



# **Tiger Lake Platform UFS Programming Guide**

**User Guide**

**March 2019**

**Revision 0.7**

**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).

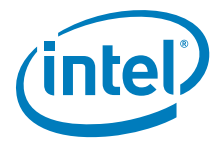
The original equipment manufacturer must provide TPM functionality, which requires a TPM-supported BIOS. TPM functionality must be initialized and may not be available in all countries.

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.

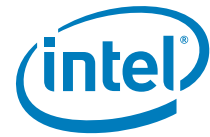
Copyright © 2018, Intel Corporation. All rights reserved.





# Contents

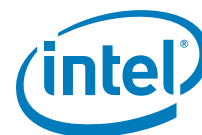
<b>1</b>	<b>Introduction</b>	9
1.1	Overview	9
1.2	Terminology	10
1.3	Reference Documents	10
<b>2</b>	<b>UFS Flash Architecture</b>	11
2.1	Introduction	11
2.2	Descriptor Mode	11
2.3	Boot Flow when booting from UFS NVM	11
2.4	Flash (NVM) Partitions and Regions	12
2.4.1	Flash Region Layout	13
2.4.2	Platform Settings	15
2.5	PCH UFS Flash Compatibility Requirements	16
2.5.1	Lake Field Firmware Requirements	16
<b>3</b>	<b>Descriptor Overview</b>	17
3.1	Flash Descriptor Content	19
3.1.1	Descriptor Signature and Map	20
3.1.1.1	FLVALSIG - Flash Valid Signature (Flash Descriptor Records)	20
3.1.1.2	FLMAP0 - Flash Map 0 Register (Flash Descriptor Records)	20
3.1.1.3	FLMAP1 - Flash Map 1 Register (Flash Descriptor Records)	22
3.1.1.4	FLMAP2—Flash Map 2 Register (Flash Descriptor Records)	22
3.1.1.5	FLMAP3—Flash Map 3 Register (Flash Descriptor Records)	22
3.1.2	Flash Descriptor Component Section	23
3.1.2.1	FLCOMP—Flash Components Register (Flash Descriptor Records)	23
3.1.2.2	FLILL—Flash Invalid Instructions Register (Flash Descriptor Records)	26
3.1.2.3	FLILL1—Flash Invalid Instructions Register (Flash Descriptor Records)	26
3.1.3	Flash Descriptor Region Section	28
3.1.3.1	FLREG0—Flash Region 0 (Flash Descriptor) Register (Flash Descriptor Records)	28
3.1.3.2	FLREG1—Flash Region 1 (BIOS) Register (Flash Descriptor Records)	28
3.1.3.3	FLREG2—Flash Region 2 (IFWI / Intel® CSME ROM Bypass) Register (Flash Descriptor Records)	29
3.1.4	Flash Descriptor Master Section	30
3.1.4.1	FLMSTR1—Flash Master 1 (Host CPU/ BIOS)	30
3.1.4.2	FLMSTR2—Flash Master 2 (Intel® ME)	30
3.1.5	PCH / CPU Softstraps	31
3.1.6	Descriptor Upper Map Section	31
3.1.6.1	FLUMAP1—Flash Upper Map 1 (Flash Descriptor Records)	31
3.1.6.2	IFWI / Intel® CSME ROM Bypass Size	31
3.1.6.3	MIP - Descriptor Table	31
3.1.7	Intel® CSME Vendor Specific Component Capabilities Table	32



3.1.7.1	JID0—JEDEC-ID 0 Register (Flash Descriptor Records) .....	32
3.1.7.2	VSCC0—Vendor Specific Component Capabilities 0 (Flash Descriptor Records) .....	33
3.1.7.3	JIDn—JEDEC-ID Register n (Flash Descriptor Records) .....	33
3.1.7.4	VSCCn—Vendor Specific Component Capabilities n (Flash Descriptor Records) .....	33
3.2	OEM Section .....	34
3.3	Region Access Control .....	34
<b>4</b>	<b>UFS PCH / PMC / CPU and Intel® CSME Configuration Section .....</b>	<b>35</b>
4.1	PCH Record 0 (UFS Flash Records) .....	35
4.2	PCH Record 1 (UFS Flash Records) .....	35
4.3	PCH Record 2 (UFS Flash Records) .....	36
4.4	PCH Record 3 (UFS Flash Records) .....	36
4.5	PCH Record 4 (UFS Flash Records) .....	36
4.6	PCH Record 5 (UFS Flash Records) .....	37
4.7	PCH Record 6 (UFS Flash Records) .....	37
4.8	PCH Record 7 (UFS Flash Records) .....	38
4.9	PCH Record 8 (UFS Flash Records) .....	38
4.10	PCH Record 9 (UFS Flash Records) .....	38
4.11	PCH Record 10 (UFS Flash Records) .....	39
4.12	PCH Record 11 (UFS Flash Records) .....	39
4.13	PCH Record 12 (UFS Flash Records) .....	39
4.14	PCH Record 13 (UFS Flash Records) .....	39
4.15	PCH Record 14 (UFS Flash Records) .....	40
4.16	PCH Record 15 (UFS Flash Records) .....	40
4.17	PCH Record 16 (UFS Flash Records) .....	40
4.18	PCH Record 17 (UFS Flash Records) .....	41
4.19	PCH Record 18 (UFS Flash Records) .....	41
4.20	PCH Record 19 (UFS Flash Records) .....	41
4.21	PCH Record 20 (UFS Flash Records) .....	41
4.22	PCH Record 21 (UFS Flash Records) .....	41
4.23	PCH Record 22 (UFS Flash Records) .....	42
4.24	PCH Record 23 (UFS Flash Records) .....	42
4.25	PCH Record 24 (UFS Flash Records) .....	42
4.26	PCH Record 25 (UFS Flash Records) .....	42
4.27	PCH Record 26 (UFS Flash Records) .....	42
4.28	PCH Record 27 (UFS Flash Records) .....	43
4.29	PCH Record 28 (UFS Flash Records) .....	43
4.30	PCH Record 29 (UFS Flash Records) .....	43
4.31	PCH Record 30 (UFS Flash Records) .....	43
4.32	PCH Record 31 (UFS Flash Records) .....	43
4.33	PCH Record 32 (UFS Flash Records) .....	44
4.34	PCH Record 33 (UFS Flash Records) .....	44
4.35	PCH Record 34 (UFS Flash Records) .....	44
4.36	PCH Record 35 (UFS Flash Records) .....	45
4.37	PCH Record 36 (UFS Flash Records) .....	45
4.38	PCH Record 37 (UFS Flash Records) .....	45
4.39	PCH Record 38 (UFS Flash Records) .....	45
4.40	PCH Record 39 (UFS Flash Records) .....	45
4.41	PCH Record 40 (UFS Flash Records) .....	46
4.42	PCH Record 41 (UFS Flash Records) .....	46
4.43	PCH Record 42 (UFS Flash Records) .....	46
4.44	PCH Record 43 (UFS Flash Records) .....	47



4.45	PCH Record 44 (UFS Flash Records)	47
4.46	PCH Record 45 (UFS Flash Records)	47
4.47	PCH Record 46 (UFS Flash Records)	47
4.48	PCH Record 47 (UFS Flash Records)	47
4.49	PCH Record 48 (UFS Flash Records)	48
4.50	PCH Record 49 (UFS Flash Records)	48
4.51	PCH Record 50 (UFS Flash Records)	48
4.52	PCH Record 51 (UFS Flash Records)	48
4.53	PCH Record 52 (UFS Flash Records)	48
4.54	PCH Record 53 (UFS Flash Records)	49
4.55	PCH Record 54 (UFS Flash Records)	49
4.56	PCH Record 55 (UFS Flash Records)	49
4.57	PCH Record 56 (UFS Flash Records)	49
4.58	PCH Record 57 (UFS Flash Records)	49
4.59	PCH Record 58 (UFS Flash Records)	50
4.60	PCH Record 59 (UFS Flash Records)	50
4.61	PCH Record 60 (UFS Flash Records)	51
4.62	PCH Record 61 (UFS Flash Records)	51
4.63	PCH Record 62 (UFS Flash Records)	53
4.64	PCH Record 63 (UFS Flash Records)	53
4.65	PCH Record 64 (UFS Flash Records)	53
4.66	PCH Record 65 (UFS Flash Records)	54
4.67	PCH Record 66 (UFS Flash Records)	54
4.68	PCH Record 67 (UFS Flash Records)	54
4.69	PCH Record 68 (UFS Flash Records)	54
4.70	PCH Record 70 (UFS Flash Records)	54
4.71	PCH Record 71 (UFS Flash Records)	55
4.72	PCH Record 72 (UFS Flash Records)	55
4.73	PCH Record 73 (UFS Flash Records)	55
4.74	MIP Table Record 0 (UFS Flash Records)	56
4.75	MIP Table Record 1 (UFS Flash Records)	56
4.76	MIP Table Record 2 (UFS Flash Records)	56
4.77	MIP Table Record 3 (UFS Flash Records)	56
4.78	MIP Table Record 4 (UFS Flash Records)	57
4.79	MIP Table Record 5 (UFS Flash Records)	57
4.80	MIP Table Record 6 (UFS Flash Records)	57
4.81	MIP Table Record 7 (UFS Flash Records)	57
4.82	MIP Table Record 8 (UFS Flash Records)	58
4.83	MIP Table Record 9 (UFS Flash Records)	58
4.84	PMC Record 0 (UFS Flash Records)	59
4.85	PMC Record 1 (UFS Flash Records)	60
4.86	PMC Record 2 (UFS Flash Records)	60
4.87	PMC Record 3 (UFS Flash Records)	60
4.88	PMC Record 4 (UFS Flash Records)	61
4.89	PMC Record 5 (UFS Flash Records)	61
4.90	PMC Record 6 (UFS Flash Records)	62
4.91	PMC Record 7 (UFS Flash Records)	62
4.92	PMC Record 8 (UFS Flash Records)	62
4.93	CPU Record 0 (UFS Flash Records)	63
4.94	CPU Record 1 (UFS Flash Records)	64
4.95	CPU Record 2 (UFS Flash Records)	65
4.96	CPU Record 3 (UFS Flash Records)	66
4.97	Intel® CSME Record 0 (UFS Flash Records)	67
4.98	Intel® CSME Record 1 (UFS Flash Records)	69



## Figures

2-1 Booting from UFS high level flow .....	12
2-2 UFS Boot Partition Layout.....	15
3-1 Flash Descriptor (Tiger Lake PCH) .....	18

## Tables

1-1 Terminology .....	10
1-2 Reference Documents .....	10
2-1 UFS Partitions.....	12
2-2 UFS Logical Partitions .....	13
2-3 BPDT Header .....	14

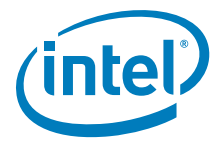


## ***Revision History***

<b>Revision Number</b>	<b>Description</b>	<b>Revision Date</b>
0.5	<ul style="list-style-type: none"><li>Initial Release</li></ul>	February 2019
0.7	<ul style="list-style-type: none"><li>Align revision number</li></ul>	March 2019

§ §







# 1 Introduction

## 1.1 Overview

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

[Chapter 2, "UFS Flash Architecture"](#)

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

[Chapter 3, "Descriptor Overview"](#)

- Overview of the descriptor and Descriptor record definition

[Chapter 4, "UFS PCH / PMC / CPU and Intel® CSME Configuration Section"](#)



## 1.2 Terminology

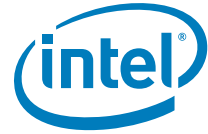
Table 1-1. Terminology

Term	Description
BIOS	Basic Input-Output System
BP	Boot partition
BPDT	Boot partition Descriptor Table
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
HDCP	High-bandwidth Digital Content Protection
IFWI	Integrated Firmware Image Layout
Tiger Lake PCH	Tiger Lake Platform Integrated I/O
Intel® Converged Security Engine Firmware (Intel® CSME FW)	Intel firmware that adds Castle Peak, Sentry Peak, etc.
Intel PCH	Intel® Platform Controller Hub
Intel PCHn family	All PCHn derivatives including PCHn (desktop) and PCHnM (mobile)
MCP	Multi-Chip package
MDTBA	MIP Descriptor Table Base Address
MIP	Master Image Profile
PCH	Platform Controller Hub
PCH-LP	Platform Controller Hub – Low Power
PMC	Power Management Controller (PCH)
RPMB	Replay Protect Memory Block
SPI	Serial Peripheral Interface – refers to serial flash memory in this document
UFS	A Type of non-serial flash block media devices
UVSCC	Upper Vendor Specific Component Capabilities
VSCC	Vendor Specific Component Capabilities

## 1.3 Reference Documents

Table 1-2. Reference Documents

Document	Document # / Location
<i>Tiger Lake PCH- LP 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.
<i>FW Bring Up Guide</i>	Root directory of latest Intel® CSME FWkit from VIP. The Kit MUST match the platform you intend to use the flash tools for.



## 2 UFS Flash Architecture

---

### 2.1 Introduction

Unlike SPI Flash which is used only to store boot FW (IFWI), UFS NVM is the main storage on the platform. It stores OS, user files and Boot FW (IFWI). Hence UFS NVM is setup differently from SPI. To keep this guide in parity with the SPI programming guide, most of the SPI Flash specific section titles will be maintained and will be marked as “Not Applicable” for UFS NVM.

If required UFS NVM can be used for OS storage only and boot the platform from SPI Flash. If booting the platform from SPI Flash, follow SPI programming guide.

### 2.2 Descriptor Mode

UFS NVM do not have descriptor mode and descriptor region. Same data structure as SPI descriptor is maintained to store soft straps and configuration on UFS NVM. On UFS this data is stored as a data structure. SPI descriptor structure is maintained for ease of OEM design.

### 2.3 Boot Flow when booting from UFS NVM

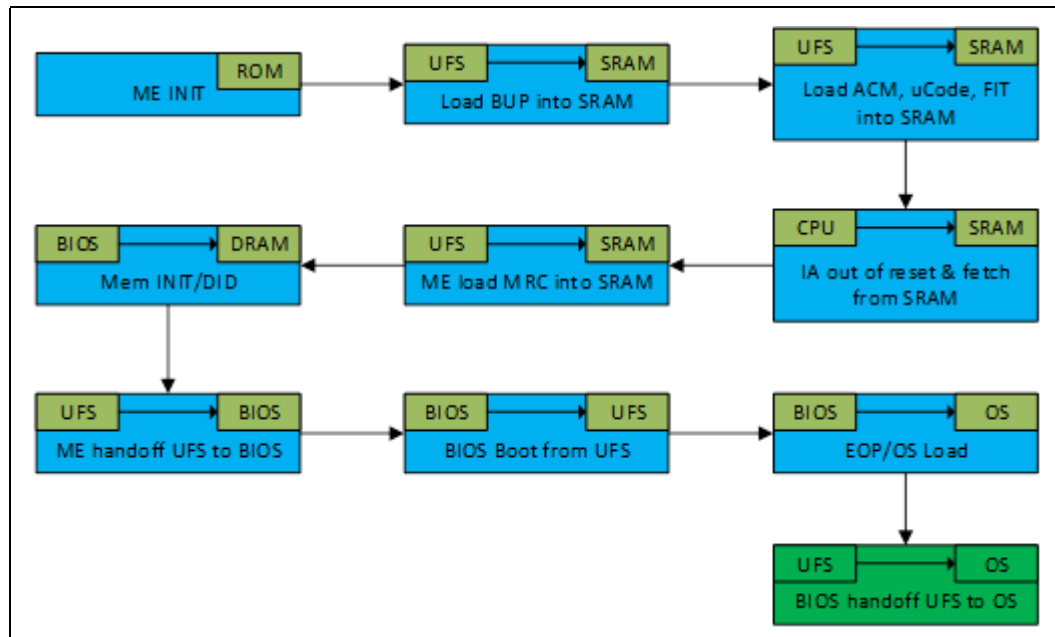
This chapter provides overview of general platform boot from UFS. Intel® Boot Guard 2.1 flow is not described here. Refer to Boot Guard 2.1 training foils for detailed boot guard flows.

When booting from SPI Flash, CPU can come out of reset and directly read the code from the SPI flash. But CPU on Lake Field platform cannot directly boot out of UFS flash. It requires assistance from Intel® CSME until BIOS comes up and load UFS driver. To assist CPU to boot, Intel® CSME will copy IBB, uCode and MRC data from UFS to internal SRAM of Intel® CSME. Intel® CSME then shares part of the SRAM to CPU. When CPU will come out of reset, it will boot from the Intel® CSME SRAM.

Since UFS controller is single headed, only one master can access the UFS NVM. On TGL platform Intel® CSME, OS and BIOS require UFS NVM access during boot and during run time. Intel® CSME have access to UFS NVM when platform comes out of reset. Once DRAM is initialized, UFS NVM access is transferred to BIOS. Intel® CSME access to UFS flash is then handled via a BIOS storage proxy driver. At end of boot, UFS NVM access is handed off to OS. Intel provides storage proxy driver in OS to allow CSME access to UFS NVM.

Below picture show high level flow of booting from UFS NVM.

**Figure 2-1. Booting from UFS high level flow**



## 2.4 Flash (NVM) Partitions and Regions

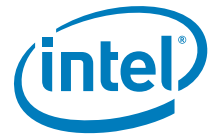
Unlike SPI, UFS NVM has physical partitions called LUNs. IFWI resides within the Boot partition and it is logically divided into regions, similar to SPI.

Coming out of the UFS vendor, only the RPMB partition is pre-defined and enabled. OEM can create partitions and configure them to the desired size as long as the Configuration Descriptor Lock UFS attribute is not set. Once this attribute is set, partitioning will no longer be allowed. UFS partitioning is supported via DnX capabilities and can be executed using the Intel® PFT SW Tool running on the host machine. Please refer to PFT\_DnX\_UserGuide for more detail.

Please see partitioning recommendation in the table below:

**Table 2-1. UFS Partitions**

Partition	Size	Use	Comments
<b>LUN0</b>	-	OS user space	Size depends upon the size of the UFS Device
<b>LUN1</b>	32MB	Boot0 (IFWI)	Raw partition - Vendor created
<b>LUN2</b>	32MB	Boot1 (Not used)	Raw partition - Vendor created
<b>LUN3</b>	8MB	Platform factory data partition	Vendor created; Post factory - Read Only partition
<b>LUN4</b>	-	Not Used	OEM Choice
<b>LUN5</b>	-	Not Used	OEM Choice
<b>LUN6</b>	4MB	Temporary CSME data store to delay the RPMB key enrollment to end of manufacturing"	Raw partition - Vendor created



Partition	Size	Use	Comments
<b>RPMB</b>	4MB	Replay protected partition: Provisioned by Intel® CSME and used for CSME file system, PTT storage and UEFI variable storage	Vendor created - Provisioned with platform specific key by CSME at EOM

### RPMB partition

Prior to EOM, all the data is written to the Temporary Data Partition (LUN6) partition. This has security implications as the host has SW access to both Intel® CSME code and data. This is unlike SPI, which prevents host SW from accessing Intel® CSME code and data, assuming the flash descriptor is programmed correctly.

At the EOM:

- Intel® CSME will derive a key unique to the chipset and program this key into UFS.
- After provisioning of the key is done, Intel® CSME will initiate data migration from Temp Data Partition (LUN6) into RPMB partition. Once migration is done, Intel® CSME will clear LUN6 partition.

After EOM, the PCH is bound with the UFS and all the data written to the RPMB partition or read from it will be signed with this key.

The Intel® CSME is responsible for maintaining the RPMB key and thus the UEFI secure variable cryptographic access to the RPMB partition.

### Logical partitions inside physical Boot0 partition (LUN1)

**Table 2-2. UFS Logical Partitions**

Region	Contents
<b>RPMB/LBP5</b>	Block settings Descriptor
<b>LBP4</b>	BIOS Region/Non Fault Tolerant Region/OBB
<b>LBP3</b>	IUP – Independent Updatable Partitions
<b>LBP2/1</b>	Fault Tolerant Code partition (BUP/IBB/ACM/KM/Manifests)
LBP -> "Logical Boot Partition" are logical partitions of IFWI stored on the Boot0 partition of UFS	

## 2.4.1 Flash Region Layout

On UFS boot partition layout the Boot Partition Descriptor Table (BPDT) is a table of offsets to all individual sub-partitions contained within the Logical Boot Partition (LBP). A sub-partition is as a sub-division of the logical boot partition.

Each LBP contains a BPDT structure: the main BPDT at offset 0 of the LBP, which points to the sub-partitions.

The BPDT contains a header, immediately followed by 0 or more entries (number of following entries is indicated in the header)

Note that the BPDT is not signed.

Table 2-3. BPDT Header

Name	Offset	Size (bytes)	Description
<b>Signature</b>	0	4	Validity signature. For a valid BPDT (aka "green"), this value must be 0x000055AA. During IFWI update, this value is modified. The value of 0x00AA55AA indicates the BPDT is valid and can be booted from, however the firmware update is still in progress (aka "yellow" - recovery mode). Any other value indicates an invalid BPDT structure (aka "red").
<b>Descriptor Count</b>	4	2	Number of BPDT entries following this header
<b>Version</b>	6	1	Version of this BPDT structure. '1' - Layout 2.0 and 1.6 '2' - Layout 1.7
<b>BPDT Configuration</b>	7	1	Bits [7:1] - Reserved Bit [0] - '1' - BPDT Redundancy supported. There should be two copies of this BPDT in place. '0' - BPDT Redundancy not supported. This is the only copy of this BPDT
<b>CRC32 Checksum</b>	8	4	CRC32 checksum of entire BPDT structure (Header and Entries)
<b>IFWI Version</b>	12	4	Version of the particular IFWI build as marked by the build server
<b>Intel® FIT tool version</b>	16	8	Major/Minor/Build/Hotfix version of the Intel® FIT tool that was used to stitch the image. Not used by firmware

TGL BIOS will only have a single copy of Fault tolerant BIOS except during BIOS Update.

During update BIOS will need to ensure that it writes the redundant copy of fault tolerant BIOS in the location where Intel® CSME will take BPDT address and subtract Top Swap size to find it.

Intel® CSME uses BPDT 4, BPDT 4 Back up, Top Swap bit and Top Swap Size will determine which version Fault tolerant BIOS that Intel® CSME will load.

#### Flash Partition Table:

There is no manifest over the FPT since it only contains data describing where sub-partitions are, not production executable code.

Each sub-partition entry contains a partition name, sub-partition type (code/data), offset in the data section and size.

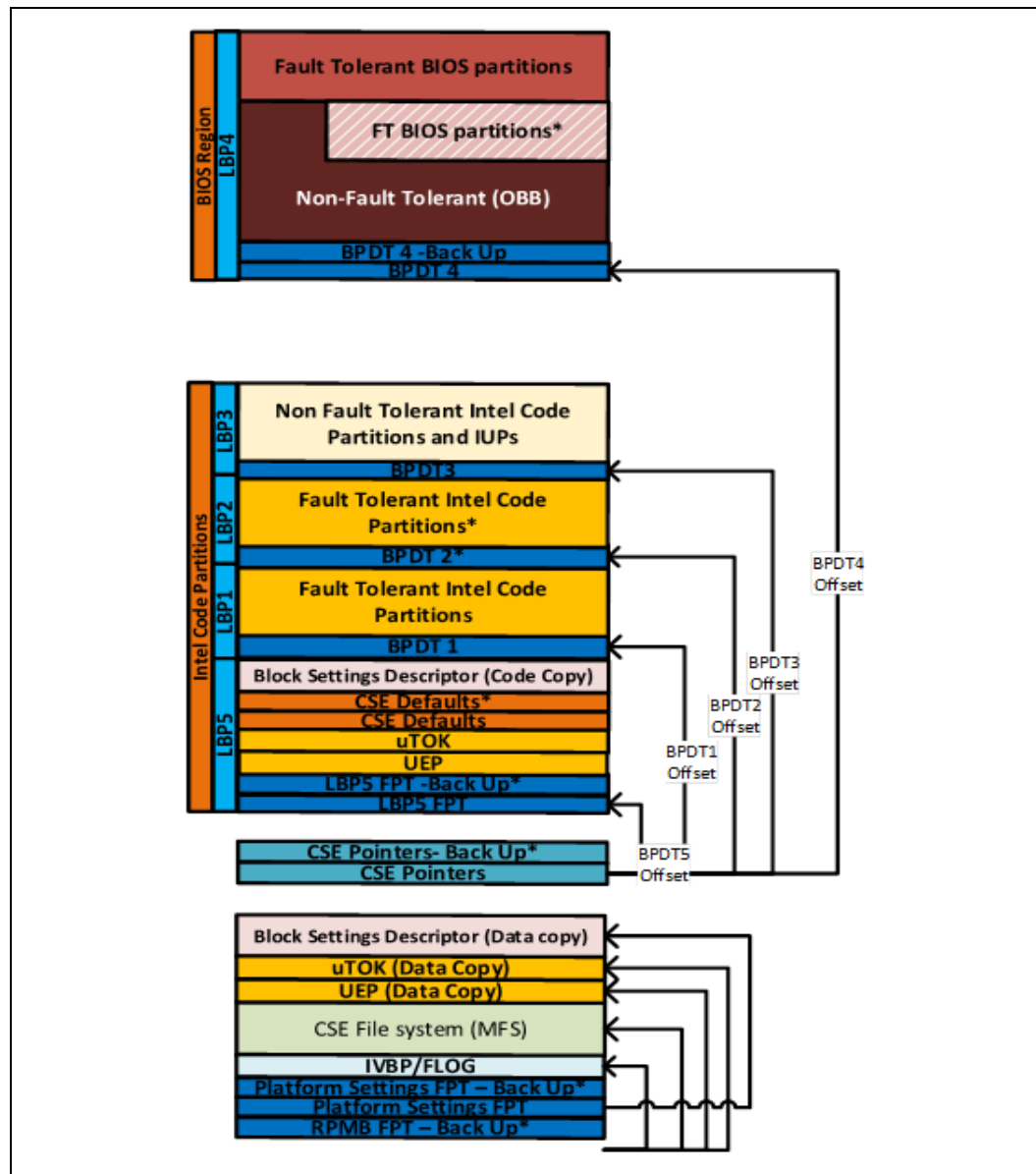
## 2.4.2 Platform Settings

The same SPI Flash descriptor structure will be used on UFS NVM with the structure maintained under LBP5. On 1st boot, Intel® CSME will pull this platform settings structure to RPMB/Temp Data Partition in order to provide the same security bar as SPI flash without the need for signing. OEM Signature / Soft straps are located at Platform Setting Offset + base descriptor offset.

Descriptor Settings not applicable to UFS are not configured by the Intel® FIT tool (some examples: SPI flash size, region offsets, master access permissions)

Signing and soft straps will be identical for UFS and SPI.

**Figure 2-2. UFS Boot Partition Layout**





## 2.5 PCH UFS Flash Compatibility Requirements

### 2.5.1 Lake Field Firmware Requirements

The user shall configure the logical units of the UFS device according to the following guidelines:

- Maximum number of logical units is specified by bMaxNumberLU supported by the UFS device.
- One or two logical units can be configured as boot logical units.
- Logical Block Size (bLogicalBlockSize) should correspond to 4KB block size (which means 0xc value). This also means that bMinAddrBlockSize should support 0x8 value.
- BootLun capability should be reserved for Intel® CSME needs.
- LUN6 should be reserved for temporary data storage. Data will be stored in LUN6 until after EOM. At EOM, Intel® CSME will perform binding between PCH and UFS after which data will be located at RPMB.
- RPMB size should at least accommodate Intel® CSME and BIOS needs for storage (RPMB for example could be as small as 128KB while Intel® CSME and BIOS data could be more ~4MB)
- UFS out of vendor has to be configured to 19.2MHz ref clock because this is the clock driven by TGL PCH

The configuration of each logical unit can be retrieved by reading the corresponding UFS Logical Unit Descriptor.

It is recommended to execute logical unit configuration during the system manufacturing phase.

For more details on UFS configuration please see UFS specifications at JEDEC website: [www.jedec.org](http://www.jedec.org).



# 3 Descriptor Overview

---

The same SPI Flash descriptor structure will be used on UFS NVM with the structure maintained under LBP5. On 1st CSME boot, CSME will pull this platform settings structure to RPMB/GPP4 in order to provide the same security bar as SPI flash w/o a need for signing. OEM Signature and Soft straps will be in the same location as on SPI.

Descriptor Settings not applicable to UFS are not configured by the Intel® FIT tool (some examples: SPI flash size, region offsets, master access permissions).

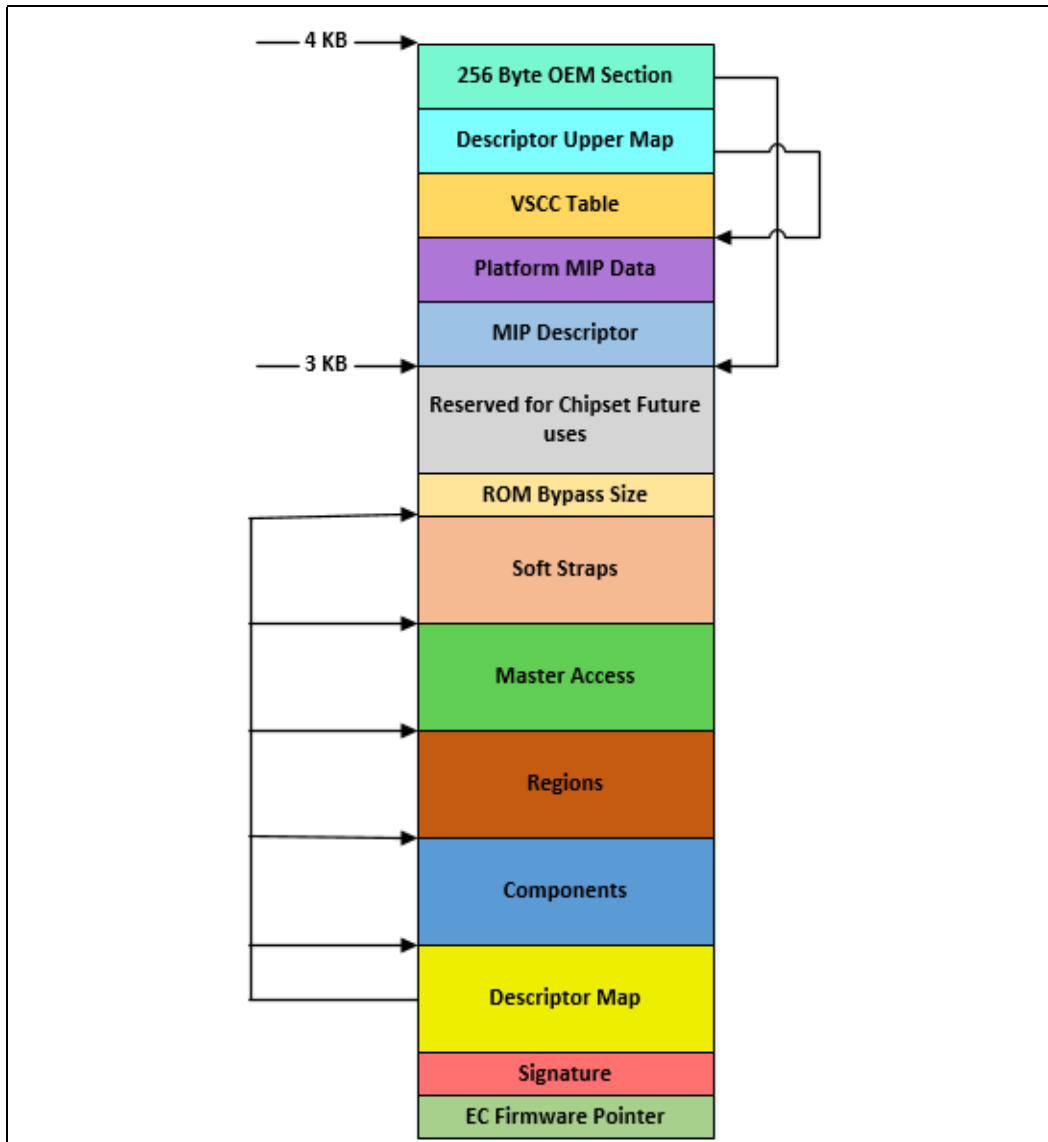
Signing and soft straps will be identical for UFS and SPI.

So this chapter will be maintained same as SPI.

The Descriptor data structure describes the layout of the flash as well as defining configuration parameters for the PCH. The maximum size of the Flash Descriptor is 4 K Bytes. It requires its own discrete erase block, so it may need greater than 4 K Bytes of flash space depending on the flash architecture that is on the target system.



**Figure 3-1. Flash Descriptor (Tiger Lake PCH)**



- The Flash signature at the bottom of the flash (offset 10h) must be 0FF0A55Ah in order to be in Descriptor mode.
- The Descriptor map has pointers to the lower five descriptor sections as well as the size of each.
- The Component section has information about the SPI flash part(s) the system. It includes the number of components, density of each component, read, write and erase frequencies and invalid instructions.
- The Region section defines the base and the limit of the BIOS, IFWI 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 CSME 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 *Tiger Lake PCH Family External Design Specification (EDS)*.

## 3.1 Flash Descriptor Content

The following sections describe the data structure of the Flash Descriptor. These are not registers or memory space within PCH. FDBAR - is address 0x0 on the SPI flash device on chip select 0 and will be the offset of LBP5 on UFS.

Recommended flash descriptor map:

Region Name	Starting Address
Signature	0x10
Component FCBA	0x30
Regions FRBA	0x40
Masters FMBA	0x80
PCH Straps FPSBA	0x100
MDTBA	0xC00
PMC Straps	0xC14
CPU Straps	0xC38
Intel® CSME Straps	0xC44
Register Init FIBA	0x340



### 3.1.1 Descriptor Signature and Map

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

Memory Address: FDBAR + 010h

Size: 32 bits

Recommended Value: 0FF0A55Ah

Bits	Description	Present in UFS
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).	<b>Yes</b>

#### 3.1.1.2 FLMAP0 - Flash Map 0 Register (Flash Descriptor Records)

Memory Address: FDBAR + 014h

Size: 32 bits

Bits	Description	Present in UFS
31:27	<b>Reserved</b>	<b>Yes</b>
26:24	<b>Reserved</b>	<b>Yes</b>
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.	<b>Yes</b>
15:13	<b>Reserved</b>	<b>Yes</b>
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.	<b>Yes</b>
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.	<b>Yes</b>
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.	<b>Yes</b>



Bits	Description	Present in UFS
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>	Yes



### 3.1.1.3 FLMAP1 - Flash Map 1 Register (Flash Descriptor Records)

Memory Address: FDBAR + 018h

Size: 32 bits

Bits	Description	Present in UFS
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 55h	<b>Yes</b>
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	<b>Yes</b>
15:11	Reserved	<b>Yes</b>
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.	<b>Yes</b>
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	<b>Yes</b>

### 3.1.1.4 FLMAP2—Flash Map 2 Register (Flash Descriptor Records)

Memory Address: FDBAR + 01Ch

Size: 32 bits

Bits	Description	Present in UFS
31:0	Reserved	<b>Yes</b>

### 3.1.1.5 FLMAP3—Flash Map 3 Register (Flash Descriptor Records)

Memory Address: FDBAR + 020h

Size: 32 bits

Bits	Description	FIT Visible
31:21	Major Version	<b>No</b>
20:14	Minor Version	<b>No</b>
13:0	Reserved	<b>No</b>



## 3.1.2 Flash Descriptor Component Section

### 3.1.2.1 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	Present in UFS
31	Reserved	No
30	<b>Dual Output Fast Read Support</b> 0 : Dual Output Fast Read is not supported 1 : Dual Output Fast Read is supported <b>Notes:</b> 1. This setting is no longer required.	No
29:27	<b>Read ID and Read Status Clock Frequency.</b> 001 = Reserved 010 = 48 MHz 100 = 30 MHz 110 = 17 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.	No
26:24	<b>Write and Erase Clock Frequency.</b> 001 = Reserved 010 = 48 MHz 100 = 30 MHz 110 = 17 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.	No
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'. 001 = Reserved 010 = 48 MHz 100 = 30 MHz 110 = 17 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.	No





Bits	Description	Present in UFS
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>	No
19:16	Reserved	No
15	<p><b>Quad I/O Read Enable (QIORE):</b>            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>	No
14	<p><b>Quad Output Read Enable (QORE):</b>            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>	No
13	<p><b>Dual I/O Read Enable (DIORE):</b>            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>	No
12	<p><b>Dual Output Read Enable (DORE):</b>            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>	No
11:10	Reserved	No



Bits	Description	Present in UFS
9	<b>SPI Voltage Select (SPI_1p8volt_sel):</b>  0 = SPI supply voltage set to 3.3 volts 1 = SPI supply voltage set to 1.8 volts  This strap sets the internal control signal on the pad for either 1.8 or 3.3 V operation.  <b>Note:</b> The strap defaults to 1.8V mode before the soft straps are loaded, i.e. before the actual supply voltage is known. This is because the pad performance is slightly better when assuming 1.8V when the actual is 3.3V than vice-versa.	No
8	Reserved	No
7:4	<b>Component 1 Density. (C1DEN)</b> This field identifies the size of the 2nd Flash component connected directly to the PCH. If there is not 2nd Flash component, the contents of this field should be read as "1111b" 0000 = 512 KB 0001 = 1 MB 0010 = 2 MB 0011 = 4 MB 0100 = 8 MB 0101 = 16 MB 0110 = 32 MB 0111 = 64 MB 1000 - 1110 = Reserved  <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.	No
3:0	<b>Component 0 Density (C0DEN).</b> This field identifies the size of the 1st or only Flash component connected directly to the PCH. 0000 = 512 KB 0001 = 1 MB 0010 = 2 MB 0011 = 4 MB 0100 = 8 MB 0101 = 16 MB 0110 = 32 MB 0111 = 64 MB 1000 - 1111 = Reserved  <b>Note:</b> This field is defaulted to "0101b" (16MB) after reset.	No



### 3.1.2.2 FLILL—Flash Invalid Instructions Register (Flash Descriptor Records)

Memory Address: FCBA + 004h

Size: 32 bits

Bits	Description	Present in UFS
31:24	<b>Invalid Instruction 3.</b> <b>Default set to 0xAD</b> See definition of Invalid Instruction 0	No
23:16	<b>Invalid Instruction 2.</b> <b>Default set to 0x60</b> See definition of Invalid Instruction 0	No
15:8	<b>Invalid Instruction 1.</b> <b>Default set to 0x42</b> See definition of Invalid Instruction 0	No
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.	No

### 3.1.2.3 FLILL1—Flash Invalid Instructions Register (Flash Descriptor Records)

Memory Address: FCBA + 008h

Size: 32 bits

Bits	Description	Present in UFS
31:24	<b>Invalid Instruction 7.</b> <b>Default set to C7</b> See definition of Invalid Instruction 0	No
23:16	<b>Invalid Instruction 6.</b> <b>Default set to 0xC4</b> See definition of Invalid Instruction 0	No
15:8	<b>Invalid Instruction 5.</b> <b>Default set to 0xB9</b> See definition of Invalid Instruction 0	No



Bits	Description	Present in UFS
7:0	<b>Invalid Instruction 4.</b> <b>Default set to 0xB7</b> See definition of Invalid Instruction 0	<b>No</b>



### 3.1.3 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.

#### 3.1.3.1 FLREG0—Flash Region 0 (Flash Descriptor) Register (Flash Descriptor Records)

Memory Address: FRBA + 000h

Size: 32 bits

Recommended Value: 00000000h

Bits	Description	Present in UFS
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. Set this field to 0b. This defines the ending address of descriptor as being FFFh.</li> <li>2. 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

#### 3.1.3.2 FLREG1—Flash Region 1 (BIOS) Register (Flash Descriptor Records)

Memory Address: FRBA + 004h

Size: 32 bits

Bits	Description	Present in UFS
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. Must be set to 0000h if Intel® CSME ROM Bypass region is unused (on Firmware hub)</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 BIOS region is not used, the Region Base must be programmed to 7FFFh	No



### 3.1.3.3 FLREG2—Flash Region 2 (IFWI / Intel® CSME ROM Bypass) Register (Flash Descriptor Records)

Memory Address: FRBA + 008h

Size: 32 bits

Bits	Description	Present in UFS
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

**Note:** Region 3 (FRBA + 0Ch), Region 4 (FRBA + 010h), Region 6 (FRBA + 018h), Region 7 (FRBA + 01Ch), Region 8 (FRBA + 020h) and Region 9 (FRBA + 024h), Region 10 (FRBA + 28h), Region 11 (FRBA + 2Ch), Region 12 (FRBA + 30h), Region 13 (FRBA + 34h), Region 14 (FRBA + 38h) and Region 15 (FRBA + 03Ch) are all reserved in client platform and should set to 7FFFh.



### 3.1.4 Flash Descriptor Master Section

#### 3.1.4.1 FLMSTR1—Flash Master 1 (Host CPU/ BIOS)

Memory Address: FMBA + 000h

Size: 32 bits

Bits	Description	Present in UFS
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	No
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.	No
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.	No
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.	No

#### 3.1.4.2 FLMSTR2—Flash Master 2 (Intel® ME)

Memory Address: FMBA + 004h

Size: 32 bits

Bits	Description	Present in UFS
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	No
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.	No
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.	No
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.	No



### 3.1.5 PCH / CPU Softstraps

See Chapter 4, “UFS PCH / PMC / CPU and Intel® CSE Configuration Section” for details.

### 3.1.6 Descriptor Upper Map Section

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

#### 3.1.6.1 FLUMAP1—Flash Upper Map 1 (Flash Descriptor Records)

Memory Address: FDBAR + EFCh

Size: 32 bits

Bits	Default	Description	Present in UFS
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.	Yes
23:16	0xFF	Reserved	Yes
15:8	0x1	<b>Intel® CSME 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)	Yes
7:0	0x1	<b>Intel® CSME 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.	Yes

#### 3.1.6.2 IFWI / Intel® CSME ROM Bypass Size

Memory Address: FDBAR + C00h

Size: 32 bits

Bits	Default	Description	Present in UFS
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

#### 3.1.6.3 MIP - Descriptor Table

Memory Address: FDBAR + MDTBA

Name	Offset	Size (bytes)	Description	Present in UFS
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 = CSME (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





Name	Offset	Size (bytes)	Description	Present in UFS
Block 1 Offset	0xE	2	Offset of block 1	Yes
Block 1 Length	0x10	2	Length of block 1 in bytes	Yes
Block 1 Reserved	0x12	2	Must be 0	Yes
.....				Yes
Block 'n' Type		2	See Block 0 type	Yes
Block 'n' Offset		2	Offset of block 'n'	Yes
Block 'n' Length		2	Length of block 'n' in bytes	Yes
Block 'n' Reserved		2	Must be 0	Yes

### 3.1.7 Intel® CSME Vendor Specific Component Capabilities Table

Entries in this table allow support for a SPI flash part for Intel® CSME capabilities.

Since Flash Partition Boundary Address (FPBA) has been removed, UVSCC and LVSCC has been replaced with VSCC0 and VSCC1 in Tiger 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 [3.1.7.4 VSCCn—Vendor Specific Component Capabilities n \(Flash Descriptor Records\)](#) for information on how to program individual entries.

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

Memory Address: VTBA + 000h

Size: 32 bits

Bits	Description	Present in UFS
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).	No
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).	No
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).	No



### 3.1.7.2 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	Present in UFS
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
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.		

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

Memory Address: VTBA + (n\*8)h

Size: 32 bits

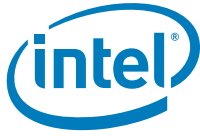
"n" is an integer denoting the index of the Intel® CSME VSCC table. See **Table 4.1.7.1** for details.

### 3.1.7.4 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® CSME VSCC table. See **Table 4.1.7.2** for details.



## **3.2 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.

## **3.3 Region Access Control**

There is no region access control on UFS NVM.



## 4 UFS 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.

For UFS same Flash address mapping as SPI is maintained. The Offset and data size will be same as SPI starting from the logical address mapping in the UFS region.

### 4.1 PCH Record 0 (UFS Flash Records)

Platform Setting Offset + 100h

Default Address: 4100h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4100h	23:0	Reserved, set to '0'		No

### 4.2 PCH Record 1 (UFS Flash Records)

Platform Setting Offset + 103h

Default Address: 4103h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4103h	7	Reserved, set to '0x1'		No
	6:4	<b>OPI Link Width (OPDMI_LW):</b> 0x0 = 1 Lane 0x1 = 2 Lanes 0x2 = 4 Lanes 0x3 = 8 Lanes	This setting configures the OPI Link Width. For further details see the Ice Lake PCH EDS.  <b>Note:</b> This strap and OPI Link Width ( <b>OPDMI_LW_DMI</b> ) must match the same lane configuration for proper platform operation.	Yes
	3:0	<b>OPI Link Speed (OPDMI_TLS):</b> 0x2 = 2 GT/s Link Speed 0x3 = 4 GT/s Link Speed	This strap must be configured when setting OPI Link Speed Strap ( <b>OPDMI_STRP</b> ).  <b>Note:</b> This strap and the OPI Link Speed Strap ( <b>OPDMI_STRP</b> ) and ( <b>OPDMI_TLS_DMI</b> ) must match the same GT configuration setting for proper platform operation.  This setting configures the OPI Link Width. For further details see the Ice Lake PCH EDS.	Yes



### 4.3 PCH Record 2 (UFS Flash Records)

Platform Setting Offset + 104h

Default Address: 4104h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4104h	7:0	Reserved, set to '0'		No

### 4.4 PCH Record 3 (UFS Flash Records)

Platform Setting Offset + 105h

Default Address: 4105h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4105h	7:0	Reserved, set to '0'		No

### 4.5 PCH Record 4 (UFS Flash Records)

Platform Setting Offset + 106h

Default Address: 4106h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4106h	7:2	Reserved, set to '0'		No
	1	<b>USB3 Port 2 Speed Select:</b> 0 = Port 2 is configured as USB3.1 Gen2 1 = Port 2 is configured as USB3.1 Gen1	This setting determines the USB3 Port 2 speed capabilities.	Yes
	0	<b>USB3 Port 1 Speed Select:</b> 0 = Port 1 is configured as USB3.1 Gen2 1 = Port 1 is configured as USB3.1 Gen1	This setting determines the USB3 Port 1 speed capabilities.	Yes



## 4.6 PCH Record 5 (UFS Flash Records)

Platform Setting Offset + 107h

Default Address: 4107h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4107h	7:2	<b>Reserved, set to '0'</b>		<b>No</b>
	1	<b>USB3 Port 2 Initialization Speed Select:</b> 0 = Port 2 will boot as USB 3.1 Gen1 and carry on LBPM if USB 3.1 Gen2 is enabled 1 = Port 2 will boot as USB 3.1 Gen2 and skip LBPM	This setting determines USB3 Port 2 speed during platform power-up.	<b>Yes</b>
	0	<b>USB3 Port 1 Initialization Speed Select:</b> 0 = Port 1 will boot as USB 3.1 Gen1 and carry on LBPM if USB 3.1 Gen2 is enabled 1 = Port 1 will boot as USB 3.1 Gen2 and skip LBPM	This setting determines USB3 Port 1 speed during platform power-up.	<b>Yes</b>

## 4.7 PCH Record 6 (UFS Flash Records)

Platform Setting Offset + 108h

Default Address: 4108h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4108h	7:4	<b>USB3 Port 2 Connector Type Select:</b> 0x0 = USB Port 2 connector set to Type C 0x1 = Reserved 0x2 = USB Port 2 connector set to Type A 0x3 = Reserved 0x4 = USB Port 2 connector set to Express Card / M.2 S2	This setting configures the physical connector type for where the USB port [Super Speed / Enhanced Super Speed] is routed.  <b>Note:</b> This Strap and USB3 Port 2 Connector Type Select Aux must match for proper operation.	<b>Yes</b>
	3:0	<b>USB3 Port 1 Connector Type Select:</b> 0x0 = USB Port 2 connector set to Type C 0x1 = Reserved 0x2 = USB Port 2 connector set to Type A 0x3 = Reserved 0x4 = USB Port 2 connector set to Express Card / M.2 S2	This setting configures the physical connector type for where the USB port [Super Speed / Enhanced Super Speed] is routed.  <b>Note:</b> This Strap and USB3 Port 1 Connector Type Select Aux must match for proper operation.	<b>Yes</b>



## 4.8 PCH Record 7 (UFS Flash Records)

Platform Setting Offset + 109h

Default Address: 4109h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4109h	7:4	<b>USB2 Port 2 Connector Type Select:</b> 0x0 = USB Port 2 connector set to Type C 0x1 = USB Port 2 connector set to Micro AB 0x2 = USB Port 2 connector set to Type A 0x3 = USB Port 2 connector set to Type B 0x4 = USB Port 2 connector set to Express Card / M.2 S2	This setting configures the USB2 Port 2 physical connector type for where the USB port is routed.	Yes
	3:0	<b>USB2 Port 1 Connector Type Select:</b> 0x0 = USB Port 1 connector set to Type C 0x1 = USB Port 1 connector set to Micro AB 0x2 = USB Port 1 connector set to Type A 0x3 = USB Port 1 connector set to Type B 0x4 = USB Port 1 connector set to Express Card / M.2 S2	This setting configures the USB2 Port 1 physical connector type for where the USB port is routed.	Yes

## 4.9 PCH Record 8 (UFS Flash Records)

Platform Setting Offset + 10Ah

Default Address: 410Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0x410Ah	7:1	<b>Reserved, set to '0'</b>		No
	0	<b>USB Type AB mode Select:</b> 0 = USB Type AB connector switches based on SW event 1 = USB Type AB connector switches based on HW event	This setting configures the mode for the USB Type AB connector.	Yes

## 4.10 PCH Record 9 (UFS Flash Records)

Platform Setting Offset + 10Bh

Default Address: 410Bh

Offset from 0	Bits	Description	Usage	FIT Visible
0x410Bh	7:0	<b>Reserved, set to '0'</b>		No



## 4.11 PCH Record 10 (UFS Flash Records)

Platform Setting Offset + 10Ch

Default Address: 410Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x410Ch	31:0	Reserved, set to '0'		No

## 4.12 PCH Record 11 (UFS Flash Records)

Platform Setting Offset + 110h

Default Address: 4110h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4110h	15:0	Reserved, set to '0'		No

## 4.13 PCH Record 12 (UFS Flash Records)

Platform Setting Offset + 112h

Default Address: 4112h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4112h	7:0	Reserved, set to '0'		No

## 4.14 PCH Record 13 (UFS Flash Records)

Platform Setting Offset + 113h

Default Address: 4113h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4113h	7:0	Reserved, set to '0'		No





## 4.15 PCH Record 14 (UFS Flash Records)

Platform Setting Offset + 114h

Default Address: 4114h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4114h	7	Reserved, set to '0'		No
	6:4	<b>Top Swap Block size (TSBS):</b>  000 = 64 KB. Invert A16 if Top Swap is enabled 001 = 128 KB. Invert A17 if Top Swap is enabled 010 = 256 KB. Invert A18 if Top Swap is enabled 011 = 512 KB. Invert A19 if Top Swap is enabled 100 = 1 MB. Invert A20 if Top Swap is enabled 101 - 111: Reserved.  <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. 3. Intel Client chipset supports top swap block size of up to 256 KB. TS block sizes of greater than 256KB are not supported.	This allows for the system to use alternate code in order to boot a platform based upon the <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

## 4.16 PCH Record 15 (UFS Flash Records)

Platform Setting Offset + 115h

Default Address: 4115h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4115h	7:0	Reserved, set to '0'		No

## 4.17 PCH Record 16 (UFS Flash Records)

Platform Setting Offset + 116h

Default Address: 4116h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4116h	7:0	Reserved, set to '0'		No



## 4.18 PCH Record 17 (UFS Flash Records)

Platform Setting Offset + 117h

Default Address: 4117h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4117h	7:0	Reserved, set to '0'		No

## 4.19 PCH Record 18 (UFS Flash Records)

Platform Setting Offset + 118h

Default Address: 4118h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4118h	7:0	Reserved, set to '0x45'		No

## 4.20 PCH Record 19 (UFS Flash Records)

Platform Setting Offset + 119h

Default Address: 4119h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4119h	7:0	Reserved, set to '0x86'		No

## 4.21 PCH Record 20 (UFS Flash Records)

Platform Setting Offset + 11Ah

Default Address: 411Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0x411Ah	7:0	Reserved, set to '0'		No

## 4.22 PCH Record 21 (UFS Flash Records)

Platform Setting Offset + 11Bh

Default Address: 411Bh

Offset from 0	Bits	Description	Usage	FIT Visible
0x411Bh	7:0	Reserved, set to '0'		No



## 4.23 PCH Record 22 (UFS Flash Records)

Platform Setting Offset + 11Ch

Default Address: 411Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x411Ch	31:0	Reserved, set to '0'		No

## 4.24 PCH Record 23 (UFS Flash Records)

Platform Setting Offset + 120h

Default Address: 4120h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4120h	7:0	Reserved, set to '0'		No

## 4.25 PCH Record 24 (UFS Flash Records)

Platform Setting Offset + 121h

Default Address: 4121h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4121h	7:0	Reserved, set to '0'		No

## 4.26 PCH Record 25 (UFS Flash Records)

Platform Setting Offset + 122h

Default Address: 4122h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4122h	7:0	Reserved, set to '0'		No

## 4.27 PCH Record 26 (UFS Flash Records)

Platform Setting Offset + 123h

Default Address: 4123h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4123h	7:0	Reserved, set to '0'		No



## 4.28 PCH Record 27 (UFS Flash Records)

Platform Setting Offset + 124h

Default Address: 4124h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4124h	7:0	Reserved, set to '0'		No

## 4.29 PCH Record 28 (UFS Flash Records)

Platform Setting Offset + 125h

Default Address: 4125h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4125h	7:0	Reserved, set to '0'		No

## 4.30 PCH Record 29 (UFS Flash Records)

Platform Setting Offset + 126h

Default Address: 4126h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4126h	7:0	Reserved, set to '0'		No

## 4.31 PCH Record 30 (UFS Flash Records)

Platform Setting Offset + 127h

Default Address: 4127h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4127h	7:0	Reserved, set to '0'		No

## 4.32 PCH Record 31 (UFS Flash Records)

Platform Setting Offset + 128h

Default Address: 4128h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4128h	31:0	Reserved, set to '0'		No



### 4.33 PCH Record 32 (UFS Flash Records)

Platform Setting Offset + 12Ch

Default Address: 412Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x412Ch	31:0	Reserved, set to '0'		No

### 4.34 PCH Record 33 (UFS Flash Records)

Platform Setting Offset + 130h

Default Address: 4130h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4130h	7:0	Reserved, set to '0'		No

### 4.35 PCH Record 34 (UFS Flash Records)

Platform Setting Offset + 131h

Default Address: 4131h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4131h	7:5	Reserved, set to '0'		No
	4:3	<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.  00 = 4x1 01 = 1x2, 2x1 10 = 2x2 11 = 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
	2	<b>PCIe Controller 1 Lane Reversal:</b>  0 = PCIe Lanes are not reversed. 1 = 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.	Yes
	1:0	Reserved, set to '0'		No



## 4.36 PCH Record 35 (UFS Flash Records)

Platform Setting Offset + 132h

Default Address: 4132h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4132h	7:0	Reserved, set to '0'		No

## 4.37 PCH Record 36 (UFS Flash Records)

Platform Setting Offset + 133h

Default Address: 4133h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4133h	7:0	Reserved, set to '0'		No

## 4.38 PCH Record 37 (UFS Flash Records)

Platform Setting Offset + 134h

Default Address: 4134h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4134h	7:0	Reserved, set to '0'		No

## 4.39 PCH Record 38 (UFS Flash Records)

Platform Setting Offset + 135h

Default Address: 4135h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4135h	7:0	Reserved, set to '0'		No

## 4.40 PCH Record 39 (UFS Flash Records)

Platform Setting Offset + 136h

Default Address: 4136h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4136h	7:0	Reserved, set to '0'		No



## 4.41 PCH Record 40 (UFS Flash Records)

Platform Setting Offset + 137h

Default Address: 4137h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4137h	7:0	Reserved, set to '0'		No

## 4.42 PCH Record 41 (UFS Flash Records)

Platform Setting Offset + 138h

Default Address: 4138h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4138h	7:0	Reserved, set to '0'		No

## 4.43 PCH Record 42 (UFS Flash Records)

Platform Setting Offset + 139h

Default Address: 4139h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4139h	7:5	Reserved, set to '0'		No
	4:3	<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.  00 = 4x1 01 = 1x2, 2x1 10 = 2x2 11 = 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.	Yes
	2	<b>PCIe Controller 2 Lane Reversal:</b>  0 = PCIe Lanes are not reversed. 1 = 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.	Yes
	1:0	Reserved, set to '0'		No



## 4.44 PCH Record 43 (UFS Flash Records)

Platform Setting Offset + 13Ah

Default Address: 413Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0x413Ah	7:0	Reserved, set to '0'		No

## 4.45 PCH Record 44 (UFS Flash Records)

Platform Setting Offset + 13Bh

Default Address: 413Bh

Offset from 0	Bits	Description	Usage	FIT Visible
0x413Bh	7:0	Reserved, set to '0'		No

## 4.46 PCH Record 45 (UFS Flash Records)

Platform Setting Offset + 13Ch

Default Address: 413Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x413Ch	7:0	Reserved, set to '0'		No

## 4.47 PCH Record 46 (UFS Flash Records)

Platform Setting Offset + 13Dh

Default Address: 413Dh

Offset from 0	Bits	Description	Usage	FIT Visible
0x413Dh	7:0	Reserved, set to '0'		No

## 4.48 PCH Record 47 (UFS Flash Records)

Platform Setting Offset + 13Eh

Default Address: 413Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0x413Eh	7:0	Reserved, set to '0'		No





## 4.49 PCH Record 48 (UFS Flash Records)

Platform Setting Offset + 13Fh

Default Address: 413Fh

Offset from 0	Bits	Description	Usage	FIT Visible
0x413Fh	7:0	Reserved, set to '0'		No

## 4.50 PCH Record 49 (UFS Flash Records)

Platform Setting Offset + 140h

Default Address: 4140h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4140h	7:0	Reserved, set to '0'		No

## 4.51 PCH Record 50 (UFS Flash Records)

Platform Setting Offset + 041h

Default Address: 141h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4141h	7:0	Reserved, set to '0'		No

## 4.52 PCH Record 51 (UFS Flash Records)

Platform Setting Offset + 042h

Default Address: 142h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4142h	7:0	Reserved, set to '0'		No

## 4.53 PCH Record 52 (UFS Flash Records)

Platform Setting Offset + 043h

Default Address: 143h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4143h	7:0	Reserved, set to '0'		No



## 4.54 PCH Record 53 (UFS Flash Records)

Platform Setting Offset + 044h

Default Address: 144h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4144h	7:0	Reserved, set to '0'		No

## 4.55 PCH Record 54 (UFS Flash Records)

Platform Setting Offset + 045h

Default Address: 145h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4145h	7:0	Reserved, set to '0'		No

## 4.56 PCH Record 55 (UFS Flash Records)

Platform Setting Offset + 046h

Default Address: 146h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4146h	7:0	Reserved, set to '0'		No

## 4.57 PCH Record 56 (UFS Flash Records)

Platform Setting Offset + 047h

Default Address: 147h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4147h	7:0	Reserved, set to '0'		No

## 4.58 PCH Record 57 (UFS Flash Records)

Platform Setting Offset + 048h

Default Address: 148h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4148h	7:0	Reserved, set to '0'		No



## 4.59 PCH Record 58 (UFS Flash Records)

Platform Setting Offset + 149h

Default Address: 4149h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4149h	7	Reserved, set to '0x1'		No
	6:4	<b>OPI Link Width (OPDMI_LW_DMI):</b>  0x0 = 1 Lane 0x1 = 2 Lanes 0x2 = 4 Lanes 0x3 = 8 Lanes	This setting configures the OPI Link Width. For further details see the Ice Lake PCH EDS.  <b>Note:</b> This strap and OPI Link Width ( <b>OPDMI_LW_FPX</b> ) must match the same lane configuration for proper platform operation.	Yes
	3:0	<b>OPI Link Speed (OPDMI_TLS_DMI):</b>  0x2 = 2 GT/s Link Speed 0x3 = 4 GT/s Link Speed	This strap must be configured when setting OPI Link Speed Strap ( <b>OPDMI_STRP</b> ).  <b>Note:</b> This strap and the OPI Link Speed Strap ( <b>OPDMI_STRP</b> ) and ( <b>OPDMI_TLS_FPX</b> ) must match the same GT configuration setting for proper platform operation function.  This setting configures the OPI Link Width. For further details see the Ice Lake PCH EDS.	Yes

## 4.60 PCH Record 59 (UFS Flash Records)

Platform Setting Offset + 04Ah

Default Address: 14Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0x414Ah	7:0	Reserved, set to '0'		No



## 4.61 PCH Record 60 (UFS Flash Records)

Platform Setting Offset + 14Bh

Default Address: 414Bh

Offset from 0	Bits	Description	Usage	FIT Visible
0x414Bh	7:6	Reserved, set to '0x1'		No
	5	Reserved, set to '0x1'		No
	3:4	Reserved, set to '0'		No
	2:1	<b>OPI Link Voltage (OPD_LVO):</b>  0 = 0.85 Volts 1 = 0.95 Volts 2 = 1.05 Volts	This strap must be configured when setting OPI Link Speed strap ( <b>OPD_LVO_STRP</b> ).  <b>Note:</b> This strap and the OPI Link Speed strap ( <b>OPD_LVO_STRP</b> ) must match the same voltage configuration setting for proper platform operation function.  This setting configures the OPI Link Voltage. For further details see Ice Lake PCH EDS.	Yes
	0	Reserved, set to '0'		No

## 4.62 PCH Record 61 (UFS Flash Records)

Platform Setting Offset + 04Ch

Default Address: 414Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x414Ch	31	Reserved, set to '0'		No
	30	<b>Intel® Trace Hub Soft Enable:</b>  0 = ROM Tracing Soft Disable 1 = ROM Tracing Soft Enable	This soft strap enables ROM based tracing in the ME.  <b>Note:</b> Only applicable if Intel® Trace Hub Debug Messages strap is also enabled	Yes
	29:22	Reserved, set to '0'		
	21	<b>Intel® Trace Hub - Emergency Mode:</b>  0 = ROM Tracing Emergency mode disabled 1 = ROM Tracing Emergency mode enabled	This option enables ROM Tracing in the base platform image.	Yes



Offset from 0	Bits	Description	Usage	FIT Visible
0x414Ch (Cont)	20	<b>Deep Sx Enable (Deep_SX_EN):</b> 0 = Deep Sx is not supported on the platform 1 = Deep Sx is supported on the platform	This requires the target platform to support Deep Sx state  <b>Note:</b> When configuring Deep Sx you must also set <b>DEEPSX_PLT_CFG_SS</b> .	<b>Yes</b>
	19:18	<b>Reserved, set to '0'</b>		<b>No</b>
	17	<b>Direct Connect Interface (DCI) Enabled:</b> 0 = DCI Disabled 1 = 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® CSME AFS Flash Idle Reclaim Enable:</b> 0 = AFS Flash Reclaim enabled 1 = AFS Flash Reclaim disabled	This controls enabling / disabling of Intel® CSME AFS Idle flash reclaim capabilities.  Note: This setting should be used for debug purposes only	<b>Yes</b>
	10	<b>Intel® CSME Reset Behavior:</b> 0 = Intel® CSME will attempt to boot from the next available image, if it exists 1 = Intel® CSME will halt		
	9	<b>Reserved, set to '0'</b>		<b>No</b>
	8	<b>Reserved, set to '0x1'</b>		<b>No</b>
	7:1	<b>Reserved, set to '0x1C'</b>		<b>No</b>
	0	<b>Firmware ROM Bypass Enable Softstrap:</b> 0 = ROM Bypass disabled 1 = ROM Bypass enabled	Firmware ROM Bypass Enable Softstrap.	<b>Yes</b>



## 4.63 PCH Record 62 (UFS Flash Records)

Platform Setting Offset + 150h

Default Address: 4150h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4150h	4	<b>DCI BSSB over USB3 Port2 Configuration (EXI_PTSS_PORT4):</b>  0 = BSSB is enabled on USB3 Port2 1 = BSSB is disabled on USB3 Port2	This setting determines if the USB port being used for <b>DCI</b> operations has BSSB (Boundary Scan Side Band) enabled.  <b>Note:</b> For S0ix and reset flows BSSB should be enabled.	<b>Yes</b>
	3	<b>Reserved, set to '0x1'</b>		<b>No</b>
	2	<b>DCI BSSB over GPIO Configuration (EXI_PTSS_PORT2):</b>  0 = BSSB is enabled over GPIO 1 = BSSB is disabled over GPIO	This setting enables BSSB (Boundary Scan Side Band) over GPIO for <b>DCI</b> operations.  <b>Note:</b> If this setting is enabled the <b>DCI Port1 Configuration</b> also needs to be enabled. <b>Note:</b> For S0ix and reset flows BSSB should be enabled.	<b>Yes</b>
	1	<b>Reserved, set to '0x1'</b>		<b>No</b>
0x4150h (Cont)	0	<b>DCI BSSB over USB3 Port1 Configuration (EXI_PTSS_PORT0):</b>  0 = BSSB is enabled on USB3 Port1 1 = BSSB is disabled on USB3 Port1	This setting determines if the USB port being used for <b>DCI</b> operations has BSSB (Boundary Scan Side Band) enabled.  <b>Note:</b> For S0ix and reset flows BSSB should be enabled.	<b>Yes</b>

## 4.64 PCH Record 63 (UFS Flash Records)

Platform Setting Offset + 151h

Default Address: 4151h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4151h	7:0	<b>Reserved, set to '0'</b>		<b>No</b>

## 4.65 PCH Record 64 (UFS Flash Records)

Platform Setting Offset + 152h

Default Address: 4152h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4152h	7:0	<b>Reserved, set to '0'</b>		<b>No</b>



## 4.66 PCH Record 65 (UFS Flash Records)

Platform Setting Offset + 153h

Default Address: 4153h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4153h	7:0	Reserved, set to '0'		No

## 4.67 PCH Record 66 (UFS Flash Records)

Platform Setting Offset + 154h

Default Address: 4154h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4154h	7:0	Reserved, set to '0'		No

## 4.68 PCH Record 67 (UFS Flash Records)

Platform Setting Offset + 155h

Default Address: 4155h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4155h	7:0	Reserved, set to '0'		No

## 4.69 PCH Record 68 (UFS Flash Records)

Platform Setting Offset + 156h

Default Address: 4156h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4156h	7:0	Reserved, set to '0'		No

## 4.70 PCH Record 70 (UFS Flash Records)

Platform Setting Offset + 157h

Default Address: 4157h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4157h	7:0	Reserved, set to '0'		No



## 4.71 PCH Record 71 (UFS Flash Records)

Platform Setting Offset + 158h

Default Address: 4158h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4158h	31:0	Reserved, set to '0'		No

## 4.72 PCH Record 72 (UFS Flash Records)

Platform Setting Offset + 15Ch

Default Address: 415Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x415Ch	31:0	Reserved, set to '0'		No

## 4.73 PCH Record 73 (UFS Flash Records)

Platform Setting Offset + 160h

Default Address: 4160h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4160h	7:1	Reserved, set to '0'		No
	0	<b>TPM Over SPI Bus Enabled (TOS):</b> 0 = TPM is not on SPI 1 = TPM is on SPI	This field identifies the frequency that should be used with the TPM on SPI. This field is undefined if the TPM on SPI is disabled by softstrap	Yes





## 4.74 MIP Table Record 0 (UFS Flash Records)

Platform Setting Offset + C00h

Default Address: 4C00h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4C00h	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.	No

## 4.75 MIP Table Record 1 (UFS Flash Records)

Platform Setting Offset + C02h

Default Address: 4C02h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4C02h	15:0	<b>Size of MIP Descriptor Entry:</b> <b>Set to '0x50'</b>	This setting determines the size in bytes of the MIP Descriptor Entry structure.	No

## 4.76 MIP Table Record 2 (UFS Flash Records)

Platform Setting Offset + C04h

Default Address: 4C04h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4C04h	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.	No

## 4.77 MIP Table Record 3 (UFS Flash Records)

Platform Setting Offset + C06h

Default Address: 4C06h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4C06h	15:0	<b>MIP Descriptor Block 0 Offset:</b> <b>Set to '0x14h'</b>	This setting determines the offset location of the MIP Descriptor Table Entries.	No



## 4.78 MIP Table Record 4 (UFS Flash Records)

Platform Setting Offset + C08h

Default Address: 4C08h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4C08h	15:0	<b>MIP Descriptor Block 0 Length:</b> Set to '0x48h'	This setting determine the length of the MIP Descriptor Block 0.	No

## 4.79 MIP Table Record 5 (UFS Flash Records)

Platform Setting Offset + C0Ah

Default Address: 4C0Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0x4C0Ah	15:0	Reserved, set to '0'		No

## 4.80 MIP Table Record 6 (UFS Flash Records)

Platform Setting Offset + C0Ch

Default Address: 4C0Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x4C0Ch	15:0	<b>MIP Descriptor Block 1 Type:</b> Set to '0'	This setting determines what the data type is for the MIP Descriptor.	No

## 4.81 MIP Table Record 7 (UFS Flash Records)

Platform Setting Offset + C0Eh

Default Address: 4C0Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0x4C0Eh	15:0	<b>MIP Descriptor Block 1 Offset:</b> Set to '0x48h'	This setting determines the offset location of the MIP Descriptor Table Entries.	No



## 4.82 MIP Table Record 8 (UFS Flash Records)

Platform Setting Offset + C10h

Default Address: 4C10h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4C10h	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.	No

## 4.83 MIP Table Record 9 (UFS Flash Records)

Platform Setting Offset + C12h

Default Address: 4C12h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4C12h	15:0	<b>Reserved, set to '0'</b>		No



## 4.84 PMC Record 0 (UFS Flash Records)

Platform Setting Offset + C14h

Default Address: 4C14h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4C14h	31:28	<b>Reserved, set to '0'</b>		<b>No</b>
	27	<b>Intel® Trace Hub Debug Messages Enable:</b>  0 = PCH Tracing debug messages Disabled 1 = 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"	<b>Yes</b>
	26	<b>Reserved, set to '0'</b>		<b>No</b>
	25	<b>Power Reporting Enable (THERM_PWR_REP_DIS):</b>  0 = Power Reporting is enabled. 1 = 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.	<b>Yes</b>
	24	<b>PCIe* Power Stable Timer (tPCH33 timer):</b>  0 = tPCH33 timer is disabled 1 = PCH will count 99ms from PWROK assertion before PLTRST# is de-asserted.	Board dependent. Default is disabled, Platform is required to ensure timing of PWROK and SYS_PWROK in such a way that it satisfies the PCIe timing requirement of power stable to reset de-assertion.	<b>Yes</b>
	23	<b>Reserved, set to '0'</b>		<b>No</b>
	22:21	<b>APWROK Timing (APWROK_TIMING):</b>  00 = 2 ms 01 = 4 ms 10 = 8 ms 11 = 16 ms	This soft strap determines the time between the SLP_A# pin de-asserting and the APWROK timer expiration.	<b>Yes</b>
	20	<b>DeepSx Platform Configuration (DEEPSX_PLT_CFG_SS):</b>  0 = The platform does not support DeepSx. 1 = The platform supports DeepSx		<b>Yes</b>
	19	<b>Reserved, set to '0'</b>		<b>No</b>
	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.	<b>Yes</b>
	15:12	<b>Reserved, set to '0'</b>		<b>No</b>



Offset from 0	Bits	Description	Usage	FIT Visible
0x4C14h (cont)	11:10	<b>tPCH46 Timing:</b> 00 = 1 ms 01 = Reserved 10 = 5 ms 11 = 2 ms	tPch46: PROCPWRGD and SYS_PWROK high to SUS_STAT# deassertion. Refer to EDS for details.	Yes
	9:8	<b>tPCH45 Timing:</b> 00 = 100 ms 01 = 50 ms 10 = 5 ms 11 = 1 ms	tPCH45: PCH clock output stable to PROCPWRGD high. Refer to EDS for details.	Yes
	7:0	Reserved, set to '0x7c'		No

## 4.85 PMC Record 1 (UFS Flash Records)

Platform Setting Offset + C18h

Default Address: 4C18h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4C18h	31:8	Reserved, set to '0x200000'		No
	7	<b>Integrated Sensor Hub Supported:</b> 0 = Enable Integrated Sensor Hub 1 = Disable Integrated Sensor Hub		Yes
	6:1	Reserved, set to '0x4'		No
	0	Reserved, set to '0x1'		No

## 4.86 PMC Record 2 (UFS Flash Records)

Platform Setting Offset + C1Ch

Default Address: 4C1Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x4C1Ch	31:0	Reserved, set to '0x43CD7410'		No

## 4.87 PMC Record 3 (UFS Flash Records)

Platform Setting Offset + C20h

Default Address: 4C20h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4C20h	31:0	Reserved, set to '0x0'		No



## 4.88 PMC Record 4 (UFS Flash Records)

Platform Setting Offset + C24h

Default Address: 4C24h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4C24h	31:18	Reserved, set to '0x80'		No
	17	<b>SLP_S0# Tunnel (SLP_S0_TUNNEL_DIS):</b>  0 = SLP_S0# Tunnel enabled 1 = 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
	16:11	Reserved, set to '0'		No
	10:9	<b>OPI Link Voltage Strap (OPD_LVO_STRP):</b>  0x0 = 0.85 Volts 0x1 = 0.95 Volts 0x2 = 1.05 Volts	This strap must be configured when setting OPI Link Voltage strap ( <b>OPD_LVO</b> ).  <b>Note:</b> This strap and the OPI Link Voltage strap ( <b>OPD_LVO</b> ) must match the same voltage configuration setting for proper platform operation function.	Yes
	8	<b>OPI Link Speed Strap (OPDMI_STRP):</b>  0x0 = 2 / GT/s Link Speed 0x1 = 4 / GT/s Link Speed	This strap must be configured when setting OPI Link Speed strap ( <b>OPDMI_TLS</b> ).  <b>Note:</b> This strap and the OPI Link Speed strap ( <b>OPDMI_TLS_DMI</b> ) and ( <b>OPDMI_TLS_DMI</b> ) must match the same GT configuration setting for proper platform operation function.	Yes
	7:0	Reserved, set to '0'		No

## 4.89 PMC Record 5 (UFS Flash Records)

Platform Setting Offset + C28h

Default Address: 4C28h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4C28h	31	Reserved, set to '0'		No
	25	<b>Boot Media Sx Reset Policy:</b>  0 = BM_Reset# Asserted 1 = BM_Reset# Not Asserted	This setting determine that behavior of Boot Media Sx Reset.	Yes
	24	<b>Boot Media Second Reset Policy:</b>  0 = BM_Reset# Asserted 1 = BM_Reset# Not Asserted	This setting determine that behavior of Boot Media Second Reset.	Yes
	23:2	Reserved, set to '0'		No
	1:0	<b>I2C Communication Speed:</b>  1 = Standard 2 = Fast 3 = High Speed	This setting determines the communication speed over the I2C interface.	Yes



## 4.90 PMC Record 6 (UFS Flash Records)

Platform Setting Offset + C2Ch

Default Address: 4C2Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x4C2Ch	31:0	Reserved, set to '0'		No

## 4.91 PMC Record 7 (UFS Flash Records)

Platform Setting Offset + C30h

Default Address: 4C30h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4C30h	31:0	Reserved, set to '0'		No

## 4.92 PMC Record 8 (UFS Flash Records)

Platform Setting Offset + C34h

Default Address: 4C34h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4C34h	31:15	Reserved, set to '0'		No
	14:8	Reserved, set to '0x64'		No
	7:0	Reserved, set to '0'		No



## 4.93 CPU Record 0 (UFS Flash Records)

Platform Setting Offset + C38h

Default Address: 4C38h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4C38h	31:27	<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 0xBh</b>		No
	26:0	<b>Reserved, set to '0'</b>		No





## 4.94 CPU Record 1 (UFS Flash Records)

Platform Setting Offset + C3Ch

Default Address: 4C3Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x4C3Ch	31	<b>Reserved, set to '0x1'</b>		<b>No</b>
	30:16	<b>Reserved, set to '0'</b>		<b>No</b>
	17	<b>Encrypted Debug Enable:</b> 0 = 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>Yes</b>
	14:15	<b>Reserved, set to '0'</b>		<b>No</b>
	13	<b>JTAG Power Disable:</b> 0 = Disable JTAG Power for C10 and deeper states 1 = Enable JTAG Power for C10 and deeper states	This setting determines if JTAG power will be maintained on C10 or lower power states.  <b>Note:</b> This strap is intended for debugging purposed only.	<b>Yes</b>
	12	<b>Processor Boot Max Non-Turbo Frequency:</b> 0 = Disable Boot Non-Turbo Max Frequency 1 = Enable Boot Non-Turbo Max Frequency	This setting determines if the processor will operate at maximum Non-Turbo frequency at power-on and boot.  <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> 0 = Disable BIST at Reset 1 = Enable BIST at Reset	This setting determines if BIST will be run at platform reset after BIOS requested actions.  <b>Note:</b> This strap is intended for debugging purposed only.	<b>Yes</b>
	4:1	<b>Number of Active 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 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> 0 = Enable Hyper Threading 1 = 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>

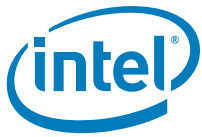


## 4.95 CPU Record 2 (UFS Flash Records)

Platform Setting Offset + C40h

Default Address: 4C40h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4C40h	31	<b>Platform IMON Disable:</b> '0x1'	<b>Note:</b> This strap should be left at the recommended default setting.	<b>Yes</b>
	30	<b>SVID Presence:</b> 0 = SVID is present 1 = No SVID is present	This setting determine if SVID rails are present on the platform. See Processor EDS for details.	<b>Yes</b>
	29	<b>VCC IN SVID VR Type:</b> 0 = VCC IN SVID VR Type SVID 1 = VCC IN SVID VR Type is fixed VR	This setting determines the VCC IN SVID VR. See Processor EDS for details.	<b>Yes</b>
	28:25	<b>VCC IN SVID VR Address:</b> '0'	This setting determines the VCC IN SVID VR Address for the platform.	<b>Yes</b>
	24:6	<b>Reserved, set to '0'</b>		<b>No</b>
	5	<b>VCCIN Aux Level LP</b> 0 = VCCIN Aux Level LP 1.8v 1 = VCCIN Aux Level LP 1.65v	This setting determines the VCCIN Aux Level LP voltage.  <b>Note:</b> Y based MCPs this setting can be configured to 1.65v. On all MCP types set to 1.8v.	<b>Yes</b>
	4	<b>VCC SFR OC PG Present:</b> 0 = VCC SFR OC PG Present 1 = VCC SFR OC PG Not Present	This setting determines if VCC SFR OC PG is present on the platform.	<b>Yes</b>
	3	<b>VCC ST PG Present:</b> 0 = VCC ST PG Present 1 = VCC ST PG Not Present	This setting determines if VCC ST PG is present on the platform	<b>Yes</b>
	2	<b>VCC STG PG Present:</b> 0 = VCC STG PG Present 1 = VCC STG PG Not Present	This setting determines the SA power plane topology. See Processor EDS for details.  <b>Note:</b> This strap should be left at the recommended default setting.	<b>Yes</b>
	1	<b>VDDQ TX Rail Supply:</b> 0 = Tied to VDDQ (1.1/1.2v) 1 = Tied to LP4x (0.6v)	This setting determines if the VDDQ TX Rail supply is tied to VDDQ or LP4x.	<b>Yes</b>
	0	<b>VCC Aux Present:</b> 0 = VCC Aux is not Present 1 = VCC Aux is Present	This setting determines if VCC Aux exists as a separate VR.	<b>Yes</b>



## 4.96 CPU Record 3 (UFS Flash Records)

Platform Setting Offset + C44h

Default Address: 4C44h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4C44h	31:0	Reserved, set to '0'		No



## 4.97 Intel® CSME Record 0 (UFS Flash Records)

Platform Setting Offset + C48h

Default Address: 4C48h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4C48h	31:20	Reserved, set to '0'		No
	19:18	<b>USB2 Port 10 DbC AFE Signal Strength:</b>  0x0 – Unused 0x1– Weak 0x2 – Medium 0x3 – Strong	This setting determines the DbC Analog Front End signal strength for USB2 port 10.	Yes
	17:16	<b>USB2 Port 9 DbC AFE Signal Strength:</b>  0x0 – Unused 0x1– Weak 0x2 – Medium 0x3 – Strong	This setting determines the DbC Analog Front End signal strength for USB2 port 9.	Yes
	15:14	<b>USB2 Port 8 DbC AFE Signal Strength:</b>  0x0 – Unused 0x1– Weak 0x2 – Medium 0x3 – Strong	This setting determines the DbC Analog Front End signal strength for USB2 port 8.	Yes
	13:12	<b>USB2 Port 7 DbC AFE Signal Strength:</b>  0x0 – Unused 0x1– Weak 0x2 – Medium 0x3 – Strong	This setting determines the DbC Analog Front End signal strength for USB2 port 7.	Yes
	11:10	<b>USB2 / USB3 Port 6 DbC AFE Signal Strength:</b>  0x0 – Unused 0x1– Weak 0x2 – Medium 0x3 – Strong	This setting determines the DbC Analog Front End signal strength for USB2 / USB3 port 6.	Yes
	9:8	<b>USB2 / USB3 Port 5 DbC AFE Signal Strength:</b>  0x0 – Unused 0x1– Weak 0x2 – Medium 0x3 – Strong	This setting determines the DbC Analog Front End signal strength for USB2 / USB3 port 5.	Yes



Offset from 0	Bits	Description	Usage	FIT Visible
0x4C48h (Cont)	7:6	<b>USB2 / USB3 Port 4 DbC AFE Signal Strength:</b>  0x0 – Unused 0x1– Weak 0x2 – Medium 0x3 – Strong	This setting determines the DbC Analog Front End signal strength for USB2 / USB3 port 4.	Yes
	5:4	<b>USB2 / USB3 Port 3 DbC AFE Signal Strength:</b>  0x0 – Unused 0x1– Weak 0x2 – Medium 0x3 – Strong	This setting determines the DbC Analog Front End signal strength for USB2 / USB3 port 3.	Yes
	3:2	<b>USB2 / USB3 Port 2 DbC AFE Signal Strength:</b>  0x0 – Unused 0x1– Weak 0x2 – Medium 0x3 – Strong	This setting determines the DbC Analog Front End signal strength for USB2 / USB3 port 2.	Yes
	1:0	<b>USB2 / USB3 Port 1 DbC AFE Signal Strength:</b>  0x0 – Unused 0x1– Weak 0x2 – Medium 0x3 – Strong	This setting determines the DbC Analog Front End signal strength for USB2 / USB3 port 1.	Yes



## 4.98 Intel® CSME Record 1 (UFS Flash Records)

Platform Setting Offset + C4Ch

Default Address: 4C4Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x4C4Ch	31:24	<b>Reserved, set to '0'</b>		<b>No</b>
	23:16	<b>Early USB DbC Intel® CSME Boot Stall Enable:</b> 0 = Intel® CSME Boot Stall not enabled 1 = Intel® CSME Boot Stall enabled	This setting enables a delay during Intel® CSME FW bring-up to allow USB DCI to be established and Early DbC arbitration to be granted.	<b>Yes</b>
	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.	<b>Yes</b>
	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.	<b>Yes</b>

