



# **Raptor Lake-S Client Platform**

## **SPI Programming Guide**

**November 2021**

**Revision 0.81**

**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](http://www.intel.com/products/processor_number).

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

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

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

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

Copyright © 2021, Intel Corporation. All rights reserved.

# Contents

<b>1</b>	<b>Introduction</b>	16
1.1	Overview	16
1.2	Terminology	17
1.3	Reference Documents	17
<b>2</b>	<b>PCH SPI Flash Architecture</b>	19
2.1	Descriptor Mode	19
2.2	Serial Flash Discoverable Parameter (SFDP)	19
2.3	SPI Fast Read	19
2.4	Intel® Trusted Platform Module (Intel® TPM) on SPI Bus	19
2.5	Boot Flow for Raptor Lake PCH Family	19
2.6	Flash Regions	20
2.6.1	Flash Region Layout	20
2.6.2	Flash Region Sizes	22
2.7	Hardware Sequencing	22
<b>3</b>	<b>PCH SPI Flash Compatibility Requirement</b>	23
3.1	Raptor Lake PCH SPI Flash Requirements	23
3.1.1	General Requirements	23
3.1.2	Bios Requirement	24
3.1.3	Software / Firmware Requirements	24
3.1.4	JEDEC ID (Opcode 9Fh)	25
3.1.5	Multiple Page Write Usage Model	25
3.1.6	Hardware Sequencing Requirements	25
3.2	Raptor Lake PCH SPI AC Electrical Compatibility Guidelines	26
<b>4</b>	<b>Descriptor Overview</b>	27
4.1	Flash Descriptor Content	28
4.1.1	Descriptor Signature and Map	29
4.1.1.1	FLVALSIG - Flash Valid Signature (Flash Descriptor Records)	29
4.1.1.2	FLMAP0 - Flash Map 0 Register (Flash Descriptor Records)	29
4.1.1.3	FLMAP1 - Flash Map 1 Register (Flash Descriptor Records)	31
4.1.1.4	FLMAP2—Flash Map 2 Register (Flash Descriptor Records)	31
4.1.1.5	FLMAP3—Flash Map 3 Register (Flash Descriptor Records)	31
4.1.2	Flash Descriptor Component Section	33
4.1.2.1	FLCOMP—Flash Components Register (Flash Descriptor Records)	33
4.1.2.2	FLILL—Flash Invalid Instructions Register (Flash Descriptor Records)	36
4.1.2.3	FLILL1—Flash Invalid Instructions Register (Flash Descriptor Records)	36
4.1.3	Flash Descriptor Region Section	37
4.1.3.1	FLREG0—Flash Region 0 (Flash Descriptor) Register (Flash Descriptor Records)	38
4.1.3.2	FLREG1—Flash Region 1 (BIOS) Register (Flash Descriptor Records)	38
4.1.3.3	FLREG2—Flash Region 2 (Intel® CSME) Register (Flash Descriptor Records)	38

4.1.3.4	FLREG3—Flash Region 3 (GbE) Register (Flash Descriptor Records)	39
4.1.3.5	FLREG4—Flash Region 4 (Platform Data) Register (Flash Descriptor Records)	39
4.1.3.6	FLREG8—Flash Region 8 (Embedded Controller) Register (Flash Descriptor Records)	39
4.1.4	Flash Descriptor Master Section	41
4.1.4.1	FLMSTR1—Flash Master 1 (Host CPU/ BIOS)	41
4.1.4.2	FLMSTR2—Flash Master 2 (Intel® CSME)	41
4.1.4.3	FLMSTR3—Flash Master 3 (GbE)	41
4.1.4.4	FLMSTR4—Flash Master 4 (Reserved)	42
4.1.4.5	FLMSTR5—Flash Master 5 (EC)	42
4.1.5	PCH / CPU Softstraps	42
4.1.6	Descriptor Upper Map Section	42
4.1.6.1	FLUMAP1—Flash Upper Map 1 (Flash Descriptor Records)	43
4.1.6.2	IFWI / Intel® CSME ROM Bypass Size	43
4.1.6.3	MIP - Descriptor Table	43
4.1.7	Intel® CSME Vendor Specific Component Capabilities Table	44
4.1.7.1	JID0—JEDEC-ID 0 Register (Flash Descriptor Records)	44
4.1.7.2	VSCC0—Vendor Specific Component Capabilities 0 (Flash Descriptor Records)	44
4.1.7.3	JIDn—JEDEC-ID Register n (Flash Descriptor Records)	45
4.1.7.4	VSCCn—Vendor Specific Component Capabilities n (Flash Descriptor Records)	45
4.2	OEM Section	45
4.2.1	Region Access Control	46
4.2.2	Intel Recommended Permissions for Region Access	47
4.2.3	Overriding Region Access	47
4.3	Intel® CSME Vendor-Specific Component Capabilities (Intel® CSME VSCC) Table	48
4.4	How to Set a VSCC Entry in Intel® CSME VSCC Table for Raptor Lake PCH Platforms	48
4.4.1	Intel® CSME VSCC Table Settings for Raptor Lake PCH Family Systems	50
<b>5</b>	<b>Serial Flash Discoverable Parameter (SFDP) Overview</b>	<b>51</b>
5.1	Introduction	51
5.2	Discoverable Parameter Opcode and Flash Cycle	51
5.3	Parameter Table Supported on PCH	51
5.4	Detailed JEDEC Specification	52
<b>6</b>	<b>Configuring BIOS/GbE for SPI Flash Access</b>	<b>53</b>
6.1	Unlocking SPI Flash Device Protection for Raptor Lake PCH Platform	53
6.2	Locking SPI Flash via Status Register	54
6.3	SPI Protected Range Register Recommendations	54
6.4	Recommendations for Flash Configuration Lockdown and Vendor Component Lock Bits	54
6.4.1	Flash Configuration Lockdown	54
6.4.2	Vendor Component Lock	55
6.5	Host Vendor Specific Component Control Registers (VSCC)	55
6.6	Host VSCC Register Settings	59
<b>7</b>	<b>IFWI / Intel® CSME Disable for Debug/Flash Burning Purposes</b>	<b>60</b>
7.1	IFWI / Intel® CSME Disable	60
7.1.1	Erasing/Programming Intel® CSME Region	60
<b>8</b>	<b>Recommendations for SPI Flash Programming in Manufacturing Environments</b>	<b>61</b>
<b>9</b>	<b>Flash Descriptor PCH / PMC / CPU and Intel® CSME Configuration Section</b>	<b>62</b>
9.1	PCH Descriptor Record 0 (Flash Descriptor Records)	62

[illegible]

9.57	PCH Descriptor Record 56 (Flash Descriptor Records)	78
9.58	PCH Descriptor Record 57 (Flash Descriptor Records)	78
9.59	PCH Descriptor Record 58 (Flash Descriptor Records)	78
9.60	PCH Descriptor Record 59 (Flash Descriptor Records)	79
9.61	PCH Descriptor Record 60 (Flash Descriptor Records)	79
9.62	PCH Descriptor Record 61 (Flash Descriptor Records)	79
9.63	PCH Descriptor Record 62 (Flash Descriptor Records)	79
9.64	PCH Descriptor Record 63 (Flash Descriptor Records)	79
9.65	PCH Descriptor Record 64 (Flash Descriptor Records)	80
9.66	PCH Descriptor Record 65 (Flash Descriptor Records)	80
9.67	PCH Descriptor Record 66 (Flash Descriptor Records)	80
9.68	PCH Descriptor Record 67 (Flash Descriptor Records)	81
9.69	PCH Descriptor Record 68 (Flash Descriptor Records)	82
9.70	PCH Descriptor Record 69 (Flash Descriptor Records)	83
9.71	PCH Descriptor Record 70 (Flash Descriptor Records)	83
9.72	PCH Descriptor Record 71 (Flash Descriptor Records)	83
9.73	PCH Descriptor Record 72 (Flash Descriptor Records)	84
9.74	PCH Descriptor Record 73 (Flash Descriptor Records)	84
9.75	PCH Descriptor Record 74 (Flash Descriptor Records)	84
9.76	PCH Descriptor Record 75 (Flash Descriptor Records)	85
9.77	PCH Descriptor Record 76 (Flash Descriptor Records)	85
9.78	PCH Descriptor Record 77 (Flash Descriptor Records)	85
9.79	PCH Descriptor Record 78 (Flash Descriptor Records)	86
9.80	PCH Descriptor Record 79 (Flash Descriptor Records)	86
9.81	PCH Descriptor Record 80 (Flash Descriptor Records)	86
9.82	PCH Descriptor Record 81 (Flash Descriptor Records)	87
9.83	PCH Descriptor Record 82 (Flash Descriptor Records)	87
9.84	PCH Descriptor Record 83 (Flash Descriptor Records)	87
9.85	PCH Descriptor Record 84 (Flash Descriptor Records)	88
9.86	PCH Descriptor Record 85 (Flash Descriptor Records)	88
9.87	PCH Descriptor Record 86 (Flash Descriptor Records)	89
9.88	PCH Descriptor Record 87 (Flash Descriptor Records)	90
9.89	PCH Descriptor Record 88 (Flash Descriptor Records)	90
9.90	PCH Descriptor Record 89 (Flash Descriptor Records)	90
9.91	PCH Descriptor Record 90 (Flash Descriptor Records)	90
9.92	PCH Descriptor Record 91 (Flash Descriptor Records)	91
9.93	PCH Descriptor Record 92 (Flash Descriptor Records)	91
9.94	PCH Descriptor Record 93 (Flash Descriptor Records)	91
9.95	PCH Descriptor Record 94 (Flash Descriptor Records)	92
9.96	PCH Descriptor Record 95 (Flash Descriptor Records)	92
9.97	PCH Descriptor Record 96 (Flash Descriptor Records)	92
9.98	PCH Descriptor Record 97 (Flash Descriptor Records)	93
9.99	PCH Descriptor Record 98 (Flash Descriptor Records)	94
9.100	PCH Descriptor Record 99 (Flash Descriptor Records)	94
9.101	PCH Descriptor Record 100 (Flash Descriptor Records)	94
9.102	PCH Descriptor Record 101 (Flash Descriptor Records)	95
9.103	PCH Descriptor Record 102 (Flash Descriptor Records)	95
9.104	PCH Descriptor Record 103 (Flash Descriptor Records)	95
9.105	PCH Descriptor Record 104 (Flash Descriptor Records)	96
9.106	PCH Descriptor Record 105 (Flash Descriptor Records)	97
9.107	PCH Descriptor Record 106 (Flash Descriptor Records)	97
9.108	PCH Descriptor Record 107 (Flash Descriptor Records)	98
9.109	PCH Descriptor Record 108 (Flash Descriptor Records)	98
9.110	PCH Descriptor Record 109 (Flash Descriptor Records)	98
9.111	PCH Descriptor Record 110 (Flash Descriptor Records)	99

[illegible]



[illegible]



[illegible]

[illegible]

[illegible]

9.387	MIP Table Descriptor Record 3 (Flash Descriptor Records)	175
9.388	MIP Table Descriptor Record 4 (Flash Descriptor Records)	176
9.389	MIP Table Descriptor Record 5 (Flash Descriptor Records)	176
9.390	MIP Table Descriptor Record 6 (Flash Descriptor Records)	176
9.391	MIP Table Descriptor Record 7 (Flash Descriptor Records)	176
9.392	MIP Table Descriptor Record 8 (Flash Descriptor Records)	177
9.393	MIP Table Descriptor Record 9 (Flash Descriptor Records)	177
9.394	PMC Descriptor Record 0 (Flash Descriptor Records)	178
9.395	PMC Descriptor Record 1 (Flash Descriptor Records)	179
9.396	PMC Descriptor Record 2 (Flash Descriptor Records)	180
9.397	PMC Descriptor Record 3 (Flash Descriptor Records)	180
9.398	PMC Descriptor Record 4 (Flash Descriptor Records)	180
9.399	PMC Descriptor Record 5 (Flash Descriptor Records)	181
9.400	PMC Descriptor Record 6 (Flash Descriptor Records)	181
9.401	PMC Descriptor Record 7 (Flash Descriptor Records)	181
9.402	PMC Descriptor Record 8 (Flash Descriptor Records)	182
9.403	PMC Descriptor Record 9 (Flash Descriptor Records)	182
9.404	PMC Descriptor Record 10 (Flash Descriptor Records)	183
9.405	PMC Descriptor Record 11 (Flash Descriptor Records)	184
9.406	PMC Descriptor Record 12 (Flash Descriptor Records)	185
9.407	PMC Descriptor Record 13 (Flash Descriptor Records)	186
9.408	PMC Descriptor Record 14 (Flash Descriptor Records)	187
9.409	PMC Descriptor Record 15 (Flash Descriptor Records)	187
9.410	PMC Descriptor Record 16 (Flash Descriptor Records)	187
9.411	CPU Descriptor Record 0 (Flash Descriptor Records)	188
9.412	CPU Descriptor Record 1 (Flash Descriptor Records)	189
9.413	CPU Descriptor Record 2 (Flash Descriptor Records)	191
9.414	CPU Descriptor Record 3 (Flash Descriptor Records)	192
9.415	CPU Descriptor Record 4 (Flash Descriptor Records)	192
9.416	CPU Descriptor Record 5 (Flash Descriptor Records)	192
9.417	CPU Descriptor Record 6 (Flash Descriptor Records)	192
9.418	CPU Descriptor Record 7 (Flash Descriptor Records)	192
9.419	CPU Descriptor Record 8 (Flash Descriptor Records)	193
9.420	CPU Descriptor Record 9 (Flash Descriptor Records)	193
9.421	CPU Descriptor Record 10 (Flash Descriptor Records)	193
9.422	CPU Descriptor Record 11 (Flash Descriptor Records)	194
9.423	CPU Descriptor Record 12 (Flash Descriptor Records)	194
9.424	CPU Descriptor Record 13 (Flash Descriptor Records)	194
9.425	CPU Descriptor Record 14 (Flash Descriptor Records)	194
9.426	CPU Descriptor Record 15 (Flash Descriptor Records)	194
9.427	CPU Descriptor Record 16 (Flash Descriptor Records)	195
9.428	CPU Descriptor Record 17 (Flash Descriptor Records)	195
9.429	CPU Descriptor Record 18 (Flash Descriptor Records)	195
9.430	CPU Descriptor Record 19 (Flash Descriptor Records)	195
9.431	CPU Descriptor Record 20 (Flash Descriptor Records)	195
9.432	Intel® ME Descriptor Record 0 (Flash Descriptor Records)	196
9.433	Intel® ME Descriptor Record 1 (Flash Descriptor Records)	197
<b>10</b>	<b>Configuration Dependencies</b>	<b>198</b>
10.1	Descriptor Configuration Setting Enabling Dependencies	198
10.1.1	High Speed IO (HSIO) Port Enabling	198
10.1.1.1	Configuring PCIe on HSIO	201
10.1.2	Intel® Integrated LAN Controller Enabling	202
10.1.3	Intel® Wireless LAN Controller Enabling	202
10.1.4	Deep Sx Enabling Dependencies	203

10.1.5	Intel® SMBus Enabling .....	203
10.1.6	SMLink0 Enabling Dependencies .....	204
10.1.7	SMLink1 Enabling Dependencies .....	204
10.1.8	TPM over SPI Enabling Dependencies .....	205
10.1.9	mSATA/M.2 / SATA Express Enabling .....	206
10.1.9.1	SATA 0-3 / PCIe 13-16 mSATA /M.2 / SATA Express Enabling .....	206
10.1.9.2	SATA 4-7 / PCIe 17-20 mSATA /M.2 / SATA Express Enabling .....	208
10.1.10	USB 3.2 Enabling .....	210
10.1.10.1	USB 3.2 Port 1 and 2: .....	210
10.1.10.2	USB 3.2 Port 3 and 4: .....	212
10.1.10.3	USB 3.2 Port 5 and 6: .....	214
10.1.10.4	USB 3.2 Port 7 and 8: .....	216
10.1.10.5	USB 3.2 Port 9 and 10: .....	218
<b>11</b>	<b>RPMC Configuration .....</b>	<b>220</b>
11.1	System Components - High-Level Architecture Block Diagram .....	221
11.2	Monotonic counters .....	221
11.3	Binding at End of Manufacturing (EOM) .....	221
11.3.1	RPMC binding on Dual SPI configuration .....	222
11.4	Refurbish flows impact .....	222
11.4.1	PCH replacement .....	222
11.4.2	SPI replacement .....	222
11.4.3	SPI re-flash .....	222
11.5	RPMC re-binding .....	223
11.6	Tools - Intel® mFIT .....	223
<b>A</b>	<b>FAQ and Troubleshooting .....</b>	<b>224</b>

## Figures

2-1 SPI Flash Region Layout.....	21
4-1 Flash Descriptor (Raptor Lake PCH-S) .....	27
5-1 SFDP Read Instruction Sequence.....	51

## Tables

1-1 Terminology .....	17
1-2 Reference Documents.....	17
4-1 Region Access Control Table Options.....	46
4-2 Recommended Read/Write Permissions.....	47
4-3 Recommended Read/Write Settings for Platforms .....	47
4-4 Jidn - JEDEC ID Portion of Intel® ME VSCC Table.....	48
4-5 Vscn - Vendor-Specific Component Capabilities Portion of the Raptor Lake PCH Platforms .....	48
6-1 VSCC0 - Vendor-Specific Component Capabilities Register for SPI Component 0 .....	55
6-2 VSCC1 - Vendor Specific Component Capabilities Register for SPI Component 1 .....	57
6-3 Description of How WSR and WEWS is Used.....	58
10-1Raptor Lake-S Flex I/O Map.....	198
10-2HSIO Lane Muxing Selection .....	199

## Revision History

---

Document Number	Revision Number	Description	Revision Date
	0.7	<ul style="list-style-type: none"><li>Initial Release</li></ul>	March 2021
	0.8	<ul style="list-style-type: none"><li>Updated with current changes</li></ul>	August 2021
	0.81	<ul style="list-style-type: none"><li>Added note about Region 9 (FRBA + 024h)</li></ul>	November 2021



# 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 Raptor Lake PCH 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 Raptor Lake PCH 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® CSME Disable for Debug/Flash Burning Purposes"](#)

- Methods of disabling Intel Converged Security and 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 Raptor 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
Intel® 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
Raptor Lake PCH-S	Raptor Lake Platform Integrated I/O
Intel® Converged Security and Management Engine Firmware (Intel® CSME)	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 as a FWH reside
LVSCC	Lower Vendor Specific Component Capabilities
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
<i>Raptor Lake PCH-LP-S External Design Specification (EDS)</i>	Contact your Intel field representative.
<i>Intel® Flash Image Tool (FIT)</i>	\\System Tools\\Flash Image Tool of latest Intel® CSME kit from VIP. The Kit MUST match the platform you intend to use the flash tools for.
<i>Intel® Flash Programming Tool (FPT)</i>	\\System Tools\\Flash Programming Tool of latest Intel® CSME from VIP. The Kit MUST match the platform you intend to use the flash tools for.

**Table 1-2. Reference Documents**

Document	Document # / Location
<i>FW Bring Up Guide</i>	Root directory of latest Intel® Converged Security and 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 Raptor 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:** Raptor Lake only supports Descriptor mode.

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

Raptor 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 Raptor Lake PCH Family for more detailed information. 50-MHz support requires SPI component that meet 50-MHz timing.

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

Raptor Lake PCH 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 Raptor Lake PCH Family for more detailed information.

### 2.5 Boot Flow for Raptor Lake PCH Family

See Boot BIOS strap in the **Functional Straps** of the latest Intel Platform Controller Hub Family External Design Specification (EDS) for Raptor 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) <sup>1</sup>
3	GbE – Location for Integrated LAN firmware and MAC address
4	PDR – Platform Data Region (Optional) <sup>2</sup>
8	EC - Embedded Controller (Optional) <sup>3</sup>

**Notes:**

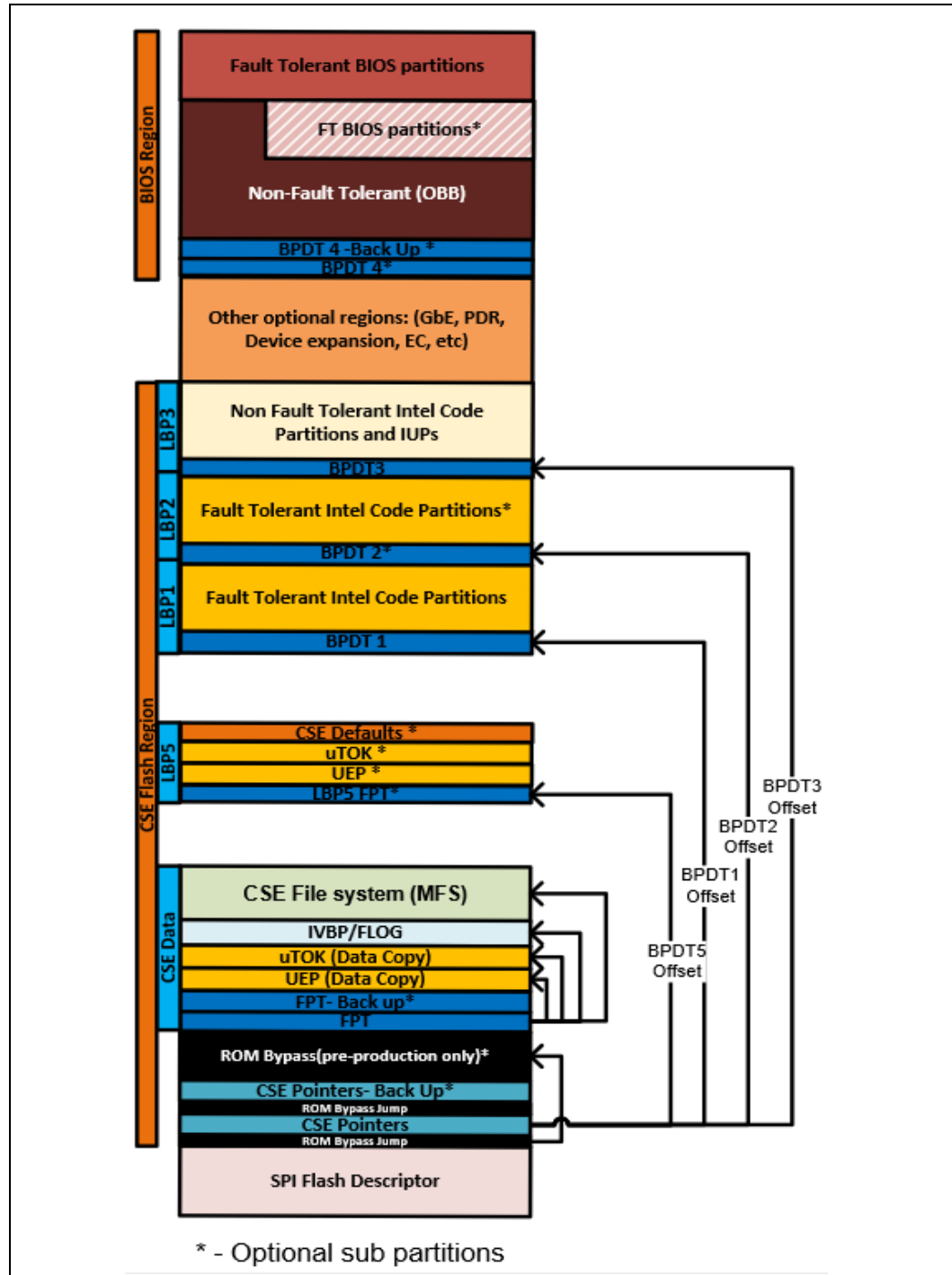
1. Also include as a part of IFWI in some instances is Intel® Management Engine (Intel® ME FW) ROM Bypass
2. The PDR region is optional and is not applicable for Raptor Lake PCH-LP or not required for proper platform operation.
3. The EC region is optional and is not required for proper platform operation.

See ***SPI Flash Regions*** section of the latest Intel Platform Controller Hub Family External Design Specification (EDS) for Raptor Lake PCH 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® CSME ROM Bypass Region:** Starting from offset 4K. This region is used for Intel® CSME ROM Bypass. When Intel® CSME ROM Bypass does not exist, this region size is 0.
2. **IFWI Region:** This region starts after the Intel® CSME 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 Raptor Lake PCH 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.

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

**Note:** Host / BIOS Software Sequencing is not supported in Raptor 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 *Raptor Lake PCH Family External Design Specification (EDS)* for more details.

§ §



# 3 PCH SPI Flash Compatibility Requirement

---

## 3.1 Raptor Lake PCH SPI Flash Requirements

- Raptor Lake PCH Family allows for up to two SPI flash devices to store BIOS, Intel® CSME FW and integrated LAN information.
  - **Intel® ME FW is required for Raptor 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 14 MHz, 25 MHz, 33 MHz and 50 MHz frequencies.
- SPI Dual Output and Dual I/O Fast Read instruction is supported at frequencies of 14 MHz, 25 MHz, 33 MHz and 50 MHz.
- SPI Quad Output and Quad I/O Fast read instruction is supported at frequencies of 14 MHz, 25 MHz, 33 MHz and 50 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 FFFFFFFh 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 Raptor Lake PCH 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](http://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	<a href="#">See Section 3.1.4 for more information</a>
Dual Output Fast Read	3Bh/ Discoverable	Discoverable opcodes are obtained from each component's SFDP table
Dual I/O Fast Read	Discoverable	Opcode is obtained from each component's SFDP table
Quad I/O Fast Read	Discoverable	Opcode is obtained from each component's SFDP table

## 3.2 Raptor Lake PCH SPI AC Electrical Compatibility Guidelines

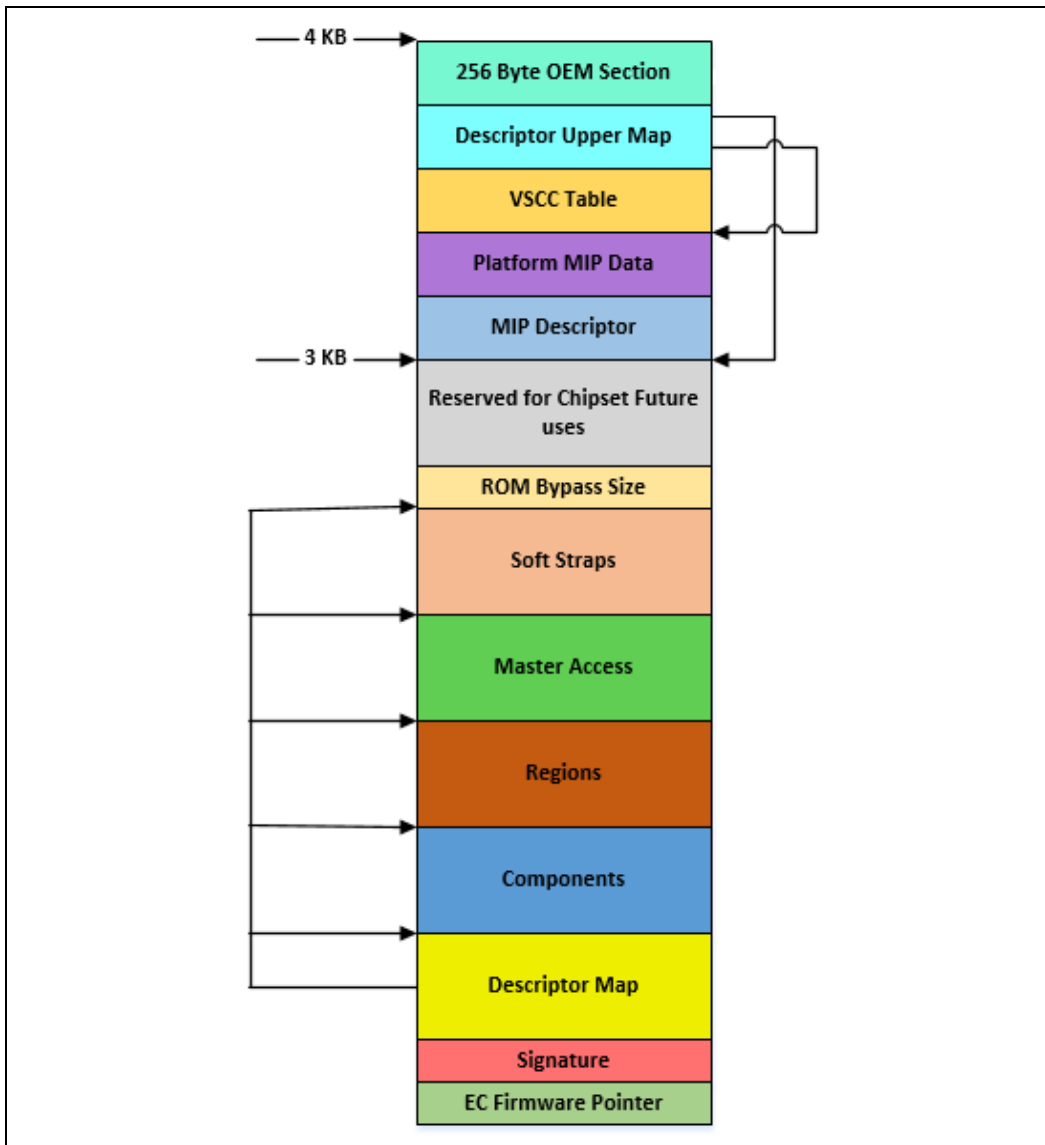
For further details on Raptor Lake electrical, thermal and timing related specifications see EDS/Raptor Lake PCH Electrical and Thermal Specifications #xxxxxx.

## 4 Descriptor Overview

The Flash Descriptor is a data structure that is programmed on the SPI flash part on Raptor 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 (Raptor Lake PCH-S)**



- EC Firmware Pointer is located in the first 16 bit 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, Intel® CSME, GbE, PDR (Optional) and Embedded Controller (EC) 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® CSME VSCC Table.
- The Intel® CSME 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 *Raptor Lake PCH 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
MDTBA	0xC00
PMC Straps	0xC14
CPU Straps	0xC60
Intel® CSME Straps	0xC90
Register Init FIBA	0x340

## 4.1.1 Descriptor Signature and Map

### 4.1.1.1 FLVALSIG - Flash Valid Signature (Flash Descriptor Records)

Memory Address: FDBAR + 010h

Size: 32 bits

Recommended Value: 0FF0A55Ah

Bits	Description	FIT Visible
31:0	<b>Flash Valid Signature.</b> 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 ( <b>Note:</b> 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	<b>Reserved</b>	No
26:24	<b>Reserved</b>	No
23:16	<b>Flash Region Base Address (FRBA).</b> 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	<b>Reserved</b>	No
12	<b>Fingerprint sensor on shared flash/TPM SPI bus</b>  0 = No fingerprint sensor is connected to CS1 1 = Fingerprint sensor is connected to CS1 and acting as a flash device  <b>Note:</b> 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	<b>Touch on dedicated SPI bus</b>  0 = No Touch device is connected to the dedicated Touch SPI bus 1 = Touch device is connected to the dedicated Touch SPI bus  <b>Note:</b> 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	<b>Touch on shared flash/TPM SPI bus</b>  0 = No Touch device is connected to CS1 1 = Touch device is connected to CS1 and acting as a flash device  <b>Note:</b> 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	<p><b>Number Of Components (NC).</b> This field identifies the total number of Flash Components. Each supported Flash Component requires a separate chip select.</p> <p>00 = 1 Component 01 = 2 Components All other settings = Reserved</p> <p><b>Note:</b> 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.</p>	Yes
7:0	<p><b>Flash Component Base Address (FCBA).</b> This identifies address bits [11:4] for the Component portion of the Flash Descriptor. Bits [24:12] and bits [3:0] are 0.</p> <p>set this field to 03h. This will define FCBA as 30h</p>	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	<b>PCH Strap Length (PSL).</b> 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 <b>MUST</b> be set to 72h	No
23:16	<b>Flash PCH Strap Base Address (FPSBA).</b> 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	<b>Number Of Masters (NM).</b> This field identifies the total number of Flash Masters. <b>Note:</b> This field is not used by the Flash Controller.	No
7:0	<b>Flash Master Base Address (FMBA).</b> 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
31:24	Reserved	No
23:16	<b>CPU Soft Strap Length</b> Represents the total number of CPU Soft Strap Dwords <b>Set to 0x14</b>	No
15:12	Reserved	No
11:2	<b>CPU Soft Strap Offset from PMC Base</b> 4 bytes aligned -- Offset of CPU straps from PMC base i.e 0xC00 (MDTBA) CPU strap pointer = MDTBA + FLMAP[11:2] <b>Set to 0x5C</b>	No
1:0	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	<b>Descriptor Major Revision ID</b>	No
20:14	<b>Descriptor Minor Revision ID</b>	No

Bits	Description	FIT Visible
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
31:30	Reserved	No
29:27	<b>Read ID and Read Status Clock Frequency.</b> 000 = 100 MHz 001 = 50 MHz 011 = 33 MHz 100 = 25 MHz 110 = 14 MHz All other Settings = Reserved  <b>Notes:</b> 1. If more than one Flash component exists, this field must be set to the lowest common frequency of the different Flash components. 2. The 100 MHz frequency setting is not supported on client. This setting is only applicable to IoTG platforms.	Yes
26:24	<b>Write and Erase Clock Frequency.</b> 000 = 100 MHz 001 = 50 MHz 011 = 33 MHz 100 = 25 MHz 110 = 14 MHz All other Settings = Reserved  <b>Notes:</b> 1. If more than one Flash component exists, this field must be set to the lowest common frequency of the different Flash components. 2. The 100 MHz frequency setting is not supported on client. This setting is only applicable to IoTG platforms.	Yes
23:21	<b>Fast Read Clock Frequency.</b> 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'. 000 = 100 MHz 001 = 50 MHz 011 = 33 MHz 100 = 25 MHz 110 = 14 MHz All other Settings = Reserved  <b>Notes:</b> 1. If more than one Flash component exists, this field must be set to the lowest common frequency of the different Flash components. 2. The 100 MHz frequency setting is not supported on client. This setting is only applicable to IoTG platforms.	Yes

Bits	Description	FIT Visible
20	<p><b>Fast Read Support.</b>  0 = Fast Read is not Supported  1 = Fast Read is supported</p> <p>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".</p> <p>Reads to the Flash Descriptor always use the Read command independent of the setting of this bit.</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. If more than one Flash component exists, this field can only be set to '1' if both components support Fast Read.</li> <li>2. It is strongly recommended to set this bit to 1b</li> </ol>	Yes
19:16	Reserved	No
15	<p><b>Quad I/O Read Enable (QIORE):</b></p> <p>0 = Quad I/O Read is disabled  1 = Quad I/O Read is enabled</p> <p>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.</p>	Yes
14	<p><b>Quad Output Read Enable (QORE):</b></p> <p>0 = Quad Output Read is disabled  1 = Quad Output Read is enabled</p> <p>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.</p>	Yes
13	<p><b>Dual I/O Read Enable (DIORE):</b></p> <p>0 = Dual I/O Read is disabled  1 = Dual I/O Read is enabled</p> <p>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.</p>	Yes
12	<p><b>Dual Output Read Enable (DORE):</b></p> <p>0 = Dual Output Read is disabled  1 = Dual Output Read is enabled</p> <p>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.</p>	Yes
11:8	Reserved	No

Bits	Description	FIT Visible
7:4	<p><b>Component 1 Density.</b> (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"</p> <p>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</p> <p><b>Note:</b> This field is defaulted to "1111b" after reset  <b>Note:</b> C1DEN field will be <b>ignored</b> if FLMAPO.NC bit [9:8] is set to 00 i.e. 1 component only.</p>	Yes
3:0	<p><b>Component 0 Density (C0DEN).</b> This field identifies the size of the 1st or only Flash component connected directly to the PCH.</p> <p>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</p> <p><b>Note:</b> This field is defaulted to "0101b" (16MB) after reset.</p>	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	<b>Invalid Instruction 3.</b> <b>Default set to 0xAD</b> See definition of Invalid Instruction 0	Yes
23:16	<b>Invalid Instruction 2.</b> <b>Default set to 0x60</b> See definition of Invalid Instruction 0	Yes
15:8	<b>Invalid Instruction 1.</b> <b>Default set to 0x42</b> See definition of Invalid Instruction 0	Yes
7:0	<b>Invalid Instruction 0.</b> <b>Default set to 0x21</b> <b>Note:</b> 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	<b>Invalid Instruction 7.</b> <b>Default set to C7</b> See definition of Invalid Instruction 0	Yes
23:16	<b>Invalid Instruction 6.</b> <b>Default set to 0xC4</b> See definition of Invalid Instruction 0	Yes
15:8	<b>Invalid Instruction 5.</b> <b>Default set to 0xB9</b> See definition of Invalid Instruction 0	Yes



Bits	Description	FIT Visible
7:0	<b>Invalid Instruction 4.</b> <b>Default set to 0xB7</b> See definition of Invalid Instruction 0	<b>Yes</b>

### 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	<b>Region Limit.</b> This specifies bits 26:12 of the ending address for this Region. <b>Notes:</b> <ol style="list-style-type: none"> <li>Set this field to 0b. This defines the ending address of descriptor as being FFFh.</li> <li>Region limit address Bits[11:0] are assumed to be FFFh</li> </ol>	No
15	Reserved	No
14:0	<b>Region Base.</b> This specifies address bits 26:12 for the Region Base. <b>Note:</b> 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	<b>Region Limit.</b> This specifies bits 26:12 of the ending address for this Region. <b>Notes:</b> <ol style="list-style-type: none"> <li>Must be set to 0000h if Intel® ME ROM Bypass region is unused (on Firmware hub)</li> <li>Ensure BIOS region size is a correct reflection of actual BIOS image that will be used in the platform</li> <li>Region limit address Bits[11:0] are assumed to be FFFh</li> </ol>	No
15	Reserved	No
14:0	<b>Region Base.</b> This specifies address bits 26:12 for the Region Base. <b>Note:</b> If the BIOS region is not used, the Region Base must be programmed to 7FFFh	No

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

Memory Address: FRBA + 008h

Size: 32 bits

Bits	Description	FIT Visible
31	Reserved	No
30:16	<b>Region Limit.</b> This specifies bits 26:12 of the ending address for this Region. <b>Notes:</b> <ol style="list-style-type: none"> <li>Ensure size is a correct reflection of IFWI size that will be used in the platform</li> <li>Region limit address Bits[11:0] are assumed to be FFFh</li> </ol>	No
15	Reserved	No
14:0	<b>Region Base.</b> 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	<b>Region Limit.</b> This specifies bits 26:12 of the ending address for this Region. <b>Notes:</b> <ol style="list-style-type: none"> <li>1. The maximum Region Limit is 128KB above the region base.</li> <li>2. If the GbE region is not used, the Region Limit must be programmed to 0000h</li> <li>3. Region limit address Bits[11:0] are assumed to be FFFh</li> </ol>	No
15	Reserved	No
14:0	<b>Region Base.</b> This specifies address bits 26:12 for the Region Base. <b>Note:</b> 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	<b>Region Limit.</b> This specifies bits 26:12 of the ending address for this Region. <b>Notes:</b> <ol style="list-style-type: none"> <li>1. If PDR Region is not used, the Region Limit must be programmed to 0000h</li> <li>2. Ensure BIOS region size is a correct reflection of actual BIOS image that will be used in the platform</li> <li>3. Region limit address Bits[11:0] are assumed to be FFFh</li> </ol>	No
15	Reserved	No
14:0	<b>Region Base.</b> This specifies address bits 26:12 for the Region Base. <b>Note:</b> 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	<b>Region Limit (RL):</b> 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	<b>Region Base.</b> 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), 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.

**Please Note:** that Region 9 (FRBA + 024h) is used by the Intel® mFIT tool for any remaining free on the SPI flash part that is not specifically used by any of the other flash regions. The value for this descriptor location is expected to vary.

## 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	<b>Master Region Write Access:</b> 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	<b>Master Region Read Access:</b> 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	<b>Extended Region Write Access:</b> 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	<b>Extended Region Read Access:</b> 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® CSME)

Memory Address: FMBA + 004h

Size:32 bits

Bits	Description	FIT Visible
31:20	<b>Master Region Write Access:</b> 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	<b>Master Region Read Access:</b> 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	<b>Extended Region Write Access:</b> 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	<b>Extended Region Read Access:</b> 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	<b>Master Region Write Access:</b> 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	<b>Master Region Read Access:</b> 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	<b>Extended Region Write Access:</b> 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.	<b>Yes</b>
3:0	<b>Extended Region Read Access:</b> 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.	<b>Yes</b>

#### 4.1.4.4 FLMSTR4—Flash Master 4 (Reserved)

Memory Address: FMBA + 00Ch

Size:32 bits

Bits	Description	FIT Visible
31:20	<b>Master Region Write Access:</b> 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	<b>No</b>
19:8	<b>Master Region Read Access:</b> 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.	<b>No</b>
7:4	<b>Extended Region Write Access:</b> 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.	<b>No</b>
3:0	<b>Extended Region Read Access:</b> 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.	<b>No</b>

#### 4.1.4.5 FLMSTR5—Flash Master 5 (EC)

Memory Address: FMBA + 010h

Size:32 bits

Bits	Description	
31:20	<b>Master Region Write Access:</b> 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	<b>Yes</b>
19:8	<b>Master Region Read Access:</b> 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.	<b>Yes</b>
7:4	<b>Extended Region Write Access:</b> 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.	<b>Yes</b>
3:0	<b>Extended Region Read Access:</b> 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.	<b>Yes</b>

#### 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	<b>MIP Descriptor Table Base Address (MDTBA).</b> 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	<b>Intel® ME VSCC Table Length (VTL).</b> 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	<b>Intel® ME VSCC Table Base Address (VTBA).</b> 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® CSME ROM Bypass Size

Memory Address: FDBAR + C00h

Size: 32 bits

Bits	Default	Description	FIT Visible
31:0	0xFF	<b>ROM BYPASS Size.</b> ROM reads this value to determine the size of the region. <b>Only applicable for A0 stepping.</b>	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  <b>Note:</b> In order to simplify handling a new block type can be defined for each usage	Yes
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

Name	Offset	Size (bytes)	Description	FIT Visible
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® CSME Vendor Specific Component Capabilities Table

Entries in this table allow support for a SPI flash part for Intel® Converged Security and 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 Raptor Lake PCH. 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 4.3 Intel® CSME Vendor-Specific Component Capabilities (Intel® CSME 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	<b>SPI Component Device ID 1.</b> 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	<b>SPI Component Device ID 0.</b> 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	<b>SPI Component Vendor ID.</b> 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	<b>Erase Opcode (EO).</b> This field must be programmed with the Flash erase instruction opcode that corresponds to the erase size that is in BES.	No



Bits	Description	FIT Visible
7:5	<b>Quad Enable Requirements (QER)</b> 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 <b>Note:</b> Please refer to Table note#1 below for details.	No
4:0	<b>Reserved set to 00101b</b>	No
<b>Notes:</b> 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.

## 4.2.1 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
Intel® ME Data (15)	Not Accessible	Read / Write	Not Accessible	Not Accessible
<b>Notes:</b> <ol style="list-style-type: none"> <li>1. The Region Access values listed above represent post manufacturing configuration only.</li> <li>2. Descriptor and PDR region is not a master, so they will not have Master R/W access.</li> <li>3. Descriptor should NOT have write access by any master in production systems.</li> <li>4. PDR region should only have read and/or write access by CPU/Host. GbE and ME should NOT have access to PDR region.</li> </ol>				

## 4.2.2 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:**

- ‡ = Host access to PDR is the discretion of the customer. Implementation of PDR is optional.
- † = Optional BIOS access to the EC region.
- \* = 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‡ 1111 = 0x0†‡F	0b 0000 0001 0000 00*1 = 0x0101 or 0x0103
Write	0b 0000 0000 0000 1100 = 0x0004	0b 0000 0000 0000 1000 = 0x0008	0b 0000 000† 000‡ 1010 = 0x0†‡A	0b 0000 0001 0000 0000 = 0x0100

**Note:**

- ‡ = Value dependent on if PDR is implemented and if Host access is desired.
- † = Optional BIOS access to the EC region.
- \* = Optional EC Read access to BIOS.

## 4.2.3 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.

## 4.3 Intel® CSME Vendor-Specific Component Capabilities (Intel® CSME VSCC) Table

The Intel® CSME VSCC Table defines how the Intel® CSME 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	<b>SPI Component Device ID 1:</b> 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	<b>SPI Component Device ID 0:</b> 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	<b>SPI Component Vendor ID:</b> 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® CSME 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 How to Set a VSCC Entry in Intel® CSME VSCC Table for Raptor Lake PCH 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) VSCC0 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 [4.4.1 Intel® CSME VSCC Table Settings for Raptor Lake PCH Family Systems](#).

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

**Table 4-5. Vscn – Vendor-Specific Component Capabilities Portion of the Raptor Lake PCH Platforms (Sheet 1 of 2)**

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

**Table 4-5. Vscn – Vendor-Specific Component Capabilities Portion of the Raptor Lake PCH Platforms (Sheet 2 of 2)**

Bits	Description	FIT Visible
7:5	<b>Quad Enable Requirements (QER)</b> 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).  <b>Note:</b> Please refer to Table note#6 below for details.	No
4	<b>Write Enable on Write Status (WEWS)</b> 0 = 50h is the opcode used to unlock the status register on SPI flash if <b>WSR</b> (bit 3) is set to 1b. 1 = 06h is the opcode used to unlock the status register on SPI flash if <b>WSR</b> (bit 3) is set to 1b. <b>Note:</b> Please refer to Table Note #4 below for a description how this bit is used.	No
3	<b>Write Status Required (WSR)</b> 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. <b>Note:</b> Please refer to Table Note #5 below for a description how this bit is used.	No
2	<b>Write Granularity (WG).</b> 0 = 1 Byte 1 = 64 Bytes	No
1:0	<b>Block/Sector Erase Size (BES).</b> 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
<b>Notes:</b> 1. Bit 3 ( <b>WEWS</b> ) and/or bit 4 ( <b>WSR</b> ) 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 ( <b>WSR</b> ) and 4 ( <b>WEWS</b> ) 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 ( <b>WSR</b> ) is set to 1b and bit 4 ( <b>WEWS</b> ) 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 ( <b>WSR</b> ) is set to 0b and bit 4 ( <b>WEWS</b> ) 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 be 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 be 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 be 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 Raptor Lake PCH 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 be set to all zeros.

#### 4.4.1 Intel® CSME VSCC Table Settings for Raptor Lake PCH 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.

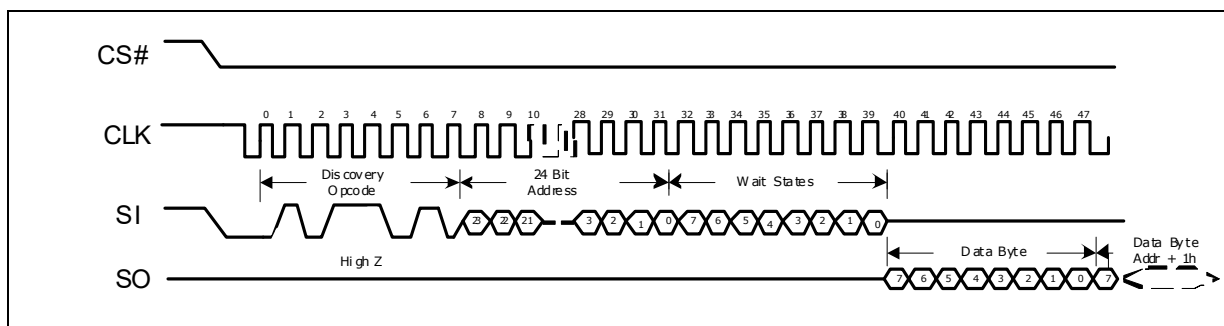
These guidelines are a standard that will allow for individual vendors to have their value add features, but will allow for a controller to discover the attributes needed to operate.

### 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](http://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 Raptor Lake PCH 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 Intel® CSME or GbE regions.

All the SPI flash devices that meet the SPI flash requirements in the *Raptor Lake-S PCH 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 *Raptor Lake PCH-S 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® CSME FW and/or integrated GbE. BIOS must ensure that any flash based protection will apply to BIOS region only. It should not affect the Intel® CSME 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+4h bit 13))** is set, do not set a Protected range to cover the Intel® CSME 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® CSME 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 Programming Registers section in the Raptor Lake PCH 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 Raptor Lake PCH 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 Raptor Lake PCH-. VSCC0 is for SPI component 0 and VSCC1 is for SPI component 1. SPI controller will determine which VSCC (VSCC0 or VSCC1) to be used by comparing Flash Linear Address (FLA) with size of SPI component 0 (C0DEN). When  $FLA \leq C0DEN$  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 Raptor Lake PCH 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	<b>Component Property Parameter Table Valid (CPPTV) - RO:</b> 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 ( <b>VCL</b> ) 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	<p><b>Erase Opcode (EO)</b>— 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</p> <p>This register is locked by the Vendor Component Lock (<b>VCL</b>) bit.</p> <p><b>Note:</b> If CPPTV is 1 and the SPDP0 table shows 4k erase capability, the SFDP0 erase code is used instead of this register</p>
7:5	<p><b>Quad Enable Requirements (QER)</b> 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).</p> <p><b>Note:</b> This register is locked by the Vendor Component Lock (VCL) bit.</p>
4	<p><b>Write Enable on Write Status (WEWS)</b> — RW: '0' = 50h will be the opcode used to unlock the status register on the SPI flash if <b>WSR</b> (bit 3) is set to 1b. '1' = 06h will be the opcode used to unlock the status register on the SPI flash if <b>WSR</b> (bit 3) is set to 1b.</p> <p>This register is locked by the Vendor Component Lock (VCL) bit.</p> <p><b>Note:</b> Please refer to <a href="#">Table 6-3</a> for a description of how these bits is used.</p>
3	<p><b>Write Status Required (WSR)</b> — 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.</p> <p>This register is locked by the Vendor Component Lock (<b>VCL</b>) bit.</p> <p><b>Note:</b> Please refer to <a href="#">Table 6-3</a> for a description of how these bits is used.</p>
2	<p><b>Write Granularity (WG)</b> — RW: 0: 1 Byte 1: 64 Byte This register is locked by the Vendor Component Lock (<b>VCL</b>) bit.</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>If more than one Flash component exists, this field must be set to the lowest common write granularity of the different Flash components</li> <li>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.</li> </ol>

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

Bit	Description
1:0	<p><b>Block/Sector Erase Size (BES)— RW:</b>  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 (<b>VCL</b>) 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.</p>

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

Bit	Description
31	<p><b>Component Property Parameter Table Valid (CPPTV) - RO:</b>  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.</p>
30:16	Reserved
15:8	<p><b>Erase Opcode (EO)— RW:</b>  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 (<b>VCL</b>) bit.</p>
7:5	<p><b>Quad Enable Requirements (QER)</b>  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).  <b>Note:</b> This register is locked by the Vendor Component Lock (VCL) bit.</p>
4	<p><b>Write Enable on Write to Status (WEWS) — RW:</b>  '0' = 50h will be the opcode used to unlock the status register if <b>WSR</b> (bit 3) is set to 1b.  '1' = 06h will be the opcode used to unlock the status register if <b>WSR</b> (bit 3) is set to 1b.  This register is locked by the Vendor Component Lock (<b>VCL</b>) bit.  Please refer to <a href="#">Table 6-3</a> for a description of how these bits is used.</p>

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

Bit	Description
3	<p><b>Write Status Required (WSR)</b> — RW:</p> <p>'0' = No automatic write of 00h will be made to the SPI flash's status register</p> <p>'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.</p> <p>This register is locked by the Vendor Component Lock (<b>VCL</b>) bit.</p> <p><b>Note:</b> Please refer to <a href="#">Table 6-3</a> for a description of how these bits is used.</p>
2	<p><b>Write Granularity (WG)</b> — RW:</p> <p>0: 1 Byte</p> <p>1: 64 Byte</p> <p>This register is locked by the Vendor Component Lock (<b>VCL</b>) bit.</p> <p>If more than one Flash component exists, this field must be set to the lowest common write granularity of the different Flash components.</p> <p>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.</p>
1:0	<p><b>Block/Sector Erase Size (BES)</b>— RW: This field identifies the erasable sector size for all Flash components.</p> <p>Valid Bit Settings:</p> <p>00: 256 Byte</p> <p>01: 4 KByte</p> <p>10: 8 KByte</p> <p>11: 64 K</p> <p>This register is locked by the Vendor Component Lock (<b>VCL</b>) bit.</p> <p>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.</p>

**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 Raptor Lake PCH 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® CSME Disable for Debug/Flash Burning Purposes

---

This section is purely for debug purposes. Intel® CSME FW is the only supported configuration for Raptor Lake PCH based system.

## 7.1 IFWI / Intel® CSME Disable

Here are the ways one can disable the Intel® CSME 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 Intel® CSME region unlock - There is a HECI command that allows Intel® CSME 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® CSME functionality.

### 7.1.1 Erasing/Programming Intel® CSME Region

If CPU/Host has access to Intel® CSME region, then one could either erase/program the Intel® CSME 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® CSME when erasing any address in IFWI region.

§ §



## 8 Recommendations for SPI Flash Programming in Manufacturing Environments

---

It is recommended that the Intel® CSME be disabled when you are programming the Intel® CSME region. Intel® CSME FW performs regular writes/erases to the Intel® CSME 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® CSME FW. The following methods are for Intel® CSME 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
0x100	7:0	Reserved, set to '0x8'		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
0x101	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
0x102	7:0	Reserved, set to '0xF0'		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
0x103	7:0	Reserved, set to '0x1F'		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
0x104	7:0	Reserved, set to '0x8'		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
0x105	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
0x106	7:0	Reserved, set to '0xF0'		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
0x107	7:0	Reserved, set to '0x1F'		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
0x108	7:0	Reserved, set to '0x8'		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
0x109	7:0	Reserved, set to '0'		No

## 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
0x10A	7:0	Reserved, set to '0xF0'		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
0x10B	7:0	Reserved, set to '0x1F'		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
0x10C	7:0	Reserved, set to '0x8'		No

## 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
0x10D	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
0x10E	7:0	Reserved, set to '0xF0'		No

## 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
0x10F	7:0	Reserved, set to '0x1F'		No

## 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
0x110	7:0	Reserved, set to '0x8'		No

## 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
0x111	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
0x112	7:0	Reserved, set to '0xF0'		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
0x113	7:0	Reserved, set to '0x1F'		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
0x114	7:0	Reserved, set to '0x8'		No

## 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
0x115	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
0x116	7:0	Reserved, set to '0xF0'		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
0x117	7:0	Reserved, set to '0x1F'		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
0x118	7:0	Reserved, set to '0x8'		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
0x119	7:0	Reserved, set to '0xF0'		No

## 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
0x11A	7:0	Reserved, set to '0x1F'		No

## 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
0x11B	7:0	Reserved, set to '0'		No

## 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
0x11C	7:0	Reserved, set to '0xF8'		No

### 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
0x11D	15:0	Reserved, set to '0xF000'		No

### 9.31 PCH Descriptor Record 30 (Flash Descriptor Records)

Flash Address: FPSBA + 01Fh

Default Flash Address: 11Fh

Offset from 0	Bits	Description	Usage	FIT Visible
0x11F	7:0	Reserved, set to '0'		No

### 9.32 PCH Descriptor Record 31 (Flash Descriptor Records)

Flash Address: FPSBA + 020h

Default Flash Address: 120h

Offset from 0	Bits	Description	Usage	FIT Visible
0x120	7:0	Reserved, set to '0xF8'		No

### 9.33 PCH Descriptor Record 32 (Flash Descriptor Records)

Flash Address: FPSBA + 021h

Default Flash Address: 121h

Offset from 0	Bits	Description	Usage	FIT Visible
0x121	15:0	Reserved, set to '0xF000'		No

### 9.34 PCH Descriptor Record 33 (Flash Descriptor Records)

Flash Address: FPSBA + 023h

Default Flash Address: 123h

Offset from 0	Bits	Description	Usage	FIT Visible
0x123	7:0	Reserved, set to '0'		No



## 9.35 PCH Descriptor Record 34 (Flash Descriptor Records)

Flash Address: FPSBA + 024h

Default Flash Address: 124h

Offset from 0	Bits	Description	Usage	FIT Visible
0x124	7:0	Reserved, set to '0xF8'		No

## 9.36 PCH Descriptor Record 35 (Flash Descriptor Records)

Flash Address: FPSBA + 025h

Default Flash Address: 125h

Offset from 0	Bits	Description	Usage	FIT Visible
0x125	15:0	Reserved, set to '0xF000'		No

## 9.37 PCH Descriptor Record 36 (Flash Descriptor Records)

Flash Address: FPSBA + 027h

Default Flash Address: 127h

Offset from 0	Bits	Description	Usage	FIT Visible
0x127	7:0	Reserved, set to '0'		No

## 9.38 PCH Descriptor Record 37 (Flash Descriptor Records)

Flash Address: FPSBA + 028h

Default Flash Address: 128h

Offset from 0	Bits	Description	Usage	FIT Visible
0x128	31:0	Reserved, set to '0'		No

## 9.39 PCH Descriptor Record 38 (Flash Descriptor Records)

Flash Address: FPSBA + 02Ch

Default Flash Address: 12Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x12C	7:1	Reserved, set to '0'		No
	0	<b>GPP_D Group Master Voltage Select (GPPD_VCCIO):</b>  0x0 = GPP_D Master Voltage Select set to 3.3v 0x1 = GPP_D Master Voltage Select set to 1.8v	This setting controls configures the VCCIO voltage for all of the GPP_D GPIO pins.  <b>Note:</b> When a GPIO is configured as 1.8V or 3.3V, both the group power pin and the voltage configuration soft strap setting must be set to the corresponding voltage. Any PU on the signal then needs to be pulled to the correct voltage as well.	Yes

## 9.40 PCH Descriptor Record 39 (Flash Descriptor Records)

Flash Address: FPSBA + 02Dh

Default Flash Address: 12Dh

Offset from 0	Bits	Description	Usage	FIT Visible
0x12D	7:0	Reserved, set to '0'		No

## 9.41 PCH Descriptor Record 40 (Flash Descriptor Records)

Flash Address: FPSBA + 02Eh

Default Flash Address: 12Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0x12E	7:0	Reserved, set to '0'		No

## 9.42 PCH Descriptor Record 41 (Flash Descriptor Records)

Flash Address: FPSBA + 02Fh

Default Flash Address: 12Fh

Offset from 0	Bits	Description	Usage	FIT Visible
0x12F	7:0	Reserved, set to '0'		No

## 9.43 PCH Descriptor Record 42 (Flash Descriptor Records)

Flash Address: FPSBA + 030h

Default Flash Address: 130h

Offset from 0	Bits	Description	Usage	FIT Visible
0x130	7:3	Reserved, set to '0'		No
	2	<b>GPP_F Group Master Voltage Select (GPPF_VCCIO):</b>  0x0 = GPP_F Master Voltage Select set to 3.3v 0x1 = GPP_F Master Voltage Select set to 1.8v	This setting controls configures the VCCIO voltage for all of the GPP_F GPIO pins.  <b>Note:</b> When a GPIO is configured as 1.8V or 3.3V, both the group power pin and the voltage configuration soft strap setting must be set to the corresponding voltage. Any PU on the signal then needs to be pulled to the correct voltage as well.	Yes
	1	<b>GPP_K Group Master Voltage Select (GPPK_VCCIO):</b>  0x0 = GPP_K Master Voltage Select set to 3.3v 0x1 = GPP_K Master Voltage Select set to 1.8v	This setting controls configures the VCCIO voltage for all of the GPP_K GPIO pins.  <b>Note:</b> When a GPIO is configured as 1.8V or 3.3V, both the group power pin and the voltage configuration soft strap setting must be set to the corresponding voltage. Any PU on the signal then needs to be pulled to the correct voltage as well.	Yes
	0	<b>GPP_E Group Master Voltage Select (GPPE_VCCIO):</b>  0x0 = GPP_E Master Voltage Select set to 3.3v 0x1 = GPP_E Master Voltage Select set to 1.8v	This setting controls configures the VCCIO voltage for all of the GPP_E GPIO pins.  <b>Note:</b> When a GPIO is configured as 1.8V or 3.3V, both the group power pin and the voltage configuration soft strap setting must be set to the corresponding voltage. Any PU on the signal then needs to be pulled to the correct voltage as well.	Yes

## 9.44 PCH Descriptor Record 43 (Flash Descriptor Records)

Flash Address: FPSBA + 031h

Default Flash Address: 131h

Offset from 0	Bits	Description	Usage	FIT Visible
0x131	7:0	Reserved, set to '0'		No

## 9.45 PCH Descriptor Record 44 (Flash Descriptor Records)

Flash Address: FPSBA + 032h

Default Flash Address: 132h

Offset from 0	Bits	Description	Usage	FIT Visible
0x132	7:6	<b>SATA / PCIe GP Select for Port 3 (SATA_PCIE_GP3):</b>  0x0 = PCIe Port 16 is statically assigned to SATA Port 3 0x1 = PCIe Port 16 is statically assigned to PCIe (or GbE) 0x3 = Assigned based on the polarity of SATAXPcie2 determined by SPS2	This strap must also be configured when setting the PCIe / SATA Combo Port 5 ( <b>FIA/LOSL29</b> ).  <b>Note:</b> This strap and the PCIe / SATA Combo Port 6 ( <b>FIA/LOSL29</b> ) and ( <b>SATA_PCIE_SP3</b> ) must match for proper port function.  <b>Note:</b> For unused SATA/PCIe* Combo Lanes, Flex I/O Lanes that can be configured as PCIe* or SATA, the lanes must be statically assigned to SATA or PCIe*. These unused SATA/PCIe* Combo Lanes must not be assigned as polarity based.	No
	5:4	<b>SATA / PCIe GP Select for Port 2 (SATA_PCIE_GP2):</b>  0x0 = PCIe Port 15 is statically assigned to SATA Port 2 0x1 = PCIe Port 15 is statically assigned to PCIe (or GbE) 0x3 = Assigned based on the polarity of SATAXPcie2 determined by SPS2	This strap must also be configured when setting the PCIe / SATA Combo Port 4 ( <b>FIA/LOSL28</b> ).  <b>Note:</b> This strap and the PCIe / SATA Combo Port 5 ( <b>FIA/LOSL28</b> ) and ( <b>SATA_PCIE_SP2</b> ) must match for proper port function.  <b>Note:</b> For unused SATA/PCIe* Combo Lanes, Flex I/O Lanes that can be configured as PCIe* or SATA, the lanes must be statically assigned to SATA or PCIe*. These unused SATA/PCIe* Combo Lanes must not be assigned as polarity based.	No
	3:2	<b>SATA / PCIe GP Select for Port 1 (SATA_PCIE_GP1):</b>  0x0 = PCIe Port 12 or PCIe Port 14 is statically assigned to SATA Port 1 0x1 = PCIe Port 12 or PCIe Port 14 is statically assigned to PCIe (or GbE) 0x3 = Assigned based on the polarity of SATAXPcie1 determined by SPS1	This strap must also be configured when setting the PCIe / SATA Combo Port 1 Strap ( <b>FIA/LOSL25</b> ) or SATA / PCIe Combo Port 3 Strap ( <b>FIA/LOSL27</b> ).  <b>Note:</b> This strap and the PCIe / SATA Combo Port 1 Strap ( <b>FIA/LOSL25</b> ) or PCIe / SATA Combo Port 3 Strap ( <b>FIA/LOSL27</b> ) and ( <b>SATA_PCIE_SP1</b> ) must match for proper port function.  <b>Note:</b> For unused SATA/PCIe* Combo Lanes, Flex I/O Lanes that can be configured as PCIe* or SATA, the lanes must be statically assigned to SATA or PCIe*. These unused SATA/PCIe* Combo Lanes must not be assigned as polarity based.	No

Offset from 0	Bits	Description	Usage	FIT Visible
0x132 (Cont)	1:0	<b>SATA / PCIe GP Select for Port 0 (SATA_PCIE_GP0):</b>  0x0 = PCIe Port 11 or Port 13 is statically assigned to SATA Port 0 0x1 = PCIe Port 11 or Port 13 is statically assigned to PCIe (or GbE) 0x3 = Assigned based on the polarity of SATAXPCEIO determined by SPS0	This strap must also be configured when setting the PCIe / SATA Combo Port 0 ( <b>FIA/LOSL24</b> ) or SATA Combo Port 2 ( <b>FIA/LOSL26</b> ).  <b>Note:</b> This strap and the PCIe / SATA Combo Port 0 ( <b>FIA/LOSL24</b> ) or PCIe /SATA Combo Port 2 Strap ( <b>FIA/LOSL26</b> ) and ( <b>SATA_PCIE_SP0</b> ) must match for proper port function.  <b>Note:</b> For unused SATA/PCIe* Combo Lanes, Flex I/O Lanes that can be configured as PCIe* or SATA, the lanes must be statically assigned to SATA or PCIe*. These unused SATA/PCIe* Combo Lanes must not be assigned as polarity based.	No

## 9.46 PCH Descriptor Record 45 (Flash Descriptor Records)

Flash Address:FPSBA + 033h

Default Flash Address: 133h

Offset from 0	Bits	Description	Usage	FIT Visible
0x133	7:6	<b>SATA / PCIe GP Select for Port 7 (SATA_PCIE_GP7):</b>  0x0 = PCIe Port 20 is statically assigned to SATA Port 7 0x1 = PCIe Port 20 is statically assigned to PCIe (or GbE) 0x3 = Assigned based on the polarity of SATAXPCEIO determined by SPS0	This strap must also be configured when setting the PCIe / SATA Combo Port 9 ( <b>FIA/LOSL33</b> ).  <b>Note:</b> This strap and the PCIe / SATA Combo Port 9 ( <b>FIA/LOSL33</b> ) and ( <b>SATA_PCIE_SP7</b> ) must match for proper port function.  <b>Note:</b> For unused SATA/PCIe* Combo Lanes, Flex I/O Lanes that can be configured as PCIe* or SATA, the lanes must be statically assigned to SATA or PCIe*. These unused SATA/PCIe* Combo Lanes must not be assigned as polarity based.	No
	5:4	<b>SATA / PCIe GP Select for Port 6 (SATA_PCIE_GP6):</b>  0x0 = PCIe Port 19 is statically assigned to SATA Port 6 0x1 = PCIe Port 19 is statically assigned to PCIe (or GbE) 0x3 = Assigned based on the polarity of SATAXPCEIO determined by SPS0	This strap must also be configured when setting the PCIe / SATA Combo Port 8 ( <b>FIA/LOSL32</b> ).  <b>Note:</b> This strap and the PCIe / SATA Combo Port 8 ( <b>FIA/LOSL32</b> ) and ( <b>SATA_PCIE_SP6</b> ) must match for proper port function.  <b>Note:</b> For unused SATA/PCIe* Combo Lanes, Flex I/O Lanes that can be configured as PCIe* or SATA, the lanes must be statically assigned to SATA or PCIe*. These unused SATA/PCIe* Combo Lanes must not be assigned as polarity based.	No

Offset from 0	Bits	Description	Usage	FIT Visible
0x133 (Cont)	3:2	<b>SATA / PCIe GP Select for Port 5 (SATA_PCIE_GP5):</b>  0x0 = PCIe Port 18 is statically assigned to SATA Port 5 0x1 = PCIe Port 18 is statically assigned to PCIe (or GbE) 10 = Reserved 0x3 = Assigned based on the polarity of SATAXPcie0 determined by SPS0	This strap must also be configured when setting the PCIe / SATA Combo Port 7 ( <b>FIA/LOSL31</b> ).  <b>Note:</b> This strap and the PCIe / SATA Combo Port 7 ( <b>FIA/LOSL31</b> ) and ( <b>SATA_PCIE_SP5</b> ) must match for proper port function.  <b>Note:</b> For unused SATA/PCIe* Combo Lanes, Flex I/O Lanes that can be configured as PCIe* or SATA, the lanes must be statically assigned to SATA or PCIe*. These unused SATA/PCIe* Combo Lanes must not be assigned as polarity based.	No
	1:0	<b>SATA / PCIe GP Select for Port 4 (SATA_PCIE_GP4):</b>  0x0 = PCIe Port 17 is statically assigned to SATA Port 4 0x1 = PCIe Port 17 is statically assigned to PCIe (or GbE) 10 = Reserved 0x3 = Assigned based on the polarity of SATAXPcie0 determined by SPS0	This strap must also be configured when setting the PCIe / SATA Combo Port 6 ( <b>FIA/LOSL30</b> ).  <b>Note:</b> This strap and the PCIe / SATA Combo Port 6 ( <b>FIA/LOSL30</b> ) and ( <b>SATA_PCIE_SP4</b> ) must match for proper port function.  <b>Note:</b> For unused SATA/PCIe* Combo Lanes, Flex I/O Lanes that can be configured as PCIe* or SATA, the lanes must be statically assigned to SATA or PCIe*. These unused SATA/PCIe* Combo Lanes must not be assigned as polarity based.	No

## 9.47 PCH Descriptor Record 46 (Flash Descriptor Records)

Flash Address: FPSBA + 034h

Default Flash Address: 134h

Offset from 0	Bits	Description	Usage	FIT Visible
0x134	7:2	Reserved, set to '0'		No
	1	<b>Intel® SMBus ASD Mode Configuration (SMBALERTB):</b>  0x0 = Configured as GPP_C2 0x1 = Configured as Intel® SMBus ASD	This setting determines the native mode for the SMBAlert signal.	Yes
	0	<b>GPP_C Group Master Voltage Select (GPPC_VCCIO):</b>  0x0 = GPP_C Master Voltage Select set to 3.3v 0x1 = GPP_C Master Voltage Select set to 1.8v	This setting controls configures the VCCIO voltage for all of the GPP_C GPIO pins.  <b>Note:</b> When a GPIO is configured as 1.8V or 3.3V, both the group power pin and the voltage configuration soft strap setting must be set to the corresponding voltage. Any PU on the signal then needs to be pulled to the correct voltage as well.	Yes

## 9.48 PCH Descriptor Record 47 (Flash Descriptor Records)

Flash Address: FPSBA + 035h

Default Flash Address: 135h

Offset from 0	Bits	Description	Usage	FIT Visible
0x135	7:0	Reserved, set to '0'		No

## 9.49 PCH Descriptor Record 48 (Flash Descriptor Records)

Flash Address: FPSBA + 036h

Default Flash Address: 136h

Offset from 0	Bits	Description	Usage	FIT Visible
0x136	7:0	Reserved, set to '0'		No

## 9.50 PCH Descriptor Record 49 (Flash Descriptor Records)

Flash Address: FPSBA + 037h

Default Flash Address: 137h

Offset from 0	Bits	Description	Usage	FIT Visible
0x137	7:0	Reserved, set to '0'		No

## 9.51 PCH Descriptor Record 50 (Flash Descriptor Records)

Flash Address: FPSBA + 038h

Default Flash Address: 138h

Offset from 0	Bits	Description	Usage	FIT Visible
0x138	7:6	Reserved, set to '0'		No
	5	SLP_S5# / GPD10 Signal Configuration:  0x0 = Use as SLP_S5# 0x1 = Use as GPD10		Yes
	4	LAN PHY Power Control GPD11 Signal Configuration:  0x0 = Use as LANPHYPC 0x1 = Use as GPD11  <b>Note:</b> 4. LANPHYPC can only be driven low if SLP_LAN# is deasserted. 5. Signal can instead be used as GPD11.	<b>LAN PHY Power Control:</b> 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

Offset from 0	Bits	Description	Usage	FIT Visible
<b>0x138 (Cont)</b>	3	<b>SLP_WLAN# / GPD9 Signal Configuration:</b>  0x0 = Use as SLP_WLAN# 0x1 = Use as GPD9	<b>LAN Sub-System Sleep Control:</b> 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.	<b>Yes</b>
	2	<b>SLP_A# / GPD6 Signal Configuration:</b>  0x0 = Use as SLP_A# 0x1 = Use as GPD6		<b>Yes</b>
	1	<b>SLP_S4# / GPD5 Signal Configuration:</b>  0x0 = Use as SLP_S4# 0x1 = Use as GPD5		<b>Yes</b>
	0	<b>SLP_S3# / GPD4 Signal Configuration:</b>  0x0 = Use as SLP_S3# 0x1 = Use as GPD4		<b>Yes</b>

## 9.52 PCH Descriptor Record 51 (Flash Descriptor Records)

Flash Address:FPSBA + 039h

Default Flash Address: 139h

Offset from 0	Bits	Description	Usage	FIT Visible
<b>0x139</b>	7:0	<b>Reserved, set to '0'</b>		<b>No</b>

## 9.53 PCH Descriptor Record 52 (Flash Descriptor Records)

Flash Address:FPSBA + 03Ah

Default Flash Address: 13Ah

Offset from 0	Bits	Description	Usage	FIT Visible
<b>0x13A</b>	7:0	<b>Reserved, set to '0'</b>		<b>No</b>

## 9.54 PCH Descriptor Record 53 (Flash Descriptor Records)

Flash Address:FPSBA + 03Bh

Default Flash Address: 13Bh

Offset from 0	Bits	Description	Usage	FIT Visible
<b>0x13B</b>	7:0	<b>Reserved, set to '0'</b>		<b>No</b>



## 9.55 PCH Descriptor Record 54 (Flash Descriptor Records)

Flash Address: FPSBA + 03Ch

Default Flash Address: 13Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x13C	7:4	Reserved, set to '0'		No
	3	<b>Clockout 48 Mode Configuration (CLKOUT_48):</b>  0x0 = Configured as CLKOUT_48 0x1 = Configured as GPP_B6	This setting determines the native mode for the Clockout 48 signal.	Yes
	2	<b>GPP_H Group Master Voltage Select (GPPH_VCCIO):</b>  0x0 = GPP_H Master Voltage Select set to 3.3v 0x1 = GPP_H Master Voltage Select set to 1.8v	This setting controls configures the VCCIO voltage for all of the GPP_H GPIO pins.  <b>Note:</b> When a GPIO is configured as 1.8V or 3.3V, both the group power pin and the voltage configuration soft strap setting must be set to the corresponding voltage. Any PU on the signal then needs to be pulled to the correct voltage as well.	Yes
	1	<b>GPP_G Group Master Voltage Select (GPPG_VCCIO):</b>  0x0 = GPP_G Master Voltage Select set to 3.3v 0x1 = GPP_G Master Voltage Select set to 1.8v	This setting controls configures the VCCIO voltage for all of the GPP_G GPIO pins.  <b>Note:</b> When a GPIO is configured as 1.8V or 3.3V, both the group power pin and the voltage configuration soft strap setting must be set to the corresponding voltage. Any PU on the signal then needs to be pulled to the correct voltage as well.	Yes
	0	<b>GPP_B Group Master Voltage Select (GPPB_VCCIO):</b>  0x0 = GPP_B Master Voltage Select set to 3.3v 0x1 = GPP_B Master Voltage Select set to 1.8v	This setting controls configures the VCCIO voltage for all of the GPP_B GPIO pins.  <b>Note:</b> When a GPIO is configured as 1.8V or 3.3V, both the group power pin and the voltage configuration soft strap setting must be set to the corresponding voltage. Any PU on the signal then needs to be pulled to the correct voltage as well.	Yes

## 9.56 PCH Descriptor Record 55 (Flash Descriptor Records)

Flash Address: FPSBA + 03Dh

Default Flash Address: 13Dh

Offset from 0	Bits	Description	Usage	FIT Visible
0x13D	7:0	Reserved, set to '0'		No

## 9.57 PCH Descriptor Record 56 (Flash Descriptor Records)

Flash Address: FPSBA + 03Eh

Default Flash Address: 13Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0x13E	7:0	Reserved, set to '0'		No

## 9.58 PCH Descriptor Record 57 (Flash Descriptor Records)

Flash Address: FPSBA + 03Fh

Default Flash Address: 13Fh

Offset from 0	Bits	Description	Usage	FIT Visible
0x13F	7:0	Reserved, set to '0'		No

## 9.59 PCH Descriptor Record 58 (Flash Descriptor Records)

Flash Address: FPSBA + 040h

Default Flash Address: 140h

Offset from 0	Bits	Description	Usage	FIT Visible
0x140	7:3	Reserved, set to '0'		No
	2	<b>GPP_J Group Master Voltage Select (GPPJ_VCCIO):</b>  0x0 = GPP_J Master Voltage Select set to 3.3v 0x1 = GPP_J Master Voltage Select set to 1.8v	This setting controls configures the VCCIO voltage for all of the GPP_J GPIO pins.  <b>Note:</b> When a GPIO is configured as 1.8V or 3.3V, both the group power pin and the voltage configuration soft strap setting must be set to the corresponding voltage. Any PU on the signal then needs to be pulled to the correct voltage as well.	Yes
	1	<b>Intel® HD Audio Voltage Select (GPPR_VCCIO):</b>  0x0 = Intel® HD Audio Voltage Select to 3.3v 0x1 = 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.  <b>Note:</b> When a GPIO is configured as 1.8V or 3.3V, both the group power pin and the voltage configuration soft strap setting must be set to the corresponding voltage. Any PU on the signal then needs to be pulled to the correct voltage as well.	Yes
	0	<b>GPP_I Group Master Voltage Select (GPPI_VCCIO):</b>  0x0 = GPP_I Master Voltage Select set to 3.3v 0x1 = GPP_I Master Voltage Select set to 1.8v	This setting controls configures the VCCIO voltage for all of the GPP_I GPIO pins.  <b>Note:</b> When a GPIO is configured as 1.8V or 3.3V, both the group power pin and the voltage configuration soft strap setting must be set to the corresponding voltage. Any PU on the signal then needs to be pulled to the correct voltage as well.	Yes

## 9.60 PCH Descriptor Record 59 (Flash Descriptor Records)

Flash Address: FPSBA + 041h

Default Flash Address: 141h

Offset from 0	Bits	Description	Usage	FIT Visible
0x141	7:0	Reserved, set to '0'		No

## 9.61 PCH Descriptor Record 60 (Flash Descriptor Records)

Flash Address: FPSBA + 042h

Default Flash Address: 142h

Offset from 0	Bits	Description	Usage	FIT Visible
0x142	7:0	Reserved, set to '0'		No

## 9.62 PCH Descriptor Record 61 (Flash Descriptor Records)

Flash Address: FPSBA + 043h

Default Flash Address: 143h

Offset from 0	Bits	Description	Usage	FIT Visible
0x143	7:0	Reserved, set to '0'		No

## 9.63 PCH Descriptor Record 62 (Flash Descriptor Records)

Flash Address: FPSBA + 044h

Default Flash Address: 144h

Offset from 0	Bits	Description	Usage	FIT Visible
0x144	7:0	Reserved, set to '0'		No

## 9.64 PCH Descriptor Record 63 (Flash Descriptor Records)

Flash Address: FPSBA + 045h

Default Flash Address: 145h

Offset from 0	Bits	Description	Usage	FIT Visible
0x145	7:0	Reserved, set to '0'		No

## 9.65 PCH Descriptor Record 64 (Flash Descriptor Records)

Flash Address: FPSBA + 046h

Default Flash Address: 146h

Offset from 0	Bits	Description	Usage	FIT Visible
0x146	7:0	Reserved, set to '0'		No

## 9.66 PCH Descriptor Record 65 (Flash Descriptor Records)

Flash Address: FPSBA + 047h

Default Flash Address: 147h

Offset from 0	Bits	Description	Usage	FIT Visible
0x147	7:0	Reserved, set to '0'		No

## 9.67 PCH Descriptor Record 66 (Flash Descriptor Records)

Flash Address: FPSBA + 048h

Default Flash Address: 148h

Offset from 0	Bits	Description	Usage	FIT Visible
0x148	7	<b>USB3 Port 8 Speed Select (USB3_1_DISABLE_STRAP_PORT8):</b>  0x0 = Port 8 advertises speed as USB3.1 Gen2 or USB3.2 0x1 = Port 8 advertises speed as USB3.1 Gen1	This setting determines the USB3 Port 8 speed capabilities.	Yes
	6	<b>USB3 Port 7 Speed Select (USB3_1_DISABLE_STRAP_PORT7):</b>  0x0 = Port 7 advertises speed as USB3.1 Gen2 or USB3.2 0x1 = Port 7 advertises speed as USB3.1 Gen1	This setting determines the USB3 Port 7 speed capabilities.	Yes
	5	<b>USB3 Port 6 Speed Select (USB3_1_DISABLE_STRAP_PORT6):</b>  0x0 = Port 6 advertises speed as USB3.1 Gen2 or USB3.2 0x1 = Port 6 advertises speed as USB3.1 Gen1	This setting determines the USB3 Port 6 speed capabilities.	Yes
	4	<b>USB3 Port 5 Speed Select (USB3_1_DISABLE_STRAP_PORT5):</b>  0x0 = Port 5 advertises speed as USB3.1 Gen2 or USB3.2 0x1 = Port 5 advertises speed as USB3.1 Gen1	This setting determines the USB3 Port 5 speed capabilities.	Yes

Offset from 0	Bits	Description	Usage	FIT Visible
<b>0x148 (Cont)</b>	3	<b>USB3 Port 4 Speed Select (USB3_1_DISABLE_STRAP_PORT4):</b>  0x0 = Port 4 advertises speed as USB3.1 Gen2 or USB3.2 0x1 = Port 4 advertises speed as USB3.1 Gen1	This setting determines the USB3 Port 4 speed capabilities.	<b>Yes</b>
	2	<b>USB3 Port 3 Speed Select (USB3_1_DISABLE_STRAP_PORT3):</b>  0x0 = Port 3 advertises speed as USB3.1 Gen2 or USB3.2 0x1 = Port 3 advertises speed as USB3.1 Gen1	This setting determines the USB3 Port 3 speed capabilities.	<b>Yes</b>
	1	<b>USB3 Port 2 Speed Select (USB3_1_DISABLE_STRAP_PORT2):</b>  0x0 = Port 2 advertises speed as USB3.1 Gen2 or USB3.2 0x1 = Port 2 advertises speed as USB3.1 Gen1	This setting determines the USB3 Port 2 speed capabilities.	<b>Yes</b>
	0	<b>USB3 Port 1 Speed Select (USB3_1_DISABLE_STRAP_PORT1):</b>  0x0 = Port 1 advertises speed as USB3.1 Gen2 or USB3.2 0x1 = Port 1 advertises speed as USB3.1 Gen1	This setting determines the USB3 Port 1 speed capabilities.	<b>Yes</b>

## 9.68 PCH Descriptor Record 67 (Flash Descriptor Records)

Flash Address: FPSBA + 049h

Default Flash Address: 149h

Offset from 0	Bits	Description	Usage	FIT Visible
<b>0x149</b>	7:2	<b>Reserved, set to '0'</b>		<b>No</b>
	1	<b>USB3 Port 10 Speed Select (USB3_1_DISABLE_STRAP_PORT10):</b>  0x0 = Port 10 advertises speed as USB3.1 Gen2 or USB3.2 0x1 = Port 10 advertises speed as USB3.1 Gen1	This setting determines the USB3 Port 10 speed capabilities.	<b>Yes</b>
	0	<b>USB3 Port 9 Speed Select (USB3_1_DISABLE_STRAP_PORT9):</b>  0x0 = Port 9 advertises speed as USB3.1 Gen2 or USB3.2 0x1 = Port 9 advertises speed as USB3.1 Gen1	This setting determines the USB3 Port 9 speed capabilities.	<b>Yes</b>

## 9.69 PCH Descriptor Record 68 (Flash Descriptor Records)

Flash Address: FPSBA + 04Ah

Default Flash Address: 14Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0x14A	7	<b>USB3 Lane Reversal Port 8:</b> 0x0 = Port 8 Lane connections are straight 0x1 = Port 8 Lane connection are reversed	For combo configuration (USB3.2/USB3.1), this strap is only applicable if Lane Pairing Strap is enabled.	<b>Yes</b>
	6	<b>USB3 Lane Reversal Port 7:</b> 0x0 = Port 7 Lane connections are straight 0x1 = Port 7 Lane connection are reversed	For combo configuration (USB3.2/USB3.1), this strap is only applicable if Lane Pairing Strap is enabled.	<b>Yes</b>
	5	<b>USB3 Lane Reversal Port 6:</b> 0x0 = Port 6 Lane connections are straight 0x1 = Port 6 Lane connection are reversed	For combo configuration (USB3.2/USB3.1), this strap is only applicable if Lane Pairing Strap is enabled.	<b>Yes</b>
	4	<b>USB3 Lane Reversal Port 5:</b> 0x0 = Port 5 Lane connections are straight 0x1 = Port 5 Lane connection are reversed	For combo configuration (USB3.2/USB3.1), this strap is only applicable if Lane Pairing Strap is enabled.	<b>Yes</b>
	3	<b>USB3 Lane Reversal Port 4:</b> 0x0 = Port 4 Lane connections are straight 0x1 = Port 4 Lane connection are reversed	For combo configuration (USB3.2/USB3.1), this strap is only applicable if Lane Pairing Strap is enabled.	<b>Yes</b>
	2	<b>USB3 Lane Reversal Port 3:</b> 0x0 = Port 3 Lane connections are straight 0x1 = Port 3 Lane connection are reversed	For combo configuration (USB3.2/USB3.1), this strap is only applicable if Lane Pairing Strap is enabled.	<b>Yes</b>
	1	<b>USB3 Lane Reversal Port 2:</b> 0x0 = Port 2 Lane connections are straight 0x1 = Port 2 Lane connection are reversed	For combo configuration (USB3.2/USB3.1), this strap is only applicable if Lane Pairing Strap is enabled.	<b>Yes</b>
	0	<b>USB3 Lane Reversal Port 1:</b> 0x0 = Port 1 Lane connections are straight 0x1 = Port 1 Lane connection are reversed	For combo configuration (USB3.2/USB3.1), this strap is only applicable if Lane Pairing Strap is enabled.	<b>Yes</b>

## 9.70 PCH Descriptor Record 69 (Flash Descriptor Records)

Flash Address: FPSBA + 04Bh

Default Flash Address: 14Bh

Offset from 0	Bits	Description	Usage	FIT Visible
0x14B	7:3	Reserved, set to '0'		No
	1	<b>USB3 Lane Reversal Port 10:</b> 0x0 = Port 10 Lane connections are straight 0x1 = Port 10 Lane connection are reversed	For combo configuration (USB3.2/USB3.1), this strap is only applicable if Lane Pairing Strap is enabled.	Yes
	2	<b>USB3 Lane Reversal Port 9:</b> 0x0 = Port 9 Lane connections are straight 0x1 = Port 9 Lane connection are reversed	For combo configuration (USB3.2/USB3.1), this strap is only applicable if Lane Pairing Strap is enabled.	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
0x14C	7:4	<b>USB3 Port 2 Connector Type Select:</b> 0x0 = USB Port 2 connector set to Type C 0x2 = USB Port 2 connector set to Type A	This setting configures the physical connector type for where the USB port [Super Speed / Enhanced Super Speed] is routed.	Yes
	3:0	<b>USB3 Port 1 Connector Type Select:</b> 0x0 = USB Port 1 connector set to Type C 0x2 = USB Port 1 connector set to Type A	This setting configures the physical connector type for where the USB port [Super Speed / Enhanced Super Speed] is routed.	Yes

## 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
0x14D	7:4	<b>USB3 Port 4 Connector Type Select:</b> 0x0 = USB Port 4 connector set to Type C 0x2 = USB Port 4 connector set to Type A	This setting configures the physical connector type for where the USB port [Super Speed / Enhanced Super Speed] is routed.	Yes
	3:0	<b>USB3 Port 3 Connector Type Select:</b> 0x0 = USB Port 3 connector set to Type C 0x2 = USB Port 3 connector set to Type A	This setting configures the physical connector type for where the USB port [Super Speed / Enhanced Super Speed] is routed.	Yes

## 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
0x14E	7:4	<b>USB3 Port 6 Connector Type Select:</b> 0x0 = USB Port 6 connector set to Type C 0x2 = USB Port 6 connector set to Type A	This setting configures the physical connector type for where the USB port [Super Speed / Enhanced Super Speed] is routed.	Yes
	3:0	<b>USB3 Port 5 Connector Type Select:</b> 0x0 = USB Port 5 connector set to Type C 0x2 = USB Port 5 connector set to Type A	This setting configures the physical connector type for where the USB port [Super Speed / Enhanced Super Speed] is routed.	Yes

## 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
0x14F	7:4	<b>USB3 Port 8 Connector Type Select:</b> 0x0 = USB Port 8 connector set to Type C 0x2 = USB Port 8 connector set to Type A	This setting configures the physical connector type for where the USB port [Super Speed / Enhanced Super Speed] is routed.	Yes
	3:0	<b>USB3 Port 7 Connector Type Select:</b> 0x0 = USB Port 7 connector set to Type C 0x2 = USB Port 7 connector set to Type A	This setting configures the physical connector type for where the USB port [Super Speed / Enhanced Super Speed] is routed.	Yes

## 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
0x150	7:4	<b>USB3 Port 10 Connector Type Select:</b> 0x0 = USB Port 10 connector set to Type C 0x2 = USB Port 10 connector set to Type A	This setting configures the physical connector type for where the USB port [Super Speed / Enhanced Super Speed] is routed.	Yes
	3:0	<b>USB3 Port 9 Connector Type Select:</b> 0x0 = USB Port 9 connector set to Type C 0x2 = USB Port 9 connector set to Type A	This setting configures the physical connector type for where the USB port [Super Speed / Enhanced Super Speed] is routed.	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
0x151	7:4	<b>USB2 Port 2 Connector Type Select:</b> 0x0 = USB Port 2 connector set to Type C 0x2 = USB Port 2 connector set to Type A	This setting configures the USB2 Port 2 physical connector type for where the USB port is routed.	Yes
	3:0	<b>USB2 Port 1 Connector Type Select:</b> 0x0 = USB Port 1 connector set to Type C 0x2 = USB Port 1 connector set to Type A	This setting configures the USB2 Port 1 physical connector type for where the USB port is routed.	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
0x152	7:4	<b>USB2 Port 4 Connector Type Select:</b> 0x0 = USB Port 4 connector set to Type C 0x2 = USB Port 4 connector set to Type A	This setting configures the USB2 Port 4 physical connector type for where the USB port is routed.	Yes
	3:0	<b>USB2 Port 3 Connector Type Select:</b> 0x0 = USB Port 3 connector set to Type C 0x2 = USB Port 3 connector set to Type A	This setting configures the USB2 Port 3 physical connector type for where the USB port is routed.	Yes

## 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
0x153	7:4	<b>USB2 Port 6 Connector Type Select:</b> 0x0 = USB Port 6 connector set to Type C 0x2 = USB Port 6 connector set to Type A	This setting configures the USB2 Port 6 physical connector type for where the USB port is routed.	Yes
	3:0	<b>USB2 Port 5 Connector Type Select:</b> 0x0 = USB Port 7 connector set to Type C 0x2 = USB Port 7 connector set to Type A	This setting configures the USB2 Port 5 physical connector type for where the USB port is routed.	Yes

## 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
0x154	7:4	<b>USB2 Port 8 Connector Type Select:</b> 0x0 = USB Port 8 connector set to Type C 0x2 = USB Port 8 connector set to Type A	This setting configures the USB2 Port 8 physical connector type for where the USB port is routed.	Yes
	3:0	<b>USB2 Port 7 Connector Type Select:</b> 0x0 = USB Port 7 connector set to Type C 0x2 = USB Port 7 connector set to Type A	This setting configures the USB2 Port 7 physical connector type for where the USB port is routed.	Yes

## 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
0x155	7:4	<b>USB2 Port 10 Connector Type Select:</b> 0x0 = USB Port 10 connector set to Type C 0x2 = USB Port 10 connector set to Type A	This setting configures the USB2 Port 10 physical connector type for where the USB port is routed.	Yes
	3:0	<b>USB2 Port 9 Connector Type Select:</b> 0x0 = USB Port 9 connector set to Type C 0x2 = USB Port 9 connector set to Type A	This setting configures the USB2 Port 9 physical connector type for where the USB port is routed.	Yes

## 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
0x156	7:4	<b>USB2 Port 12 Connector Type Select:</b> 0x0 = USB Port 12 connector set to Type C 0x2 = USB Port 12 connector set to Type A	This setting configures the USB2 Port 12 physical connector type for where the USB port is routed.	Yes
	3:0	<b>USB2 Port 11 Connector Type Select:</b> 0x0 = USB Port 11 connector set to Type C 0x2 = USB Port 11 connector set to Type A	This setting configures the USB2 Port 11 physical connector type for where the USB port is routed.	Yes

## 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
0x157	7:4	<b>USB2 Port 14 Connector Type Select:</b> 0x0 = USB Port 14 connector set to Type C 0x2 = USB Port 14 connector set to Type A	This setting configures the USB2 Port 14 physical connector type for where the USB port is routed.	Yes
	3:0	<b>USB2 Port 13 Connector Type Select:</b> 0x0 = USB Port 13 connector set to Type C 0x2 = USB Port 13 connector set to Type A	This setting configures the USB2 Port 13 physical connector type for where the USB port is routed.	Yes

## 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
0x158	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
0x159	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
0x15A	7:6	<b>USB3.2 Port 7 and 8 Pairing:</b> 0x0 = USB3.2 Port 7 and 8 lane pairing is enabled 0x3 = USB3.2 Port 7 and 8 lane pairing is disabled	This setting determines USB3.2 Port 7 and 8 lane pairing is enabled.  <b>Note:</b> This setting is only applicable when operating in USB3.2 mode.	Yes
	5:4	<b>USB3.2 Port 5 and 6 Pairing:</b> 0x0 = USB3.2 Port 5 and 6 lane pairing is enabled 0x3 = USB3.2 Port 5 and 6 lane pairing is disabled	This setting determines USB3.2 Port 5 and 6 lane pairing is enabled.  <b>Note:</b> This setting is only applicable when operating in USB3.2 mode.	Yes
	3:2	<b>USB3.2 Ports 3 and 4 Pairing:</b> 0x0 = USB3.2 Port 3 and 4 lane pairing is enabled 0x3 = USB3.2 Port 3 and 4 lane pairing is disabled	This setting determines USB3.2 Port 3 and 4 lane pairing is enabled.  <b>Note:</b> This setting is only applicable when operating in USB3.2 mode.	Yes
	1:0	<b>USB3.2 Ports 1 and 2 Pairing:</b> 0x0 = USB3.2 Port 1 and 2 lane pairing is enabled 0x3 = USB3.2 Port 1 and 2 lane pairing is disabled	This setting determines USB3.2 Port 1 and 2 lane pairing is enabled.  <b>Note:</b> This setting is only applicable when operating in USB3.2 mode.	Yes

## 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
0x15B	7:2	Reserved, set to '0'		No
	1:0	<b>USB3.2 Port 9 and 10 Pairing:</b> 0x0 = USB3.2 Port 9 and 10 lane pairing is enabled 0x3 = USB3.2 Port 9 and 10 lane pairing is disabled	This setting determines USB3.2 Port 9 and 10 lane pairing is enabled.  <b>Note:</b> This setting is only applicable when operating in USB3.2 mode.	Yes

## 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
0x15C	7	<b>USB3.2 Port 8 Speed Select (USB3_2_DISABLE_STRAP_PORT8):</b>  0x0 = Port 8 advertises speed as USB 3.2 0x1 = Port 8 advertises speed as USB3.1 Gen1 or USB3.1 Gen2	This setting determines the USB3.2 Port 8 speed capabilities.  <b>Note:</b> In order to use USB3.2 speeds the USB3 Port 6 Speed Select must be set to "advertises speed as USB3.1 or USB 3.2".	Yes
	6	<b>USB3.2 Port 7 Speed Select (USB3_2_DISABLE_STRAP_PORT7):</b>  0x0 = Port 7 advertises speed as USB 3.2 0x1 = Port 7 advertises speed as USB3.1 Gen1 or USB3.1 Gen2	This setting determines the USB3.2 Port 7 speed capabilities.  <b>Note:</b> In order to use USB3.2 speeds the USB3 Port 6 Speed Select must be set to "advertises speed as USB3.1 or USB 3.2".	Yes
	5	<b>USB3.2 Port 6 Speed Select (USB3_2_DISABLE_STRAP_PORT6):</b>  0x0 = Port 3 advertises speed as USB 3.2 0x1 = Port 3 advertises speed as USB3.1 Gen1 or USB3.1 Gen2	This setting determines the USB3.2 Port 6 speed capabilities.  <b>Note:</b> In order to use USB3.2 speeds the USB3 Port 6 Speed Select must be set to "advertises speed as USB3.1 or USB 3.2".	Yes
	4	<b>USB3.2 Port 5 Speed Select (USB3_2_DISABLE_STRAP_PORT5):</b>  0x0 = Port 3 advertises speed as USB 3.2 0x1 = Port 3 advertises speed as USB3.1 Gen1 or USB3.1 Gen2	This setting determines the USB3.2 Port 5 speed capabilities.  <b>Note:</b> In order to use USB3.2 speeds the USB3 Port 5 Speed Select must be set to "advertises speed as USB3.1 or USB 3.2".	Yes
	3	<b>USB3.2 Port 4 Speed Select (USB3_2_DISABLE_STRAP_PORT4):</b>  0x0 = Port 3 advertises speed as USB 3.2 0x1 = Port 3 advertises speed as USB3.1 Gen1 or USB3.1 Gen2	This setting determines the USB3.2 Port 4 speed capabilities.  <b>Note:</b> In order to use USB3.2 speeds the USB3 Port 4 Speed Select must be set to "advertises speed as USB3.1 or USB 3.2".	Yes
	2	<b>USB3.2 Port 3 Speed Select (USB3_2_DISABLE_STRAP_PORT3):</b>  0x0 = Port 3 advertises speed as USB 3.2 0x1 = Port 3 advertises speed as USB3.1 Gen1 or USB3.1 Gen2	This setting determines the USB3.2 Port 3 speed capabilities.  <b>Note:</b> In order to use USB3.2 speeds the USB3 Port 3 Speed Select must be set to "advertises speed as USB3.1 or USB 3.2".	Yes
	1	<b>USB3.2 Port 2 Speed Select (USB3_2_DISABLE_STRAP_PORT2):</b>  0x0 = Port 2 advertises speed as USB 3.2 0x1 = Port 2 advertises speed as USB3.1 Gen1 or USB3.1 Gen2	This setting determines the USB3.2 Port 2 speed capabilities.  <b>Note:</b> In order to use USB3.2 speeds the USB3 Port 2 Speed Select must be set to "advertises speed as USB3.1 or USB 3.2".	Yes
	0	<b>USB3.2 Port 1 Speed Select (USB3_2_DISABLE_STRAP_PORT1):</b>  0x0 = Port 1 advertises speed as USB 3.2 0x1 = Port 1 advertises speed as USB3.1 Gen1 or USB3.1 Gen2	This setting determines the USB3.2 Port 1 speed capabilities.  <b>Note:</b> In order to use USB3.2 speeds the USB3 Port 1 Speed Select must be set to "advertises speed as USB3.1 or USB 3.2".	Yes

## 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
0x15D	7:2	Reserved, set to '0'		No
	1	<b>USB3.2 Port 10 Speed Select (USB3_2_DISABLE_STRAP_PORT10):</b>  0x0 = Port 10 advertises speed as USB 3.2 0x1 = Port 10 advertises speed as USB3.1 Gen1 or USB3.1 Gen2	This setting determines the USB3.2 Port 10 speed capabilities.  <b>Note:</b> In order to use USB3.2 speeds the USB3 Port 2 Speed Select must be set to "advertises speed as USB3.1 or USB 3.2".	Yes
	0	<b>USB3.2 Port 9 Speed Select (USB3_2_DISABLE_STRAP_PORT9):</b>  0x0 = Port 9 advertises speed as USB 3.2 0x1 = Port 9 advertises speed as USB3.1 Gen1 or USB3.1 Gen2	This setting determines the USB3.2 Port 9 speed capabilities.  <b>Note:</b> In order to use USB3.2 speeds the USB3 Port 1 Speed Select must be set to "advertises speed as USB3.1 or USB 3.2".	Yes

## 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
0x15E	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
0x15F	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
0x160	31:0	Reserved, set to '0'		No

## 9.92 PCH Descriptor Record 91 (Flash Descriptor Records)

Flash Address: FPSBA + 064h

Default Flash Address: 164h

Offset from 0	Bits	Description	Usage	FIT Visible
0x164	15:0	Reserved, set to '0'		No

## 9.93 PCH Descriptor Record 92 (Flash Descriptor Records)

Flash Address: FPSBA + 066h

Default Flash Address: 166h

Offset from 0	Bits	Description	Usage	FIT Visible
0x166	7:0	Reserved, set to '0xFF'		No

## 9.94 PCH Descriptor Record 93 (Flash Descriptor Records)

Flash Address: FPSBA + 067h

Default Flash Address: 167h

Offset from 0	Bits	Description	Usage	FIT Visible
0x167	7:0	Reserved, set to '0'		No

## 9.95 PCH Descriptor Record 94 (Flash Descriptor Records)

Flash Address:FPSBA + 068h

Default Flash Address: 168h

Offset from 0	Bits	Description	Usage	FIT Visible
0x168	7	Reserved, set to '0'		No
	6:4	<b>Top Swap Block size (TSBS):</b>  0x0 = 64 KB. Invert A16 if Top Swap is enabled 0x1 = 128 KB. Invert A17 if Top Swap is enabled 0x2 = 256 KB. Invert A18 if Top Swap is enabled 0x3 = 512 KB. Invert A19 if Top Swap is enabled 0x4 = 1 MB. Invert A20 if Top Swap is enabled 0x5 = 2 MB Invert A21 if Top Swap is enabled 0x6 = 4 MB Invert A22 if Top Swap is enabled 0x7 = 8 MB Invert A23 if Top Swap is enabled  <b>Notes:</b> 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.	This allows for the system to use alternate code in order to boot a platform based upon the <b>Top Swap</b> (GPIO66/SDIO_D0 pulled low during the rising edge of <b>PWROK</b> .) strap being asserted.  <b>Top Swap</b> 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.  <b>Note:</b> 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

## 9.96 PCH Descriptor Record 95 (Flash Descriptor Records)

Flash Address:FPSBA + 069h

Default Flash Address: 169h

Offset from 0	Bits	Description	Usage	FIT Visible
0x169	7:0	Reserved, set to '0'		No

## 9.97 PCH Descriptor Record 96 (Flash Descriptor Records)

Flash Address:FPSBA + 06Ah

Default Flash Address: 16Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0x16A	7:0	Reserved, set to '0'		No



## 9.98 PCH Descriptor Record 97 (Flash Descriptor Records)

Flash Address: FPSBA + 06Bh

Default Flash Address: 16Bh

Offset from 0	Bits	Description	Usage	FIT Visible
0x16B	7:6	<b>SPI Maximum write and erase Resume to Suspend intervals:</b>  0x0 = 128us 0x1 = 256us 0x2 = 512us 0x3 = No Ceiling	This setting specifies the maximum value for the write and erase Resume to Suspend intervals.	Yes
	5	<b>SPI Out of Order operation Enable:</b>  0x0 = Out or Order operation Enabled 0x1 = 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	<b>SPI Suspend / Resume Enable:</b>  0x0 = Enable suspend / resume 0x1 = 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	<b>SPI Resume Holdoff Delay:</b>  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	<b>Reserved, set to '0'</b>		No

## 9.99 PCH Descriptor Record 98 (Flash Descriptor Records)

Flash Address: FPSBA + 06Ch

Default Flash Address: 16Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x16C	7:4	Reserved, set to '0'		No
	3:0	<b>SPI Idle to Deep Power Down Timeout:</b> 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

## 9.100 PCH Descriptor Record 99 (Flash Descriptor Records)

Flash Address: FPSBA + 06Dh

Default Flash Address: 16Dh

Offset from 0	Bits	Description	Usage	FIT Visible
0x16D	7	Reserved, set to '0x1'		No
	6:3	Reserved, set to '0'		No
	2:0	<b>SPI TPM Clock Frequency (STCF):</b> This field is defined with a broad range to support both SOC and PCH implementations. The listed frequencies are approximate.  0x2 = 48MHz 0x4 = 30 MHz 0x6 = 17 MHz  <b>Notes:</b> 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

## 9.101 PCH Descriptor Record 100 (Flash Descriptor Records)

Flash Address: FPSBA + 06Eh

Default Flash Address: 16Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0x16E	7:0	Reserved, set to '0'		No

## 9.102 PCH Descriptor Record 101 (Flash Descriptor Records)

Flash Address: FPSBA + 06Fh

Default Flash Address: 16Fh

Offset from 0	Bits	Description	Usage	FIT Visible
0x16F	7:0	Reserved, set to '0x5'		No

## 9.103 PCH Descriptor Record 102 (Flash Descriptor Records)

Flash Address: FPSBA + 070h

Default Flash Address: 170h

Offset from 0	Bits	Description	Usage	FIT Visible
0x170	31:0	<b>Global Protected Range Default (GPRD):</b>  Set to '0'	Sets the default value of the GPR0 register in the SPI Flash Controller.	Yes

## 9.104 PCH Descriptor Record 103 (Flash Descriptor Records)

Flash Address: FPSBA + 074h

Default Flash Address: 174h

Offset from 0	Bits	Description	Usage	FIT Visible
0x174	7:0	Reserved, set to '0'		No
	5:3	<b>eSPI / EC Bus Frequency:</b>  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 = 25MHz 0x2 = 33 MHz 0x4 = 50MHz		Yes
	2:0	Reserved, set to '0'		No

## 9.105 PCH Descriptor Record 104 (Flash Descriptor Records)

Flash Address: FPSBA + 075h

Default Flash Address: 175h

Offset from 0	Bits	Description	Usage	FIT Visible
0x175	7:5	<b>Reserved, set to '0'</b>		<b>No</b>
	4	<b>eSPI / EC Slave 1 Device Enable:</b> 0x0 = CS1# (Slave 1) is disabled 0x1 = CS1# (Slave 1) is enabled		<b>Yes</b>
	3	<b>eSPI / EC Slave 1 Device Maximum I/O Mode:</b> 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		<b>Yes</b>
	2:1	<b>Reserved, set to '0x1'</b>		<b>No</b>
	0	<b>eSPI / EC CRC Check Enable For Slave 0 (EC/BMC):</b> 0x0 = CRC Checking enabled 0x1 = CRC checking disabled		<b>Yes</b>

## 9.106 PCH Descriptor Record 105 (Flash Descriptor Records)

Flash Address: FPSBA + 076h

Default Flash Address: 176h

Offset from 0	Bits	Description	Usage	FIT Visible
0x176	7	Reserved, set to '0'		No
	6	Reserved, set to '0x1'		No
	5	<b>eSPI / EC CRC Check Enable For Slave 1 (EC/BMC):</b>  0x0 = CRC Checking enabled 0x1 = CRC checking disabled		Yes
	4:3	<b>eSPI / EC Slave 1 Device Maximum I/O Mode:</b> 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
	2:0	<b>eSPI / EC Slave 1 Device Bus Frequency:</b> For Slave 1 (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 = 25MHz 0x2 = 33 MHz 0x4 = 50MHz		Yes

## 9.107 PCH Descriptor Record 106 (Flash Descriptor Records)

Flash Address: FPSBA + 077h

Default Flash Address: 177h

Offset from 0	Bits	Description	Usage	FIT Visible
0x177	7:0	Reserved, set to '0'		No

## 9.108 PCH Descriptor Record 107 (Flash Descriptor Records)

Flash Address: FPSBA + 078h

Default Flash Address: 178h

Offset from 0	Bits	Description	Usage	FIT Visible
0x178	7:2	Reserved, set to '0'		No
	1	<b>eSPI / EC Slave Attached Flash Channel 000 Enable:</b>  0x0 = In-Order SAF Requests 0x1 = Out-of-Order SAF Requests		Yes
	0	<b>eSPI / EC Slave Attached Flash Multiple Outstanding Requests Enable:</b>  0x0 = Single Outstanding SAF Request 0x1 = Multiple Outstanding SAF Requests		Yes

## 9.109 PCH Descriptor Record 108 (Flash Descriptor Records)

Flash Address: FPSBA + 079h

Default Flash Address: 179h

Offset from 0	Bits	Description	Usage	FIT Visible
0x179	7:1	Reserved, set to '0'		No
	0	<b>eSPI / EC Max Outstanding Request for Master Attached Flash Channel:</b>  0x0 = Maximum of 2 outstanding requests allowed 0x1 = Maximum of 1 outstanding requests allowed		Yes

## 9.110 PCH Descriptor Record 109 (Flash Descriptor Records)

Flash Address: FPSBA + 07Ah

Default Flash Address: 17Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0x17A	7	Reserved, set to '0'		No
	6	<b>eSPI Low Frequency Debug Override:</b>  0x0 = eSPI Low Frequency Debug Override Enabled 0x1 = eSPI Low Frequency Debug Override Disabled	When enabled this setting will divide eSPI clock frequency by 8.  <b>Note:</b> 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

## 9.111 PCH Descriptor Record 110 (Flash Descriptor Records)

Flash Address: FPSBA + 07Bh

Default Flash Address: 17Bh

Offset from 0	Bits	Description	Usage	FIT Visible
0x17B	7:0	Reserved, set to '0'		No

## 9.112 PCH Descriptor Record 111 (Flash Descriptor Records)

Flash Address: FPSBA + 07Ch

Default Flash Address: 17Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x17C	7:6	<b>eSPI / EC Slave 2 Device Maximum I/O Mode:</b> 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
	4	<b>eSPI / EC CRC Check Enable For Slave 2 (EC/BMC):</b>  0x0 = CRC Checking enabled 0x1 = CRC checking disabled		Yes
	3:1	Reserved, set to '0'		No
	0	<b>eSPI / EC Slave 2 Device Enable:</b>  0x0 = CS1# (Slave 2) is disabled 0x1 = CS1# (Slave 2) is enabled		Yes

### 9.113 PCH Descriptor Record 112 (Flash Descriptor Records)

Flash Address: FPSBA + 07Dh

Default Flash Address: 17Dh

Offset from 0	Bits	Description	Usage	FIT Visible
0x17D	7:3	Reserved, set to '0'		No
	2:0	<b>eSPI / EC Slave 2 Device Bus Frequency:</b> For Slave 2 (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 = 25MHz 0x2 = 33 MHz 0x4 = 50MHz		Yes

### 9.114 PCH Descriptor Record 113 (Flash Descriptor Records)

Flash Address: FPSBA + 07Eh

Default Flash Address: 17Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0x17E	7:0	Reserved, set to '0'		No

### 9.115 PCH Descriptor Record 114 (Flash Descriptor Records)

Flash Address: FPSBA + 07Fh

Default Flash Address: 17Fh

Offset from 0	Bits	Description	Usage	FIT Visible
0x17F	7:0	Reserved, set to '0'		No



## 9.116 PCH Descriptor Record 115 (Flash Descriptor Records)

Flash Address: FPSBA + 080h

Default Flash Address: 180h

Offset from 0	Bits	Description	Usage	FIT Visible
0x180	7:6	<b>eSPI / EC Slave 3 Device Maximum I/O Mode:</b> 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
	4	<b>eSPI / EC CRC Check Enable For Slave 3 (EC/BMC):</b>  0x0 = CRC Checking enabled 0x1 = CRC checking disabled		Yes
	3:1	<b>Reserved</b>		No
	0	<b>eSPI / EC Slave 3 Device Enable:</b>  0x0 = CS1# (Slave 3) is disabled 0x1 = CS1# (Slave 3) is enabled		Yes

## 9.117 PCH Descriptor Record 116 (Flash Descriptor Records)

Flash Address: FPSBA + 081h

Default Flash Address: 181h

Offset from 0	Bits	Description	Usage	FIT Visible
0x181	7:3	<b>Reserved, set to '0'</b>		No
	2:0	<b>eSPI / EC Slave 3 Device Bus Frequency:</b> For Slave 3 (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 = 25MHz 0x2 = 33 MHz 0x4 = 50MHz		Yes

## 9.118 PCH Descriptor Record 117 (Flash Descriptor Records)

Flash Address: FPSBA + 082h

Default Flash Address: 182h

Offset from 0	Bits	Description	Usage	FIT Visible
0x182	7:0	Reserved, set to '0'		No

## 9.119 PCH Descriptor Record 118 (Flash Descriptor Records)

Flash Address: FPSBA + 083h

Default Flash Address: 183h

Offset from 0	Bits	Description	Usage	FIT Visible
0x183	7:0	Reserved, set to '0'		No

## 9.120 PCH Descriptor Record 119 (Flash Descriptor Records)

Flash Address: FPSBA + 084h

Default Flash Address: 184h

Offset from 0	Bits	Description	Usage	FIT Visible
0x184	7:4	Reserved, set to '0x8'		No
	3:1	<b>PCIe Controller 1 (Port 1-4):</b> Straps to set the default value of the PCI Express Port Configuration 1 register covering PCIe ports 1-4.  0x0 = 4x1 0x1 = 1x2, 2x1 0x2 = 2x2 0x3 = 1x4  <b>Note:</b> 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.  <b>Note:</b> This field must be determined by the PCI Express port requirements of the design. The platform hardware designer must determine this setting.	Yes
	0	<b>PCIe Controller 1 Lane Reversal:</b>  0x0 = PCIe Lanes are not reversed. 0x1 = PCIe Lanes are reversed.  <b>Note:</b> Refer to EDS supported Lane reversal configuration.	This bit controls lane reversal behavior for PCIe Controller 1 for PCIe.  PCI Express port lane reversal can be done to aid in the laying out of the board.  <b>Note:</b> This setting is dependent on the board design. The platform hardware designer must determine if this port needs lane reversal.	No

## 9.121 PCH Descriptor Record 120 (Flash Descriptor Records)

Flash Address: FPSBA + 085h

Default Flash Address: 185h

Offset from 0	Bits	Description	Usage	FIT Visible
0x185	7:0	Reserved, set to '0x3'		No

## 9.122 PCH Descriptor Record 121 (Flash Descriptor Records)

Flash Address: FPSBA + 086h

Default Flash Address: 186h

Offset from 0	Bits	Description	Usage	FIT Visible
0x186	7:0	Reserved, set to '0x8'		No

## 9.123 PCH Descriptor Record 122 (Flash Descriptor Records)

Flash Address: FPSBA + 087h

Default Flash Address: 187h

Offset from 0	Bits	Description	Usage	FIT Visible
0x187	7:0	Reserved, set to '0x10'		No

## 9.124 PCH Descriptor Record 123 (Flash Descriptor Records)

Flash Address: FPSBA + 088h

Default Flash Address: 188h

Offset from 0	Bits	Description	Usage	FIT Visible
0x188	7:0	Reserved, set to '0x8'		No

## 9.125 PCH Descriptor Record 124 (Flash Descriptor Records)

Flash Address: FPSBA + 089h

Default Flash Address: 189h

Offset from 0	Bits	Description	Usage	FIT Visible
0x189	7:0	Reserved, set to '0x10'		No

## 9.126 PCH Descriptor Record 125 (Flash Descriptor Records)

Flash Address: FPSBA + 08Ah

Default Flash Address: 18Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0x18A	7:0	Reserved, set to '0x8'		No

## 9.127 PCH Descriptor Record 126 (Flash Descriptor Records)

Flash Address: FPSBA + 08Bh

Default Flash Address: 18Bh

Offset from 0	Bits	Description	Usage	FIT Visible
0x18B	7:0	Reserved, set to '0x10'		No

## 9.128 PCH Descriptor Record 127 (Flash Descriptor Records)

Flash Address: FPSBA + 08Ch

Default Flash Address: 18Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x18C	7:0	Reserved, set to '0x8'		No

## 9.129 PCH Descriptor Record 128 (Flash Descriptor Records)

Flash Address: FPSBA + 08Dh

Default Flash Address: 18Dh

Offset from 0	Bits	Description	Usage	FIT Visible
0x18D	24:0	Reserved, set to '0x10'		No

## 9.130 PCH Descriptor Record 129 (Flash Descriptor Records)

Flash Address: FPSBA + 090h

Default Flash Address: 190h

Offset from 0	Bits	Description	Usage	FIT Visible
0x190	7:4	<b>Reserved, set to '0x8'</b>		<b>No</b>
	3:1	<b>PCIe Controller 2 (Port 5-8):</b> Straps to set the default value of the PCI Express Port Configuration 1 register covering PCIe ports 5-8. 0x0 = 4x1 0x1 = 1x2, 2x1 0x2 = 2x2 0x3 = 1x4 <b>Note:</b> Refer to EDS for PCIe supported port configurations.	Setting of this field depend on what PCIe ports 5-8 configurations are desired by the board manufacturer.  <b>Note:</b> This field must be determined by the PCI Express port requirements of the design. The platform hardware designer must determine this setting.	<b>Yes</b>
	0	<b>PCIe Controller 2 Lane Reversal:</b> 0x0 = PCIe Lanes are not reversed. 0x1 = PCIe Lanes are reversed. <b>Note:</b> Refer to EDS supported Lane reversal configuration.	This bit controls lane reversal behavior for PCIe Controller 2.  PCI Express port lane reversal can be done to aid in the laying out of the board.  <b>Note:</b> This setting is dependent on the board design. The platform hardware designer must determine if this port needs lane reversal.	<b>No</b>

## 9.131 PCH Descriptor Record 130 (Flash Descriptor Records)

Flash Address: FPSBA + 091h

Default Flash Address: 191h

Offset from 0	Bits	Description	Usage	FIT Visible
0x191	7:0	<b>Reserved, set to '0x3'</b>		<b>No</b>

## 9.132 PCH Descriptor Record 131 (Flash Descriptor Records)

Flash Address: FPSBA + 092h

Default Flash Address: 192h

Offset from 0	Bits	Description	Usage	FIT Visible
0x192	7:0	<b>Reserved, set to '0x8'</b>		<b>No</b>

### 9.133 PCH Descriptor Record 132 (Flash Descriptor Records)

Flash Address: FPSBA + 093h

Default Flash Address: 193h

Offset from 0	Bits	Description	Usage	FIT Visible
0x193	7:0	Reserved, set to '0x10'		No

### 9.134 PCH Descriptor Record 133 (Flash Descriptor Records)

Flash Address: FPSBA + 094h

Default Flash Address: 194h

Offset from 0	Bits	Description	Usage	FIT Visible
0x194	7:0	Reserved, set to '0x8'		No

### 9.135 PCH Descriptor Record 134 (Flash Descriptor Records)

Flash Address: FPSBA + 095h

Default Flash Address: 195h

Offset from 0	Bits	Description	Usage	FIT Visible
0x195	7:0	Reserved, set to '0x10'		No

### 9.136 PCH Descriptor Record 135 (Flash Descriptor Records)

Flash Address: FPSBA + 096h

Default Flash Address: 196h

Offset from 0	Bits	Description	Usage	FIT Visible
0x196	7:0	Reserved, set to '0x8'		No

### 9.137 PCH Descriptor Record 136 (Flash Descriptor Records)

Flash Address: FPSBA + 097h

Default Flash Address: 197h

Offset from 0	Bits	Description	Usage	FIT Visible
0x197	7:0	Reserved, set to '0x10'		No

## 9.138 PCH Descriptor Record 137 (Flash Descriptor Records)

Flash Address: FPSBA + 098h

Default Flash Address: 198h

Offset from 0	Bits	Description	Usage	FIT Visible
0x198	7:0	Reserved, set to '0x8'		No

## 9.139 PCH Descriptor Record 138 (Flash Descriptor Records)

Flash Address: FPSBA + 099h

Default Flash Address: 199h

Offset from 0	Bits	Description	Usage	FIT Visible
0x199	24:0	Reserved, set to '0x10'		No

## 9.140 PCH Descriptor Record 139 (Flash Descriptor Records)

Flash Address: FPSBA + 09Ch

Default Flash Address: 19Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x19C	7:4	Reserved, set to '0x8'		No
	3:1	<b>PCIe Controller 3 (Port 9-12):</b> Straps to set the default value of the PCI Express Port Configuration 1 register covering PCIe ports 9-12.  0x0 = 4x1 0x1 = 1x2, 2x1 0x2 = 2x2 0x3 = 1x4  <b>Note:</b> Refer to EDS for PCIe supported port configurations	Setting of this field depend on what PCIe ports 9-12 configurations are desired by the board manufacturer.  <b>Note:</b> This field must be determined by the PCI Express port requirements of the design. The platform hardware designer must determine this setting.	Yes
	0	<b>PCIe Controller 3 Lane Reversal:</b>  This bit controls lane reversal behavior for PCIe Controller 3.  0x0 = PCIe Lanes are not reversed. 0x1 = PCIe Lanes are reversed.  <b>Note:</b> Refer to EDS supported Lane reversal configuration.	Configuring PCIe Controller 3 for PCIe Lane reversal is done via this strap.  PCI Express port lane reversal can be done to aid in the laying out of the board.  <b>Note:</b> This setting is dependent on the board design. The platform hardware designer must determine if this port needs lane reversal.	No

## 9.141 PCH Descriptor Record 140 (Flash Descriptor Records)

Flash Address: FPSBA + 09Dh

Default Flash Address: 19Dh

Offset from 0	Bits	Description	Usage	FIT Visible
0x19D	7:0	Reserved, set to '0x3'		No

## 9.142 PCH Descriptor Record 141 (Flash Descriptor Records)

Flash Address: FPSBA + 09Eh

Default Flash Address: 19Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0x19E	7:0	Reserved, set to '0x8'		No

## 9.143 PCH Descriptor Record 142 (Flash Descriptor Records)

Flash Address: FPSBA + 09Fh

Default Flash Address: 19Fh

Offset from 0	Bits	Description	Usage	FIT Visible
0x19F	7:0	Reserved, set to '0x10'		No

## 9.144 PCH Descriptor Record 143 (Flash Descriptor Records)

Flash Address: FPSBA + 0A0h

Default Flash Address: 1A0h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1A0	7:0	Reserved, set to '0x8'		No

## 9.145 PCH Descriptor Record 144 (Flash Descriptor Records)

Flash Address: FPSBA + 0A1h

Default Flash Address: 1A1h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1A1	7:0	Reserved, set to '0x10'		No



## 9.146 PCH Descriptor Record 145 (Flash Descriptor Records)

Flash Address: FPSBA + 0A2h

Default Flash Address: 1A2h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1A2	7:0	Reserved, set to '0x8'		No

## 9.147 PCH Descriptor Record 146 (Flash Descriptor Records)

Flash Address: FPSBA + 0A3h

Default Flash Address: 1A3h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1A3	7:0	Reserved, set to '0x10'		No

## 9.148 PCH Descriptor Record 147 (Flash Descriptor Records)

Flash Address: FPSBA + 0A4h

Default Flash Address: 1A4h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1A4	7:0	Reserved, set to '0x8'		No

## 9.149 PCH Descriptor Record 148 (Flash Descriptor Records)

Flash Address: FPSBA + 0A5h

Default Flash Address: 1A5h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1A5	24:0	Reserved, set to '0x10'		No

## 9.150 PCH Descriptor Record 149 (Flash Descriptor Records)

Flash Address: FPSBA + 0A8h

Default Flash Address: 1A8h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1A8	7:4	Reserved, set to '0x8'		No
	3:1	<b>PCIe Controller 4 (Port 13-16):</b> Straps to set the default value of the PCI Express Port Configuration 4 register covering PCIe ports 13-16.  0x0 = 4x1 0x1 = 1x2, 2x1 0x2 = 2x2 0x3 = 1x4  <b>Note:</b> Refer to EDS for PCIe supported port configurations.	Setting of this field depend on what PCIe ports 13-16 configurations are desired by the board manufacturer.  <b>Note:</b> This field must be determined by the PCI Express port requirements of the design. The platform hardware designer must determine this setting.	Yes
	0	<b>PCIe Controller 4 Lane Reversal:</b>  0x0 = PCIe Lanes are not reversed. 0x1 = PCIe Lanes are reversed.  <b>Note:</b> Refer to EDS supported Lane reversal configuration.	This bit controls lane reversal behavior for PCIe Controller 4.  PCI Express port lane reversal can be done to aid in the laying out of the board.  <b>Note:</b> This setting is dependent on the board design. The platform hardware designer must determine if this port needs lane reversal.	No

## 9.151 PCH Descriptor Record 150 (Flash Descriptor Records)

Flash Address: FPSBA + 0A9h

Default Flash Address: 1A9h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1A9	7:0	Reserved, set to '0x3'		No

## 9.152 PCH Descriptor Record 151 (Flash Descriptor Records)

Flash Address: FPSBA + 0AAh

Default Flash Address: 1AAh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1AA	7:0	Reserved, set to '0x8'		No

## 9.153 PCH Descriptor Record 152 (Flash Descriptor Records)

Flash Address: FPSBA + 0ABh

Default Flash Address: 1ABh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1AB	7:0	Reserved, set to '0x10'		No

## 9.154 PCH Descriptor Record 153 (Flash Descriptor Records)

Flash Address: FPSBA + 0ACh

Default Flash Address: 1ACh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1AC	7:0	Reserved, set to '0x8'		No

## 9.155 PCH Descriptor Record 154 (Flash Descriptor Records)

Flash Address: FPSBA + 0ADh

Default Flash Address: 1ADh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1AD	7:0	Reserved, set to '0x10'		No

## 9.156 PCH Descriptor Record 155 (Flash Descriptor Records)

Flash Address: FPSBA + 0AEh

Default Flash Address: 1AEh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1AE	7:0	Reserved, set to '0x8'		No

## 9.157 PCH Descriptor Record 156 (Flash Descriptor Records)

Flash Address: FPSBA + 0AFh

Default Flash Address: 1AFh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1AF	7:0	Reserved, set to '0x10'		No

## 9.158 PCH Descriptor Record 157 (Flash Descriptor Records)

Flash Address: FPSBA + 0B0h

Default Flash Address: 1B0h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1B0	7:0	Reserved, set to '0x8'		No

## 9.159 PCH Descriptor Record 158 (Flash Descriptor Records)

Flash Address: FPSBA + 0B1h

Default Flash Address: 1B1h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1B1	24:0	Reserved, set to '0x16'		No

## 9.160 PCH Descriptor Record 159 (Flash Descriptor Records)

Flash Address: FPSBA + 0B4h

Default Flash Address: 1B4h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1B4	7:4	Reserved, set to '0x8'		No
	3:1	<b>PCIe Controller 5 (Port 17-20):</b> Straps to set the default value of the PCI Express Port Configuration 4 register covering PCIe ports 17-20.  0x0 = 4x1 0x1 = 1x2, 2x1 0x2 = 2x2 0x3 = 1x4  <b>Note:</b> Refer to EDS for PCIe supported port configurations.	Setting of this field depend on what PCIe ports 17-20 configurations are desired by the board manufacturer.  <b>Note:</b> This field must be determined by the PCI Express port requirements of the design. The platform hardware designer must determine this setting.	Yes
	0	<b>PCIe Controller 5 Lane Reversal:</b>  0x0 = PCIe Lanes are not reversed. 0x1 = PCIe Lanes are reversed.  <b>Note:</b> Refer to EDS supported Lane reversal configuration.	This bit controls lane reversal behavior for PCIe Controller 5.  PCI Express port lane reversal can be done to aid in the laying out of the board.  <b>Note:</b> This setting is dependent on the board design. The platform hardware designer must determine if this port needs lane reversal.	No

## 9.161 PCH Descriptor Record 160 (Flash Descriptor Records)

Flash Address: FPSBA + 0B5h

Default Flash Address: 1B5h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1B5	7:0	Reserved, set to '0x3'		No

## 9.162 PCH Descriptor Record 161 (Flash Descriptor Records)

Flash Address: FPSBA + 0B6h

Default Flash Address: 1B6h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1B6	7:0	Reserved, set to '0x8'		No

## 9.163 PCH Descriptor Record 162 (Flash Descriptor Records)

Flash Address: FPSBA + 0B7h

Default Flash Address: 1B7h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1B7	7:0	Reserved, set to '0x10'		No

## 9.164 PCH Descriptor Record 163 (Flash Descriptor Records)

Flash Address: FPSBA + 0B8h

Default Flash Address: 1B8h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1B8	7:0	Reserved, set to '0x8'		No

## 9.165 PCH Descriptor Record 164 (Flash Descriptor Records)

Flash Address: FPSBA + 0B9h

Default Flash Address: 1ADh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1B9	7:0	Reserved, set to '0x10'		No

## 9.166 PCH Descriptor Record 165 (Flash Descriptor Records)

Flash Address: FPSBA + 0BAh

Default Flash Address: 1BAh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1BA	7:0	Reserved, set to '0x8'		No

## 9.167 PCH Descriptor Record 166 (Flash Descriptor Records)

Flash Address: FPSBA + 0BBh

Default Flash Address: 1BBh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1BB	7:0	Reserved, set to '0x10'		No

## 9.168 PCH Descriptor Record 167 (Flash Descriptor Records)

Flash Address: FPSBA + 0BCh

Default Flash Address: 1BCh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1BC	7:0	Reserved, set to '0x8'		No

## 9.169 PCH Descriptor Record 168 (Flash Descriptor Records)

Flash Address: FPSBA + 0BDh

Default Flash Address: 1BDh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1BD	24:0	Reserved, set to '0x10'		No

## 9.170 PCH Descriptor Record 169 (Flash Descriptor Records)

Flash Address: FPSBA + 0C0h

Default Flash Address: 1C0h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1C0	7:4	Reserved, set to '0x8'		No
	3:1	<b>PCIe Controller 6 (Port 21-24):</b> Straps to set the default value of the PCI Express Port Configuration 4 register covering PCIe ports 21-24.  0x0 = 4x1 0x1 = 1x2, 2x1 0x2 = 2x2 0x3 = 1x4  <b>Note:</b> Refer to EDS for PCIe supported port configurations.	Setting of this field depend on what PCIe ports 21-24 configurations are desired by the board manufacturer.  <b>Note:</b> This field must be determined by the PCI Express port requirements of the design. The platform hardware designer must determine this setting.	Yes
	0	<b>PCIe Controller 6 Lane Reversal:</b>  0x0 = PCIe Lanes are not reversed. 0x1 = PCIe Lanes are reversed.  <b>Note:</b> Refer to EDS supported Lane reversal configuration.	This bit controls lane reversal behavior for PCIe Controller 6.  PCI Express port lane reversal can be done to aid in the laying out of the board.  <b>Note:</b> This setting is dependent on the board design. The platform hardware designer must determine if this port needs lane reversal.	No

## 9.171 PCH Descriptor Record 170 (Flash Descriptor Records)

Flash Address: FPSBA + 0C1h

Default Flash Address: 1C1h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1C1	7:0	Reserved, set to '0x3'		No

## 9.172 PCH Descriptor Record 171 (Flash Descriptor Records)

Flash Address: FPSBA + 0C2h

Default Flash Address: 1C2h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1C2	7:0	Reserved, set to '0x8'		No

### 9.173 PCH Descriptor Record 172 (Flash Descriptor Records)

Flash Address:FPSBA + 0C3h

Default Flash Address: 1C3h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1C3	7:0	Reserved, set to '0x10'		No

### 9.174 PCH Descriptor Record 173 (Flash Descriptor Records)

Flash Address:FPSBA + 0C4h

Default Flash Address: 1C4h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1C4	7:0	Reserved, set to '0x8'		No

### 9.175 PCH Descriptor Record 174 (Flash Descriptor Records)

Flash Address:FPSBA + 0C5h

Default Flash Address: 1C5h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1C5	7:0	Reserved, set to '0x10'		No

### 9.176 PCH Descriptor Record 175 (Flash Descriptor Records)

Flash Address:FPSBA + 0C6h

Default Flash Address: 1C6h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1C6	7:0	Reserved, set to '0x8'		No

### 9.177 PCH Descriptor Record 176 (Flash Descriptor Records)

Flash Address:FPSBA + 0C7h

Default Flash Address: 1C7h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1C7	7:0	Reserved, set to '0x10'		No



## 9.178 PCH Descriptor Record 177 (Flash Descriptor Records)

Flash Address: FPSBA + 0C8h

Default Flash Address: 1C8h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1C8	7:0	Reserved, set to '0x8'		No

## 9.179 PCH Descriptor Record 178 (Flash Descriptor Records)

Flash Address: FPSBA + 0C9h

Default Flash Address: 1C9h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1C9	24:0	Reserved, set to '0x10'		No

## 9.180 PCH Descriptor Record 179 (Flash Descriptor Records)

Flash Address: FPSBA + 0CCh

Default Flash Address: 1CCh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1CC	7:4	Reserved, set to '0x8'		No
	3:1	<b>PCIe Controller 7 (Port 25-28):</b> Straps to set the default value of the PCI Express Port Configuration 4 register covering PCIe ports 21-24.  0x0 = 4x1 0x1 = 1x2, 2x1 0x2 = 2x2 0x3 = 1x4  <b>Note:</b> Refer to EDS for PCIe supported port configurations.	Setting of this field depend on what PCIe ports 21-24 configurations are desired by the board manufacturer.  <b>Note:</b> This field must be determined by the PCI Express port requirements of the design. The platform hardware designer must determine this setting.	Yes
	0	<b>PCIe Controller 7 Lane Reversal:</b>  0x0 = PCIe Lanes are not reversed. 0x1 = PCIe Lanes are reversed.  <b>Note:</b> Refer to EDS supported Lane reversal configuration.	This bit controls lane reversal behavior for PCIe Controller 6.  PCI Express port lane reversal can be done to aid in the laying out of the board.  <b>Note:</b> This setting is dependent on the board design. The platform hardware designer must determine if this port needs lane reversal.	No

**9.181 PCH Descriptor Record 180 (Flash Descriptor Records)**

Flash Address: FPSBA + 0CDh

Default Flash Address: 1CDh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1CD	7:0	Reserved, set to '0x3'		No

**9.182 PCH Descriptor Record 181 (Flash Descriptor Records)**

Flash Address: FPSBA + 0CEh

Default Flash Address: 1CEh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1CE	7:0	Reserved, set to '0x8'		No

**9.183 PCH Descriptor Record 182 (Flash Descriptor Records)**

Flash Address: FPSBA + 0CFh

Default Flash Address: 1CFh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1CF	7:0	Reserved, set to '0x10'		No

**9.184 PCH Descriptor Record 183 (Flash Descriptor Records)**

Flash Address: FPSBA + 0D0h

Default Flash Address: 1D0h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1D0	7:0	Reserved, set to '0x8'		No

**9.185 PCH Descriptor Record 184 (Flash Descriptor Records)**

Flash Address: FPSBA + 0D1h

Default Flash Address: 1D1h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1D1	7:0	Reserved, set to '0x10'		No

## 9.186 PCH Descriptor Record 185 (Flash Descriptor Records)

Flash Address: FPSBA + 0D2h

Default Flash Address: 1D2h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1D2	7:0	Reserved, set to '0x8'		No

## 9.187 PCH Descriptor Record 186 (Flash Descriptor Records)

Flash Address: FPSBA + 0D3h

Default Flash Address: 1D3h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1D3	7:0	Reserved, set to '0x10'		No

## 9.188 PCH Descriptor Record 187 (Flash Descriptor Records)

Flash Address: FPSBA + 0D4h

Default Flash Address: 1D4h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1D4	7:0	Reserved, set to '0x8'		No

## 9.189 PCH Descriptor Record 188 (Flash Descriptor Records)

Flash Address: FPSBA + 0D5h

Default Flash Address: 1D5h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1D5	24:0	Reserved, set to '0x10'		No

## 9.190 PCH Descriptor Record 189 (Flash Descriptor Records)

Flash Address: FPSBA + 0D8h

Default Flash Address: 1D8h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1D8	7:1	Reserved, set to '0xCA'		No

Offset from 0	Bits	Description	Usage	FIT Visible
<b>0x1D8 (Cont)</b>	0	<b>DMI Lane Reversal (DMILR):</b> 0x0 = DMI Lanes are not reversed. 0x1 = 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.  <b>Note:</b> This setting is dependent on the board design. The platform hardware designer must determine if DMI needs lane reversal.	<b>Yes</b>

## 9.191 PCH Descriptor Record 190 (Flash Descriptor Records)

Flash Address: FPSBA + 0D9h

Default Flash Address: 1D9h

Offset from 0	Bits	Description	Usage	FIT Visible
<b>0x1D9</b>	7:0	<b>Reserved, set to '0x1'</b>		<b>No</b>

## 9.192 PCH Descriptor Record 191 (Flash Descriptor Records)

Flash Address: FPSBA + 0DAh

Default Flash Address: 1DAh

Offset from 0	Bits	Description	Usage	FIT Visible
<b>0x1DA</b>	7:6	<b>Reserved, set to '0'</b>		<b>No</b>
	5	<b>DMI AC Coupling (DMI_ACCSS):</b> 0x0 = DMI is operating in DC-coupling mode 0x1 = DMI is operating in AC-coupling mode	This setting determines if DMI is operating in AC or DC coupled mode.	<b>Yes</b>
	4:0	<b>Reserved, set to '0x8'</b>		<b>No</b>

## 9.193 PCH Descriptor Record 192 (Flash Descriptor Records)

Flash Address: FPSBA + 0DBh

Default Flash Address: 1DBh

Offset from 0	Bits	Description	Usage	FIT Visible
<b>0x1DB</b>	7:4	<b>Reserved, set to '0x2'</b>		<b>No</b>
	3:1	<b>DMI Lane Width (DMI_FDP1):</b> 0x2 = DMI x4 0x3 = DMI x8	This setting determines the number of DMI lanes available.	<b>Yes</b>
	0	<b>Reserved, set to '0'</b>		<b>No</b>

## 9.194 PCH Descriptor Record 193 (Flash Descriptor Records)

Flash Address: FPSBA + 0DCh

Default Flash Address: 1DCh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1DC	31	<b>Reserved, set to '0x1'</b>		<b>No</b>
	30	<b>Intel® Trace Hub Soft Enable:</b> 0x0 = ROM Tracing Soft Disable 0x1 = ROM Tracing Soft Enable	This soft strap enables ROM based tracing in the Intel® CSME.  Only applicable if Intel® Trace Hub Debug Messages strap is also enabled	<b>Yes</b>
	29:22	<b>Reserved, set to '0'</b>		<b>No</b>
	21	<b>Intel® Trace Hub - Emergency Mode:</b> 0x0 = ROM Tracing Emergency mode disabled 0x1 = ROM Tracing Emergency mode enabled	This option enables ROM Tracing in the base platform image.	<b>Yes</b>
	20	<b>Deep Sx Enable (Deep_SX_EN):</b> 0x0 = Deep Sx is not supported on the platform 0x1 = Deep Sx is supported on the platform	This requires the target platform to support Deep Sx state  <b>Note:</b> When configuring Deep Sx you must also set <b>DEEPSX_PLT_CFG_SS</b> .	<b>Yes</b>
	19	<b>Software Re-Binding Enabled:</b> 0x0 = SPI Re-Binding disabled 0x1 = SPI Re-Binding enabled	When enabled this settings will allow for SPI re-binding to a new PCH during manufacturing and re-manufacturing flows prior to platform EOM.  <b>Note:</b> Re-binding to a replacement PCH can only be done a maximum of 5 times before the SPI part needs to be re-flashed.	<b>Yes</b>
	18	<b>Reserved, set to '0'</b>		<b>No</b>
	17	<b>Direct Connect Interface (DCI) Enabled:</b> 0x0 = DCI Disabled 0x1 = DCI Enabled		<b>Yes</b>
	16	<b>Reserved, set to '0'</b>		<b>Yes</b>
	15:12	<b>Reserved, set to '0'</b>		<b>No</b>
	11	<b>Intel® ME AFS Flash Idle Reclaim Enable:</b> 0x0 = AFS Flash Reclaim enabled 0x1 = AFS Flash Reclaim disabled	This controls enabling / disabling of Intel® ME AFS Idle flash reclaim capabilities.  <b>Note:</b> This setting should be used for debug purposes only	<b>Yes</b>
	10	<b>Intel® ME Reset Behavior:</b> 0x0 = Intel® ME shall attempt to boot from the next available image, if exists. 0x1 = Intel® ME will halt		<b>Yes</b>
	9:1	<b>Reserved, set to '0x58'</b>		<b>No</b>
	0	<b>Firmware ROM Bypass Enable Softstrap:</b> 0x0 = ROM Bypass disabled 0x1 = ROM Bypass enabled	This determines if firmware boots from the PCH on-board ROM or SPI.  <b>Note:</b> This setting only has affect when the firmware being used has ROM Bypass code present.	<b>Yes</b>

## 9.195 PCH Descriptor Record 194 (Flash Descriptor Records)

Flash Address: FPSBA + 0E0h

Default Flash Address: 1E0h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1E0	7:0	Reserved, set to '0'		No

## 9.196 PCH Descriptor Record 195 (Flash Descriptor Records)

Flash Address: FPSBA + 0E1h

Default Flash Address: 1E1h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1E1	7:0	Reserved, set to '0'		No

## 9.197 PCH Descriptor Record 196 (Flash Descriptor Records)

Flash Address: FPSBA + 0E2h

Default Flash Address: 1E2h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1E2	7:0	Reserved, set to '0'		No

## 9.198 PCH Descriptor Record 197 (Flash Descriptor Records)

Flash Address: FPSBA + 0E3h

Default Flash Address: 1E3h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1E3	7:0	Reserved, set to '0'		No

## 9.199 PCH Descriptor Record 198 (Flash Descriptor Records)

Flash Address: FPSBA + 0E4h

Default Flash Address: 1E4h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1E4	7:1	Reserved, set to '0'		No
	0	<b>SMBus / SMLink TCO Slave Connection:</b> 0x0 = TCO Slave connected to Intel® ME SMBus 0x1 = TCO Slave connected to Intel® ME SMBus and SMLink0	See: Raptor Lake Platform Controller Hub (PCH-) EDS for more details.	Yes

## 9.200 PCH Descriptor Record 199 (Flash Descriptor Records)

Flash Address: FPSBA + 0E5h

Default Flash Address: 1E5h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1E5	7:1	Reserved, set to '0'		No
	0	<b>SMT1 State (SMTEN):</b> 0x0 = SMT1 Disabled 0x1 = SMT1 Enabled	On images that support manageability, the parameter will behave as set. E.g. "Enabled" will enable the SMT1. On images that do not support manageability, the firmware automatically disables SMT1 to allow S0i3.4. To bypass this behavior, setting this parameter to "Disabled" will indicate the firmware to enable SMT1.	Yes

## 9.201 PCH Descriptor Record 200 (Flash Descriptor Records)

Flash Address: FPSBA + 0E6h

Default Flash Address: 1E6h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1E6	7:0	Reserved, set to '0'		No

## 9.202 PCH Descriptor Record 201 (Flash Descriptor Records)

Flash Address: FPSBA + 0E7h

Default Flash Address: 1E7h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1E7	7	Reserved, set to '0'		No
	6:0	<b>Intel® ME SMBus I<sup>2</sup>C Address (MESMI2CA):</b> Defines 7 bit Intel ME SMBus I2C target address <b>Default set to '0'</b> <b>Note:</b> This field is only used for testing purposes.	This address is only used by Intel® ME FW for testing purposes. If <b>MESMI2CEN</b> (Offset 0x10A bit 0) is set to 1 then the address used in this field must be non-zero and not conflict with any other devices on the segment.	Yes

## 9.203 PCH Descriptor Record 202 (Flash Descriptor Records)

Flash Address: FPSBA + 0E8h

Default Flash Address: 1E8h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1E8	7	Reserved, set to '0'		No
	6:0	<b>Intel® ME SMBus ASD Address (MESMASDA):</b> Intel® ME SMBus Controller ASD Target Address. ASD: Alert Sending Device  <b>Default set to '0'</b>  <b>Note:</b> This field is only applicable if there is an ASD attached to SMBus and using Intel® AMT	If <b>MESMASDEN (PCH Descriptor Record 8 bit 0)</b> is set to '1' there must be a valid address for ASD. The address must be determined by the BIOS developer based on the requirements below.  A valid address must be: <ul style="list-style-type: none"> <li>Non-zero value</li> <li>Must be a unique address on the Host SMBus segment</li> <li>Be compatible with the master on SMBus - For example, if the ASD address the master that needs write thermal information to an address "xy"h. Then this field must be set to xy"h.</li> </ul>	Yes

## 9.204 PCH Descriptor Record 203 (Flash Descriptor Records)

Flash Address: FPSBA + 0E9h

Default Flash Address: 1E9h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1E9	7:0	Reserved, set to '0'		No

## 9.205 PCH Descriptor Record 204 (Flash Descriptor Records)

Flash Address: FPSBA + 0EAh

Default Flash Address: 1EAh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1EA	7:1	Reserved, set to '0'		No
	0	<b>Intel® ME SMBus I<sup>2</sup>C Address Enable (MESMI2CEN):</b>  0x0 = Intel® ME SMBus I <sup>2</sup> C Address is disabled 0x1 = Intel® ME SMBus I <sup>2</sup> C Address is enabled  <b>Note:</b> This field is only used for testing purposes.	This field should only be set to '1' for testing purposes	Yes



## 9.206 PCH Descriptor Record 205 (Flash Descriptor Records)

Flash Address: FPSBA + 0EBh

Default Flash Address: 1EBh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1EB	7:1	Reserved, set to '0'		No
	0	<b>Intel® ME SMBus ASD Address Enable (MESMASDEN):</b> 0x0 = Intel® ME SMBus ASD Address is disabled 0x1 = Intel® ME SMBus ASD Address is enabled <b>Note:</b> This field is only applicable if there is an ASD attached to SMBus and using Intel® AMT	This bit must only be set to '1' when there is an ASD (Alert Sending Device) attached to Host SMBus. This is only applicable in platforms using Intel® AMT. <b>Note:</b> This setting is not the same for all designs, is dependent on the board design. The setting of this field must be determined by the BIOS developer and the platform hardware designer.	Yes

## 9.207 PCH Descriptor Record 206 (Flash Descriptor Records)

Flash Address: FPSBA + 0ECh

Default Flash Address: 1ECh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1EC	7:0	Reserved, set to '0'		No

## 9.208 PCH Descriptor Record 207 (Flash Descriptor Records)

Flash Address: FPSBA + 0EDh

Default Flash Address: 1EDh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1ED	7:0	Reserved, set to '0'		No

## 9.209 PCH Descriptor Record 208 (Flash Descriptor Records)

Flash Address: FPSBA + 0EEh

Default Flash Address: 1EEh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1EE	31:0	<b>Intel® ME SMBus Subsystem Device ID for ASF (MESMA2UDID):</b> MESMAUDID[15:0] - <b>Subsystem Vendor ID</b> MESMAUDID[31:16] - <b>Subsystem Device ID</b>  The values contained in MESMAUDID[15:0] and MESMAUDID[31:16] are provided as bytes 8-9 and 10-11 of the data payload to an external master when it initiates a Directed GET UDID Block Read Command to the Alert Sending Device ASD's address.  <b>Default set to '0'</b>	This bit must only be set to '1' when there is an ASD (Alert Sending Device) attached to SMBus and when MESMASDEN (FPSBA + 0x173h) is set to '1'. This is only applicable in platforms using Intel® AMT. Set this if you want to add a 4 byte payload to an external master when a GET UDID Block read command is made to Intel ME SMBus ASD's address.	<b>Yes</b>

## 9.210 PCH Descriptor Record 209 (Flash Descriptor Records)

Flash Address: FPSBA + 0F2h

Default Flash Address: 1F2h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1F2	31:0	Reserved, set to '0'		No

## 9.211 PCH Descriptor Record 210 (Flash Descriptor Records)

Flash Address: FPSBA + 0F6h

Default Flash Address: 1F6h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1F6	7:2	Reserved, set to '0'		No
	1:0	<b>Intel® ME SMBus Frequency (SMB0FRQ):</b> The value of these bits determine the physical bus speed supported by the HW.  <b>Set to '0x1'</b>	Intel® ME SMBus	No

## 9.212 PCH Descriptor Record 211 (Flash Descriptor Records)

Flash Address: FPSBA + 0F7h

Default Flash Address: 1F7h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1F7	7:0	Reserved, set to '0'		No

## 9.213 PCH Descriptor Record 212 (Flash Descriptor Records)

Flash Address:FPSBA + 0F8h

Default Flash Address: 1F8h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1F8	7:0	Reserved, set to '0x1'		No

## 9.214 PCH Descriptor Record 213 (Flash Descriptor Records)

Flash Address:FPSBA + 0F9h

Default Flash Address: 1F9h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1F9	7:1	Reserved, set to '0'		No
	0	<b>SMLink0 Enable (SML0_EN):</b> Configures if SMLink0 segment is enabled  0 = Disabled 1 = Enabled  <b>Notes:</b> 1. This bit MUST be set to '1' when utilizing integrated LAN controller. 2. The SMBus TCO Slave controller must be routed to this SMLink 0 Segment. 3. This segment should be set to 0 in one of the following cases: a. Disabled by the user.	The Intel PHY SMBus controller must be routed to this SMLink 0 Segment.  <b>Note:</b> This setting is not the same for all designs, is dependent on the board design. The setting of this field must be determined by the BIOS developer and the platform hardware designer.	Yes

## 9.215 PCH Descriptor Record 214 (Flash Descriptor Records)

Flash Address:FPSBA + 0FAh

Default Flash Address: 1FAh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1FA	7:0	Reserved, set to '0'		No

## 9.216 PCH Descriptor Record 215 (Flash Descriptor Records)

Flash Address:FPSBA + 0FBh

Default Flash Address: 1FBh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1FB	7:0	Reserved, set to '0'		No

## 9.217 PCH Descriptor Record 216 (Flash Descriptor Records)

Flash Address: FPSBA + 0FCh

Default Flash Address: 1FCh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1FC	7:0	Reserved, set to '0'		No

## 9.218 PCH Descriptor Record 217 (Flash Descriptor Records)

Flash Address: FPSBA + 0FDh

Default Flash Address: 1FDh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1FD	7:0	Intel® SMLink0 MCTP Address (SMT2_MCTP_ADDR): 0x0 - 0x7F	This setting configures the Intel(R) SMLink0 MCTP Address. <b>Note:</b> This setting is only used for testing.	Yes

## 9.219 PCH Descriptor Record 218 (Flash Descriptor Records)

Flash Address: FPSBA + 0FEh

Default Flash Address: 1FEh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1FE	7:0	Reserved, set to '0'		No

## 9.220 PCH Descriptor Record 219 (Flash Descriptor Records)

Flash Address: FPSBA + 0FFh

Default Flash Address: 1FFh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1FF	7:0	Reserved, set to '0'		No

## 9.221 PCH Descriptor Record 220 (Flash Descriptor Records)

Flash Address:FPSBA + 100h

Default Flash Address: 200h

Offset from 0	Bits	Description	Usage	FIT Visible
0x200	7:0	<b>Intel® SMLink0 MCTP Address Enabled (SMT2_MCTP_EN):</b> 0x0 = Intel® SMLink0 MCTP Address Disabled 0x1 = Intel® SMLink0 MCTP Address Enabled	This setting enables / disables the Intel(R) SMLink0 MCTP Address.  <b>Note:</b> This setting is only used for testing purposes.	Yes

## 9.222 PCH Descriptor Record 221 (Flash Descriptor Records)

Flash Address:FPSBA + 101h

Default Flash Address: 201h

Offset from 0	Bits	Description	Usage	FIT Visible
0x201	7:0	Reserved, set to '0'		No

## 9.223 PCH Descriptor Record 222 (Flash Descriptor Records)

Flash Address:FPSBA + 102h

Default Flash Address: 202h

Offset from 0	Bits	Description	Usage	FIT Visible
0x202	31:0	Reserved, set to '0'		No

## 9.224 PCH Descriptor Record 223 (Flash Descriptor Records)

Flash Address:FPSBA + 106h

Default Flash Address: 206h

Offset from 0	Bits	Description	Usage	FIT Visible
0x206	31:0	Reserved, set to '0'		No

## 9.225 PCH Descriptor Record 224 (Flash Descriptor Records)

Flash Address: FPSBA + 10Ah

Default Flash Address: 20Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0x20A	7:2	Reserved, set to '0'		No
	1:0	<b>SMLink0 Frequency (SML0FRQ):</b> These bits determine the physical bus speed supported by the HW.  0x1 = Standard Mode - up to 100 kHz 0x2 = Fast Mode - up to 400 kHz 0x3 = Fast Mode Plus - up to 1 MHz	Speed is dependent on board topology and layout.	Yes

## 9.226 PCH Descriptor Record 225 (Flash Descriptor Records)

Flash Address: FPSBA + 10Bh

Default Flash Address: 20Bh

Offset from 0	Bits	Description	Usage	FIT Visible
0x20B	7:0	Reserved, set to '0'		No

## 9.227 PCH Descriptor Record 226 (Flash Descriptor Records)

Flash Address: FPSBA + 10Ch

Default Flash Address: 20Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x20C	7:0	Reserved, set to '0'		No

## 9.228 PCH Descriptor Record 227 (Flash Descriptor Records)

Flash Address: FPSBA + 10Dh

Default Flash Address: 20Dh

Offset from 0	Bits	Description	Usage	FIT Visible
0x20D	7:1	Reserved, set to '0'		No
	0	<b>SMLink1 Enable (SML1_EN):</b> Configures if SMLink1 segment is enabled  0 = Disabled 1 = Enabled  <b>Note:</b> This must be set to '1' platforms that use PCH SMBus based thermal reporting.	This bit must be set to '1' if using the PCH's Thermal reporting. If setting this bit to '0', there must be an external solution that gathers temperature information from PCH and processor.  <b>Note:</b> This setting is not the same for all designs, is dependent on the board design. The setting of this field must be determined by the BIOS developer and the platform hardware designer.	Yes

## 9.229 PCH Descriptor Record 228 (Flash Descriptor Records)

Flash Address: FPSBA + 10Eh

Default Flash Address: 20Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0x20E	7:1	<b>SMLink1 GP Target Address (SML1GPA):</b> SMLink1 controller General Purpose Target Address (7:1)  <b>Notes:</b> <ol style="list-style-type: none"> <li>This field is not active unless SML1GPAEN is set to '1'.</li> <li>This address MUST be set if there is a device on the SMLink1 segment that will use SMBus based PCH thermal reporting.</li> <li>If SML1GPAEN = '1' then this field must be a valid 7 bit, non-zero address that does not conflict with any other devices on SMLink1 segment.</li> </ol> <b>Default set to '0'</b>	When <b>SML1GPAEN</b> = '1', there needs to be a valid GP address in this field. This address used here is design specific. The BIOS developer and / or platform hardware designer must supply an address with the criteria below.  A valid address must be: <ul style="list-style-type: none"> <li>Non-zero value</li> <li>Must be a unique address on the SMLink1 segment</li> <li>Be compatible with the master on SMLink1 - For example if the GP address the master that needs read thermal information from a certain address, then this field must be set accordingly.</li> </ul>	<b>Yes</b>
	0	<b>SMLink1 GP Target Address Enable (SML1GPAEN):</b>  SMLink1 controller General Purpose Target Address Enable  0x0 = SMLink1 GP Address is disabled 0x1 = SMLink1 GP Address is enabled  This bit MUST set to '1' if there is a device on the SMLink1 segment that will use SMBus based PCH thermal reporting. This bit MUST be set to '0' if PCH thermal reporting is not used.	This bit must be set in cases where SMLink1 has a master that requires SMBus based Thermal Reporting that is supplied by the PCH. Some examples of this master could be an Embedded Controller, a BMC, or any other SMBus Capable device that needs Processor or PCH temperature information. If no master on the SMLink1 segment is capable of utilizing thermal reporting, then this field must be set to '0'.  <b>Note:</b> This setting is not the same for all designs, is dependent on the board design. The setting of this field must be determined by the BIOS developer and the platform hardware designer.	<b>Yes</b>

## 9.230 PCH Descriptor Record 229 (Flash Descriptor Records)

Flash Address: FPSBA + 10Fh

Default Flash Address: 20Fh

Offset from 0	Bits	Description	Usage	FIT Visible
0x20F	7	<b>Reserved, set to '0'</b>		<b>No</b>
	6:0	<b>SMLink1 I<sup>2</sup>C* Target Address (SML1I2CA):</b> Defines the 7 bit I2C target address for PCH Thermal Reporting on SMLink1.  <b>Notes:</b> <ol style="list-style-type: none"> <li>This field is not active unless SML1I2CAEN is set to '1'.</li> <li>This address MUST be set if there is a device on the SMLink1 segment that will use thermal reporting supplied by PCH.</li> <li>If SML1I2CAEN = '1' then this field must be a valid 7 bit, non-zero address that does not conflict with any other devices on SMLink1 segment.</li> <li>This address can be different for every design, ensure BIOS developer supplies the address.</li> </ol> <b>Default set to '0'</b>	When <b>SML1I2CAEN(PCHSTRP11 bit 24)</b> = '1', there needs to be a valid I2C address in this field. This address used here is design specific. The BIOS developer and/or platform hardware designer must supply an address with the criteria below.  <b>A valid address must be:</b> <ul style="list-style-type: none"> <li>Non-zero value</li> <li>Must be a unique address on the SMLink1 segment</li> <li>Be compatible with the master on SMLink1 - For example, if the I<sup>2</sup>C address the master that needs write thermal information to a address "xy"h. Then this field must be to "xy"h.</li> </ul>	<b>Yes</b>

## 9.231 PCH Descriptor Record 230 (Flash Descriptor Records)

Flash Address: FPSBA + 110h

Default Flash Address: 210h

Offset from 0	Bits	Description	Usage	FIT Visible
0x210	7:0	Reserved, set to '0'		No

## 9.232 PCH Descriptor Record 231 (Flash Descriptor Records)

Flash Address: FPSBA + 111h

Default Flash Address: 211h

Offset from 0	Bits	Description	Usage	FIT Visible
0x211	7	Reserved, set to '0'		No
	6:0	<b>SMLink1 MCTP Address:</b> Defines 7 bit Intel ME SMLink1 MCTP target address  <b>Default set to '0'</b>  <b>Note:</b> This field is only used for testing purposes.	If Intel® ME SMLink MCTP Address Enable is set to 1 then the address used in this field must be non-zero and not conflict with any other devices on the segment.	Yes

## 9.233 PCH Descriptor Record 231 (Flash Descriptor Records)

Flash Address: FPSBA + 112h

Default Flash Address: 212h

Offset from 0	Bits	Description	Usage	FIT Visible
0x212	7:1	Reserved, set to '0'		No
	0	<b>SMLink1 I<sup>2</sup>C Address Enable:</b>  0x0 = Intel® ME SMLink I <sup>2</sup> C Address is disabled 0x1 = Intel® ME SMLink I <sup>2</sup> C Address is enabled  <b>Note:</b> This field is only used for testing purposes.	This field should only be set to '1' for testing purposes	Yes

## 9.234 PCH Descriptor Record 233 (Flash Descriptor Records)

Flash Address: FPSBA + 113h

Default Flash Address: 213h

Offset from 0	Bits	Description	Usage	FIT Visible
0x213	7:0	Reserved, set to '0'		No



## 9.235 PCH Descriptor Record 234 (Flash Descriptor Records)

Flash Address: FPSBA + 114h

Default Flash Address: 214h

Offset from 0	Bits	Description	Usage	FIT Visible
0x214	7:1	Reserved, set to '0'		No
	0	<b>SMLink1 MCTP Address Enable:</b> 0x0 = Intel ME SMBus MCTP Address is disabled 0x1 = Intel ME SMBus MCTP Address is enabled <b>Note:</b> This field is only used for testing purposes.		Yes

## 9.236 PCH Descriptor Record 235 (Flash Descriptor Records)

Flash Address: FPSBA + 115h

Default Flash Address: 215h

Offset from 0	Bits	Description	Usage	FIT Visible
0x215	7:0	Reserved, set to '0'		No

## 9.237 PCH Descriptor Record 236 (Flash Descriptor Records)

Flash Address: FPSBA + 116h

Default Flash Address: 216h

Offset from 0	Bits	Description	Usage	FIT Visible
0x216	31:0	Reserved, set to '0'		No

## 9.238 PCH Descriptor Record 237 (Flash Descriptor Records)

Flash Address: FPSBA + 11Ah

Default Flash Address: 21Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0x21A	31:0	Reserved, set to '0'		No

## 9.239 PCH Descriptor Record 238 (Flash Descriptor Records)

Flash Address: FPSBA + 11Eh

Default Flash Address: 21Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0x21E	7:2	Reserved, set to '0'		No
	1:0	<b>SMLink1 Frequency (SML1FRQ) Frequency</b> 0x1 = Standard Mode - up to 100 kHz 0x2 = Fast Mode - up to 400 kHz 0x3 = Fast Mode Plus - up to 1 MHz		Yes

## 9.240 PCH Descriptor Record 239 (Flash Descriptor Records)

Flash Address: FPSBA + 11Fh

Default Flash Address: 21Fh

Offset from 0	Bits	Description	Usage	FIT Visible
0x21F	7:0	Reserved, set to '0'		No

## 9.241 PCH Descriptor Record 240 (Flash Descriptor Records)

Flash Address: FPSBA + 120h

Default Flash Address: 220h

Offset from 0	Bits	Description	Usage	FIT Visible
0x220	7:0	Reserved, set to '0'		No

## 9.242 PCH Descriptor Record 241 (Flash Descriptor Records)

Flash Address: FPSBA + 121h

Default Flash Address: 221h

Offset from 0	Bits	Description	Usage	FIT Visible
0x221	7:1	Reserved, set to '0'		No
	0	<b>SMLink2 Enable (SML2_EN):</b> Configures if SMLink2 segment is enabled  0 = Disabled 1 = Enabled  <b>Note:</b> This must be set to '1' platforms that use PCH SMBus based thermal reporting.	This bit must be set to '1' if using the PCH's Thermal reporting. If setting this bit to '0', there must be an external solution that gathers temperature information from PCH and processor.  <b>Note:</b> This setting is not the same for all designs, is dependent on the board design. The setting of this field must be determined by the BIOS developer and the platform hardware designer.	Yes

## 9.243 PCH Descriptor Record 242 (Flash Descriptor Records)

Flash Address: FPSBA + 122h

Default Flash Address: 222h

Offset from 0	Bits	Description	Usage	FIT Visible
0x222	7:0	Reserved, set to '0'		No

## 9.244 PCH Descriptor Record 243 (Flash Descriptor Records)

Flash Address: FPSBA + 123h

Default Flash Address: 223h

Offset from 0	Bits	Description	Usage	FIT Visible
0x223	7:0	Reserved, set to '0'		No

## 9.245 PCH Descriptor Record 244 (Flash Descriptor Records)

Flash Address: FPSBA + 124h

Default Flash Address: 224h

Offset from 0	Bits	Description	Usage	FIT Visible
0x224	7:0	Reserved, set to '0'		No

## 9.246 PCH Descriptor Record 245 (Flash Descriptor Records)

Flash Address: FPSBA + 125h

Default Flash Address: 225h

Offset from 0	Bits	Description	Usage	FIT Visible
0x225	7:1	Reserved, set to '0'		No
	0	<b>SMLink2 MCTP Address Enable:</b> 0x0 = SMLink2 MCTP Address is disabled 0x1 = SMLink2 MCTP Address is enabled  <b>Note:</b> This field is only used for testing purposes.	This setting configures the SMLink2 MCTP Address. Note: This setting is only used for testing purposes. The default setting is "0000000"	Yes

## 9.247 PCH Descriptor Record 246 (Flash Descriptor Records)

Flash Address: FPSBA + 126h

Default Flash Address: 226h

Offset from 0	Bits	Description	Usage	FIT Visible
0x226	7:0	Reserved, set to '0'		No

## 9.248 PCH Descriptor Record 247 (Flash Descriptor Records)

Flash Address: FPSBA + 127h

Default Flash Address: 227h

Offset from 0	Bits	Description	Usage	FIT Visible
0x227	7:0	Reserved, set to '0'		No

## 9.249 PCH Descriptor Record 248 (Flash Descriptor Records)

Flash Address: FPSBA + 128h

Default Flash Address: 228h

Offset from 0	Bits	Description	Usage	FIT Visible
0x228	7:1	Reserved, set to '0'		No
	0	<b>SMLink2 MCTP Address Enable:</b> 0x0 = SMLink2 MCTP Address is disabled 0x1 = SMLink2 MCTP Address is enabled  <b>Note:</b> This field is only used for testing purposes.	This setting enables / disables the SMLink2 MCTP Address. Note: This setting is only used for testing purposes. The recommended setting is "No" SMBus / SMLink	Yes

## 9.250 PCH Descriptor Record 249 (Flash Descriptor Records)

Flash Address: FPSBA + 129h

Default Flash Address: 229h

Offset from 0	Bits	Description	Usage	FIT Visible
0x229	7:0	Reserved, set to '0'		No

## 9.251 PCH Descriptor Record 250 (Flash Descriptor Records)

Flash Address: FPSBA + 12Ah

Default Flash Address: 22Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0x22A	31:0	Reserved, set to '0'		No

## 9.252 PCH Descriptor Record 251 (Flash Descriptor Records)

Flash Address: FPSBA + 12Eh

Default Flash Address: 22Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0x22E	31:0	Reserved, set to '0'		No

## 9.253 PCH Descriptor Record 252 (Flash Descriptor Records)

Flash Address: FPSBA + 132h

Default Flash Address: 232h

Offset from 0	Bits	Description	Usage	FIT Visible
0x232	7:2	Reserved, set to '0'		No
	1:0	<b>SMLink2 Frequency (SML2FRQ) Frequency</b> 0x1 = Standard Mode - up to 100 kHz 0x2 = Fast Mode - up to 400 kHz 0x3 = Fast Mode Plus - up to 1 MHz		Yes

## 9.254 PCH Descriptor Record 253 (Flash Descriptor Records)

Flash Address: FPSBA + 133h

Default Flash Address: 233h

Offset from 0	Bits	Description	Usage	FIT Visible
0x233	7:0	Reserved, set to '0'		No

## 9.255 PCH Descriptor Record 254 (Flash Descriptor Records)

Flash Address: FPSBA + 134h

Default Flash Address: 234h

Offset from 0	Bits	Description	Usage	FIT Visible
0x234	7:0	Reserved, set to '0'		No

## 9.256 PCH Descriptor Record 255 (Flash Descriptor Records)

Flash Address: FPSBA + 135h

Default Flash Address: 235h

Offset from 0	Bits	Description	Usage	FIT Visible
0x235	7:0	Reserved, set to '0'		No

## 9.257 PCH Descriptor Record 256 (Flash Descriptor Records)

Flash Address: FPSBA + 136h

Default Flash Address: 236h

Offset from 0	Bits	Description	Usage	FIT Visible
0x236	7:0	Reserved, set to '0'		No

## 9.258 PCH Descriptor Record 257 (Flash Descriptor Records)

Flash Address: FPSBA + 137h

Default Flash Address: 237h

Offset from 0	Bits	Description	Usage	FIT Visible
0x237	7:0	Reserved, set to '0'		No

## 9.259 PCH Descriptor Record 258 (Flash Descriptor Records)

Flash Address: FPSBA + 138h

Default Flash Address: 238h

Offset from 0	Bits	Description	Usage	FIT Visible
0x238	7:0	Reserved, set to '0'		No

## 9.260 PCH Descriptor Record 259 (Flash Descriptor Records)

Flash Address: FPSBA + 139h

Default Flash Address: 239h

Offset from 0	Bits	Description	Usage	FIT Visible
0x239	7:0	Reserved, set to '0'		No

## 9.261 PCH Descriptor Record 260 (Flash Descriptor Records)

Flash Address: FPSBA + 13Ah

Default Flash Address: 23Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0x23A	7:0	Reserved, set to '0'		No

## 9.262 PCH Descriptor Record 261 (Flash Descriptor Records)

Flash Address: FPSBA + 13Bh

Default Flash Address: 23Bh

Offset from 0	Bits	Description	Usage	FIT Visible
0x23B	7:0	Reserved, set to '0'		No

## 9.263 PCH Descriptor Record 262 (Flash Descriptor Records)

Flash Address: FPSBA + 13Ch

Default Flash Address: 23Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x23C	7:0	Reserved, set to '0'		No

## 9.264 PCH Descriptor Record 263 (Flash Descriptor Records)

Flash Address: FPSBA + 13Dh

Default Flash Address: 23Dh

Offset from 0	Bits	Description	Usage	FIT Visible
0x23D	7:0	Reserved, set to '0'		No

## 9.265 PCH Descriptor Record 264 (Flash Descriptor Records)

Flash Address: FPSBA + 13Eh

Default Flash Address: 23Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0x23E	31:0	Reserved, set to '0'		No

## 9.266 PCH Descriptor Record 265 (Flash Descriptor Records)

Flash Address: FPSBA + 142h

Default Flash Address: 242h

Offset from 0	Bits	Description	Usage	FIT Visible
0x242	31:0	Reserved, set to '0x1'		No

## 9.267 PCH Descriptor Record 266 (Flash Descriptor Records)

Flash Address: FPSBA + 146h

Default Flash Address: 246h

Offset from 0	Bits	Description	Usage	FIT Visible
0x246	7:0	Reserved, set to '0'		No

## 9.268 PCH Descriptor Record 267 (Flash Descriptor Records)

Flash Address: FPSBA + 147h

Default Flash Address: 247h

Offset from 0	Bits	Description	Usage	FIT Visible
0x247	7:0	Reserved, set to '0'		No

## 9.269 PCH Descriptor Record 268 (Flash Descriptor Records)

Flash Address: FPSBA + 148h

Default Flash Address: 248h

Offset from 0	Bits	Description	Usage	FIT Visible
0x248	7:0	Reserved, set to '0'		No



## 9.270 PCH Descriptor Record 269 (Flash Descriptor Records)

Flash Address: FPSBA + 149h

Default Flash Address: 249h

Offset from 0	Bits	Description	Usage	FIT Visible
0x249	7:0	Reserved, set to '0'		No

## 9.271 PCH Descriptor Record 270 (Flash Descriptor Records)

Flash Address: FPSBA + 14Ah

Default Flash Address: 24Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0x24A	7:0	Reserved, set to '0'		No

## 9.272 PCH Descriptor Record 271 (Flash Descriptor Records)

Flash Address: FPSBA + 14Bh

Default Flash Address: 24Bh

Offset from 0	Bits	Description	Usage	FIT Visible
0x24B	7:0	Reserved, set to '0'		No

## 9.273 PCH Descriptor Record 272 (Flash Descriptor Records)

Flash Address: FPSBA + 14Ch

Default Flash Address: 24Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x24C	7:0	Reserved, set to '0'		No

## 9.274 PCH Descriptor Record 273 (Flash Descriptor Records)

Flash Address: FPSBA + 14Dh

Default Flash Address: 24Dh

Offset from 0	Bits	Description	Usage	FIT Visible
0x24D	7:0	Reserved, set to '0'		No

## 9.275 PCH Descriptor Record 274 (Flash Descriptor Records)

Flash Address: FPSBA + 14Eh

Default Flash Address: 24Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0x24E	7:0	Reserved, set to '0'		No

## 9.276 PCH Descriptor Record 275 (Flash Descriptor Records)

Flash Address: FPSBA + 14Fh

Default Flash Address: 24Fh

Offset from 0	Bits	Description	Usage	FIT Visible
0x24F	7:0	Reserved, set to '0'		No

## 9.277 PCH Descriptor Record 276 (Flash Descriptor Records)

Flash Address: FPSBA + 150h

Default Flash Address: 250h

Offset from 0	Bits	Description	Usage	FIT Visible
0x250	7:0	Reserved, set to '0'		No

## 9.278 PCH Descriptor Record 277 (Flash Descriptor Records)

Flash Address: FPSBA + 151h

Default Flash Address: 251h

Offset from 0	Bits	Description	Usage	FIT Visible
0x251	7:0	Reserved, set to '0'		No

## 9.279 PCH Descriptor Record 278 (Flash Descriptor Records)

Flash Address: FPSBA + 152h

Default Flash Address: 252h

Offset from 0	Bits	Description	Usage	FIT Visible
0x252	31:0	Reserved, set to '0'		No

## 9.280 PCH Descriptor Record 279 (Flash Descriptor Records)

Flash Address: FPSBA + 156h

Default Flash Address: 256h

Offset from 0	Bits	Description	Usage	FIT Visible
0x256	31:0	Reserved, set to '0'		No

## 9.281 PCH Descriptor Record 280 (Flash Descriptor Records)

Flash Address: FPSBA + 15Ah

Default Flash Address: 25Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0x25A	7:0	Reserved, set to '0'		No

## 9.282 PCH Descriptor Record 281 (Flash Descriptor Records)

Flash Address: FPSBA + 25Bh

Default Flash Address: 25Bh

Offset from 0	Bits	Description	Usage	FIT Visible
0x25B	7:0	Reserved, set to '0'		No

## 9.283 PCH Descriptor Record 282 (Flash Descriptor Records)

Flash Address: FPSBA + 15Ch

Default Flash Address: 25Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x25C	7:0	Reserved, set to '0x7'		No

## 9.284 PCH Descriptor Record 283 (Flash Descriptor Records)

Flash Address: FPSBA + 15Dh

Default Flash Address: 25Dh

Offset from 0	Bits	Description	Usage	FIT Visible
0x25D	7:0	Reserved, set to '0'		No

## 9.285 PCH Descriptor Record 284 (Flash Descriptor Records)

Flash Address: FPSBA + 15Eh

Default Flash Address: 25Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0x25E	7:0	Reserved, set to '0'		No

## 9.286 PCH Descriptor Record 285 (Flash Descriptor Records)

Flash Address: FPSBA + 15Fh

Default Flash Address: 25Fh

Offset from 0	Bits	Description	Usage	FIT Visible
0x25F	7:0	Reserved, set to '0'		No

## 9.287 PCH Descriptor Record 286 (Flash Descriptor Records)

Flash Address: FPSBA + 160h

Default Flash Address: 260h

Offset from 0	Bits	Description	Usage	FIT Visible
0x260	7	Reserved, set to '0'		No
	6:0	<b>GbE MAC SMBus Address:</b> This is the 7 bit SMBus address to accept SMBus cycles from the PHY.  <b>Notes:</b> This field must be programmed to <b>70h</b> .	This is the Intel integrated wired MAC's SMBus address. This field must be programmed to 70h.  GbE PHY SMBus Address and GbE MAC address have to be programmed to 64h and 70h in order to ensure proper arbitration of SMBus communication between the Intel integrated MAC and PHY.	Yes

## 9.288 PCH Descriptor Record 287 (Flash Descriptor Records)

Flash Address: FPSBA + 161h

Default Flash Address: 261h

Offset from 0	Bits	Description	Usage	FIT Visible
0x261	7:0	Reserved, set to '0'		No

## 9.289 PCH Descriptor Record 288 (Flash Descriptor Records)

Flash Address: FPSBA + 162h

Default Flash Address: 262h

Offset from 0	Bits	Description	Usage	FIT Visible
0x262	7:0	Reserved, set to '0'		No

## 9.290 PCH Descriptor Record 289 (Flash Descriptor Records)

Flash Address: FPSBA + 163h

Default Flash Address: 263h

Offset from 0	Bits	Description	Usage	FIT Visible
0x263	7:1	Reserved, set to '0'		No
	0	<b>Gbe MAC SMBus Address Enable (GBEMAC_SMBUS_ADDR_EN):</b>  0x0 = Disabled 0x1 = Enabled  <b>Notes:</b> 1. This bit MUST be set to '1' when utilizing Intel integrated wired LAN. 2. If not using Intel integrated wired LAN solution or if disabling it, then this segment must be set to '0'.	This bit must be set to '1' if Intel integrated wired LAN solution is used. If not using, or if disabling Intel integrated wired LAN solution, then this field must be set to '0'.	Yes

## 9.291 PCH Descriptor Record 290 (Flash Descriptor Records)

Flash Address: FPSBA + 164h

Default Flash Address: 264h

Offset from 0	Bits	Description	Usage	FIT Visible
0x264	7:0	Reserved, set to '0x3'		No

## 9.292 PCH Descriptor Record 291 (Flash Descriptor Records)

Flash Address: FPSBA + 165h

Default Flash Address: 265h

Offset from 0	Bits	Description	Usage	FIT Visible
0x265	7:0	Reserved, set to '0x2'		No

## 9.293 PCH Descriptor Record 292 (Flash Descriptor Records)

Flash Address:FPSBA + 166h

Default Flash Address: 266h

Offset from 0	Bits	Description	Usage	FIT Visible
0x266	7:0	Reserved, set to '0'		No

## 9.294 PCH Descriptor Record 293 (Flash Descriptor Records)

Flash Address:FPSBA + 167h

Default Flash Address: 267h

Offset from 0	Bits	Description	Usage	FIT Visible
0x267	7:0	Reserved, set to '0'		No

## 9.295 PCH Descriptor Record 294 (Flash Descriptor Records)

Flash Address:FPSBA + 168h

Default Flash Address: 268h

Offset from 0	Bits	Description	Usage	FIT Visible
0x268	7	Reserved, set to '0'		No
	6:0	<b>GbE PHY SMBus Address:</b> This is the 7 bit SMBus address the PHY uses to accept SMBus cycles from the MAC.  This field must be programmed to <b>64h</b> .	This is the Intel PHY's SMBus address. This field must be programmed to 64h.  GbE PHY SMBus Address and GbE MAC address have to be programmed to 64h and 70h in order to ensure proper arbitration of SMBus communication between the Intel integrated MAC and PHY.	Yes

## 9.296 PCH Descriptor Record 295 (Flash Descriptor Records)

Flash Address:FPSBA + 169h

Default Flash Address: 269h

Offset from 0	Bits	Description	Usage	FIT Visible
0x269	7:0	Reserved, set to '0'		No

## 9.297 PCH Descriptor Record 296 (Flash Descriptor Records)

Flash Address: FPSBA + 16Ah

Default Flash Address: 26Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0x26A	7:6	Reserved, set to '0'		No

## 9.298 PCH Descriptor Record 297 (Flash Descriptor Records)

Flash Address: FPSBA + 16Bh

Default Flash Address: 26Bh

Offset from 0	Bits	Description	Usage	FIT Visible
0x26B	7:6	Reserved, set to '0'		No

## 9.299 PCH Descriptor Record 298 (Flash Descriptor Records)

Flash Address: FPSBA + 16Ch

Default Flash Address: 26Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x26C	7:0	Reserved, set to '0'		No

## 9.300 PCH Descriptor Record 299 (Flash Descriptor Records)

Flash Address: FPSBA + 16Dh

Default Flash Address: 26Dh

Offset from 0	Bits	Description	Usage	FIT Visible
0x26D	7:0	Reserved, set to '0x3'		No

## 9.301 PCH Descriptor Record 300 (Flash Descriptor Records)

Flash Address: FPSBA + 16Eh

Default Flash Address: 26Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0x26E	7:0	Reserved, set to '0'		No

## 9.302 PCH Descriptor Record 301 (Flash Descriptor Records)

Flash Address: FPSBA + 16Fh

Default Flash Address: 26Fh

Offset from 0	Bits	Description	Usage	FIT Visible
0x26F	7:0	Reserved, set to '0'		No

## 9.303 PCH Descriptor Record 302 (Flash Descriptor Records)

Flash Address: FPSBA + 170h

Default Flash Address: 270h

Offset from 0	Bits	Description	Usage	FIT Visible
0x270	31:0	Reserved, Set to '0x3'		No

## 9.304 PCH Descriptor Record 303 (Flash Descriptor Records)

Flash Address: FPSBA + 174h

Default Flash Address: 274h

Offset from 0	Bits	Description	Usage	FIT Visible
0x274	31:0	Reserved, Set to '0x3'		No



## 9.305 PCH Descriptor Record 304 (Flash Descriptor Records)

Flash Address: FPSBA + 178h

Default Flash Address: 278h

Offset from 0	Bits	Description	Usage	FIT Visible
0x278	7	<b>DCI OOB over USB3 Port8 Enabled (EXI_PTSS_PORT7):</b>  0x0 = DCI OOB is enabled on USB3 Port8 0x1 = DCI OOB is disabled on USB3 Port8	This setting determines if the USB port being enabled for DCI OOB. If disabled it will block DCI OOB connection.	<b>Yes</b>
	6	<b>DCI OOB over USB3 Port7 Enabled (EXI_PTSS_PORT6):</b>  0x0 = DCI OOB is enabled on USB3 Port7 0x1 = DCI OOB is disabled on USB3 Port7	This setting determines if the USB port being enabled for DCI OOB. If disabled it will block DCI OOB connection.	<b>Yes</b>
	5	<b>DCI OOB over USB3 Port6 Enabled (EXI_PTSS_PORT5):</b>  0x0 = DCI OOB is enabled on USB3 Port6 0x1 = DCI OOB is disabled on USB3 Port6	This setting determines if the USB port being enabled for DCI OOB. If disabled it will block DCI OOB connection.	<b>Yes</b>
	4	<b>DCI OOB over USB3 Port5 Enabled (EXI_PTSS_PORT4):</b>  0x0 = DCI OOB is enabled on USB3 Port5 0x1 = DCI OOB is disabled on USB3 Port5	This setting determines if the USB port being enabled for DCI OOB. If disabled it will block DCI OOB connection.	<b>Yes</b>
	3	<b>DCI OOB over USB3 Port4 Enabled (EXI_PTSS_PORT3):</b>  0x0 = DCI OOB is enabled on USB3 Port4 0x1 = DCI OOB is disabled on USB3 Port4	This setting determines if the USB port being enabled for DCI OOB. If disabled it will block DCI OOB connection.	<b>Yes</b>
	2	<b>DCI OOB over USB3 Port3 Enabled (EXI_PTSS_PORT2):</b>  0x0 = DCI OOB is enabled on USB3 Port3 0x1 = DCI OOB is disabled on USB3 Port3	This setting determines if the USB port being enabled for DCI OOB. If disabled it will block DCI OOB connection.	<b>Yes</b>
	1	<b>DCI OOB over USB3 Port2 Enabled (EXI_PTSS_PORT1):</b>  0x0 = DCI OOB is enabled on USB3 Port2 0x1 = DCI OOB is disabled on USB3 Port2	This setting determines if the USB port being enabled for DCI OOB. If disabled it will block DCI OOB connection.	<b>Yes</b>
	0	<b>DCI OOB over USB3 Port1 Enabled (EXI_PTSS_PORT0):</b>  0x0 = DCI OOB is enabled on USB3 Port1 0x1 = DCI OOB is disabled on USB3 Port1	This setting determines if the USB port being enabled for DCI OOB. If disabled it will block DCI OOB connection.	<b>Yes</b>

## 9.306 PCH Descriptor Record 305 (Flash Descriptor Records)

Flash Address: FPSBA + 179h

Default Flash Address: 279h

Offset from 0	Bits	Description	Usage	FIT Visible
0x279	7:2	Reserved, Set to '0'		No
	1	<b>DCI OOB over USB3 Port10 Enabled (EXI_PTSS_PORT9):</b>  0x0 = DCI OOB is enabled on USB3 Port10 0x1 = DCI OOB is disabled on USB3 Port10	This setting determines if the USB port being enabled for DCI OOB. If disabled it will block DCI OOB connection.	Yes
	0	<b>DCI OOB over USB3 Port9 Enabled (EXI_PTSS_PORT8):</b>  0x0 = DCI OOB is enabled on USB3 Port9 0x1 = DCI OOB is disabled on USB3 Port9	This setting determines if the USB port being enabled for DCI OOB. If disabled it will block DCI OOB connection.	Yes

## 9.307 PCH Descriptor Record 306 (Flash Descriptor Records)

Flash Address: FPSBA + 17Ah

Default Flash Address: 27Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0x27A	7:0	Reserved, Set to '0'		No

## 9.308 PCH Descriptor Record 307 (Flash Descriptor Records)

Flash Address: FPSBA + 17Bh

Default Flash Address: 27Bh

Offset from 0	Bits	Description	Usage	FIT Visible
0x27B	7:0	Reserved, Set to '0'		No

## 9.309 PCH Descriptor Record 308 (Flash Descriptor Records)

Flash Address: FPSBA + 17Ch

Default Flash Address: 27Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x27C	7:0	Reserved, Set to '0'		No

### 9.310 PCH Descriptor Record 309 (Flash Descriptor Records)

Flash Address: FPSBA + 17Dh

Default Flash Address: 27Dh

Offset from 0	Bits	Description	Usage	FIT Visible
0x27D	7:0	Reserved, Set to '0'		No

### 9.311 PCH Descriptor Record 310 (Flash Descriptor Records)

Flash Address: FPSBA + 17Eh

Default Flash Address: 27Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0x27E	7:0	Reserved, Set to '0x7'		No

### 9.312 PCH Descriptor Record 311 (Flash Descriptor Records)

Flash Address: FPSBA + 17Fh

Default Flash Address: 27Fh

Offset from 0	Bits	Description	Usage	FIT Visible
0x27F	7:0	Reserved, Set to '0x68'		No

### 9.313 PCH Descriptor Record 312 (Flash Descriptor Records)

Flash Address: FPSBA + 180h

Default Flash Address: 280h

Offset from 0	Bits	Description	Usage	FIT Visible
0x280	7:0	Reserved, Set to '0'		No

### 9.314 PCH Descriptor Record 313 (Flash Descriptor Records)

Flash Address: FPSBA + 181h

Default Flash Address: 281h

Offset from 0	Bits	Description	Usage	FIT Visible
0x281	7:0	Reserved, Set to '0'		No

### 9.315 PCH Descriptor Record 314 (Flash Descriptor Records)

Flash Address: FPSBA + 182h

Default Flash Address: 282h

Offset from 0	Bits	Description	Usage	FIT Visible
0x282	7:0	Reserved, Set to '0'		No

### 9.316 PCH Descriptor Record 315 (Flash Descriptor Records)

Flash Address: FPSBA + 183h

Default Flash Address: 283h

Offset from 0	Bits	Description	Usage	FIT Visible
0x283	7:0	Reserved, Set to '0'		No

### 9.317 PCH Descriptor Record 316 (Flash Descriptor Records)

Flash Address: FPSBA + 184h

Default Flash Address: 284h

Offset from 0	Bits	Description	Usage	FIT Visible
0x284	31:0	Reserved, Set to '0'		No

### 9.318 PCH Descriptor Record 317 (Flash Descriptor Records)

Flash Address: FPSBA + 188h

Default Flash Address: 288h

Offset from 0	Bits	Description	Usage	FIT Visible
0x288	7:0	Reserved, Set to '0x6'		No

### 9.319 PCH Descriptor Record 318 (Flash Descriptor Records)

Flash Address: FPSBA + 189h

Default Flash Address: 289h

Offset from 0	Bits	Description	Usage	FIT Visible
0x289	7:0	Reserved, Set to '0'		No

## 9.320 PCH Descriptor Record 319 (Flash Descriptor Records)

Flash Address: FPSBA + 18Ah

Default Flash Address: 28Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0x28A	7:0	Reserved, Set to '0'		No

## 9.321 PCH Descriptor Record 320 (Flash Descriptor Records)

Flash Address: FPSBA + 18Bh

Default Flash Address: 28Bh

Offset from 0	Bits	Description	Usage	FIT Visible
0x28B	7:0	Reserved, Set to '0'		No

## 9.322 PCH Descriptor Record 321 (Flash Descriptor Records)

Flash Address: FPSBA + 18Ch

Default Flash Address: 28Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x28C	7:2	Reserved, Set to '0'		No
	1	<b>BIOS Guard protection override enable (LPC/spi_strap_prr_ts_ovr):</b>  0x0 = BIOS Guard Fault Tolerant Update Capability is disabled 0x1 = 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.  <b>Note:</b> For further details please review Intel® Platform Protection Technology with BIOS Guard 2.0 BIOS Specification regarding Fault Tolerant Update (FTU).	Yes
	0	<b>TPM Over SPI Bus Enabled (TOS):</b>  0x0 = TPM is not on SPI 0x1 = 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

## 9.323 PCH Descriptor Record 322 (Flash Descriptor Records)

Flash Address: FPSBA + 18Dh

Default Flash Address: 28Dh

Offset from 0	Bits	Description	Usage	FIT Visible
0x28D	7:0	Reserved, set to '0'		No

### 9.324 PCH Descriptor Record 323 (Flash Descriptor Records)

Flash Address: FPSBA + 18Eh

Default Flash Address: 28Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0x28E	7:0	Reserved, set to '0'		No

### 9.325 PCH Descriptor Record 324 (Flash Descriptor Records)

Flash Address: FPSBA + 18Fh

Default Flash Address: 28Fh

Offset from 0	Bits	Description	Usage	FIT Visible
0x28F	7:0	Reserved, set to '0'		No

### 9.326 PCH Descriptor Record 325 (Flash Descriptor Records)

Flash Address: FPSBA + 190h

Default Flash Address: 290h

Offset from 0	Bits	Description	Usage	FIT Visible
0x290	7:2	Reserved, set to '0xC'		No
	1	DMI / PCIe Port Staggering Enable (FIA_PD/PSE): 0x0 = Disabled 0x1 = Enabled		Yes
	0	Reserved, set to '0'		No

### 9.327 PCH Descriptor Record 326 (Flash Descriptor Records)

Flash Address: FPSBA + 191h

Default Flash Address: 291h

Offset from 0	Bits	Description	Usage	FIT Visible
0x291	7:0	Reserved, set to '0x66'		No

## 9.328 PCH Descriptor Record 327 (Flash Descriptor Records)

Flash Address: FPSBA + 192h

Default Flash Address: 292h

Offset from 0	Bits	Description	Usage	FIT Visible
0x292	7:0	Reserved, set to '0x66'		No

## 9.329 PCH Descriptor Record 328 (Flash Descriptor Records)

Flash Address: FPSBA + 193h

Default Flash Address: 293h

Offset from 0	Bits	Description	Usage	FIT Visible
0x293	7:0	Reserved, set to '0x66'		No

## 9.330 PCH Descriptor Record 329 (Flash Descriptor Records)

Flash Address: FPSBA + 194h

Default Flash Address: 294h

Offset from 0	Bits	Description	Usage	FIT Visible
0x294	7:0	Reserved, set to '0x56'		No

## 9.331 PCH Descriptor Record 330 (Flash Descriptor Records)

Flash Address: FPSBA + 195h

Default Flash Address: 295h

Offset from 0	Bits	Description	Usage	FIT Visible
0x295	7:0	Reserved, set to '0x55'		No

## 9.332 PCH Descriptor Record 331 (Flash Descriptor Records)

Flash Address: FPSBA + 196h

Default Flash Address: 296h

Offset from 0	Bits	Description	Usage	FIT Visible
0x296	7:0	Reserved, set to '0x55'		No

### 9.333 PCH Descriptor Record 332 (Flash Descriptor Records)

Flash Address: FPSBA + 197h

Default Flash Address: 297h

Offset from 0	Bits	Description	Usage	FIT Visible
0x297	7:0	Reserved, set to '0'		No

### 9.334 PCH Descriptor Record 333 (Flash Descriptor Records)

Flash Address: FPSBA + 198h

Default Flash Address: 298h

Offset from 0	Bits	Description	Usage	FIT Visible
0x298	7:0	Reserved, set to '0'		No

### 9.335 PCH Descriptor Record 334 (Flash Descriptor Records)

Flash Address: FPSBA + 199h

Default Flash Address: 299h

Offset from 0	Bits	Description	Usage	FIT Visible
0x299	7:0	Reserved, set to '0'		No

### 9.336 PCH Descriptor Record 335 (Flash Descriptor Records)

Flash Address: FPSBA + 19Ah

Default Flash Address: 29Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0x29A	7:0	Reserved, set to '0'		No

### 9.337 PCH Descriptor Record 336 (Flash Descriptor Records)

Flash Address: FPSBA + 19Bh

Default Flash Address: 29Bh

Offset from 0	Bits	Description	Usage	FIT Visible
0x29B	7:0	Reserved, set to '0'		No



## 9.338 PCH Descriptor Record 337 (Flash Descriptor Records)

Flash Address: FPSBA + 19Ch

Default Flash Address: 29Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x29C	7:2	Reserved, set to '0x5'		No
	1	DMI / PCIe Port Staggering Enable (FIA_PGS/PSE):  0x0 = Disabled 0x1 = Enabled		Yes
	0	Reserved, set to '0'		No

## 9.339 PCH Descriptor Record 338 (Flash Descriptor Records)

Flash Address: FPSBA + 19Dh

Default Flash Address: 29Dh

Offset from 0	Bits	Description	Usage	FIT Visible
0x29D	7:4	GBE PCIe* Select Port 3 (FIA_PGS/LOSL2):  0x5 = assigned as PCIe Port 3 0x8 = assigned as GbE	This field tells the PCH which PCI Express* port an Intel® PHY is connected.  If PHY_PCIE_EN is = '0', then the GbE setting in this field is ignored.  <b>Note:</b> This setting is not the same for all designs, is dependent on the board design. The platform hardware designer or schematic review can determine what PCIe Port the Intel wired PHY is routed.  <b>Note:</b> This is tied into GBE PCIe Port Select drop down option in Intel® mFIT tool.	Yes
	3:0	Reserved, set to '0x5'		No

## 9.340 PCH Descriptor Record 339 (Flash Descriptor Records)

Flash Address: FPSBA + 19Eh

Default Flash Address: 29Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0x29E	7:0	Reserved, set to '0x55'		No

## 9.341 PCH Descriptor Record 340 (Flash Descriptor Records)

Flash Address: FPSBA + 19Fh

Default Flash Address: 29Fh

Offset from 0	Bits	Description	Usage	FIT Visible
0x29F	7:4	<b>GBE / PCIe* Select Port 7 (FIA_PGS/LOSL6):</b>  0x5 = assigned as PCIe Port 7 0x8 = assigned as GbE	This field tells the PCH which PCI Express* port an Intel® PHY is connected.  If PHY_PCIE_EN is '0', then the GbE setting in this field is ignored.  <b>Note:</b> This setting is not the same for all designs, is dependent on the board design. The platform hardware designer or schematic review can determine what PCIe Port the Intel wired PHY is routed.  <b>Note:</b> This is tied into GbE PCIe Port Select drop down option in Intel® mFIT tool.	Yes
	3:0	Reserved, set to '0x5'		No

## 9.342 PCH Descriptor Record 341 (Flash Descriptor Records)

Flash Address: FPSBA + 1A0h

Default Flash Address: 2A0h

Offset from 0	Bits	Description	Usage	FIT Visible
0x2A0	7:0	Reserved, set to '0x55'		No

## 9.343 PCH Descriptor Record 342 (Flash Descriptor Records)

Flash Address: FPSBA + 1A1h

Default Flash Address: 2A1h

Offset from 0	Bits	Description	Usage	FIT Visible
0x2A1	7:0	Reserved, set to '0x55'		No

## 9.344 PCH Descriptor Record 343 (Flash Descriptor Records)

Flash Address: FPSBA + 1A2h

Default Flash Address: 2A2h

Offset from 0	Bits	Description	Usage	FIT Visible
0x2A2	7:4	<b>SATA/PCIe Combo Port 0 Strap (FIA_PGS/LOSL12):</b>  0x5 = PCIe Port 13 is statically assigned as PCIe 0x7 = PCIe Port 13 is statically assigned as SATA Port 0  0xC = based on GPIO for SATA vs PCIe. Value '0' to select SATA while value '1' to select PCIe. (NGFF M.2 or SATAe Connector)  0xD = selection based on GPIO for SATA vs PCIe. Value '1' to select SATA while value '0' to select PCIe. (mSATA Connector)	This setting determine if PCIe / SATA Combo Port 0a is configured natively for SATA or PCIe.  <b>Note:</b> If using GPIO Polarity control settings '0xC' or '0xD' must match the (SPS0).  <b>Note:</b> The settings for this strap and the SATA / PCIe Select for Port 0 (SATA_PCIE_SPO) and (SATA_PCIE_GPO) must match for proper port function.  <b>Note:</b> For unused SATA/PCIe* Combo Lanes, Flex I/O Lanes that can be configured as PCIe* or SATA, the lanes must be statically assigned to SATA or PCIe*. These unused SATA/PCIe* Combo Lanes must not be assigned as polarity based.	Yes
	3:0	Reserved, set to '0x5'		No

## 9.345 PCH Descriptor Record 344 (Flash Descriptor Records)

Flash Address: FPSBA + 1A3h

Default Flash Address: 2A3h

Offset from 0	Bits	Description	Usage	FIT Visible
0x2A3	7:4	<b>SATA/PCIe Combo Port 2 Strap (FIA_PGS/LOSL14):</b>  0x5 = PCIe Port 15 is statically assigned as PCIe (or GbE) 0x7 = PCIe Port 15 is statically assigned as SATA Port 2 0x8 = PCIe Port 15 is statically assigned as GbE 0xC = based on GPIO for SATA vs PCIe. Value '0' to select SATA while value '1' to select PCIe. (NGFF M.2 or SATAe Connector)  0xD = selection based on GPIO for SATA vs PCIe. Value '1' to select SATA while value '0' to select PCIe. (mSATA Connector)	This setting determine if PCIe/SATA Combo Port 2 is configured natively for SATA or PCIe.  <b>Note:</b> If using GPIO Polarity control settings '0xC' or '0xD' must match the (SPS2).  <b>Note:</b> The settings for this strap SATA / PCIe Select for Port 2 (SATA_PCIE_SP2) and (SATA_PCIE_GP2) must match for proper port function.  <b>Note:</b> For unused SATA/PCIe* Combo Lanes, Flex I/O Lanes that can be configured as PCIe* or SATA, the lanes must be statically assigned to SATA or PCIe*. These unused SATA/PCIe* Combo Lanes must not be assigned as polarity based.  <b>Note:</b> This is tied into GBE PCIe Port Select drop down option in Intel® mFIT tool.	Yes

Offset from 0	Bits	Description	Usage	FIT Visible
<b>0x2A3 (Cont)</b>	3:0	<b>SATA/PCIe Combo Port 1 Strap (FIA_PGS/LOSL13):</b>  0x5 = PCIe Port 14 is statically assigned as PCIe 0x7 = PCIe Port 14 is statically assigned as SATA Port 1 0xC = based on GPIO for SATA vs PCIe. Value '0' to select SATA while value '1' to select PCIe. (NGFF M.2 or SATAe Connector) 0xD = selection based on GPIO for SATA vs PCIe. Value '1' to select SATA while value '0' to select PCIe. (mSATA Connector)	This setting determine if PCIe / SATA Combo Port 1 is configured natively for SATA or PCIe.  <b>Note:</b> If using GPIO Polarity control settings '0xC' or '0xD' must match the ( <b>SPS1</b> ).  <b>Note:</b> The settings for this strap and the SATA / PCIe Select for Port 1 ( <b>SATA_PCIE_SP1</b> ) and ( <b>SATA_PCIE_GP1</b> ) must match for proper port function.  <b>Note:</b> For unused SATA/PCIe* Combo Lanes, Flex I/O Lanes that can be configured as PCIe* or SATA, the lanes must be statically assigned to SATA or PCIe*. These unused SATA/PCIe* Combo Lanes must not be assigned as polarity based.	<b>Yes</b>

## 9.346 PCH Descriptor Record 345 (Flash Descriptor Records)

Flash Address: FPSBA + 1A4h

Default Flash Address: 2A4h

Offset from 0	Bits	Description	Usage	FIT Visible
<b>0x2A4</b>	7:4	<b>SATA/PCIe Combo Port 4 Strap (FIA_PGS/LOSL16):</b>  0x5 = PCIe Port 17 is statically assigned as PCIe 0x7 = PCIe Port 17 is statically assigned as SATA Port 4 0xC = based on GPIO for SATA vs PCIe. Value '0' to select SATA while value '1' to select PCIe. (NGFF M.2 or SATAe Connector) 0xD = selection based on GPIO for SATA vs PCIe. Value '1' to select SATA while value '0' to select PCIe. (mSATA Connector)	This setting determine if PCIe/SATA Combo Port 4 is configured natively for SATA or PCIe.  <b>Note:</b> If using GPIO Polarity control settings '0xC' or '0xD' must match the ( <b>SPS4</b> ).  <b>Note:</b> The settings for this strap and the SATA / PCIe Select for Port 4 ( <b>SATA_PCIE_SP4</b> ) and ( <b>SATA_PCIE_GP4</b> ) strap must match for proper port function  <b>Note:</b> For unused SATA/PCIe* Combo Lanes, Flex I/O Lanes that can be configured as PCIe* or SATA, the lanes must be statically assigned to SATA or PCIe*. These unused SATA/PCIe* Combo Lanes must not be assigned as polarity based.	<b>Yes</b>

Offset from 0	Bits	Description	Usage	FIT Visible
<b>0x2A4 (Cont)</b>	3:0	<b>SATA/PCIe Combo Port 3 Strap (FIA_PGS/LOSL15):</b>  0x5 = PCIe Port 16 is statically assigned as PCIe 0x7 = PCIe Port 16 is statically assigned as SATA Port 3 0xC = based on GPIO for SATA vs PCIe. Value '0' to select SATA while value '1' to select PCIe. (NGFF M.2 or SATAe Connector) 0xD = selection based on GPIO for SATA vs PCIe. Value '1' to select SATA while value '0' to select PCIe. (mSATA Connector)	This setting determine if PCIe/SATA Combo Port 3 is configured natively for SATA or PCIe.  <b>Note:</b> If using GPIO Polarity control settings '0xC' or '0xD' must match the (SPS3).  <b>Note:</b> The settings for this strap and the SATA / PCIe Select for Port 3 (SATA_PCIE_SP3) and (SATA_PCIE_GP3) strap must match for proper port function.  <b>Note:</b> For unused SATA/PCIe* Combo Lanes, Flex I/O Lanes that can be configured as PCIe* or SATA, the lanes must be statically assigned to SATA or PCIe*. These unused SATA/PCIe* Combo Lanes must not be assigned as polarity based.	<b>Yes</b>

## 9.347 PCH Descriptor Record 346 (Flash Descriptor Records)

Flash Address:FPSBA + 1A5h

Default Flash Address: 2A5h

Offset from 0	Bits	Description	Usage	FIT Visible
<b>0x2A5</b>	7:4	<b>SATA/PCIe Combo Port 6 Strap (FIA_PGS/LOSL18):</b>  0x5 = PCIe Port 19 is statically assigned as PCIe 0x7 = PCIe Port 19 is statically assigned as SATA Port 6 0xC = based on GPIO for SATA vs PCIe. Value '0' to select SATA while value '1' to select PCIe. (NGFF M.2 or SATAe Connector) 0xD = selection based on GPIO for SATA vs PCIe. Value '1' to select SATA while value '0' to select PCIe. (mSATA Connector)	This setting determine if PCIe/SATA Combo Port 6 is configured natively for SATA or PCIe.  <b>Note:</b> If using GPIO Polarity control settings '0xC' or '0xD' must match the (SPS6).  <b>Note:</b> The settings for this strap and the SATA / PCIe Select for Port 6 (SATA_PCIE_SP6) and (SATA_PCIE_GP6) strap must match for proper port function.  <b>Note:</b> For unused SATA/PCIe* Combo Lanes, Flex I/O Lanes that can be configured as PCIe* or SATA, the lanes must be statically assigned to SATA or PCIe*. These unused SATA/PCIe* Combo Lanes must not be assigned as polarity based.	<b>Yes</b>

Offset from 0	Bits	Description	Usage	FIT Visible
<b>0x2A5 (Cont)</b>	3:0	<b>SATA/PCIe Combo Port 5 Strap (FIA_PGS/LOSL17):</b>  0x5 = PCIe Port 18 is statically assigned as PCIe 0x7 = PCIe Port 18 is statically assigned as SATA Port 5 0xC = based on GPIO for SATA vs PCIe. Value '0' to select SATA while value '1' to select PCIe. (NGFF M.2 or SATAe Connector) 0xD = selection based on GPIO for SATA vs PCIe. Value '1' to select SATA while value '0' to select PCIe. (mSATA Connector)	This setting determine if PCIe/SATA Combo Port 5 is configured natively for SATA or PCIe.  <b>Note:</b> If using GPIO Polarity control settings '0xC' or '0xD' must match the (SPS5).  <b>Note:</b> The settings for this strap and the SATA / PCIe Select for Port 5 (SATA_PCIE_SP5) and (SATA_PCIE_GP5) strap must match for proper port function.  <b>Note:</b> For unused SATA/PCIe* Combo Lanes, Flex I/O Lanes that can be configured as PCIe* or SATA, the lanes must be statically assigned to SATA or PCIe*. These unused SATA/PCIe* Combo Lanes must not be assigned as polarity based.	<b>Yes</b>

## 9.348 PCH Descriptor Record 347 (Flash Descriptor Records)

Flash Address:FPSBA + 1A6h

Default Flash Address: 2A6h

Offset from 0	Bits	Description	Usage	FIT Visible
<b>0x2A6</b>	7	<b>SATA / PCIe Combo Port 3 Mode Select (FIA_PGS/CP3CLKREQDEVSLPM):</b>  0x0 = SATA / PCIe Combo Port 3 mode configured as PCIe CLKREQ# 0x1 = SATA / PCIe Combo Port 3 mode configured as SATA DEVSLP#	This setting determines the configuration for the SATA / PCIe Combo Port 3 CLKREQ#.  <b>Note:</b> The corresponding CLKREQ# GPIO can only function as DEVSLP if the SATA / PCIe Combo Port Fuse, Strap and SATA_GP are assigned to SATA, and CLKREQ DEVSLP Mode is also set.	<b>Yes</b>
	6	<b>SATA / PCIe Combo Port 2 Mode Select (FIA_PGS/CP2CLKREQDEVSLPM):</b>  0x0 = SATA / PCIe Combo Port 2 mode configured as PCIe CLKREQ# 0x1 = SATA / PCIe Combo Port 2 mode configured as SATA DEVSLP#	This setting determines the configuration for the SATA / PCIe Combo Port 2 CLKREQ#.  <b>Note:</b> The corresponding CLKREQ# GPIO can only function as DEVSLP if the SATA / PCIe Combo Port Fuse, Strap and SATA_GP are assigned to SATA, and CLKREQ DEVSLP Mode is also set.	<b>Yes</b>
	5	<b>SATA / PCIe Combo Port 1 Mode Select (FIA_PGS/CP1CLKREQDEVSLPM):</b>  0x0 = SATA / PCIe Combo Port 1 mode configured as PCIe CLKREQ# 0x1 = SATA / PCIe Combo Port 1 mode configured as SATA DEVSLP#	This setting determines the configuration for the SATA / PCIe Combo Port 1 CLKREQ#.  <b>Note:</b> The corresponding CLKREQ# GPIO can only function as DEVSLP if the SATA / PCIe Combo Port Fuse, Strap and SATA_GP are assigned to SATA, and CLKREQ DEVSLP Mode is also set.	<b>Yes</b>
	4	<b>SATA / PCIe Combo Port 0 Mode Select (FIA_PGS/CP0CLKREQDEVSLPM):</b>  0x0 = SATA / PCIe Combo Port 0 mode configured as PCIe CLKREQ# 0x1 = SATA / PCIe Combo Port 0 mode configured as SATA DEVSLP#	This setting determines the configuration for the SATA / PCIe Combo Port 0 CLKREQ#.  <b>Note:</b> The corresponding CLKREQ# GPIO can only function as DEVSLP if the SATA / PCIe Combo Port Fuse, Strap and SATA_GP are assigned to SATA, and CLKREQ DEVSLP Mode is also set.	<b>Yes</b>

Offset from 0	Bits	Description	Usage	FIT Visible
<b>0x2A6 (Cont)</b>	3:0	<b>SATA/PCIe Combo Port 7 Strap (FIA_PGS/LOSL19):</b>  0x5 = PCIe Port 20 is statically assigned as PCIe 0x7 = PCIe Port 20 is statically assigned as SATA Port 7  0xC = based on GPIO for SATA vs PCIe. Value '0' to select SATA while value '1' to select PCIe. (NGFF M.2 or SATAe Connector) 0xD = selection based on GPIO for SATA vs PCIe. Value '1' to select SATA while value '0' to select PCIe. (mSATA Connector)	This setting determine if PCIe/SATA Combo Port 7 is configured natively for SATA or PCIe.  <b>Note:</b> If using GPIO Polarity control settings '0xC' or '0xD' must match the (SPS7).  <b>Note:</b> The settings for this strap and the SATA / PCIe Select for Port 7 (SATA_PCIE_SP7) and (SATA_PCIE_GP7) must match for proper port function.  <b>Note:</b> For unused SATA/PCIe* Combo Lanes, Flex I/O Lanes that can be configured as PCIe* or SATA, the lanes must be statically assigned to SATA or PCIe*. These unused SATA/PCIe* Combo Lanes must not be assigned as polarity based.	<b>Yes</b>

## 9.349 PCH Descriptor Record 348 (Flash Descriptor Records)

Flash Address: FPSBA + 1A7h

Default Flash Address: 2A7h

Offset from 0	Bits	Description	Usage	FIT Visible
<b>0x2A7</b>	7:4	<b>Reserved, set to '0'</b>		<b>No</b>
	3	<b>SATA / PCIe Combo Port 7 Mode Select (FIA/CP7CLKREQDEVSLPM):</b>  0x0 = SATA / PCIe Combo Port 7 mode configured as PCIe CLKREQ# 0x1 = SATA / PCIe Combo Port 7 mode configured as SATA DEVSLP#	This setting determines the configuration for the SATA / PCIe Combo Port 7 CLKREQ#.  <b>Note:</b> The corresponding CLKREQ# GPIO can only function as DEVSLP if the SATA / PCIe Combo Port Fuse, Strap and SATA_GP are assigned to SATA, and CLKREQ DEVSLP Mode is also set.	<b>Yes</b>
	2	<b>SATA / PCIe Combo Port 6 Mode Select (FIA/CP6CLKREQDEVSLPM):</b>  0x0 = SATA / PCIe Combo Port 6 mode configured as PCIe CLKREQ# 0x1 = SATA / PCIe Combo Port 6 mode configured as SATA DEVSLP#	This setting determines the configuration for the SATA / PCIe Combo Port 6 CLKREQ#.  <b>Note:</b> The corresponding CLKREQ# GPIO can only function as DEVSLP if the SATA / PCIe Combo Port Fuse, Strap and SATA_GP are assigned to SATA, and CLKREQ DEVSLP Mode is also set.	<b>Yes</b>
	1	<b>SATA / PCIe Combo Port 5 Mode Select (FIA/CP5CLKREQDEVSLPM):</b>  0x0 = SATA / PCIe Combo Port 5 mode configured as PCIe CLKREQ# 0x1 = SATA / PCIe Combo Port 5 mode configured as SATA DEVSLP#	This setting determines the configuration for the SATA / PCIe Combo Port 5 CLKREQ#.  <b>Note:</b> The corresponding CLKREQ# GPIO can only function as DEVSLP if the SATA / PCIe Combo Port Fuse, Strap and SATA_GP are assigned to SATA, and CLKREQ DEVSLP Mode is also set.	<b>Yes</b>
	0	<b>SATA / PCIe Combo Port 4 Mode Select (FIA/CP4CLKREQDEVSLPM):</b>  0x0 = SATA / PCIe Combo Port 4 mode configured as PCIe CLKREQ# 0x1 = SATA / PCIe Combo Port 4 mode configured as SATA DEVSLP#	This setting determines the configuration for the SATA / PCIe Combo Port 4 CLKREQ#.  <b>Note:</b> The corresponding CLKREQ# GPIO can only function as DEVSLP if the SATA / PCIe Combo Port Fuse, Strap and SATA_GP are assigned to SATA, and CLKREQ DEVSLP Mode is also set.	<b>Yes</b>

### 9.350 PCH Descriptor Record 349 (Flash Descriptor Records)

Flash Address: FPSBA + 1A8h

Default Flash Address: 2A8h

Offset from 0	Bits	Description	Usage	FIT Visible
0x2A8	7:0	Reserved, set to '0x6'		No

### 9.351 PCH Descriptor Record 350 (Flash Descriptor Records)

Flash Address: FPSBA + 1A9h

Default Flash Address: 2A9h

Offset from 0	Bits	Description	Usage	FIT Visible
0x2A9	7:0	Reserved, set to '0x11'		No

### 9.352 PCH Descriptor Record 351 (Flash Descriptor Records)

Flash Address: FPSBA + 1AAh

Default Flash Address: 2AAh

Offset from 0	Bits	Description	Usage	FIT Visible
0x2AA	7:0	Reserved, set to '0x11'		No

### 9.353 PCH Descriptor Record 352 (Flash Descriptor Records)

Flash Address: FPSBA + 1ABh

Default Flash Address: 2ABh

Offset from 0	Bits	Description	Usage	FIT Visible
0x2AB	7:0	Reserved, set to '0x11'		No

### 9.354 PCH Descriptor Record 353 (Flash Descriptor Records)

Flash Address: FPSBA + 1ACh

Default Flash Address: 2ACh

Offset from 0	Bits	Description	Usage	FIT Visible
0x2AC	7:0	Reserved, set to '0x11'		No



## 9.355 PCH Descriptor Record 354 (Flash Descriptor Records)

Flash Address: FPSBA + 1ADh

Default Flash Address: 2ADh

Offset from 0	Bits	Description	Usage	FIT Visible
0x2AD	7:0	Reserved, set to '0x1'		No

## 9.356 PCH Descriptor Record 355 (Flash Descriptor Records)

Flash Address: FPSBA + 1AEh

Default Flash Address: 2AEh

Offset from 0	Bits	Description	Usage	FIT Visible
0x2AE	7:0	Reserved, set to '0'		No

## 9.357 PCH Descriptor Record 356 (Flash Descriptor Records)

Flash Address: FPSBA + 1AFh

Default Flash Address: 2AFh

Offset from 0	Bits	Description	Usage	FIT Visible
0x2AF	7:0	Reserved, set to '0'		No

## 9.358 PCH Descriptor Record 357 (Flash Descriptor Records)

Flash Address: FPSBA + 1B0h

Default Flash Address: 2B0h

Offset from 0	Bits	Description	Usage	FIT Visible
0x2B0	7:6	<b>SATA / PCIe Select for Port 3 (SATA_PCIE_SP3):</b>  0x0 = PCIe Port 16 is statically assigned to SATA Port 3 0x1 = PCIe Port 16 is statically assigned to PCIe 0x3 = Assigned based on the polarity of SATA_PCIE3 determined by SPS3	This strap must also be configured when setting the PCIe / SATA Combo Port 3 (FIA_PGS/LOSL15).  <b>Note:</b> This strap and the PCIe / SATA Combo Port 3 (FIA_PGS/LOSL15) and (SATA_PCIE_GP3) must match for proper port function.  <b>Note:</b> For unused SATA/PCIe* Combo Lanes, Flex I/O Lanes that can be configured as PCIe* or SATA, the lanes must be statically assigned to SATA or PCIe*. These unused SATA/PCIe* Combo Lanes must not be assigned as polarity based.	No

Offset from 0	Bits	Description	Usage	FIT Visible
<b>0x2B0 (Cont)</b>	5:4	<b>SATA / PCIe Select for Port 2 (SATA_PCIE_SP2):</b>  0x0 = PCIe Port 15 is statically assigned to SATA Port 2 0x1 = PCIe Port 15 is statically assigned to PCIe (or GbE) 0x3 = Assigned based on the polarity of SATAxPCIE2 determined by SPS2	This strap must also be configured when setting the PCIe / SATA Combo Port 2 ( <b>FIA_PGS/LOSL14</b> ).  <b>Note:</b> This strap and the PCIe / SATA Combo Port 2 ( <b>FIA_PGS/LOSL14</b> ) and ( <b>SATA_PCIE_GP2</b> ) must match for proper port function.  <b>Note:</b> For unused SATA/PCIe* Combo Lanes, Flex I/O Lanes that can be configured as PCIe* or SATA, the lanes must be statically assigned to SATA or PCIe*. These unused SATA/PCIe* Combo Lanes must not be assigned as polarity based.  <b>Note:</b>	<b>No</b>
	3:2	<b>SATA / PCIe Select for Port 1 (SATA_PCIE_SP1):</b>  0x0 = PCIe Port 14 is statically assigned to SATA Port 1 0x1 = PCIe Port 14 is statically assigned to PCIe 0x3 = Assigned based on the polarity of SATAxPCIE1 determined by SPS1	This strap must also be configured when setting the PCIe / SATA Combo Port 1 Strap ( <b>FIA_PGS/LOSL13</b> ).  <b>Note:</b> This strap and the PCIe / SATA Combo Port 1 Strap ( <b>FIA_PGS/LOSL13</b> ) and ( <b>SATA_PCIE_GP1</b> ) must match for proper port function.  <b>Note:</b> For unused SATA/PCIe* Combo Lanes, Flex I/O Lanes that can be configured as PCIe* or SATA, the lanes must be statically assigned to SATA or PCIe*. These unused SATA/PCIe* Combo Lanes must not be assigned as polarity based.	<b>No</b>
	1:0	<b>SATA / PCIe Select for Port 0 (SATA_PCIE_SP0):</b>  0x0 = PCIe Port 13 is statically assigned to SATA Port 0 0x1 = PCIe Port 13 is statically assigned to PCIe 0x3 = Assigned based on the polarity of SATAxPCIE0 determined by SPS0	This strap must also be configured when setting the PCIe / SATA Combo Port 0 Strap ( <b>FIA_PGS/LOSL12</b> ).  <b>Note:</b> This strap and the PCIe / SATA Combo Port 0 Strap ( <b>FIA_PGS/LOSL12</b> ) and ( <b>SATA_PCIE_GP0</b> ) must match for proper port function.  <b>Note:</b> For unused SATA/PCIe* Combo Lanes, Flex I/O Lanes that can be configured as PCIe* or SATA, the lanes must be statically assigned to SATA or PCIe*. These unused SATA/PCIe* Combo Lanes must not be assigned as polarity based.	<b>No</b>

## 9.359 PCH Descriptor Record 358 (Flash Descriptor Records)

Flash Address: FPSBA + 1B1h

Default Flash Address: 2B1h

Offset from 0	Bits	Description	Usage	FIT Visible
0x2B1	7:6	<b>SATA / PCIe Select for Port 7 (SATA_PCIE_SP7):</b> 0x0 = PCIe Port 20 is statically assigned to SATA Port 7 0x1 = PCIe Port 20 is statically assigned to PCIe 0x3 = Assigned based on the polarity of SATAxPCIE5 determined by SPS7	This strap must also be configured when setting the PCIe / SATA Combo Port 7 ( <b>FIA_PGS/LOSL19</b> ).  <b>Note:</b> This strap and the PCIe / SATA Combo Port 7 ( <b>FIA_PGS/LOSL19</b> ) and ( <b>SATA_PCIE_GP7</b> ) must match for proper port function.  <b>Note:</b> For unused SATA/PCIe* Combo Lanes, Flex I/O Lanes that can be configured as PCIe* or SATA, the lanes must be statically assigned to SATA or PCIe*. These unused SATA/PCIe* Combo Lanes must not be assigned as polarity based.	No
	5:4	<b>SATA / PCIe Select for Port 6 (SATA_PCIE_SP6):</b> 0x0 = PCIe Port 19 is statically assigned to SATA Port 6 0x1 = PCIe Port 19 is statically assigned to PCIe 0x3 = Assigned based on the polarity of SATAxPCIE5 determined by SPS6	This strap must also be configured when setting the PCIe / SATA Combo Port 6 ( <b>FIA_PGS/LOSL18</b> ).  <b>Note:</b> This strap and the PCIe / SATA Combo Port 6 ( <b>FIA_PGS/LOSL18</b> ) and ( <b>SATA_PCIE_GP6</b> ) must match for proper port function.  <b>Note:</b> For unused SATA/PCIe* Combo Lanes, Flex I/O Lanes that can be configured as PCIe* or SATA, the lanes must be statically assigned to SATA or PCIe*. These unused SATA/PCIe* Combo Lanes must not be assigned as polarity based.	No
	3:2	<b>SATA / PCIe Select for Port 5 (SATA_PCIE_SP5):</b> 0x0 = PCIe Port 18 is statically assigned to SATA Port 5 0x1 = PCIe Port 18 is statically assigned to PCIe 0x3 = Assigned based on the polarity of SATAxPCIE5 determined by SPS5	This strap must also be configured when setting the PCIe / SATA Combo Port 5 ( <b>FIA_PGS/LOSL17</b> ).  <b>Note:</b> This strap and the PCIe / SATA Combo Port 5 ( <b>FIA_PGS/LOSL17</b> ) and ( <b>SATA_PCIE_GP5</b> ) must match for proper port function.  <b>Note:</b> For unused SATA/PCIe* Combo Lanes, Flex I/O Lanes that can be configured as PCIe* or SATA, the lanes must be statically assigned to SATA or PCIe*. These unused SATA/PCIe* Combo Lanes must not be assigned as polarity based.	No

Offset from 0	Bits	Description	Usage	FIT Visible
<b>0x2B1 (Cont)</b>	1:0	<b>SATA / PCIe Select for Port 4 (SATA_PCIE_SP4):</b> 0x0 = PCIe Port 17 is statically assigned to SATA Port 4 0x1 = PCIe Port 17 is statically assigned to PCIe 0x3 = Assigned based on the polarity of SATAXPCIE4 determined by SPS4	This strap must also be configured when setting the PCIe / SATA Combo Port 4 ( <b>FIA_PGS/LOSL16</b> ).  <b>Note:</b> This strap and the PCIe / SATA Combo Port 4 ( <b>FIA_PGS/LOSL16</b> ) and ( <b>SATA_PCIE_GP4</b> ) must match for proper port function.  <b>Note:</b> For unused SATA/PCIe* Combo Lanes, Flex I/O Lanes that can be configured as PCIe* or SATA, the lanes must be statically assigned to SATA or PCIe*. These unused SATA/PCIe* Combo Lanes must not be assigned as polarity based.  <b>Note:</b>	<b>No</b>

## 9.360 PCH Descriptor Record 359 (Flash Descriptor Records)

Flash Address:FPSBA + 1B2h

Default Flash Address: 2AEh

Offset from 0	Bits	Description	Usage	FIT Visible
<b>0x2B2</b>	7	<b>SATA / PCIe GPIO Polarity Port 7 (SPS7)</b>  0x0 = GPIO Polarity Port 7 is set to PCIe mode when the SATAXPCIE7 pin is '0' and SATA when SATAXPCIE7 pin is '1' 0x1 = GPIO Polarity Port 7 is set to SATA mode when the SATAXPCIE7 pin is '0' and PCIe when SATAXPCIE7 pin is '1'	This strap must also be configured if PCIe/ <b>SATA Combo Port 7 Strap (FIA_PGS/LOSL18)</b> is configured to '0xC' or '0xD'  <b>Note:</b> This setting only has effect when SATA / PCIe Select for Port 7 ( <b>SATA_PCIE_SP7</b> ) is configured to '11'	<b>Yes</b>
	6	<b>SATA / PCIe GPIO Polarity Port 6 (SPS6)</b>  0x0 = GPIO Polarity Port 6 is set to PCIe mode when the SATAXPCIE6 pin is '0' and SATA when SATAXPCIE6 pin is '1' 0x1 = GPIO Polarity Port 6 is set to SATA mode when the SATAXPCIE6 pin is '0' and PCIe when SATAXPCIE6 pin is '1'	This strap must also be configured if PCIe/ <b>SATA Combo Port 6 Strap (FIA_PGS/LOSL17)</b> is configured to '0xC' or '0xD'  <b>Note:</b> This setting only has effect when SATA / PCIe Select for Port 6 ( <b>SATA_PCIE_SP6</b> ) is configured to '11'	<b>Yes</b>
	5	<b>SATA / PCIe GPIO Polarity Port 5 (SPS5)</b>  0x0 = GPIO Polarity Port 5 is set to PCIe mode when the SATAXPCIE5 pin is '0' and SATA when SATAXPCIE5 pin is '1' 0x1 = GPIO Polarity Port 5 is set to SATA mode when the SATAXPCIE5 pin is '0' and PCIe when SATAXPCIE5 pin is '1'	This strap must also be configured if PCIe/ <b>SATA Combo Port 5 Strap (FIA_PGS/LOSL16)</b> is configured to '0xC' or '0xD'  <b>Note:</b> This setting only has effect when SATA / PCIe Select for Port 5 ( <b>SATA_PCIE_SP5</b> ) is configured to '11'	<b>Yes</b>

Offset from 0	Bits	Description	Usage	FIT Visible
<b>0x2B2 (Cont)</b>	4	<b>SATA / PCIe GPIO Polarity Port 4 (SPS4)</b>  0x0 = GPIO Polarity Port 4 is set to PCIe mode when the SATAXPCE4 pin is '0' and SATA when SATAXPCE4 pin is '1' 0x1 = GPIO Polarity Port 4 is set to SATA mode when the SATAXPCE4 pin is '0' and PCIe when SATAXPCE4 pin is '1'	This strap must also be configured if PCIe/ <b>SATA Combo Port 4 Strap (FIA_PGS/ LOSL15)</b> is configured to '0xC' or '0xD'  <b>Note:</b> This setting only has effect when SATA / PCIe Select for Port 4 ( <b>SATA_PCIE_SP4</b> ) is configured to '11'	<b>Yes</b>
	3	<b>SATA / PCIe GPIO Polarity Port 3 (SPS3)</b>  0x0 = GPIO Polarity Port 3 is set to PCIe mode when the SATAXPCE3 pin is '0' and SATA when SATAXPCE3 pin is '1' 0x1 = GPIO Polarity Port 3 is set to SATA mode when the SATAXPCE3 pin is '0' and PCIe when SATAXPCE3 pin is '1'	This strap must also be configured if PCIe/ <b>SATA Combo Port 3 Strap (FIA_PGS/ LOSL15)</b> is configured to '0xC' or '0xD'  <b>Note:</b> This setting only has effect when SATA / PCIe Select for Port 3 ( <b>SATA_PCIE_SP3</b> ) is configured to '11'	<b>Yes</b>
	2	<b>SATA / PCIe GPIO Polarity Port 2 (SPS2)</b>  0x0 = GPIO Polarity Port 2 is set to PCIe mode when the SATAXPCE2 pin is '0' and SATA when SATAXPCE2 pin is '1' 0x1 = GPIO Polarity Port 2 is set to SATA mode when the SATAXPCE2 pin is '0' and PCIe when SATAXPCE2 pin is '1'	This strap must also be configured if PCIe/ <b>SATA Combo Port 2 Strap (FIA_PGS/ LOSL14)</b> is configured to '0xC' or '0xD'  <b>Note:</b> This setting only has effect when SATA / PCIe Select for Port 2 ( <b>SATA_PCIE_SP2</b> ) is configured to '11'	<b>Yes</b>
	1	<b>SATA / PCIe GPIO Polarity Port 1 (SPS1)</b>  0x0 = GPIO Polarity Port 1 is set to PCIe mode when the SATAXPCE1 pin is '0' and SATA when SATAXPCE1 pin is '1' 0x1 = GPIO Polarity Port 1 is set to SATA mode when the SATAXPCE1 pin is '0' and PCIe when SATAXPCE1 pin is '1'	This strap must also be configured if PCIe/ <b>SATA Combo Port 1 strap (FIA_PGS/ LOSL13)</b> is configured to '0xC' or '0xD'  <b>Note:</b> This setting only has effect when SATA / PCIe Select for Port 1 ( <b>SATA_PCIE_SP1</b> ) is configured to '11'	<b>Yes</b>
	0	<b>SATA / PCIe GPIO Polarity Port 0 (SPS0)</b>  0x0 = GPIO Polarity Port 0 is set to PCIe mode when the SATAXPCE0 pin is '0' and SATA when SATAXPCE0 pin is '1' 0x1 = GPIO Polarity Port 0 is set to SATA mode when the SATAXPCE0 pin is '0' and PCIe when SATAXPCE0 pin is '1'	This strap must also be configured if PCIe/ <b>SATA Combo Port 0 strap (FIA_PGS/ LOSL12)</b> is configured to '0xC' or '0xD'  <b>Note:</b> This setting only has effect when SATA / PCIe Select for Port 0 ( <b>SATA_PCIE_SPO</b> ) is configured to '11'	<b>Yes</b>

## 9.361 PCH Descriptor Record 360 (Flash Descriptor Records)

Flash Address: FPSBA + 1B3h

Default Flash Address: 2B3h

Offset from 0	Bits	Description	Usage	FIT Visible
<b>0x2B3</b>	7:0	<b>Reserved, set to '0'</b>		<b>No</b>

### 9.362 PCH Descriptor Record 361 (Flash Descriptor Records)

Flash Address: FPSBA + 1B4h

Default Flash Address: 2B4h

Offset from 0	Bits	Description	Usage	FIT Visible
0x2B4	7:0	Reserved, set to '0'		No

### 9.363 PCH Descriptor Record 362 (Flash Descriptor Records)

Flash Address: FPSBA + 1B5h

Default Flash Address: 2B5h

Offset from 0	Bits	Description	Usage	FIT Visible
0x2B5	7:0	Reserved, set to '0'		No

### 9.364 PCH Descriptor Record 363 (Flash Descriptor Records)

Flash Address: FPSBA + 1B6h

Default Flash Address: 2B6h

Offset from 0	Bits	Description	Usage	FIT Visible
0x2B6	7:0	Reserved, set to '0xF5'		No

### 9.365 PCH Descriptor Record 364 (Flash Descriptor Records)

Flash Address: FPSBA + 1B7h

Default Flash Address: 2B7h

Offset from 0	Bits	Description	Usage	FIT Visible
0x2B7	7:0	Reserved, set to '0x16'		No

### 9.366 PCH Descriptor Record 365 (Flash Descriptor Records)

Flash Address: FPSBA + 1B8h

Default Flash Address: 2B8h

Offset from 0	Bits	Description	Usage	FIT Visible
0x2B8	7:0	Reserved, set to '021'		No

### 9.367 PCH Descriptor Record 366 (Flash Descriptor Records)

Flash Address: FPSBA + 1B9h

Default Flash Address: 2B9h

Offset from 0	Bits	Description	Usage	FIT Visible
0x2B9	7:0	Reserved, set to '0x43'		No

### 9.368 PCH Descriptor Record 367 (Flash Descriptor Records)

Flash Address: FPSBA + 1BAh

Default Flash Address: 2BAh

Offset from 0	Bits	Description	Usage	FIT Visible
0x2BA	7:0	Reserved, set to '0x65'		No

### 9.369 PCH Descriptor Record 368 (Flash Descriptor Records)

Flash Address: FPSBA + 1BBh

Default Flash Address: 2BBh

Offset from 0	Bits	Description	Usage	FIT Visible
0x2BB	7:0	Reserved, set to '0x87'		No

### 9.370 PCH Descriptor Record 369 (Flash Descriptor Records)

Flash Address: FPSBA + 1BCh

Default Flash Address: 2BCh

Offset from 0	Bits	Description	Usage	FIT Visible
0x2BC	7:0	Reserved, set to '0xA9'		No

### 9.371 PCH Descriptor Record 370 (Flash Descriptor Records)

Flash Address: FPSBA + 1BDh

Default Flash Address: 2BDh

Offset from 0	Bits	Description	Usage	FIT Visible
0x2BD	7:0	Reserved, set to '0xCB'		No

### 9.372 PCH Descriptor Record 371 (Flash Descriptor Records)

Flash Address: FPSBA + 1BEh

Default Flash Address: 2BEh

Offset from 0	Bits	Description	Usage	FIT Visible
0x2BE	7:0	Reserved, set to '0x88'		No

### 9.373 PCH Descriptor Record 372 (Flash Descriptor Records)

Flash Address: FPSBA + 1BFh

Default Flash Address: 2BFh

Offset from 0	Bits	Description	Usage	FIT Visible
0x2BF	7:0	Reserved, set to '0x88'		No

### 9.374 PCH Descriptor Record 373 (Flash Descriptor Records)

Flash Address: FPSBA + 1C0h

Default Flash Address: 2C0h

Offset from 0	Bits	Description	Usage	FIT Visible
0x2C0	7:2	Reserved, Set to '0x24'		No
	1:0	Reserved, Set to '0x3'		No

### 9.375 PCH Descriptor Record 374 (Flash Descriptor Records)

Flash Address: FPSBA + 1C1h

Default Flash Address: 2C1h

Offset from 0	Bits	Description	Usage	FIT Visible
0x2C1	7	Reserved, Set to '0x1'		No
	6:0	Reserved, Set to '0x70'		No



## 9.376 PCH Descriptor Record 375 (Flash Descriptor Records)

Flash Address:FPSBA + 1C2h

Default Flash Address: 2C2h

Offset from 0	Bits	Description	Usage	FIT Visible
0x2C2	7:3	Reserved, set to '0x1'		No
	2:0	<b>PHY Connection (PHYCON):</b> This field determines if Intel® wired PHY is connected.  0x0 = No PHY connected 0x1 = PHY on SMBus 0x2 = PHY on SMLink0 0x3 = PHY on SMLink1	This field must be set to "10" if Intel integrated wired LAN solution is used. If not using, or if disabling Intel integrated wired LAN solution, then field must be set to "00".	Yes

## 9.377 PCH Descriptor Record 376 (Flash Descriptor Records)

Flash Address:FPSBA + 1C3h

Default Flash Address: 2C3h

Offset from 0	Bits	Description	Usage	FIT Visible
0x2C3	7:4	Reserved, set to '0xf'		No
	3:2	Reserved, set to '0x3'		No
	1:0	Reserved, set to '0x3'		No

## 9.378 PCH Descriptor Record 377 (Flash Descriptor Records)

Flash Address:FPSBA + 1C4h

Default Flash Address: 2C4h

Offset from 0	Bits	Description	Usage	FIT Visible
0x2C4	7:4	Reserved, set to '0xf'		No
	3:2	Reserved, set to '0x1'		No
	1:0	Reserved, set to '0'		No

## 9.379 PCH Descriptor Record 378 (Flash Descriptor Records)

Flash Address:FPSBA + 1C5h

Default Flash Address: 2C5h

Offset from 0	Bits	Description	Usage	FIT Visible
0x2C5	7:2	Reserved, set to '0x3f'		No
	1:0	Reserved, set to '0'		No

### 9.380 PCH Descriptor Record 379 (Flash Descriptor Records)

Flash Address:FPSBA + 1C6h

Default Flash Address: 2C6h

Offset from 0	Bits	Description	Usage	FIT Visible
0x2C6	7:2	Reserved, set to '0x3f'		No
	1:0	Reserved, set to '0'		No

### 9.381 PCH Descriptor Record 380 (Flash Descriptor Records)

Flash Address:FPSBA + 1C7h

Default Flash Address: 2C7h

Offset from 0	Bits	Description	Usage	FIT Visible
0x2C7	7:2	Reserved, set to '0x3f'		No
	1:0	Reserved, set to '0'		No

### 9.382 PCH Descriptor Record 381 (Flash Descriptor Records)

Flash Address:FPSBA + 1C8h

Default Flash Address: 2C8h

Offset from 0	Bits	Description	Usage	FIT Visible
0x2C8	7:0	Reserved, set to '0x1'		No

### 9.383 PCH Descriptor Record 382 (Flash Descriptor Records)

Flash Address:FPSBA + 1C9h

Default Flash Address: 2C9h

Offset from 0	Bits	Description	Usage	FIT Visible
0x2C9	23:0	Reserved, set to '0'		No

## 9.384 MIP Table Descriptor Record 0 (Flash Descriptor Records)

Flash Address:MDTBA + 000h

Default Flash Address: C00h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC00	15:0	<b>Number of MIP Table Descriptor Entries:</b> <b>Set to '0x2'</b>	This setting determines the total number of MIP Table Descriptor entries present in the SPI image.	<b>Yes</b>

## 9.385 MIP Table Descriptor Record 1 (Flash Descriptor Records)

Flash Address:MDTBA + 002h

Default Flash Address: C02h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC02	15:0	<b>Size of MIP Descriptor Entry:</b> <b>Set to '0xB4'</b>	This setting determines the size in bytes of the MIP Descriptor Entry structure.	<b>Yes</b>

## 9.386 MIP Table Descriptor Record 2 (Flash Descriptor Records)

Flash Address:MDTBA + 004h

Default Flash Address: C04h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC04	15:0	<b>MIP Descriptor Block 0:</b> <b>Set to '0x1'</b>	This setting determines what the data type is for the MIP Descriptor.	<b>Yes</b>

## 9.387 MIP Table Descriptor Record 3 (Flash Descriptor Records)

Flash Address:MDTBA + 006h

Default Flash Address: C06h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC06	15:0	<b>MIP Descriptor Block 0 Offset:</b> <b>Set to '0x14'</b>	This setting determines the offset location of the MIP Descriptor Table Entries.	<b>Yes</b>

## 9.388 MIP Table Descriptor Record 4 (Flash Descriptor Records)

Flash Address:MDTBA + 008h

Default Flash Address: C08h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC08	15:0	<b>MIP Descriptor Block 0 Length:</b> Set to '0xA0'	This setting determine the length of the MIP Descriptor Block 0.	Yes

## 9.389 MIP Table Descriptor Record 5 (Flash Descriptor Records)

Flash Address:MDTBA + 00Ah

Default Flash Address: C0Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0xC0A	15:0	Reserved, set to '0'		No

## 9.390 MIP Table Descriptor Record 6 (Flash Descriptor Records)

Flash Address:MDTBA + 00Ch

Default Flash Address: C0Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0xC0C	15:0	<b>MIP Descriptor Block 1 Type:</b> Set to '0'	This setting determines what the data type is for the MIP Descriptor.	Yes

## 9.391 MIP Table Descriptor Record 7 (Flash Descriptor Records)

Flash Address:MDTBA + 00Eh

Default Flash Address: C0Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0xC0E	15:0	<b>MIP Descriptor Block 1 Offset:</b> Set to '0xAC'	This setting determines the offset location of the MIP Descriptor Table Entries.	Yes

## 9.392 MIP Table Descriptor Record 8 (Flash Descriptor Records)

Flash Address:MDTBA + 010h

Default Flash Address: C10h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC10	15:0	<b>MIP Descriptor Block 1 Length:</b> <b>Set to '0x8h'</b>	This setting determine the length of the MIP Descriptor Block 0.	<b>Yes</b>

## 9.393 MIP Table Descriptor Record 9 (Flash Descriptor Records)

Flash Address:MDTBA + 012h

Default Flash Address: C12h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC12	15:0	<b>Reserved, set to '0'</b>		<b>No</b>

## 9.394 PMC Descriptor Record 0 (Flash Descriptor Records)

Flash Address:MDTBA + 014h

Default Flash Address: C14h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC14	31:28	Reserved, set to '0'		No
	27	<b>Intel® Trace Hub Debug Messages Enable:</b>  0x0 = PCH Tracing debug messages Disabled 0x1 = PCH Tracing debug messages Enabled	This setting enables debug messages on the Intel® Trace Hub.  <b>Note:</b> You will also need to set the Intel® Trace Hub Soft Enable to "Enabled"	Yes
	26	Reserved, set to '0'		No
	25	<b>Power Reporting Enable (THERM_PWR_REP_DIS):</b>  0x0 = Power Reporting is enabled. 0x1 = Power Reporting is completely disabled, regardless of the settings in the Thermal Power Reporting configuration registers.  <b>Note:</b> 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.  <b>Note:</b> A once-per-second timer interrupt is enabled which triggers firmware to report power and temperature information as enabled by configuration registers.	Yes
	24	<b>PCIe* Power Stable Timer (tPCH33 timer):</b>  0x0 = tPCH33 timer is disabled 0x1 = 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	<b>APWROK Timing (APWROK_TIMING):</b>  0x0 = 2 ms 0x1 = 4 ms 0x2 = 8 ms 0x3 = 16 ms	This soft strap determines the time between the SLP_A# pin de-asserting and the APWROK timer expiration.	Yes
	20	<b>DeepSx Platform Configuration (DEEPSX_PLT_CFG_SS):</b>  0x0 =The platform does not support DeepSx. 0x1 =The platform supports DeepSx		Yes
	19	<b>LAN PHY Power Up Time (LAN_PHY_PU_TIME):</b>  0x0 =100ms 0x1 =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
0xC14 (cont)	18:16	<b>Over-Clocking WDT Self-Start Enable (OC_WDT_SS_EN):</b>  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	<b>tPCH46 Timing:</b>  0x0 = 1 ms 0x1 = Reserved 0x2 = 5 ms 0x3 = 2 ms	tPch46: PROCPWRGD and SYS_PWROK high to SUS_STAT# deassertion. Refer to EDS for details.	Yes
	9:8	<b>tPCH45 Timing:</b>  0x0 = 100 ms 0x1 = 50 ms 0x2 = 5 ms 0x3 = 1 ms	tPCH45: PCH clock output stable to PROCPWRGD high. Refer to EDS for details.	Yes
	7:0	Reserved, set to '0x68'		No

## 9.395 PMC Descriptor Record 1 (Flash Descriptor Records)

Flash Address:MDTBA + 018h

Default Flash Address: C18h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC18	31:8	Reserved, set to '0'		No
	7	<b>Integrated Sensor Hub Supported:</b>  0x0 = Enable Integrated Sensor Hub 0x1 = Disable Integrated Sensor Hub		Yes
	6:1	Reserved, set to '0'		No
	0	<b>Intel® Integrated wired LAN Enable (IWL_EN):</b>  0x0 = Enabled Intel® Integrated wired LAN Solution 0x1 = Disabled Intel® Integrated wired LAN Solution  <b>Note:</b> 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

## 9.396 PMC Descriptor Record 2 (Flash Descriptor Records)

Flash Address:MDTBA + 01Ch

Default Flash Address: C1Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0xC1C	31:0	Reserved, set to '0x7EC12000'		No

## 9.397 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 '0x40'		No

## 9.398 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 '0'		No
	17	<b>SLP_S0# Tunnel (SLP_S0_TUNNEL_DIS):</b>  0x0 = SLP_S0# Tunnel enabled 0x1 = SLP_S0# Tunnel disabled	This setting enables / disabled the SLP_S0# tunneling over the eSPI to EC interface.  <b>Note:</b> On eSPI enabled platforms this should be set to disabled for proper Sleep S0 operation.	Yes
	16:8	Reserved, set to '0'		No
	7:3	<b>USB2 DbC port enable:</b>  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



## 9.399 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 '0x79200000'		No

## 9.400 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

## 9.401 PMC Descriptor Record 7 (Flash Descriptor Records)

Flash Address:MDTBA + 030h

Default Flash Address: C30h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC30h	31:17	Reserved, set to '0'		No
	16	<b>MIPI 1.24 Rail Sourced from Platform (VCC_MIPI_DPHY_LP_IS_1p24):</b>  0x0 = MIPI 1.24 rail from platform 0x1 = MIPI 1.24 rail not from platform	This setting determines if MIPI 1.24 Rail Source is provided by the platform.  Yes = MIPI 1.24 Rail provided by Platform No = MIPI 1.24 Rail not provided	Yes
	15:14	<b>BCLK Mode Configuration (DEF_CPU_BCLK_CFG):</b>  0x0 = Discrete External BCLK 0x2 = Integrated CPU BCLK	This setting determines which mode CPU BCLK PLL will be using on board CPU BCLK (Integrated) or Discrete BCLK (External).	Yes
	13	<b>External Clock Mode (PEG_DMI_CFG):</b>  0x0 = External Clock Mode disabled 0x1 = External Clock Mode enabled	This setting determines if the PEG / DMI clock source is from ICC or from an external discrete oscillator.	Yes
	12:0	Reserved, set to '0'		No

## 9.402 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

## 9.403 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 '0x2'		No
	1	<b>Re-timer Power Gating Enable:</b> 0x0 = Re-timer PG is disabled 0x1 = Re-timer PD is enabled	This indicates if platform re-timer power gating is enabled.	Yes
	0	<b>PMC-PD Controller USB Type-C Mode:</b> 0x0 = eSPI Mode 0x1 = SMBus Mode		No

## 9.404 PMC Descriptor Record 10 (Flash Descriptor Records)

Flash Address:MDTBA + 03Ch

Default Flash Address: C3Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0xC3Ch	31:28	<b>Reserved, set to '0'</b>		<b>No</b>
	27	<b>Type-C Port 1 Re-timer Configuration Type:</b>  0x0 = 1 Re-Timer present 0x1 = 2 Re-Timers present	This setting determines the number of Re-Timers being use for Type-C Port 1.	<b>Yes</b>
	26:23	<b>USB3 Port Number associated for Type-C Port 1:</b>  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.	<b>Yes</b>
	22:19	<b>USB2 Port Number associated for Type-C Port 1:</b>  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.	<b>Yes</b>
	18:11	<b>Reserved, set to '0'</b>		<b>No</b>
	10:3	<b>Type C Port 1 SMBus Address:</b>  Port 1 SMBus address value: 0x0-0xFF	This setting configures the SMBus address for Type-C Port 1.	<b>Yes</b>
	2	<b>Type-C Port 1 Re-timer Configuration Enable:</b>  0x0 = Port 1 Re-timer configured by PD Controller 0x1 = Port 1 Re-timer configured by PMC Controller	This setting indicates how Type-C Port 1 re-timer configuration is handled.	<b>Yes</b>
	1	<b>Type-C Port 1 Re-Timer Present:</b>  0x0 = Port 1 Re-timer is not present 0x1 = Port 1 Re-timer is present	This setting indicates if a re-timer is present for Type-C Port 1.	<b>Yes</b>
	0	<b>Type-C port 1 Enable:</b>  0x0 = Port 1 disabled 0x1 = Port 1 enabled	This setting indicates if Type-C Port 1 is enabled.	<b>Yes</b>

## 9.405 PMC Descriptor Record 11 (Flash Descriptor Records)

Flash Address:MDTBA + 040h

Default Flash Address: C40h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC40h	31:28	<b>Reserved, set to '0'</b>		<b>No</b>
	27	<b>Type-C Port 2 Re-timer Configuration Type:</b>  0x0 = 1 Re-Timer present 0x1 = 2 Re-Timers present	This setting determines the number of Re-Timers being use for Type-C Port 2.	<b>Yes</b>
	26:23	<b>USB3 Port Number associated for Type-C Port 2:</b>  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.	<b>Yes</b>
	22:19	<b>USB2 Port Number associated for Type-C Port 2:</b>  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.	<b>Yes</b>
	18:11	<b>Reserved, set to '0'</b>		<b>No</b>
	10:3	<b>Type C Port 2 SMBus Address:</b>  Port 2 SMBus address value: 0x0-0xFF	This setting configures the SMBus address for Type-C Port 2.	<b>Yes</b>
	2	<b>Type-C Port 2 Re-timer Configuration Enable:</b>  0x0 = Port 2 Re-timer configured by PD Controller 0x1 = Port 2 Re-timer configured by PMC Controller	This setting indicates how Type-C Port 2 re-timer configuration is handled.	<b>Yes</b>
	1	<b>Type-C Port 2 Re-Timer Present:</b>  0x0 = Port 2 Re-timer is not present 0x1 = Port 2 Re-timer is present	This setting indicates if a re-timer is present for Type-C Port 2.	<b>Yes</b>
	0	<b>Type-C port 2 Enable:</b>  0x0 = Port 2 disabled 0x1 = Port 2 enabled	This setting indicates if Type-C Port 2 is enabled.	<b>Yes</b>

## 9.406 PMC Descriptor Record 12 (Flash Descriptor Records)

Flash Address:MDTBA + 044h

Default Flash Address: C44h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC44h	31:28	<b>Reserved, set to '0'</b>		<b>No</b>
	27	<b>Type-C Port 3 Re-timer Configuration Type:</b>  0x0 = 1 Re-Timer present 0x1 = 2 Re-Timers present	This setting determines the number of Re-Timers being use for Type-C Port 3.	<b>Yes</b>
	26:23	<b>USB3 Port Number associated for Type-C Port 3:</b>  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.	<b>Yes</b>
	22:19	<b>USB2 Port Number associated for Type-C Port 3:</b>  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.	<b>Yes</b>
	18:11	<b>Reserved, set to '0'</b>		<b>No</b>
	10:3	<b>Type C Port 3 SMBus Address:</b>  Port 3 SMBus address value: 0x0-0xFF	This setting configures the SMBus address for Type-C Port 3.	<b>Yes</b>
	2	<b>Type-C Port 3 Re-timer Configuration Enable:</b>  0x0 = Port 3 Re-timer configured by PD Controller 0x1 = Port 3 Re-timer configured by PMC Controller	This setting indicates how Type-C Port 3 re-timer configuration is handled.	<b>Yes</b>
	1	<b>Type-C Port 3 Re-Timer Present:</b>  0x0 = Port 3 Re-timer is not present 0x1 = Port 3 Re-timer is present	This setting indicates if a re-timer is present for Type-C Port 3.	<b>Yes</b>
	0	<b>Type-C port 3 Enable:</b>  0x0 = Port 3 disabled 0x1 = Port 3 enabled	This setting indicates if Type-C Port 3 is enabled.	<b>Yes</b>

## 9.407 PMC Descriptor Record 13 (Flash Descriptor Records)

Flash Address:MDTBA + 048h

Default Flash Address: C48h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC48h	31:28	<b>Reserved, set to '0'</b>		<b>No</b>
	27	<b>Type-C Port 4 Re-timer Configuration Type:</b>  0x0 = 1 Re-Timer present 0x1 = 2 Re-Timers present	This setting determines the number of Re-Timers being use for Type-C Port 4.	<b>Yes</b>
	26:23	<b>USB3 Port Number associated for Type-C Port 4:</b>  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.	<b>Yes</b>
	22:19	<b>USB2 Port Number associated for Type-C Port 4:</b>  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.	<b>Yes</b>
	18:11	<b>Reserved, set to '0'</b>		<b>No</b>
	10:3	<b>Type C Port 4 SMBus Address:</b>  Port 3 SMBus address value: 0x0-0xFF	This setting configures the SMBus address for Type-C Port 4.	<b>Yes</b>
	2	<b>Type-C Port 4 Re-timer Configuration Enable:</b>  0x0 = Port 4 Re-timer configured by PD Controller 0x1 = Port 4 Re-timer configured by PMC Controller	This setting indicates how Type-C Port 4 re-timer configuration is handled.	<b>Yes</b>
	1	<b>Type-C Port 4 Re-Timer Present:</b>  0x0 = Port 4 Re-timer is not present 0x1 = Port 4 Re-timer is present	This setting indicates if a re-timer is present for Type-C Port 4.	<b>Yes</b>
	0	<b>Type-C port 4 Enable:</b>  0x0 = Port 4 disabled 0x1 = Port 4 enabled	This setting indicates if Type-C Port 4 is enabled.	<b>Yes</b>

## 9.408 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

## 9.409 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

## 9.410 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

## 9.411 CPU Descriptor Record 0 (Flash Descriptor Records)

Flash Address:MDTBA + 058h

Default Flash Address: C58h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC58	31:24	<b>CPU Strap Length (CPUSL):</b>  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.  <b>Set this field to 0x14</b>		<b>No</b>
	23:0	<b>Reserved, set to '0'</b>		<b>No</b>



## 9.412 CPU Descriptor Record 1 (Flash Descriptor Records)

Flash Address:MDTBA + 05Ch

Default Flash Address: C5Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0xC5C	31:23	<b>Reserved, set to '0'</b>		<b>No</b>
	22:17	<b>Number of Active Small Cores:</b>  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 Small processor cores.  <b>Note:</b> This strap is intended for debugging purposed only. See BIOS Spec for more details on enabling / disabling processor cores.	<b>Yes</b>
	16	<b>Encrypted Debug Enable:</b>  0x0 = Encrypted Debug Enabled 1 = Encrypted Debug Disabled	This setting determines if encrypted debugging is enabled  <b>Note:</b> This strap is intended for debugging purposes only.	<b>No</b>
	14:15	<b>Reserved, set to '0'</b>		<b>No</b>
	13	<b>JTAG Power Disable:</b>  0x0 = 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.  <b>Note:</b> This strap is intended for debugging purposed only.	<b>Yes</b>
	12	<b>Processor Boot Max Non-Turbo Frequency:</b>  0x0 = Disable Boot Non-Turbo Max Frequency 0x1 = Enable Boot Non-Turbo Max Frequency	This setting determines if the processor will operate at maximum Non-Turbo frequency at power-on and boot.  <b>Note:</b> This strap is intended for debugging purposed only.	<b>Yes</b>
	11:6	<b>Flex Ratio:</b>  '0x0'	This setting controls the maximum processor non-turbo ratio.  <b>Note:</b> This strap is intended for debugging purposed only. See BIOS Spec for more details on maximum processor non-turbo ratio configuration.	<b>Yes</b>
	5	<b>BIST Initialization:</b>  0x0 = Disable BIST at Reset 0x1 = Enable BIST at Reset	This setting determines if BIST will be run at platform reset after BIOS requested actions.  <b>Note:</b> This strap is intended for debugging purposed only.	<b>Yes</b>

Offset from 0	Bits	Description	Usage	FIT Visible
<b>0xC5C (Cont)</b>	4:1	<b>Number of Active Big Cores:</b>  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	This setting controls the number of active Big processor cores.  <b>Note:</b> This strap is intended for debugging purposed only. See BIOS Spec for more details on enabling / disabling processor cores.	<b>Yes</b>
	0	<b>Disable Hyper threading:</b>  0x0 = Enable Hyper Threading 0x1 = Disable Hyper Threading	This setting control enabling / disabling of Hyper threading.  <b>Note:</b> This strap is intended for debugging purposed only. See BIOS Spec for more details on enabling / disabling Hyper threading	<b>Yes</b>

## 9.413 CPU Descriptor Record 2 (Flash Descriptor Records)

Flash Address:MDTBA + 060h

Default Flash Address: C60h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC60	31	<b>Platform IMON:</b> 0x1 = IMON Disabled	<b>Note:</b> This strap should be left at the recommended default setting.	<b>Yes</b>
	30:19	<b>Reserved, set to '0'</b>		<b>No</b>
	18	<b>IA VR Offset VID:</b> 0x0 = IA VR Offset disabled 0x1 = IA VR Offset enabled	Enables/disables a voltage offset for the IA VR allowing voltage levels to exceed 1.52V.	<b>Yes</b>
	17	<b>GT_S VR Type:</b> 0x0 = GT Unslice VR type SVID 0x1 = GT Unslice VR type is fixed VR	This setting determines the GT Slice domain VR type. See Processor EDS for details.	<b>Yes</b>
	16:13	<b>GT_S SVID Address:</b> Min:0x0 - Max 0xf <b>Default '0x1'</b>	This setting determines the GT Slice SVID Address. See Processor EDS for details.	<b>Yes</b>
	12	<b>IA VR Type:</b> 0x0 = IA VR Type SVID 0x1 = IA VR type is fixed VR	This setting determines the IA VR type. See Processor EDS for details.	<b>Yes</b>
	11:8	<b>IA SVID Address:</b> Min:0x0 - Max 0xf	This setting determines the IA SVID Address. See Processor EDS for details.	<b>Yes</b>
	7	<b>VCCIN_AUX IMON Enabled:</b> 0x0 = VCCIN Aux IMON disabled 0x1 = VCCIN Aux IMON enabled	This setting determines if VCCIN AUX IMON is enabled.	<b>Yes</b>
	6:5	<b>Reserved, set to '0'</b>		<b>No</b>
	4	<b>Processor PCIe 1011 enabled:</b> 0x0 = Processor PCIe 1011 enabled 0x1 = Processor PCIe 1011 disabled	This setting determines if PCIe PEG 1011 is enabled or disabled.	<b>Yes</b>
	3	<b>VCCP 1.05 CPU PG Exists:</b> 0x0 = VCCP 1.05 CPU PG Not present 0x1 = VCCP 1.05 CPU PG present	This enables VCCP 1.05 CPU Power Gating capabilities if present on the platform.	<b>Yes</b>
	2	<b>Reserved, set to '0'</b>		<b>No</b>
	1	<b>VCC 1.05v CPU Source:</b> 0x0 = VCC 1.05v CPU Source PCH 0x1 = VCC 1.05v CPU source Platform Rail	This setting determines where the VCC 1.05v CPU Sourced from.	<b>Yes</b>
	0	<b>Reserved, set to '0'</b>		<b>No</b>

## 9.414 CPU Descriptor Record 3 (Flash Descriptor Records)

Flash Address:MDTBA + 064h

Default Flash Address: C64h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC64	31:0	Reserved, set to '0xBF'		No

## 9.415 CPU Descriptor Record 4 (Flash Descriptor Records)

Flash Address:MDTBA + 068h

Default Flash Address: C68h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC68	31:0	Reserved, set to '0'		No

## 9.416 CPU Descriptor Record 5 (Flash Descriptor Records)

Flash Address:MDTBA + 06Ch

Default Flash Address: C6Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0xC6C	31:0	Reserved, set to '0'		No

## 9.417 CPU Descriptor Record 6 (Flash Descriptor Records)

Flash Address:MDTBA + 070h

Default Flash Address: C70h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC70	31:0	Reserved, set to '0x55555516'		No

## 9.418 CPU Descriptor Record 7 (Flash Descriptor Records)

Flash Address:MDTBA + 074h

Default Flash Address: C74h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC74	31:0	Reserved, set to '0x55555555'		No

## 9.419 CPU Descriptor Record 8 (Flash Descriptor Records)

Flash Address:MDTBA + 078h

Default Flash Address: C78h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC78	31:0	Reserved, set to '0x5'		No

## 9.420 CPU Descriptor Record 9 (Flash Descriptor Records)

Flash Address:MDTBA + 07Ch

Default Flash Address: C7Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0xC7C	31:10	Reserved, set to '0x80180'		No
	9	<b>P2 to P2 Transition Clock Domain:</b> 0x0 = P2 to P2 Sync to PCLK 0x1 = P2 to P2 Async to PCLK	This setting controls the P2 to P2 Transition Clock Domain.	Yes
	8:0	Reserved, set to '0x19E'		No

## 9.421 CPU Descriptor Record 10 (Flash Descriptor Records)

Flash Address:MDTBA + 080h

Default Flash Address: C80h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC80	31:13	Reserved, set to '0'		No
	12	<b>HSIO Lane Rx Detection Bypass:</b> 0x0 = Rx Detect Bypass 0x1 = Rx Detect No Bypass	This setting enables/disables Receiver detection for HSIO Lane configuration.Note: This setting has no affect when the HSIO Lane Force Detect setting is configured to No Force Detect.	Yes
0xC80 (Cont)	11:9	<b>HSIO Lane Force Detect:</b> 0x0 = No Force Detect 0x1 = Force x16 Link 0x2 = Force x8 Link 0x3 = Force x4 Link Lanes 0-3 0x4 = Force x2 Link Lanes 0-1 0x5 = Force x1 Link Lane 0	This setting allow High Speed I/O lane configurations to be statically assigned to specific lane configurations (i.e. x2, x4, x8 x16 etc.) regardless of detection.	Yes
	8:0	Reserved, set to '0x6'		No

## 9.422 CPU Descriptor Record 11 (Flash Descriptor Records)

Flash Address:MDTBA + 084h

Default Flash Address: C84h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC84	31:0	Reserved, set to '0x6091E'		No

## 9.423 CPU Descriptor Record 12 (Flash Descriptor Records)

Flash Address:MDTBA + 088h

Default Flash Address: C88h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC88	31:0	Reserved, set to '0x55516'		No

## 9.424 CPU Descriptor Record 13 (Flash Descriptor Records)

Flash Address:MDTBA + 08Ch

Default Flash Address: C8Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0xC8C	31:0	Reserved, set to '0'		No

## 9.425 CPU Descriptor Record 14 (Flash Descriptor Records)

Flash Address:MDTBA + 090h

Default Flash Address: C90h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC90	31:0	Reserved, set to '0'		No

## 9.426 CPU Descriptor Record 15 (Flash Descriptor Records)

Flash Address:MDTBA + 094h

Default Flash Address: C94h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC94	31:0	Reserved, set to '0'		No

## 9.427 CPU Descriptor Record 16 (Flash Descriptor Records)

Flash Address:MDTBA + 098h

Default Flash Address: C98h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC98	31:0	Reserved, set to '0'		No

## 9.428 CPU Descriptor Record 17 (Flash Descriptor Records)

Flash Address:MDTBA + 09Ch

Default Flash Address: C9Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0xC9C	31:0	Reserved, set to '0'		No

## 9.429 CPU Descriptor Record 18 (Flash Descriptor Records)

Flash Address:MDTBA + 0A0h

Default Flash Address: CA0h

Offset from 0	Bits	Description	Usage	FIT Visible
0xCA0	31:0	Reserved, set to '0'		No

## 9.430 CPU Descriptor Record 19 (Flash Descriptor Records)

Flash Address:MDTBA + 0A4h

Default Flash Address: CA4h

Offset from 0	Bits	Description	Usage	FIT Visible
0xCA4	31:0	Reserved, set to '0'		No

## 9.431 CPU Descriptor Record 20 (Flash Descriptor Records)

Flash Address:MDTBA + 0A8h

Default Flash Address: CA8h

Offset from 0	Bits	Description	Usage	FIT Visible
0xCA8	31:0	Reserved, set to '0'		No

## 9.432 Intel® ME Descriptor Record 0 (Flash Descriptor Records)

Flash Address:MDTBA + 0ACh

Default Flash Address: CACH

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



## 9.433 Intel® ME Descriptor Record 1 (Flash Descriptor Records)

Flash Address: MDTBA + 0B0h

Default Flash Address: CB0h

Offset from 0	Bits	Description	Usage	FIT Visible
0xCB0	31:26	Reserved, set to '0'		No
	25	Reserved, set to '0'		No
	24	<b>Delayed Authentication Mode enable (DAM_EN):</b>  0x0 = DAM is disabled 0x1 = DAM is enabled	This setting Enables / Disables Delayed Authentication Mode on the platform.	No
	23:16	<b>Early USB2 DbC Enable:</b>  0x0 = Early USB2 DbC not enabled 0x1 = Early USB2 DbC enabled	This setting enables a delay during Intel® ME FW bring-up to allow USB DCI to be established and Early DbC arbitration to be granted.	Yes
	15:8	<b>USB Connector's Associated USB3 Port enable:</b>  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	<b>USB2 DbC port enable:</b>  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

## 10 Configuration Dependencies

## 10.1 Descriptor Configuration Setting Enabling Dependencies

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

### 10.1.1 High Speed IO (HSIO) Port Enabling

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

**Note:** Refer to EDS for exact number HSIO lane# supported. Some SKUs may have less HSIO lane. To get a full understanding on HSIO lane muxing architecture refer to the PCH EDS.

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

**Note:** On HSIO lanes that support SATA / PCIe these two modes configuration are mutually exclusive on the associated PCIe Controller. Only one mode can be active (i.e. if one lane is configured as SATA all lanes must be configured as SATA).

### Table 10-1. Raptor Lake-S Flex I/O Map

[illegible]

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

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

PHY Instance	HSIO Lane	Port #	Strap Offset (value)	Description
8		USB P1	No muxing	
		USB P2	No muxing	
		USB P3	No muxing	
USB P4		No muxing		
9		USB P5	No muxing	
		USB P6	No muxing	
		10	USB P7	No muxing
USB P8			No muxing	
USB P9			No muxing	
		USB P10	No muxing	
7		DMI1	No muxing	
		DMI2	No muxing	
		DMI3	No muxing	
		DMI4	No muxing	
		DMI5	No muxing	
		DMI6	No muxing	
		DMI7	No muxing	
		DMI8	No muxing	
1	Lane 0	PCIe P1	No muxing	
	Lane 1	PCIe P2	No muxing	
	Lane 2	PCIe P3	FPSBA + 19Dh[7:4] = 0x5	GBE PCIe* Select Port 3 (FIA_PGS/LOSL2)
	Lane 2	GbE P3	FPSBA + 19Dh[7:4] = 0x8	
	Lane 3	PCIe P4	No muxing	
2	Lane 0	PCIe P5	No muxing	
	Lane 1	PCIe P6	No muxing	
	Lane 2	PCIe P7	FPSBA + 19Fh[7:4] = 0x5	GBE PCIe* Select Port 7 (FIA_PGS/LOSL6)
	Lane 2	GbE P7	FPSBA + 19Fh[7:4] = 0x8	
	Lane 3	PCIe P8	No muxing	
3	Lane 0	PCIe P9	No muxing	
	Lane 1	PCIe P10	No muxing	
	Lane 2	PCIe P11	No muxing	
	Lane 3	PCIe P12	No muxing	

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

PHY Instance	HSIO Lane	Port #	Strap Offset (value)	Description
4	Lane 0	PCIe P13	FPSBA + 2A2[7:4] = 0x5	SATA/PCIe Combo Port 0 Strap (FIA_PGS/LOSL12)
	Lane 0	SATA 0	FPSBA + 2A2[7:4] = 0x7	
	Lane 1	PCIe P14	FPSBA + 2A3[3:0] = 0x5	SATA/PCIe Combo Port 1 Strap (FIA_PGS/LOSL13)
	Lane 1	SATA 1	FPSBA + 2A3[3:0] = 0x7	
	Lane 2	PCIe P15	FPSBA + 2A3[7:4] = 0x5	SATA/PCIe Combo Port 2 Strap (FIA_PGS/LOSL14)
	Lane 2	SATA 2	FPSBA + 2A3[7:4] = 0x7	
	Lane 3	PCIe P16	FPSBA + 2A4[0:3] = 0x5	SATA/PCIe Combo Port 3 Strap (FIA_PGS/LOSL15)
	Lane 3	SATA 3	FPSBA + 2A4[0:3] = 0x7	
	Lane 0	PCIe P17	FPSBA + 2A4[7:4] = 0x5	SATA/PCIe Combo Port 4 Strap (FIA_PGS/LOSL16)
	Lane 0	SATA 4	FPSBA + 2A4[7:4] = 0x7	
	Lane 1	PCIe P18	FPSBA + 2A5[3:0] = 0x5	SATA/PCIe Combo Port 5 Strap (FIA_PGS/LOSL17)
	Lane 1	SATA 5	FPSBA + 2A5[3:0] = 0x7	
	Lane 2	PCIe P19	FPSBA + 2A5[7:4] = 0x5	SATA/PCIe Combo Port 6 Strap (FIA_PGS/LOSL18)
	Lane 2	SATA 6	FPSBA + 2A5[7:4] = 0x7	
	Lane 3	PCIe P20	FPSBA + 2A6[3:0] = 0x5	SATA/PCIe Combo Port 7 Strap (FIA_PGS/LOSL19)
	Lane 3	SATA 7	FPSBA + 2A6[3:0] = 0x7	
5		PCIe P21	No muxing	
		PCIe P22	No muxing	
		PCIe P23	No muxing	
		PCIe P24	No muxing	
6		PCIe P25	No muxing	
		PCIe P26	No muxing	
		PCIe P27	No muxing	
		PCIe P28	No muxing	

### 10.1.1.1 Configuring PCIe on HSIO

For PCIe Controller #1:

Recommended Steps	Straps
1. Configure HSIO lane to be PCIe.	Refer HSIO Muxing Table
2. Configure PCIe lane, x1, x2 or x4	FPSBA + 84h[3:1]
3. Configure PCIe lane Reversal	FPSBA + 84h[0]

For PCIe Controller #2:

Recommended Steps	Straps
1. Configure HSIO lane to be PCIe.	Refer HSIO Muxing Table
2. Configure PCIe lane, x1, x2 or x4	FPSBA + 90h[3:1]
3. Configure PCIe lane Reversal	FPSBA + 90h[0]

For PCIe Controller #3:

Recommended Steps	Straps
1. Configure HSIO lane to be PCIe.	Refer HSIO Muxing Table
2. Configure PCIe lane, x1, x2 or x4	FPSBA + 9Ch[3:1]
3. Configure PCIe lane Reversal	FPSBA + 9Ch[0]

For PCIe Controller #4:

Recommended Steps	Straps
1. Configure HSIO lane to be PCIe.	Refer HSIO Muxing Table
2. Configure PCIe lane, x1, x2 or x4	FPSBA + A8h[3:1]
3. Configure PCIe lane Reversal	FPSBA + A8h[0]

For PCIe Controller #5:

Recommended Steps	Straps
1. Configure HSIO lane to be PCIe.	Refer HSIO Muxing Table
2. Configure PCIe lane, x1, x2 or x4	FPSBA + B4h[3:1]
3. Configure PCIe lane Reversal	FPSBA + B4h[0]

For PCIe Controller #6:

Recommended Steps	Straps
1. Configure HSIO lane to be PCIe.	Refer HSIO Muxing Table
2. Configure PCIe lane, x1, x2 or x4	FPSBA + C0h[3:0]
3. Configure PCIe lane Reversal	FPSBA + C0h[0]

For PCIe Controller #7:

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

## 10.1.2 Intel® Integrated LAN Controller Enabling

If Yes:

## 10.1.3 Intel® Wireless LAN Controller Enabling

Offset from 0	Bits	Required Value	Descriptor Configuration Parameter	
FPSBA + 160h	6:0	<b>0x70</b>	GbE MAC SMBus Address	
FPSBA + 163h	0	<b>0x1</b>	GbE MAC SMBus Address Enable	
FPSBA + 165h	2:0	<b>0x2</b>	Reserved	
FPSBA + 164h	1:0	<b>0x3</b>	Reserved	
FPSBA + 168h	6:0	<b>0x64</b>	GbE PHY SMBus Address	
FPSBA + 38h	4	<b>0x0</b>	LAN PHY Power Control GDP11 Signal Configuration Note: For non-Intel Wired LAN, set to 01b	
FPSBA + 19Dh	7:4	<b>0x8</b>	GBE PCIe* Port Select	GBE PCIe* Select Port 3 (FIA_PGS/LOSL2)
FPSBA + 19Fh	7:4	<b>0x8</b>		GBE PCIe* Select Port 7 (FIA_PGS/LOSL6)
FPSBA + 1C0h	1:0	<b>0x1</b>	Reserved	
FPSBA + 1C0h	7:2	<b>0x24</b>	Reserved	
FPSBA + 1C1h	6:0	<b>0x70</b>	Reserved	
FPSBA + 1C1h	7	<b>0x1</b>	Reserved	
FPSBA + 1C2h	7:3	<b>0x1</b>	Reserved	
FPSBA + 1C2h	2:0	<b>0x2</b>	PHY Connection	
FPSBA + 1C3h	3	<b>0x1</b>	LC SMBus add enable GbE_ADDREN	
FPSBA + 1C3h	2	<b>0x1</b>	LCD SMBus add enable PHY_ADDREN	
FPSBA + 1C4h	2	<b>0x1</b>	Reserved	
MDTBA + 18h	0	<b>0x0</b>	Intel® integrated wired LAN Enable	

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

Set PCIe config accordingly, x1

Then set below straps.

If yes:

Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
FPSBA + 38h	3	<b>0x0</b>	SLP_WLAN# / GDP9 Signal Configuration

## 10.1.4 Deep Sx Enabling Dependencies

To enable:

Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
FPSBA + DCh	20	<b>0x1</b>	Deep Sx Enable
MDTBA + 14h	20	<b>0x1</b>	DEEPSX_PLT_CFG_SS [See Descriptor Configuration Chapter <a href="#">Section 9.1</a> for details]

## 10.1.5 Intel® SMBus Enabling

To enable SMBus:

Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
FPSBA + E5h	0	<b>0x1</b>	SMT1 State
FPSBA + E7h	6:0	<b>User input</b>	Intel® ME SMBus I <sup>2</sup> C Address
FPSBA + E8h	6:0	<b>User Input</b>	Intel® ME SMBus ASD Address
FPSBA + E9h	6:0	<b>User Input</b>	Intel® ME SMBus MCTP Address
FPSBA + EAh	0	<b>0x1</b>	Intel® ME SMBus I <sup>2</sup> C Address Enable. To enable = 1b
FPSBA + EBh	0	<b>0x1</b>	Intel® ME SMBus ASD Address Enable
FPSBA + Ech	0	<b>0x1</b>	Intel® ME SMBus MCTP Address Enable
FPSBA + EEh	31:0	<b>User input</b>	Intel® ME SMBus Subsystem Vendor & Device ID for ASF [31:0]
FPSBA + E4h	0	<b>0x0</b>	SMBus / SMLink TCO Slave Connection
FPSBA + F6h	1:0	<b>0x1</b>	Intel® ME SMBus Frequency

### 10.1.6 SMLink0 Enabling Dependencies

To enable SMLink0:

Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
FPSBA + F9h	0	<b>0x1</b>	SMLink0 Enable
FPSBA + 10Ah	1:0	<b>0x3</b>	SMLink0 Frequency

### 10.1.7 SMLink1 Enabling Dependencies

To enable SMLink1:

Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
FPSBA + 10Dh	0	<b>0x1</b>	SMLink1 Enable
FPSBA + 10Fh	6:0	<b>User input</b>	SMLink1 I <sup>2</sup> C* Target Address
FPSBA + 10Eh	7:1	<b>User Input</b>	SMLink1 GP Target Address
FPSBA + 112h	0	<b>0x1</b>	SMLink1 I <sup>2</sup> C Target Address Enable
FPSBA + 10Eh	0	<b>0x1</b>	SMLink1 GP Target Address Enable
FPSBA + 11Eh	1:0	<b>0x1</b>	SMLink1 Frequency



## 10.1.8 TPM over SPI Enabling Dependencies

To enable TPM over SPI:

Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
FPSBA + 18Ch	0	<b>0x1</b>	TPM Over SPI Bus Enable
FPSBA + 6Dh	2:0	<b>0x6</b>	TPM Clock Frequency 010 = 48 MHz 100 = 30 MHz 110 = 17 MHz (other value not supported)

To disable TPM over SPI:

Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
FPSBA + 18Ch	0	<b>0x0</b>	TPM Over SPI Bus Enable

## 10.1.9 mSATA/M.2 / SATA Express Enabling

### 10.1.9.1 SATA 0-3 / PCIe 13-16 mSATA /M.2 / SATA Express Enabling

SATA / PCIe Combo Port Configuration	Mode	Port Mapping	Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
SATA / PCIe Combo Port's 0-3 values configuration	PCIe	PCIe 13-16	FPSBA + 1A2	7:4	0x5	FIA_PGS/LOSL12
			FPSBA + 1A3	3:0	0x5	FIA_PGS/LOSL13
			FPSBA + 1A3	7:4	0x5	FIA_PGS/LOSL14
			FPSBA + 1A4	3:0	0x5	FIA_PGS/LOSL15
			FPSBA + 32	1:0	0x1	GPCOM4/gpio_sstrap_sataxpcie_0
			FPSBA + 32	3:2	0x1	GPCOM4/gpio_sstrap_sataxpcie_1
			FPSBA + 32	5:4	0x1	GPCOM4/gpio_sstrap_sataxpcie_2
			FPSBA + 32	7:6	0x1	GPCOM4/gpio_sstrap_sataxpcie_3
			FPSBA + 1B0	1:0	0x1	SATA/SATA_PCIE_Select_for_Port_0
			FPSBA + 1B0	3:2	0x1	SATA/SATA_PCIE_Select_for_Port_1
			FPSBA + 1B0	5:4	0x1	SATA/SATA_PCIE_Select_for_Port_2
			FPSBA + 1B0	7:6	0x1	SATA/SATA_PCIE_Select_for_Port_3
	SATA	SATA 0-3	FPSBA + 1A2	7:4	0x7	FIA_PGS/LOSL12
			FPSBA + 1A3	3:0	0x7	FIA_PGS/LOSL13
			FPSBA + 1A3	7:4	0x7	FIA_PGS/LOSL14
			FPSBA + 1A4	3:0	0x7	FIA_PGS/LOSL15
			FPSBA + 32	1:0	0x0	GPCOM4/gpio_sstrap_sataxpcie_0
			FPSBA + 32	3:2	0x0	GPCOM4/gpio_sstrap_sataxpcie_1
			FPSBA + 32	5:4	0x0	GPCOM4/gpio_sstrap_sataxpcie_2
			FPSBA + 32	7:6	0x0	GPCOM4/gpio_sstrap_sataxpcie_3
			FPSBA + 1B0	1:0	0x0	SATA/SATA_PCIE_Select_for_Port_0
			FPSBA + 1B0	3:2	0x0	SATA/SATA_PCIE_Select_for_Port_1
			FPSBA + 1B0	5:4	0x0	SATA/SATA_PCIE_Select_for_Port_2
			FPSBA + 1B0	7:6	0x0	SATA/SATA_PCIE_Select_for_Port_3

SATA / PCIe Combo Port Configuration	Mode	Port Mapping	Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
SATA / PCIe Combo Port's 0-3 values configuration (Cont)	GPIO Polarity	PCIe	FPSBA + 1A2	7:4	0xC	FIA_PGS/LOSL12
			FPSBA + 1A3	3:0	0xC	FIA_PGS/LOSL13
			FPSBA + 1A3	7:4	0xC	FIA_PGS/LOSL14
			FPSBA + 1A4	3:0	0xC	FIA_PGS/LOSL15
			FPSBA + 32	1:0	0x3	GPCOM4/gpio_sstrap_sataxpcie_0
			FPSBA + 32	3:2	0x1	GPCOM4/gpio_sstrap_sataxpcie_1
			FPSBA + 32	5:4	0x1	GPCOM4/gpio_sstrap_sataxpcie_2
			FPSBA + 32	7:6	0x1	GPCOM4/gpio_sstrap_sataxpcie_3
			FPSBA + 1B0	1:0	0x3	SATA/SATA_PCIE_Select_for_Port_0
			FPSBA + 1B0	3:2	0x1	SATA/SATA_PCIE_Select_for_Port_1
			FPSBA + 1B0	5:4	0x1	SATA/SATA_PCIE_Select_for_Port_2
			FPSBA + 1B0	7:6	0x1	SATA/SATA_PCIE_Select_for_Port_3
			FPSBA + 1B2	0	0x1	SATA/SATA_PCIE_Select_GPIO_polarity_for_Port_0
			FPSBA + 1B2	1	0x0	SATA/SATA_PCIE_Select_GPIO_polarity_for_Port_1
			FPSBA + 1B2	2	0x0	SATA/SATA_PCIE_Select_GPIO_polarity_for_Port_2
			FPSBA + 1B2	3	0x0	SATA/SATA_PCIE_Select_GPIO_polarity_for_Port_3
		SATA	FPSBA + 1A2	7:4	0xD	FIA_PGS/LOSL12
			FPSBA + 1A3	3:0	0xD	FIA_PGS/LOSL13
			FPSBA + 1A3	7:4	0xD	FIA_PGS/LOSL14
			FPSBA + 1A4	3:0	0xD	FIA_PGS/LOSL15
			FPSBA + 32	1:0	0x3	GPCOM4/gpio_sstrap_sataxpcie_0
			FPSBA + 32	3:2	0x1	GPCOM4/gpio_sstrap_sataxpcie_1
			FPSBA + 32	5:4	0x1	GPCOM4/gpio_sstrap_sataxpcie_2
			FPSBA + 32	7:6	0x1	GPCOM4/gpio_sstrap_sataxpcie_3
			FPSBA + 1B0	1:0	0x3	SATA/SATA_PCIE_Select_for_Port_0
			FPSBA + 1B0	3:2	0x1	SATA/SATA_PCIE_Select_for_Port_1
			FPSBA + 1B0	5:4	0x1	SATA/SATA_PCIE_Select_for_Port_2
			FPSBA + 1B0	7:6	0x1	SATA/SATA_PCIE_Select_for_Port_3
			FPSBA + 1B2	0	0x0	SATA/SATA_PCIE_Select_GPIO_polarity_for_Port_0
			FPSBA + 1B2	1	0x1	SATA/SATA_PCIE_Select_GPIO_polarity_for_Port_1
			FPSBA + 1B2	2	0x1	SATA/SATA_PCIE_Select_GPIO_polarity_for_Port_2
			FPSBA + 1B2	3	0x1	SATA/SATA_PCIE_Select_GPIO_polarity_for_Port_3

### 10.1.9.2 SATA 4-7 / PCIe 17-20 mSATA /M.2 / SATA Express Enabling

SATA / PCIe Combo Port Configuration	Mode	Port Mapping	Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
SATA / PCIe Combo Port's 4-7 values configuration	PCIe	PCIe 17-20	FPSBA + 1A4	7:4	0x5	FIA_PGS/LOSL12
			FPSBA + 1A5	3:0	0x5	FIA_PGS/LOSL13
			FPSBA + 1A5	7:4	0x5	FIA_PGS/LOSL14
			FPSBA + 1A6	3:0	0x5	FIA_PGS/LOSL15
			FPSBA + 33	1:0	0x1	GPCOM4/gpio_sstrap_sataxpcie_0
			FPSBA + 33	3:2	0x1	GPCOM4/gpio_sstrap_sataxpcie_1
			FPSBA + 33	5:4	0x1	GPCOM4/gpio_sstrap_sataxpcie_2
			FPSBA + 33	7:6	0x1	GPCOM4/gpio_sstrap_sataxpcie_3
			FPSBA + 1B1	1:0	0x1	SATA/SATA_PCIE_Select_for_Port_0
			FPSBA + 1B1	3:2	0x1	SATA/SATA_PCIE_Select_for_Port_1
			FPSBA + 1B1	5:4	0x1	SATA/SATA_PCIE_Select_for_Port_2
			FPSBA + 1B1	7:6	0x1	SATA/SATA_PCIE_Select_for_Port_3
	SATA	SATA 4-7	FPSBA + 1A4	7:4	0x7	FIA_PGS/LOSL12
			FPSBA + 1A5	3:0	0x7	FIA_PGS/LOSL13
			FPSBA + 1A5	7:4	0x7	FIA_PGS/LOSL14
			FPSBA + 1A6	3:0	0x7	FIA_PGS/LOSL15
			FPSBA + 33	1:0	0x0	GPCOM4/gpio_sstrap_sataxpcie_0
			FPSBA + 33	3:2	0x0	GPCOM4/gpio_sstrap_sataxpcie_1
			FPSBA + 33	5:4	0x0	GPCOM4/gpio_sstrap_sataxpcie_2
			FPSBA + 33	7:6	0x0	GPCOM4/gpio_sstrap_sataxpcie_3
			FPSBA + 1B1	1:0	0x0	SATA/SATA_PCIE_Select_for_Port_0
			FPSBA + 1B1	3:2	0x0	SATA/SATA_PCIE_Select_for_Port_1
			FPSBA + 1B1	5:4	0x0	SATA/SATA_PCIE_Select_for_Port_2
			FPSBA + 1B1	7:6	0x0	SATA/SATA_PCIE_Select_for_Port_3

SATA / PCIe Combo Port Configuration	Mode	Port Mapping	Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
SATA / PCIe Combo Port's 4-7 values configuration (Cont)	GPIO Polarity	PCIe	FPSBA + 1A4	7:4	0xC	FIA_PGS/LOSL12
			FPSBA + 1A5	3:0	0xC	FIA_PGS/LOSL13
			FPSBA + 1A5	7:4	0xC	FIA_PGS/LOSL14
			FPSBA + 1A6	3:0	0xC	FIA_PGS/LOSL15
			FPSBA + 33	1:0	0x3	GPCOM4/gpio_sstrap_sataxpcie_0
			FPSBA + 33	3:2	0x1	GPCOM4/gpio_sstrap_sataxpcie_1
			FPSBA + 33	5:4	0x1	GPCOM4/gpio_sstrap_sataxpcie_2
			FPSBA + 33	7:6	0x1	GPCOM4/gpio_sstrap_sataxpcie_3
			FPSBA + 1B1	1:0	0x3	SATA/SATA_PCIE_Select_for_Port_0
			FPSBA + 1B1	3:2	0x1	SATA/SATA_PCIE_Select_for_Port_1
			FPSBA + 1B1	5:4	0x1	SATA/SATA_PCIE_Select_for_Port_2
			FPSBA + 1B1	7:6	0x1	SATA/SATA_PCIE_Select_for_Port_3
			FPSBA + 1B2	4	0x1	SATA/SATA_PCIE_Select_GPIO_polarity_for_Port_0
			FPSBA + 1B2	5	0x0	SATA/SATA_PCIE_Select_GPIO_polarity_for_Port_1
			FPSBA + 1B2	6	0x0	SATA/SATA_PCIE_Select_GPIO_polarity_for_Port_2
			FPSBA + 1B2	7	0x0	SATA/SATA_PCIE_Select_GPIO_polarity_for_Port_3
		SATA	FPSBA + 1A4	7:4	0xD	FIA_PGS/LOSL12
			FPSBA + 1A5	3:0	0xD	FIA_PGS/LOSL13
			FPSBA + 1A5	7:4	0xD	FIA_PGS/LOSL14
			FPSBA + 1A6	3:0	0xD	FIA_PGS/LOSL15
			FPSBA + 33	1:0	0x3	GPCOM4/gpio_sstrap_sataxpcie_0
			FPSBA + 33	3:2	0x1	GPCOM4/gpio_sstrap_sataxpcie_1
			FPSBA + 33	5:4	0x1	GPCOM4/gpio_sstrap_sataxpcie_2
			FPSBA + 33	7:6	0x1	GPCOM4/gpio_sstrap_sataxpcie_3
			FPSBA + 1B1	1:0	0x3	SATA/SATA_PCIE_Select_for_Port_0
			FPSBA + 1B1	3:2	0x1	SATA/SATA_PCIE_Select_for_Port_1
			FPSBA + 1B1	5:4	0x1	SATA/SATA_PCIE_Select_for_Port_2
			FPSBA + 1B1	7:6	0x1	SATA/SATA_PCIE_Select_for_Port_3
			FPSBA + 1B2	4	0x0	SATA/SATA_PCIE_Select_GPIO_polarity_for_Port_0
			FPSBA + 1B2	5	0x1	SATA/SATA_PCIE_Select_GPIO_polarity_for_Port_1
			FPSBA + 1B2	6	0x1	SATA/SATA_PCIE_Select_GPIO_polarity_for_Port_2
			FPSBA + 1B2	7	0x1	SATA/SATA_PCIE_Select_GPIO_polarity_for_Port_3

## 10.1.10 USB 3.2 Enabling

### 10.1.10.1 USB 3.2 Port 1 and 2:

USB 3.2 Port Configuration	Mode	Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
USB 3.2 Ports 1 and 2 Speed Select and Pairing	Paired	FPSBA + 5A	0	<b>0x0</b>	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_1
		FPSBA + 5A	1	<b>0x0</b>	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_2
		FPSBA + 48	0	<b>0x0</b>	USBX/USB3_1_DISABLE_STRAP_PORT1
		FPSBA + 5C	0	<b>0x0</b>	USBX/USB3_2_DISABLE_STRAP_PORT1
		FPSBA + 48	1	<b>0x0</b>	USBX/USB3_1_DISABLE_STRAP_PORT2
		FPSBA + 5C	1	<b>0x0</b>	USBX/USB3_2_DISABLE_STRAP_PORT2
		FPSBA + 4A	0	<b>0x0</b>	USBX/USB3_LANE_REVERSAL_STRAP_PORT1
		FPSBA + 4A	1	<b>0x0</b>	USBX/USB3_LANE_REVERSAL_STRAP_PORT2
	Paired Tx1/Tx2 Rx1/Rx2 Orientation	FPSBA + 5A	0	<b>0x0</b>	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_1
		FPSBA + 5A	1	<b>0x0</b>	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_2
		FPSBA + 48	0	<b>0x0</b>	USBX/USB3_1_DISABLE_STRAP_PORT1
		FPSBA + 5C	0	<b>0x0</b>	USBX/USB3_2_DISABLE_STRAP_PORT1
		FPSBA + 48	1	<b>0x0</b>	USBX/USB3_1_DISABLE_STRAP_PORT2
		FPSBA + 5C	1	<b>0x0</b>	USBX/USB3_2_DISABLE_STRAP_PORT2
		FPSBA + 4A	0	<b>0x1</b>	USBX/USB3_LANE_REVERSAL_STRAP_PORT1
		FPSBA + 4A	1	<b>0x1</b>	USBX/USB3_LANE_REVERSAL_STRAP_PORT2
	USB 3.2 Port 1 and 2 Gen 1x1	FPSBA + 5A	0	<b>0x1</b>	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_1
		FPSBA + 5A	1	<b>0x1</b>	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_2
		FPSBA + 48	0	<b>0x1</b>	USBX/USB3_1_DISABLE_STRAP_PORT1
		FPSBA + 5C	0	<b>0x1</b>	USBX/USB3_2_DISABLE_STRAP_PORT1
		FPSBA + 48	1	<b>0x1</b>	USBX/USB3_1_DISABLE_STRAP_PORT2
		FPSBA + 5C	1	<b>0x1</b>	USBX/USB3_2_DISABLE_STRAP_PORT2
		FPSBA + 4A	0	<b>0x0</b>	USBX/USB3_LANE_REVERSAL_STRAP_PORT1
		FPSBA + 4A	1	<b>0x0</b>	USBX/USB3_LANE_REVERSAL_STRAP_PORT2
	USB 3.2 Port 1 and 2 Gen 2x1	FPSBA + 5A	0	<b>0x1</b>	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_1
		FPSBA + 5A	1	<b>0x1</b>	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_2
		FPSBA + 48	0	<b>0x0</b>	USBX/USB3_1_DISABLE_STRAP_PORT1
		FPSBA + 5C	0	<b>0x1</b>	USBX/USB3_2_DISABLE_STRAP_PORT1
		FPSBA + 48	1	<b>0x0</b>	USBX/USB3_1_DISABLE_STRAP_PORT2
		FPSBA + 5C	1	<b>0x1</b>	USBX/USB3_2_DISABLE_STRAP_PORT2
		FPSBA + 4A	0	<b>0x0</b>	USBX/USB3_LANE_REVERSAL_STRAP_PORT1
		FPSBA + 4A	1	<b>0x0</b>	USBX/USB3_LANE_REVERSAL_STRAP_PORT2

USB 3.2 Port Configuration	Mode	Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
USB 3.2 Ports 1 and 2 Speed Select and Pairing (Cont)	USB 3.2 Port 1 Gen 1x1 Port 2 Gen 2x1	FPSBA + 5A	0	<b>0x1</b>	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_1
		FPSBA + 5A	1	<b>0x1</b>	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_2
		FPSBA + 48	0	<b>0x1</b>	USBX/USB3_1_DISABLE_STRAP_PORT1
		FPSBA + 5C	0	<b>0x1</b>	USBX/USB3_2_DISABLE_STRAP_PORT1
		FPSBA + 48	1	<b>0x0</b>	USBX/USB3_1_DISABLE_STRAP_PORT2
		FPSBA + 5C	1	<b>0x1</b>	USBX/USB3_2_DISABLE_STRAP_PORT2
		FPSBA + 4A	0	<b>0x0</b>	USBX/USB3_LANE_REVERSAL_STRAP_PORT1
		FPSBA + 4A	1	<b>0x0</b>	USBX/USB3_LANE_REVERSAL_STRAP_PORT2
	USB 3.2 Port 1 Gen 2x1 Port 2 Gen 1x1	FPSBA + 5A	0	<b>0x1</b>	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_1
		FPSBA + 5A	1	<b>0x1</b>	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_2
		FPSBA + 48	0	<b>0x0</b>	USBX/USB3_1_DISABLE_STRAP_PORT1
		FPSBA + 5C	0	<b>0x1</b>	USBX/USB3_2_DISABLE_STRAP_PORT1
		FPSBA + 48	1	<b>0x1</b>	USBX/USB3_1_DISABLE_STRAP_PORT2
		FPSBA + 5C	1	<b>0x1</b>	USBX/USB3_2_DISABLE_STRAP_PORT2
		FPSBA + 4A	0	<b>0x0</b>	USBX/USB3_LANE_REVERSAL_STRAP_PORT1
		FPSBA + 4A	1	<b>0x0</b>	USBX/USB3_LANE_REVERSAL_STRAP_PORT2

### 10.1.10.2 USB 3.2 Port 3 and 4:

USB 3.2 Port Configuration	Mode	Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
USB 3.2 Ports 3 and 4 Speed Select and Pairing	Paired	FPSBA + 5A	2	0x0	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_3
		FPSBA + 5A	3	0x0	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_4
		FPSBA + 48	2	0x0	USBX/USB3_1_DISABLE_STRAP_PORT3
		FPSBA + 5C	2	0x0	USBX/USB3_2_DISABLE_STRAP_PORT3
		FPSBA + 48	3	0x0	USBX/USB3_1_DISABLE_STRAP_PORT4
		FPSBA + 5C	3	0x0	USBX/USB3_2_DISABLE_STRAP_PORT4
		FPSBA + 4A	2	0x0	USBX/USB3_LANE_REVERSAL_STRAP_PORT3
		FPSBA + 4A	3	0x0	USBX/USB3_LANE_REVERSAL_STRAP_PORT4
	Paired Tx1/Tx2 Rx1/Rx2 Orientation	FPSBA + 5A	2	0x0	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_3
		FPSBA + 5A	3	0x0	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_4
		FPSBA + 48	2	0x0	USBX/USB3_1_DISABLE_STRAP_PORT3
		FPSBA + 5C	2	0x0	USBX/USB3_2_DISABLE_STRAP_PORT3
		FPSBA + 48	3	0x0	USBX/USB3_1_DISABLE_STRAP_PORT4
		FPSBA + 5C	3	0x0	USBX/USB3_2_DISABLE_STRAP_PORT4
		FPSBA + 4A	2	0x1	USBX/USB3_LANE_REVERSAL_STRAP_PORT3
		FPSBA + 4A	3	0x1	USBX/USB3_LANE_REVERSAL_STRAP_PORT4
	USB 3.2 Port 3 and 4 Gen 1x1	FPSBA + 5A	2	0x1	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_3
		FPSBA + 5A	3	0x1	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_4
		FPSBA + 48	2	0x1	USBX/USB3_1_DISABLE_STRAP_PORT3
		FPSBA + 5C	2	0x1	USBX/USB3_2_DISABLE_STRAP_PORT3
		FPSBA + 48	3	0x1	USBX/USB3_1_DISABLE_STRAP_PORT4
		FPSBA + 5C	3	0x1	USBX/USB3_2_DISABLE_STRAP_PORT4
		FPSBA + 4A	2	0x0	USBX/USB3_LANE_REVERSAL_STRAP_PORT3
		FPSBA + 4A	3	0x0	USBX/USB3_LANE_REVERSAL_STRAP_PORT4
	USB 3.2 Port 3 and 4 Gen 2x1	FPSBA + 5A	2	0x1	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_3
		FPSBA + 5A	3	0x1	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_4
		FPSBA + 48	2	0x0	USBX/USB3_1_DISABLE_STRAP_PORT3
		FPSBA + 5C	2	0x1	USBX/USB3_2_DISABLE_STRAP_PORT3
		FPSBA + 48	3	0x0	USBX/USB3_1_DISABLE_STRAP_PORT4
		FPSBA + 5C	3	0x1	USBX/USB3_2_DISABLE_STRAP_PORT4
		FPSBA + 4A	2	0x0	USBX/USB3_LANE_REVERSAL_STRAP_PORT3
		FPSBA + 4A	3	0x0	USBX/USB3_LANE_REVERSAL_STRAP_PORT4



USB 3.2 Port Configuration	Mode	Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
USB 3.2 Ports 3 and 4 Speed Select and Pairing (Cont)	USB 3.2 Port 3 Gen 1x1 Port 4 Gen 2x1	FPSBA + 5A	2	<b>0x1</b>	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_3
		FPSBA + 5A	3	<b>0x1</b>	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_4
		FPSBA + 48	2	<b>0x1</b>	USBX/USB3_1_DISABLE_STRAP_PORT3
		FPSBA + 5C	2	<b>0x1</b>	USBX/USB3_2_DISABLE_STRAP_PORT3
		FPSBA + 48	3	<b>0x0</b>	USBX/USB3_1_DISABLE_STRAP_PORT4
		FPSBA + 5C	3	<b>0x1</b>	USBX/USB3_2_DISABLE_STRAP_PORT4
		FPSBA + 4A	2	<b>0x0</b>	USBX/USB3_LANE_REVERSAL_STRAP_PORT3
		FPSBA + 4A	3	<b>0x0</b>	USBX/USB3_LANE_REVERSAL_STRAP_PORT4
	USB 3.2 Port 3 Gen 2x1 Port 4 Gen 1x1	FPSBA + 5A	2	<b>0x1</b>	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_3
		FPSBA + 5A	3	<b>0x1</b>	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_4
		FPSBA + 48	2	<b>0x0</b>	USBX/USB3_1_DISABLE_STRAP_PORT3
		FPSBA + 5C	2	<b>0x1</b>	USBX/USB3_2_DISABLE_STRAP_PORT3
		FPSBA + 48	3	<b>0x1</b>	USBX/USB3_1_DISABLE_STRAP_PORT4
		FPSBA + 5C	3	<b>0x1</b>	USBX/USB3_2_DISABLE_STRAP_PORT4
		FPSBA + 4A	2	<b>0x0</b>	USBX/USB3_LANE_REVERSAL_STRAP_PORT3
		FPSBA + 4A	3	<b>0x0</b>	USBX/USB3_LANE_REVERSAL_STRAP_PORT4

### 10.1.10.3 USB 3.2 Port 5 and 6:

USB 3.2 Port Configuration	Mode	Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
USB 3.2 Ports 5 and 6 Speed Select and Pairing	Paired	FPSBA + 5A	4	0x0	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_5
		FPSBA + 5A	5	0x0	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_6
		FPSBA + 48	4	0x0	USBX/USB3_1_DISABLE_STRAP_PORT5
		FPSBA + 5C	4	0x0	USBX/USB3_2_DISABLE_STRAP_PORT5
		FPSBA + 48	5	0x0	USBX/USB3_1_DISABLE_STRAP_PORT6
		FPSBA + 5C	5	0x0	USBX/USB3_2_DISABLE_STRAP_PORT6
		FPSBA + 4A	4	0x0	USBX/USB3_LANE_REVERSAL_STRAP_PORT5
		FPSBA + 4A	5	0x0	USBX/USB3_LANE_REVERSAL_STRAP_PORT6
	Paired Tx1/Tx2 Rx1/Rx2 Orientation	FPSBA + 5A	4	0x0	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_5
		FPSBA + 5A	5	0x0	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_6
		FPSBA + 48	4	0x0	USBX/USB3_1_DISABLE_STRAP_PORT5
		FPSBA + 5C	4	0x0	USBX/USB3_2_DISABLE_STRAP_PORT5
		FPSBA + 48	5	0x0	USBX/USB3_1_DISABLE_STRAP_PORT6
		FPSBA + 5C	5	0x0	USBX/USB3_2_DISABLE_STRAP_PORT6
		FPSBA + 4A	4	0x1	USBX/USB3_LANE_REVERSAL_STRAP_PORT5
		FPSBA + 4A	5	0x1	USBX/USB3_LANE_REVERSAL_STRAP_PORT6
	USB 3.2 Port 5 and 6 Gen 1x1	FPSBA + 5A	4	0x1	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_5
		FPSBA + 5A	5	0x1	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_6
		FPSBA + 48	4	0x1	USBX/USB3_1_DISABLE_STRAP_PORT5
		FPSBA + 5C	4	0x1	USBX/USB3_2_DISABLE_STRAP_PORT5
		FPSBA + 48	5	0x1	USBX/USB3_1_DISABLE_STRAP_PORT6
		FPSBA + 5C	5	0x1	USBX/USB3_2_DISABLE_STRAP_PORT6
		FPSBA + 4A	4	0x0	USBX/USB3_LANE_REVERSAL_STRAP_PORT5
		FPSBA + 4A	5	0x0	USBX/USB3_LANE_REVERSAL_STRAP_PORT6
	USB 3.2 Port 5 and 6 Gen 2x1	FPSBA + 5A	4	0x1	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_5
		FPSBA + 5A	5	0x1	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_6
		FPSBA + 48	4	0x0	USBX/USB3_1_DISABLE_STRAP_PORT5
		FPSBA + 5C	4	0x1	USBX/USB3_2_DISABLE_STRAP_PORT5
		FPSBA + 48	5	0x0	USBX/USB3_1_DISABLE_STRAP_PORT6
		FPSBA + 5C	5	0x1	USBX/USB3_2_DISABLE_STRAP_PORT6
		FPSBA + 4A	4	0x0	USBX/USB3_LANE_REVERSAL_STRAP_PORT5
		FPSBA + 4A	5	0x0	USBX/USB3_LANE_REVERSAL_STRAP_PORT6

USB 3.2 Port Configuration	Mode	Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
USB 3.2 Ports 5 and 6 Speed Select and Pairing (Cont)	USB 3.2 Port 5 Gen 1x1 Port 6 Gen 2x1	FPSBA + 5A	4	<b>0x1</b>	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_5
		FPSBA + 5A	5	<b>0x1</b>	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_6
		FPSBA + 48	4	<b>0x1</b>	USBX/USB3_1_DISABLE_STRAP_PORT5
		FPSBA + 5C	4	<b>0x1</b>	USBX/USB3_2_DISABLE_STRAP_PORT5
		FPSBA + 48	5	<b>0x0</b>	USBX/USB3_1_DISABLE_STRAP_PORT6
		FPSBA + 5C	5	<b>0x1</b>	USBX/USB3_2_DISABLE_STRAP_PORT6
		FPSBA + 4A	4	<b>0x0</b>	USBX/USB3_LANE_REVERSAL_STRAP_PORT5
		FPSBA + 4A	5	<b>0x0</b>	USBX/USB3_LANE_REVERSAL_STRAP_PORT6
	USB 3.2 Port 5 Gen 2x1 Port 6 Gen 1x1	FPSBA + 5A	4	<b>0x1</b>	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_5
		FPSBA + 5A	5	<b>0x1</b>	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_6
		FPSBA + 48	4	<b>0x0</b>	USBX/USB3_1_DISABLE_STRAP_PORT5
		FPSBA + 5C	4	<b>0x1</b>	USBX/USB3_2_DISABLE_STRAP_PORT5
		FPSBA + 48	5	<b>0x1</b>	USBX/USB3_1_DISABLE_STRAP_PORT6
		FPSBA + 5C	5	<b>0x1</b>	USBX/USB3_2_DISABLE_STRAP_PORT6
		FPSBA + 4A	4	<b>0x0</b>	USBX/USB3_LANE_REVERSAL_STRAP_PORT5
		FPSBA + 4A	5	<b>0x0</b>	USBX/USB3_LANE_REVERSAL_STRAP_PORT6

#### 10.1.10.4 USB 3.2 Port 7 and 8:

USB 3.2 Port Configuration	Mode	Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
USB 3.2 Ports 7 and 8 Speed Select and Pairing	Paired	FPSBA + 5A	6	0x0	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_7
		FPSBA + 5A	7	0x0	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_8
		FPSBA + 48	6	0x0	USBX/USB3_1_DISABLE_STRAP_PORT7
		FPSBA + 5C	6	0x0	USBX/USB3_2_DISABLE_STRAP_PORT7
		FPSBA + 48	7	0x0	USBX/USB3_1_DISABLE_STRAP_PORT8
		FPSBA + 5C	7	0x0	USBX/USB3_2_DISABLE_STRAP_PORT8
		FPSBA + 4A	6	0x0	USBX/USB3_LANE_REVERSAL_STRAP_PORT7
		FPSBA + 4A	7	0x0	USBX/USB3_LANE_REVERSAL_STRAP_PORT8
	Paired Tx1/Tx2 Rx1/Rx2 Orientation	FPSBA + 5A	6	0x0	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_7
		FPSBA + 5A	7	0x0	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_8
		FPSBA + 48	6	0x0	USBX/USB3_1_DISABLE_STRAP_PORT7
		FPSBA + 5C	6	0x0	USBX/USB3_2_DISABLE_STRAP_PORT7
		FPSBA + 48	7	0x0	USBX/USB3_1_DISABLE_STRAP_PORT8
		FPSBA + 5C	7	0x0	USBX/USB3_2_DISABLE_STRAP_PORT8
		FPSBA + 4A	6	0x1	USBX/USB3_LANE_REVERSAL_STRAP_PORT7
		FPSBA + 4A	7	0x1	USBX/USB3_LANE_REVERSAL_STRAP_PORT8
	USB 3.2 Port 7 and 8 Gen 1x1	FPSBA + 5A	6	0x1	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_7
		FPSBA + 5A	7	0x1	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_8
		FPSBA + 48	6	0x1	USBX/USB3_1_DISABLE_STRAP_PORT7
		FPSBA + 5C	6	0x1	USBX/USB3_2_DISABLE_STRAP_PORT7
		FPSBA + 48	7	0x1	USBX/USB3_1_DISABLE_STRAP_PORT8
		FPSBA + 5C	7	0x1	USBX/USB3_2_DISABLE_STRAP_PORT8
		FPSBA + 4A	6	0x0	USBX/USB3_LANE_REVERSAL_STRAP_PORT7
		FPSBA + 4A	7	0x0	USBX/USB3_LANE_REVERSAL_STRAP_PORT8
	USB 3.2 Port 7 and 8 Gen 2x1	FPSBA + 5A	6	0x1	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_7
		FPSBA + 5A	7	0x1	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_8
		FPSBA + 48	6	0x0	USBX/USB3_1_DISABLE_STRAP_PORT7
		FPSBA + 5C	6	0x1	USBX/USB3_2_DISABLE_STRAP_PORT7
		FPSBA + 48	7	0x0	USBX/USB3_1_DISABLE_STRAP_PORT8
		FPSBA + 5C	7	0x1	USBX/USB3_2_DISABLE_STRAP_PORT8
		FPSBA + 4A	6	0x0	USBX/USB3_LANE_REVERSAL_STRAP_PORT7
		FPSBA + 4A	7	0x0	USBX/USB3_LANE_REVERSAL_STRAP_PORT8

USB 3.2 Port Configuration	Mode	Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
USB 3.2 Ports 7 and 8 Speed Select and Pairing (Cont)	USB 3.2 Port 7 Gen 1x1 Port 8 Gen 2x1	FPSBA + 5A	6	<b>0x1</b>	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_7
		FPSBA + 5A	7	<b>0x1</b>	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_8
		FPSBA + 48	6	<b>0x1</b>	USBX/USB3_1_DISABLE_STRAP_PORT7
		FPSBA + 5C	6	<b>0x1</b>	USBX/USB3_2_DISABLE_STRAP_PORT7
		FPSBA + 48	7	<b>0x0</b>	USBX/USB3_1_DISABLE_STRAP_PORT8
		FPSBA + 5C	7	<b>0x1</b>	USBX/USB3_2_DISABLE_STRAP_PORT8
		FPSBA + 4A	6	<b>0x0</b>	USBX/USB3_LANE_REVERSAL_STRAP_PORT7
		FPSBA + 4A	7	<b>0x0</b>	USBX/USB3_LANE_REVERSAL_STRAP_PORT8
	USB 3.2 Port 7 Gen 2x1 Port 8 Gen 1x1	FPSBA + 5A	6	<b>0x1</b>	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_7
		FPSBA + 5A	7	<b>0x1</b>	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_8
		FPSBA + 48	6	<b>0x0</b>	USBX/USB3_1_DISABLE_STRAP_PORT7
		FPSBA + 5C	6	<b>0x1</b>	USBX/USB3_2_DISABLE_STRAP_PORT7
		FPSBA + 48	7	<b>0x1</b>	USBX/USB3_1_DISABLE_STRAP_PORT8
		FPSBA + 5C	7	<b>0x1</b>	USBX/USB3_2_DISABLE_STRAP_PORT8
		FPSBA + 4A	6	<b>0x0</b>	USBX/USB3_LANE_REVERSAL_STRAP_PORT7
		FPSBA + 4A	7	<b>0x0</b>	USBX/USB3_LANE_REVERSAL_STRAP_PORT8

### 10.1.10.5 USB 3.2 Port 9 and 10:

USB 3.2 Port Configuration	Mode	Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
USB 3.2 Ports 9 and 10 Speed Select and Pairing	Paired	FPSBA + 5B	0	<b>0x0</b>	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_9
		FPSBA + 5B	1	<b>0x0</b>	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_10
		FPSBA + 49	0	<b>0x0</b>	USBX/USB3_1_DISABLE_STRAP_PORT9
		FPSBA + 5D	0	<b>0x0</b>	USBX/USB3_2_DISABLE_STRAP_PORT9
		FPSBA + 49	1	<b>0x0</b>	USBX/USB3_1_DISABLE_STRAP_PORT10
		FPSBA + 5D	1	<b>0x0</b>	USBX/USB3_2_DISABLE_STRAP_PORT10
		FPSBA + 4B	0	<b>0x0</b>	USBX/USB3_LANE_REVERSAL_STRAP_PORT9
		FPSBA + 4B	1	<b>0x0</b>	USBX/USB3_LANE_REVERSAL_STRAP_PORT10
	Paired Tx1/Tx2 Rx1/Rx2 Orientation	FPSBA + 5B	0	<b>0x0</b>	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_9
		FPSBA + 5B	1	<b>0x0</b>	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_10
		FPSBA + 49	0	<b>0x0</b>	USBX/USB3_1_DISABLE_STRAP_PORT9
		FPSBA + 5D	0	<b>0x0</b>	USBX/USB3_2_DISABLE_STRAP_PORT9
		FPSBA + 49	1	<b>0x0</b>	USBX/USB3_1_DISABLE_STRAP_PORT10
		FPSBA + 5D	1	<b>0x0</b>	USBX/USB3_2_DISABLE_STRAP_PORT10
		FPSBA + 4B	0	<b>0x1</b>	USBX/USB3_LANE_REVERSAL_STRAP_PORT9
		FPSBA + 4B	1	<b>0x1</b>	USBX/USB3_LANE_REVERSAL_STRAP_PORT10
	USB 3.2 Port 9 and 10 Gen 1x1	FPSBA + 5B	0	<b>0x1</b>	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_9
		FPSBA + 5B	1	<b>0x1</b>	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_10
		FPSBA + 49	0	<b>0x1</b>	USBX/USB3_1_DISABLE_STRAP_PORT9
		FPSBA + 5D	0	<b>0x1</b>	USBX/USB3_2_DISABLE_STRAP_PORT9
		FPSBA + 49	1	<b>0x1</b>	USBX/USB3_1_DISABLE_STRAP_PORT10
		FPSBA + 5D	1	<b>0x1</b>	USBX/USB3_2_DISABLE_STRAP_PORT10
		FPSBA + 4B	0	<b>0x0</b>	USBX/USB3_LANE_REVERSAL_STRAP_PORT9
		FPSBA + 4B	1	<b>0x0</b>	USBX/USB3_LANE_REVERSAL_STRAP_PORT10
	USB 3.2 Port 9 and 10 Gen 2x1	FPSBA + 5B	0	<b>0x1</b>	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_9
		FPSBA + 5B	1	<b>0x1</b>	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_10
		FPSBA + 49	0	<b>0x0</b>	USBX/USB3_1_DISABLE_STRAP_PORT9
		FPSBA + 5D	0	<b>0x1</b>	USBX/USB3_2_DISABLE_STRAP_PORT9
		FPSBA + 49	1	<b>0x0</b>	USBX/USB3_1_DISABLE_STRAP_PORT10
		FPSBA + 5D	1	<b>0x1</b>	USBX/USB3_2_DISABLE_STRAP_PORT10
		FPSBA + 4B	0	<b>0x0</b>	USBX/USB3_LANE_REVERSAL_STRAP_PORT9
		FPSBA + 4B	1	<b>0x0</b>	USBX/USB3_LANE_REVERSAL_STRAP_PORT10

USB 3.2 Port Configuration	Mode	Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
USB 3.2 Ports 9 and 10 Speed Select and Pairing (Cont)	USB 3.2 Port 9 Gen 1x1 Port 10 Gen 2x1	FPSBA + 5B	0	<b>0x1</b>	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_9
		FPSBA + 5B	1	<b>0x1</b>	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_10
		FPSBA + 49	0	<b>0x1</b>	USBX/USB3_1_DISABLE_STRAP_PORT9
		FPSBA + 5D	0	<b>0x1</b>	USBX/USB3_2_DISABLE_STRAP_PORT9
		FPSBA + 49	1	<b>0x0</b>	USBX/USB3_1_DISABLE_STRAP_PORT10
		FPSBA + 5D	1	<b>0x1</b>	USBX/USB3_2_DISABLE_STRAP_PORT10
		FPSBA + 4B	0	<b>0x0</b>	USBX/USB3_LANE_REVERSAL_STRAP_PORT9
		FPSBA + 4B	1	<b>0x0</b>	USBX/USB3_LANE_REVERSAL_STRAP_PORT10
	USB 3.2 Port 9 Gen 2x1 Port 10 Gen 1x1	FPSBA + 5B	0	<b>0x1</b>	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_9
		FPSBA + 5B	1	<b>0x1</b>	USBX/LANE_PAIRING_DISABLE_STRAP_PORT_10
		FPSBA + 49	0	<b>0x0</b>	USBX/USB3_1_DISABLE_STRAP_PORT9
		FPSBA + 5D	0	<b>0x1</b>	USBX/USB3_2_DISABLE_STRAP_PORT9
		FPSBA + 49	1	<b>0x1</b>	USBX/USB3_1_DISABLE_STRAP_PORT10
		FPSBA + 5D	1	<b>0x1</b>	USBX/USB3_2_DISABLE_STRAP_PORT10
		FPSBA + 4B	0	<b>0x0</b>	USBX/USB3_LANE_REVERSAL_STRAP_PORT9
		FPSBA + 4B	1	<b>0x0</b>	USBX/USB3_LANE_REVERSAL_STRAP_PORT10

# 11 RPMC Configuration

Replay Protection Monotonic Counter (RPMC) is a capability providing Anti-Replay Protection using Monotonic Counters inside SPI Flash.

RPMC protection relies on:

- Special RPMC HW and logic inside the SPI Flash
- Intel® CSME FW support that utilizes RPMC capabilities within Flash

RPMC support in SPI Flash and Intel® CSME FW ensures the integrity of the data and mitigates rollback attacks.

Replay protection based RPMC is immune to power loss in case it's reset or corrupted and therefore more robust than using PRTC based monotonic counters.

OEMs can choose not to utilize RPMC on their systems. Enabling/disabling RPMC capabilities are done by setting RPMC parameters in Intel® mFIT:

## ▼ RPMC Configuration

Parameter	Value	Help Text
RPMC Supported	No	This setting determines if RPMC is enabled. Note: The SPI parts being used need to support RPMC in order to use this feat...
RPMC Rebinding Enabled	No	This setting determines if Rebinding of RPMC enabled SPI parts is enabled.

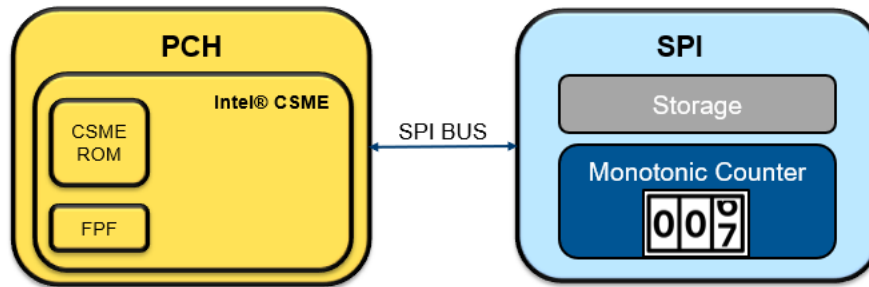
- "RPMC Supported"
  - YES
    - RPMC will be enabled on platforms with RPMC SPI
    - During Intel® End of Manufacturing PCH will be bound with RPMC SPI
  - NO
    - RPMC will be disabled, no binding at Intel® EOM
- "RPMC Rebinding Enabled"
  - YES:
    - When SPI is replaced, re-binding between the new RPMC SPI and PCH will happen automatically on first boot
  - NO:
    - When SPI is replaced, no re-binding and no RPMC support on a new SPI

**Please note RPMC default settings in Intel® mFIT, there is no RPMC support w/o enabling those settings.**

**At Intel® EOM those settings are burned into FPF and cannot be changed after.**



## 11.1 System Components - High-Level Architecture Block Diagram



**Acronyms:**

MC = Monotonic Counter  
BC = Binding Counter  
SK = Session Key  
BK = Binding Key

**Main R&R:**

CSME ROM: Derive BK, SK  
FPF: Hold binding counter  
SPI MC: hold monotonic counter in SPI HW  
CSME FW: Manage counters

## 11.2 Monotonic counters

Monotonic counters are counters on the SPI Flash maintained by Intel® CSME FW.

SPI Flash has a set of four 32-bit monotonic counters, where Intel® CSME FW uses two of these counters

Intel® CSME FW ensures FW write operations will not exceed SPI RPMC monotonic counter increment rate specified by RPMC HW during platform lifetime supported by Intel

Reading and incrementing the counters in the Flash is done using authenticated commands with a key known to both: SPI Flash and Intel® CSME FW

## 11.3 Binding at End of Manufacturing (EOM)

RPMC Binding pairs between SPI Flash and PCH by provisioning the Binding key produced by PCH into SPI Flash. This pairing is done as part of the EOM flow which usually takes place at the manufacturing line.

In cases where EOM is set in Intel® mFIT to be performed on first boot, the binding will happen at first boot, after a complete configuration was defined using Intel® mFIT, and access permission were set in the image.

In cases where EOM is not set in Intel® FIT configuration, the binding is performed using Intel® FPT tool systems when 'Intel® FPT -closemnf' is executed.

On platforms outside the manufacturing line (non PRQ parts), the binding happens when 'Intel® FPT -closemnf' is executed only if 'HW BINDING enabled' flag is set to 'Enabled' in Intel® mFIT.

Prior to the binding operation, the Intel® CSME data is Anti Replay protected using a default key.

### 11.3.1 RPMC binding on Dual SPI configuration

When only one of the two SPIs supports RPMC, it will be selected by the SPI Controller.

If both SPIs support RPMC, then the lower addressed chip will be selected.

When the selected SPI is being replaced, a rebinding flow is required.

## 11.4 Refurbish flows impact

### 11.4.1 PCH replacement

Before EOM:

PCH replacement without SPI replacement/re-flashing is supported (up to 5 replacements). RPMC is functional with a default key.

Post EOM:

PCH replacement requires SPI replacement as well as running the EOM.

### 11.4.2 SPI replacement

Before Binding (Pre-EOM):

SPI part can be replaced infinite number of times (default key is used).

After Binding (Post-EOM):

In cases where SPI Flash was removed, it cannot be used with another PCH.

If RPMC rebinding is enabled - New SPI Flash will be automatically paired with PCH.

If RPMC rebinding is disabled - RPMC will not be used. Applications whose data requires RPMC protection will not be fully functional.

### 11.4.3 SPI re-flash

Binding key not re-flashed. Monotonic counter will not be reset, data will be lost.

## 11.5 RPMC re-binding

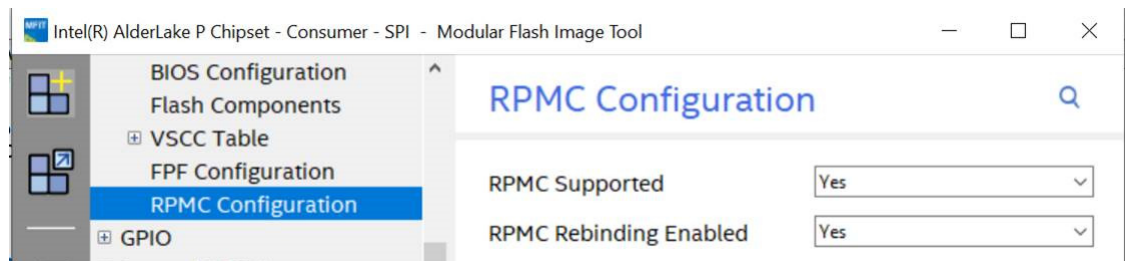
Rebinding is essential to all platforms that support refurbishing in the field.

After the initial bind has been performed, if the SPI Flash part is replaced and rebinding is enabled, the Intel® CSME FW will bind the new RPMC Flash part automatically as part of the 1<sup>st</sup> boot flow. Intel® CSME FW detects that Flash is using the default key. It then triggers rebinding flow that produces a new Binding key and sends it to the Flash

The PCH can be paired with up to 16 RPMC enabled SPI Flash parts during the platform life cycle.

Rebinding is assumed to be done in a safe & secure environment (e.g., ODM/OEM manufacturing site, or OEM service center).

## 11.6 Tools - Intel® mFIT



“RPMC Supported”:

- YES
  - RPMC will be enabled on platforms with RPMC SPI
  - During Intel® End of Manufacturing PCH will be bound with RPMC
- NO
  - RPMC will be disabled, no binding at Intel® EOM

“RPMC Rebinding Enabled”:

- YES:
  - When SPI is replaced, re-binding between the new SPI and PCH will happen automatically on first boot
- NO:
  - When SPI is replaced, no re-binding and no RPMC support on a new SPI

Please note:

- RPMC default settings in Intel® mFIT are enabled starting ADL.
- There is no RPMC support with those settings disabled.
- At Intel® EOM those settings are burned into FPF and cannot be changed after.

# 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® CSME FW kit. Please ensure that you download the appropriate kit for the target platform.

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

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

**A:** Raptor Lake PCH family based platforms, you can follow the appropriate instructions in the FW Bring-up Guide which is located in the root directory of the appropriate Intel® CSME 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 *Raptor Lake PCH Family External Design Specification (EDS)*, Intel® Converged Security and Management Engine (Intel® CSME) 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® CSME Firmware? How can I add support for a new flash to Intel® CSME Firmware?**

**A:** As long as the SPI flash devices meets the requirements defined in the *Raptor Lake PCH 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® CSME 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 Raptor 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® CSME Firmware performs periodic writes to SPI flash when it is active. Due to this the Intel® CSME region may not match the source file. There are also other system activities beside the Intel® CSME 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:** Raptor Lake PCH 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) 2007-2019, Intel Corporation. All rights reserved.
Platform: Intel(R) Qxx Express Chipset
Reading HSFSTS register... Flash Descriptor: Invalid

--- Flash Devices Found ---

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

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

Error: Timeout 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 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 *Raptor Lake PCH-LP Family External Design Specification (EDS)* for the location for the HSFS. Try reflashing the SPI device with a 3<sup>rd</sup> 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.

**§ §**