set to '0'**		**No**
	1	**Re-timer Power Gating Enable:** 0 = Re-timer PG is disabled 1 = Re-timer PD is enabled	This indicates if platform re-timer power gating is enabled.	**Yes**
	0	**Reserved, set to '0x1'**		**No**



9.182 PMC Descriptor Record 10 (Flash Descriptor Records)

Flash Address:MDTBA + 03Ch

Default Flash Address: C3Ch

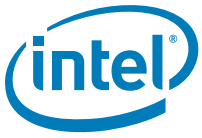
Offset from 0	Bits	Description	Usage	FIT Visible
0xC3Ch	31:27	**Reserved, set to '0'**		**No**
	26:23	**USB3 Port Number associated for Type-C Port 1:** 0x1 = Port 4 over USB3 Port 1 0x2 = Port 4 over USB3 Port 2 0x3 = Port 4 over USB3 Port 3 0x4 = Port 4 over USB3 Port 4	This setting the USB3 port is associated with Type-C Port 1.	**Yes**
	22:19	**USB2 Port Number associated for Type-C Port 1:** 0x1 = Port 4 over USB2 Port 1 0x2 = Port 4 over USB2 Port 2 0x3 = Port 4 over USB2 Port 3 0x4 = Port 4 over USB2 Port 4 0x5 = Port 4 over USB2 Port 5 0x6 = Port 4 over USB2 Port 6 0x7 = Port 4 over USB2 Port 7 0x8 = Port 4 over USB2 Port 8 0x9 = Port 4 over USB2 Port 9 0xA = Port 4 over USB2 Port 10	This setting the USB2 port is associated with Type-C Port 1.	**Yes**
	18:11	**Type-C Port 1 Re-timer SMBus Address:** Port 1 Re-timer SMBus address value: 0x0-0xFF	This setting configures the Re-timer SMBus address for Type-C Port 1.	**Yes**
	10:3	**Type C Port 1 SMBus Address:** Port 1 SMBus address value: 0x0-0xFF	This setting configures the SMBus address for Type-C Port 1.	**Yes**
	2	**Type-C Port 1 Re-timer Configuration Enable:** 0 = Port 1 Re-timer configured by PD Controller 1 = Port 1 Re-timer configured by PMC Controller	This setting indicates how Type-C Port 1 re-timer configuration is handled.	**Yes**
	1	**Type-C Port 1 Re-Timer Present:** 0 = Port 1 Re-timer is not present 1 = Port 1 Re-timer is present	This setting indicates if a re-timer is present for Type-C Port 1.	**Yes**
	0	**Type-C port 1 Enable:** 0 = Port 1 disabled 1 = Port 1 enabled	This setting indicates if Type-C Port 1 is enabled.	**Yes**

9.183 PMC Descriptor Record 11 (Flash Descriptor Records)

Flash Address:MDTBA + 040h

Default Flash Address: C40h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC40h	31:27	**Reserved, set to '0'**		**No**
	26:23	**USB3 Port Number associated for Type-C Port 2:** 0x1 = Port 4 over USB3 Port 1 0x2 = Port 4 over USB3 Port 2 0x3 = Port 4 over USB3 Port 3 0x4 = Port 4 over USB3 Port 4	This setting the USB3 port is associated with Type-C Port 2.	**Yes**
	22:19	**USB2 Port Number associated for Type-C Port 2:** 0x1 = Port 4 over USB2 Port 1 0x2 = Port 4 over USB2 Port 2 0x3 = Port 4 over USB2 Port 3 0x4 = Port 4 over USB2 Port 4 0x5 = Port 4 over USB2 Port 5 0x6 = Port 4 over USB2 Port 6 0x7 = Port 4 over USB2 Port 7 0x8 = Port 4 over USB2 Port 8 0x9 = Port 4 over USB2 Port 9 0xA = Port 4 over USB2 Port 10	This setting the USB2 port is associated with Type-C Port 2.	**Yes**
	18:11	**Type-C Port 2 Re-timer SMBus Address:** Port 2 Re-timer SMBus address value: 0x0-0xFF	This setting configures the Re-timer SMBus address for Type-C Port 2.	**Yes**
	10:3	**Type C Port 2 SMBus Address:** Port 2 SMBus address value: 0x0-0xFF	This setting configures the SMBus address for Type-C Port 2.	**Yes**
	2	**Type-C Port 2 Re-timer Configuration Enable:** 0 = Port 2 Re-timer configured by PD Controller 1 = Port 2 Re-timer configured by PMC Controller	This setting indicates how Type-C Port 2 re-timer configuration is handled.	**Yes**
	1	**Type-C Port 2 Re-Timer Present:** 0 = Port 2 Re-timer is not present 1 = Port 2 Re-timer is present	This setting indicates if a re-timer is present for Type-C Port 2.	**Yes**
	0	**Type-C port 2 Enable:** 0 = Port 2 disabled 1 = Port 2 enabled	This setting indicates if Type-C Port 2 is enabled.	**Yes**



9.184 PMC Descriptor Record 12 (Flash Descriptor Records)

Flash Address:MDTBA + 044h

Default Flash Address: C44h

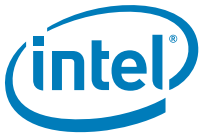
Offset from 0	Bits	Description	Usage	FIT Visible
0xC44h	31:27	**Reserved, set to '0'**		**No**
	26:23	**USB3 Port Number associated for Type-C Port 3:** 0x1 = Port 4 over USB3 Port 1 0x2 = Port 4 over USB3 Port 2 0x3 = Port 4 over USB3 Port 3 0x4 = Port 4 over USB3 Port 4	This setting the USB3 port is associated with Type-C Port 3.	**Yes**
	22:19	**USB2 Port Number associated for Type-C Port 3:** 0x1 = Port 4 over USB2 Port 1 0x2 = Port 4 over USB2 Port 2 0x3 = Port 4 over USB2 Port 3 0x4 = Port 4 over USB2 Port 4 0x5 = Port 4 over USB2 Port 5 0x6 = Port 4 over USB2 Port 6 0x7 = Port 4 over USB2 Port 7 0x8 = Port 4 over USB2 Port 8 0x9 = Port 4 over USB2 Port 9 0xA = Port 4 over USB2 Port 10	This setting the USB2 port is associated with Type-C Port 3.	**Yes**
	18:11	**Type-C Port 3 Re-timer SMBus Address:** Port 3 Re-timer SMBus address value: 0x0-0xFF	This setting configures the Re-timer SMBus address for Type-C Port 3.	**Yes**
	10:3	**Type C Port 3 SMBus Address:** Port 3 SMBus address value: 0x0-0xFF	This setting configures the SMBus address for Type-C Port 3.	**Yes**
	2	**Type-C Port 3 Re-timer Configuration Enable:** 0 = Port 3 Re-timer configured by PD Controller 1 = Port 3 Re-timer configured by PMC Controller	This setting indicates how Type-C Port 3 re-timer configuration is handled.	**Yes**
	1	**Type-C Port 3 Re-Timer Present:** 0 = Port 3 Re-timer is not present 1 = Port 3 Re-timer is present	This setting indicates if a re-timer is present for Type-C Port 3.	**Yes**
	0	**Type-C port 3 Enable:** 0 = Port 3 disabled 1 = Port 3 enabled	This setting indicates if Type-C Port 3 is enabled.	**Yes**

9.185 PMC Descriptor Record 13 (Flash Descriptor Records)

Flash Address:MDTBA + 048h

Default Flash Address: C48h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC48h	31:27	**Reserved, set to '0'**		**No**
	26:23	**USB3 Port Number associated for Type-C Port 4:** 0x1 = Port 4 over USB3 Port 1 0x2 = Port 4 over USB3 Port 2 0x3 = Port 4 over USB3 Port 3 0x4 = Port 4 over USB3 Port 4	This setting the USB3 port is associated with Type-C Port 4.	**Yes**
	22:19	**USB2 Port Number associated for Type-C Port 4:** 0x1 = Port 4 over USB2 Port 1 0x2 = Port 4 over USB2 Port 2 0x3 = Port 4 over USB2 Port 3 0x4 = Port 4 over USB2 Port 4 0x5 = Port 4 over USB2 Port 5 0x6 = Port 4 over USB2 Port 6 0x7 = Port 4 over USB2 Port 7 0x8 = Port 4 over USB2 Port 8 0x9 = Port 4 over USB2 Port 9 0xA = Port 4 over USB2 Port 10	This setting the USB2 port is associated with Type-C Port 4.	**Yes**
	18:11	**Type-C Port 4 Re-timer SMBus Address:** Port 3 Re-timer SMBus address value: 0x0-0xFF	This setting configures the Re-timer SMBus address for Type-C Port 4.	**Yes**
	10:3	**Type C Port 4 SMBus Address:** Port 3 SMBus address value: 0x0-0xFF	This setting configures the SMBus address for Type-C Port 4.	**Yes**
	2	**Type-C Port 4 Re-timer Configuration Enable:** 0 = Port 4 Re-timer configured by PD Controller 1 = Port 4 Re-timer configured by PMC Controller	This setting indicates how Type-C Port 4 re-timer configuration is handled.	**Yes**
	1	**Type-C Port 4 Re-Timer Present:** 0 = Port 4 Re-timer is not present 1 = Port 4 Re-timer is present	This setting indicates if a re-timer is present for Type-C Port 4.	**Yes**
	0	**Type-C port 4 Enable:** 0 = Port 4 disabled 1 = Port 4 enabled	This setting indicates if Type-C Port 4 is enabled.	**Yes**



9.186 PMC Descriptor Record 14 (Flash Descriptor Records)

Flash Address:MDTBA + 04Ch

Default Flash Address: C4Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0xC4Ch	31:0	**Reserved, set to '0'**		**No**

9.187 PMC Descriptor Record 15 (Flash Descriptor Records)

Flash Address:MDTBA + 050h

Default Flash Address: C50h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC50h	31:0	**Reserved, set to '0'**		**No**

9.188 PMC Descriptor Record 16 (Flash Descriptor Records)

Flash Address:MDTBA + 054h

Default Flash Address: C54h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC54h	31:0	**Reserved, set to '0'**		**No**

9.189 PMC Descriptor Record 17 (Flash Descriptor Records)

Flash Address:MDTBA + 058h

Default Flash Address: C58h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC58h	31:0	**Reserved, set to '0'**		**No**

9.190 PMC Descriptor Record 18 (Flash Descriptor Records)

Flash Address:MDTBA + 05Ch

Default Flash Address: C5Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0xC5Ch	31:0	**Reserved, set to '0'**		**No**

9.191 PMC Descriptor Record 19 (Flash Descriptor Records)

Flash Address:MDTBA + 060h

Default Flash Address: C60h

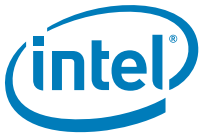
Offset from 0	Bits	Description	Usage	FIT Visible
0xC60h	31:0	**Reserved, set to '0'**		**No**

9.192 PMC Descriptor Record 20 (Flash Descriptor Records)

Flash Address:MDTBA + 064h

Default Flash Address: C64h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC64h	31:0	**Reserved, set to '0'**		**No**



9.193 CPU Descriptor Record 0 (Flash Descriptor Records)

Flash Address:MDTBA + 068h

Default Flash Address: C68h

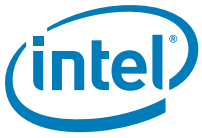
Offset from 0	Bits	Description	Usage	FIT Visible
0xC68h	31:27	**CPU Strap Length (CPUSL):** Identifies the 1's based number of Dwords of Processor Straps to be read, up to 31 DWs (1KB) max. A setting of all 0's indicates there are no Processor DW straps. **Set this field to 0xBh**		**No**
	26:0	**Reserved, set to '0'**		**No**

9.194 CPU Descriptor Record 1 (Flash Descriptor Records)

Flash Address:MDTBA + 06Ch

Default Flash Address: C6Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0xC6Ch	31	**Reserved, set to '0x1'**		**No**
	30:16	**Reserved, set to '0'**		**No**
	17	**Encrypted Debug Enable:** 0 = Encrypted Debug Enabled 1 = Encrypted Debug Disabled	This setting determines if encrypted debugging is enabled ***Note:*** This strap is intended for debugging purposes only.	**Yes**
	14:15	**Reserved, set to '0'**		**No**
	13	**JTAG Power Disable:** 0 = Disable JTAG Power for C10 and deeper states 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 Non-Turbo Frequency:** 0 = Disable Boot Non-Turbo Max Frequency 1 = Enable Boot Non-Turbo Max Frequency	This setting determines if the processor will operate at maximum Non-Turbo frequency at power-on and boot. **Note:** This strap is intended for debugging purposed only.	**Yes**
	11:6	**Flex Ratio:** '0x0'	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 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**
	4:1	**Number of Active Cores:** 0x0 = All Cores active 0x1 = One core active 0x2 = Two cores active 0x3 = Three cores active 0x4 = Four cores active 0x5 = Five cores active 0x6 = Six cores active 0x7 = Seven cores active 0x8 = Eight 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 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**



9.195 CPU Descriptor Record 2 (Flash Descriptor Records)

Flash Address:MDTBA + 070h

Default Flash Address: C70h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC70h	31	**Platform IMON Disable:** '0x1'	**Note:** This strap should be left at the recommended default setting.	**Yes**
	30	**SVID Presence:** 0 = SVID is present 1 = No SVID is present	This setting determine if SVID rails are present on the platform. See Processor EDS for details.	**Yes**
	29	**VCC IN SVID VR Type:** 0 = VCC IN SVID VR Type SVID 1 = VCC IN SVID VR Type is fixed VR	This setting determines the VCC IN SVID VR. See Processor EDS for details.	**Yes**
	28:25	**VCC IN SVID VR Address:** '0'	This setting determines the VCC IN SVID VR Address for the platform.	**Yes**
	24:6	**Reserved, set to '0'**		**No**
	5	**VCCIN Aux Level LP** 0 = VCCIN Aux Level LP 1.8v 1 = VCCIN Aux Level LP 1.65v	This setting determines the VCCIN Aux Level LP voltage. ***Note:*** Y based MCPs this setting can be configured to 1.65v. On all MCP types set to 1.8v.	**Yes**
	4	**VCC SFR OC PG Present:** 0 = VCC SFR OC PG Not Present 1 = VCC SFR OC PG Present	This setting determines if VCC SFR OC PG is present on the platform.	**Yes**
	3	**VCC ST PG Present:** 0 = VCC ST PG Not Present 1 = VCC ST PG Present	This setting determines if VCC ST PG is present on the platform	**Yes**
	2	**VCC STG PG Present:** 0 = VCC STG PG Not Present 1 = VCC STG PG Present	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**
	1	**VDDQ TX Rail Supply:** 0 = Tied to VDDQ (1.1/1.2v) 1 = Tied to LP4x (0.6v)	This setting determines if the VDDQ TX Rail supply is tied to VDDQ or LP4x.	**Yes**
	0	**VCC Aux Present:** 0 = VCC Aux is not Present 1 = VCC Aux is Present	This setting determines if VCC Aux exists as a separate VR.	**Yes**

9.196 CPU Descriptor Record 3 (Flash Descriptor Records)

Flash Address:MDTBA + 074h

Default Flash Address: C74h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC74h	31:28	**SE Key Mode:** '0x0'	**Note:** This strap should be left at the recommended default setting.	**Yes**
	27:8	**Reserved, set to '0'**		**No**
	6	**Thunderbolt™ Enable:** 0 = Thunderbolt™ Enabled 1 = Thunderbolt™ Disabled	This setting determines if the Thunderbolt™ interface is enabled on the platform.	**Yes**
	5:0	**Type-C Subsystem Port Enable Mask:** **Hex Value from 0x0 - 0x3f** 0x3f	This setting determines the Type-C Subsystem Port Enable Mask.	**Yes**

9.197 CPU Descriptor Record 4 (Flash Descriptor Records)

Flash Address:MDTBA + 078h

Default Flash Address: C78h

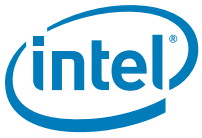
Offset from 0	Bits	Description	Usage	FIT Visible
0xC78h	31:0	**Reserved, set to '0'**		**No**

9.198 CPU Descriptor Record 5 (Flash Descriptor Records)

Flash Address:MDTBA + 07Ch

Default Flash Address: C7Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0xC7Ch	31:16	**Reserved, set to '0'**		**No**
	15:12	**Type-C Port 4 Configuration:** 0x0 = No Restrictions 0x1 = DP Fixed connection 0x2 = Reserved 0xE = No Thunderbolt™ on this port	This setting determines the configuration of Type-C Port 4.	**Yes**
	11:8	**Type-C Port 3 Configuration:** 0x0 = No Restrictions 0x1 = DP Fixed connection 0x2 = Reserved 0xE = No Thunderbolt™ on this port	This setting determines the configuration of Type-C Port 3.	**Yes**
	7:4	**Type-C Port 2 Configuration:** 0x0 = No Restrictions 0x1 = DP Fixed connection 0x2 = Reserved 0xE = No Thunderbolt™ on this port	This setting determines the configuration of Type-C Port 2.	**Yes**
	3:0	**Type-C Port 1 Configuration:** 0x0 = No Restrictions 0x1 = DP Fixed connection 0x2 = Reserved 0xE = No Thunderbolt™ on this port	This setting determines the configuration of Type-C Port 1.	**Yes**



9.199 CPU Descriptor Record 6 (Flash Descriptor Records)

Flash Address:MDTBA + 080h

Default Flash Address: C80h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC80h	31:0	**Reserved, set to '0'**		**No**
	1	**ARC Enabled:** 0 = ARC Enabled 1 = ARC Disabled	This setting enables / disables the Intel® Thunderbolt firmware connection manager.	**Yes**
	0	**Security Mode:** 0 = Security Mode Enabled 1 = Security Mode Disabled	This setting allows access to the Thunderbolt(TM) controller registers via software.	**Yes**

9.200 CPU Descriptor Record 7 (Flash Descriptor Records)

Flash Address:MDTBA + 084h

Default Flash Address: C84h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC84h	31:28	**Reserved, set to '0'**		**No**
	27	**Type-C Port 4 Initialization Speed Select:** 0 = Type-C Port 4 will boot as USB 3.1 Gen1 and carry on LBPM if USB 3.1 Gen2 is enabled 1 = Type-C Port 4 will boot as USB 3.1 Gen2 and skip LBPM	This setting determines Type-C Port 4 speed during platform power-up. ***Note:*** When configured to USB 3.1 Gen1 the port will preform LBPM if the USB port speed capability is configured for USB 3.1 Gen2.	**Yes**
	26	**Type-C Port 3 Initialization Speed Select:** 0 = Type-C Port 3 will boot as USB 3.1 Gen1 and carry on LBPM if USB 3.1 Gen2 is enabled 1 = Type-C Port 3 will boot as USB 3.1 Gen2 and skip LBPM	This setting determines Type-C Port 3 speed during platform power-up. ***Note:*** When configured to USB 3.1 Gen1 the port will preform LBPM if the USB port speed capability is configured for USB 3.1 Gen2.	**Yes**
	25	**Type-C Port 2 Initialization Speed Select:** 0 = Type-C Port 2 will boot as USB 3.1 Gen1 and carry on LBPM if USB 3.1 Gen2 is enabled 1 = Type-C Port 2 will boot as USB 3.1 Gen2 and skip LBPM	This setting determines Type-C Port 2 speed during platform power-up. ***Note:*** When configured to USB 3.1 Gen1 the port will preform LBPM if the USB port speed capability is configured for USB 3.1 Gen2.	**Yes**
	24	**Type-C Port 1 Initialization Speed Select:** 0 = Type-C Port 1 will boot as USB 3.1 Gen1 and carry on LBPM if USB 3.1 Gen2 is enabled 1 = Type-C Port 1 will boot as USB 3.1 Gen2 and skip LBPM	This setting determines Type-C Port 1 speed during platform power-up. ***Note:*** When configured to USB 3.1 Gen1 the port will preform LBPM if the USB port speed capability is configured for USB 3.1 Gen2.	**Yes**
	23:20	**Reserved, set to '0x3'**		**No**
	19	**Type-C Port 4 Speed Capabilities:** 0 = Type-C Port 4 is configured as USB3.1 Gen2 1 = Type-C Port 4 is configured as USB3.1 Gen1	This setting determines the speed capabilities for Type-C Port 4.	**Yes**
	18	**Type-C Port 3 Speed Capabilities:** 0 = Type-C Port 3 is configured as USB3.1 Gen2 1 = Type-C Port 3 is configured as USB3.1 Gen1	This setting determines the speed capabilities for Type-C Port 3.	**Yes**
	17	**Type-C Port 2 Speed Capabilities:** 0 = Type-C Port 2 is configured as USB3.1 Gen2 1 = Type-C Port 2 is configured as USB3.1 Gen1	This setting determines the speed capabilities for Type-C Port 2.	**Yes**
	16	**Type-C Port 1 Speed Capabilities:** 0 = Type-C Port 1 is configured as USB3.1 Gen2 1 = Type-C Port 1 is configured as USB3.1 Gen1	This setting determines the speed capabilities for Type-C Port 1.	**Yes**
	15:4	**Reserved, set to '0'**		**No**

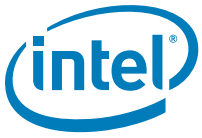
Offset from 0	Bits	Description	Usage	FIT Visible
0xC84h (Cont)	3	**Type-C XHCI Port 4 Ownership Strap (XHC_PORT4_OWNERSHIP_STRAP):** Strap to decide XHCI Port 4 Ownership between XHCI/PCIe/CSI. 0x0 = XHC Port 4 configured as XHC 0x1 = XHC Port 4 configures as Non-XHC	This setting configures Type-C Port 4 to operate as either XHCI or Non-XHCI. For further details on Flex I/O see Ice Lake Processor EDS for details.	**No**
	2	**Type-C XHCI Port 3 Ownership Strap (XHC_PORT3_OWNERSHIP_STRAP):** Strap to decide XHCI Port 3 Ownership between XHCI/PCIe/CSI. 0x0 = XHC Port 3 configured as XHC 0x1 = XHC Port 3 configures as Non-XHC	This setting configures Type-C Port 3 to operate as either XHCI or Non-XHCI. For further details on Flex I/O see Ice Lake Processor EDS for details.	**No**
	1	**Type-C XHCI Port 2 Ownership Strap (XHC_PORT2_OWNERSHIP_STRAP):** Strap to decide XHCI Port 2 Ownership between XHCI/PCIe/CSI. 0x0 = XHC Port 2 configured as XHC 0x1 = XHC Port 2 configures as Non-XHC	This setting configures Type-C Port 2 to operate as either XHCI or Non-XHCI. For further details on Flex I/O see Ice Lake Processor EDS for details.	**No**
	0	**Type-C XHCI Port 1 Ownership Strap (XHC_PORT1_OWNERSHIP_STRAP):** Strap to decide XHCI Port 1 Ownership between XHCI/PCIe/CSI. 0x0 = XHC Port 1 configured as XHC 0x1 = XHC Port 1 configures as Non-XHC	This setting configures Type-C Port 1 to operate as either XHCI or Non-XHCI. For further details on Flex I/O see Ice Lake Processor EDS for details.	**No**

9.201 CPU Descriptor Record 8 (Flash Descriptor Records)

Flash Address:MDTBA + 088h

Default Flash Address: C88h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC88h	31:0	**Reserved, set to '0'**		**No**



9.202 CPU Descriptor Record 9 (Flash Descriptor Records)

Flash Address:MDTBA + 08Ch

Default Flash Address: C8Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0xC8Ch	31:0	**Reserved, set to '0'**		**No**
	0	**Reserved, set to '0x1'**		**No**

9.203 CPU Descriptor Record 10 (Flash Descriptor Records)

Flash Address:MDTBA + 090h

Default Flash Address: C90h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC90h	31:0	**Reserved, set to '0'**		**No**

9.204 CPU Descriptor Record 11 (Flash Descriptor Records)

Flash Address:MDTBA + 094h

Default Flash Address: C94h

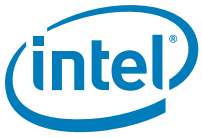
Offset from 0	Bits	Description	Usage	FIT Visible
0xC94h	31:0	**Reserved, set to '0'**		**No**

9.205 Intel® CSME Descriptor Record 0 (Flash Descriptor Records)

Flash Address:MDTBA + 098h

Default Flash Address: C98h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC98h	31:0	**Reserved, set to '0'**		**No**



9.206 Intel® CSME Descriptor Record 1 (Flash Descriptor Records)

Flash Address:MDTBA + 09Ch

Default Flash Address: C9Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0xC9Ch	31:25	**Reserved, set to '0'**		**No**
	24	**Delayed Authentication Mode enable (DAM_EN):** 0x0 = DAM is disabled 0x1 = DAM is enabled	This setting Enables / Disables Delayed Authentication Mode on the platform.	**No**
	23:16	**Early USB DbC Intel® CSME Boot Stall Enable:** 0 = Intel® CSME Boot Stall not enabled 1 = Intel® CSME Boot Stall enabled	This setting enables a delay during Intel® CSME FW bring-up to allow USB DCI to be established and Early DbC arbitration to be granted.	**Yes**
	15:8	**USB Connector's Associated USB3 Port enable:** 0x0 = USB3 Port 1 DbC enabled 0x1 = USB3 Port 2 DbC enabled 0x2 = USB3 Port 3 DbC enabled 0x3 = USB3 Port 4 DbC enabled 0x4 = USB3 Port 5 DbC enabled 0x5 = USB3 Port 6 DbC enabled 0xff = No USB3 ports are assigned to DbC All other values are Reserved	This setting determines which USB3 port goes to the target USB2 ports connector for Early DbC debugging.	**Yes**
	7:0	**USB2 DbC port enable:** 0x0 = USB2 Port 1 DbC enabled 0x1 = USB2 Port 2 DbC enabled 0x2 = USB2 Port 3 DbC enabled 0x3 = USB2 Port 4 DbC enabled 0x4 = USB2 Port 5 DbC enabled 0x5 = USB2 Port 6 DbC enabled 0x6 = USB2 Port 7 DbC enabled 0x7 = USB2 Port 8 DbC enabled 0x8 = USB2 Port 9 DbC enabled 0x9 = USB2 Port 10 DbC enabled 0xff = No USB2 ports are assigned to DbC All other values are Reserved	This setting determines which USB2 ports are enabled for Early DbC debugging.	**Yes**

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
Ice Lake	Ice Lake Platform	Intel® Management Engine 11.X (use latest version)

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

A: Ice Lake PCH-LP 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 *Ice Lake 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 *Ice Lake 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.

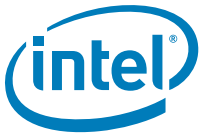
Adding support does not imply validation or guarantee a flash part will work. Platform designers/integrators will have to validate all flash parts with their platforms to ensure full functionality and reliability.

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 Ice Lake 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: Ice Lake 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 *Ice Lake 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.

§ §