

Lake Field Client Platform

UFS Programming Guide

July 2019

Revision 1.0

Intel Confidential

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

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

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

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

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

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

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

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

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

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

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

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

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

Copyright © 2018, Intel Corporation. All rights reserved.

Contents

1	Introduction	8
1.1	Overview	8
1.2	Terminology	9
1.3	Reference Documents	9
2	UFS Flash Architecture	10
2.1	Introduction	10
2.2	Descriptor Mode	10
2.3	Boot Flow when booting from UFS NVM	10
2.4	Flash (NVM) Partitions and Regions	11
2.4.1	Flash Region Layout	12
2.4.2	Platform Settings	14
2.5	PCH UFS Flash Compatibility Requirements	16
2.5.1	Lakefield Firmware Requirements	16
3	Descriptor Overview	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
3.1.2	Flash Descriptor Component Section	22
3.1.3	Flash Descriptor Region Section	22
3.1.4	Flash Descriptor Master Section	23
3.1.5	PCH / CPU Softstraps	23
3.1.6	Descriptor Upper Map Section	23
3.1.6.1	FLUMAP1—Flash Upper Map 1 (Flash Descriptor Records)	23
3.1.6.2	IFWI / Intel® CSE ROM Bypass Size	23
3.1.6.3	MIP - Descriptor Table	23
3.1.7	Intel® CSE Vendor Specific Component Capabilities Table	24
3.2	OEM Section	24
3.3	Region Access Control	24
4	UFS PCH / PMC / CPU and Intel® CSE Configuration Section	35
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)	39
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)	40
4.15	PCH Record 14 (UFS Flash Records)	40
4.16	PCH Record 15 (UFS Flash Records)	41
4.17	PCH Record 16 (UFS Flash Records)	41
4.18	PCH Record 17 (UFS Flash Records)	41
4.19	PCH Record 18 (UFS Flash Records)	42
4.20	PCH Record 19 (UFS Flash Records)	43
4.21	PCH Record 20 (UFS Flash Records)	43
4.22	PCH Record 21 (UFS Flash Records)	44
4.23	PCH Record 22 (UFS Flash Records)	44
4.24	PCH Record 23 (UFS Flash Records)	44
4.25	PCH Record 24 (UFS Flash Records)	44
4.26	PCH Record 25 (UFS Flash Records)	44
4.27	PCH Record 26 (UFS Flash Records)	45
4.28	PCH Record 27 (UFS Flash Records)	45
4.29	PCH Record 28 (UFS Flash Records)	45
4.30	PCH Record 29 (UFS Flash Records)	45
4.31	PCH Record 30 (UFS Flash Records)	45
4.32	PCH Record 31 (UFS Flash Records)	46
4.33	PCH Record 32 (UFS Flash Records)	46
4.34	PCH Record 33 (UFS Flash Records)	46
4.35	PCH Record 34 (UFS Flash Records)	46
4.36	PCH Record 35 (UFS Flash Records)	47
4.37	PCH Record 36 (UFS Flash Records)	47
4.38	PCH Record 37 (UFS Flash Records)	47
4.39	PCH Record 38 (UFS Flash Records)	48
4.40	PCH Record 39 (UFS Flash Records)	48
4.41	PCH Record 40 (UFS Flash Records)	48
4.42	PCH Record 41 (UFS Flash Records)	48
4.43	PCH Record 42 (UFS Flash Records)	48
4.44	PCH Record 43 (UFS Flash Records)	49
4.45	PCH Record 44 (UFS Flash Records)	49
4.46	PCH Record 45 (UFS Flash Records)	49
4.47	PCH Record 46 (UFS Flash Records)	50
4.48	PCH Record 47 (UFS Flash Records)	50
4.49	PCH Record 48 (UFS Flash Records)	50
4.50	PCH Record 49 (UFS Flash Records)	50
4.51	PCH Record 50 (UFS Flash Records)	50
4.52	PCH Record 51 (UFS Flash Records)	51
4.53	PCH Record 52 (UFS Flash Records)	51
4.54	PCH Record 53 (UFS Flash Records)	51
4.55	PCH Record 54 (UFS Flash Records)	51
4.56	PCH Record 55 (UFS Flash Records)	51
4.57	PCH Record 56 (UFS Flash Records)	52
4.58	PCH Record 57 (UFS Flash Records)	52
4.59	PCH Record 58 (UFS Flash Records)	52
4.60	PCH Record 59 (UFS Flash Records)	53
4.61	PCH Record 60 (UFS Flash Records)	53
4.62	PCH Record 61 (UFS Flash Records)	53
4.63	PCH Record 62 (UFS Flash Records)	54
4.64	PCH Record 63 (UFS Flash Records)	55
4.65	PCH Record 64 (UFS Flash Records)	55
4.66	PCH Record 65 (UFS Flash Records)	55
4.67	PCH Record 66 (UFS Flash Records)	55

4.68	PCH Record 67 (UFS Flash Records).....	56
4.69	PCH Record 68 (UFS Flash Records).....	56
4.70	PCH Record 69 (UFS Flash Records).....	56
4.71	PCH Record 70 (UFS Flash Records).....	56
4.72	PCH Record 71 (UFS Flash Records).....	56
4.73	PCH Record 72 (UFS Flash Records).....	57
4.74	MIP Table Record 0 (UFS Flash Records).....	57
4.75	MIP Table Record 1 (UFS Flash Records).....	57
4.76	MIP Table Record 2 (UFS Flash Records).....	57
4.77	MIP Table Record 3 (UFS Flash Records).....	58
4.78	MIP Table Record 4 (UFS Flash Records).....	58
4.79	MIP Table Record 5 (UFS Flash Records).....	58
4.80	MIP Table Record 6 (UFS Flash Records).....	58
4.81	MIP Table Record 7 (UFS Flash Records).....	59
4.82	MIP Table Record 8 (UFS Flash Records).....	59
4.83	MIP Table Record 9 (UFS Flash Records).....	59
4.84	PMC Record 0 (UFS Flash Records)	60
4.85	PMC Record 1 (UFS Flash Records)	62
4.86	PMC Record 2 (UFS Flash Records)	62
4.87	PMC Record 3 (UFS Flash Records)	62
4.88	PMC Record 4 (UFS Flash Records)	63
4.89	PMC Record 5 (UFS Flash Records)	63
4.90	PMC Record 6 (UFS Flash Records)	63
4.91	PMC Record 7 (UFS Flash Records)	64
4.92	PMC Record 8 (UFS Flash Records)	64
4.93	CPU Record 0 (UFS Flash Records).....	65
4.94	CPU Record 1 (UFS Flash Records).....	66
4.95	CPU Record 2 (UFS Flash Records).....	67
4.96	CPU Record 3 (UFS Flash Records).....	68
4.97	Intel® CSE Record 0 (UFS Flash Records)	69
4.98	Intel® CSE Record 1 (UFS Flash Records)	70

Figures

2-1 Booting from UFS high level flow11

2-2 UFS Boot Partition Layout15

3-1 Flash Descriptor (Lakefield PCH)18

Tables

1-1 Terminology 9

1-2 Reference Documents 9

2-1 Lakefield UFS Partitions11

2-2 UFS Logical Partitions.....12

2-3 BPDT Header13

Revision History

Revision Number	Description	Revision Date
0.5	<ul style="list-style-type: none">Initial Release Based on 04h RDL	February 2018
0.6	<ul style="list-style-type: none">Updated MIP Table information	March 2018
0.7	<ul style="list-style-type: none">Align revision number	April 2018
0.8	<ul style="list-style-type: none">Added RPMB details in chapter 2	September 2018
0.81	<ul style="list-style-type: none">Added FLMAP3	October 2018
0.82	<ul style="list-style-type: none">Updated Intel® CSE references	December 2018
0.83	<ul style="list-style-type: none">Added Lakefield PCH UFS Flash Compatibility Requirements	February 2019
1.0	<ul style="list-style-type: none">Updated the introductionUpdated LKF FW requirementsAdded details for more flash regionsremoved FPBAupdated PCH record details	July 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 Lakefield processor only.

[Chapter 2, “UFS Flash Architecture”](#)

- Overview of UFS flash, Descriptor, Flash Layout and compatibility requirements for Lakefield products.

[Chapter 3, “Descriptor Overview”](#)

- Overview of the descriptor and Descriptor record definition

[Chapter 4, “UFS PCH / PMC / CPU and Intel® CSE 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
Lakefield PCH	Lakefield Platform Integrated I/O
Intel® Converged Security Engine Firmware (Intel® CSE 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>Lakefield 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® CSE 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® CSE 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® CSE 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.

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.

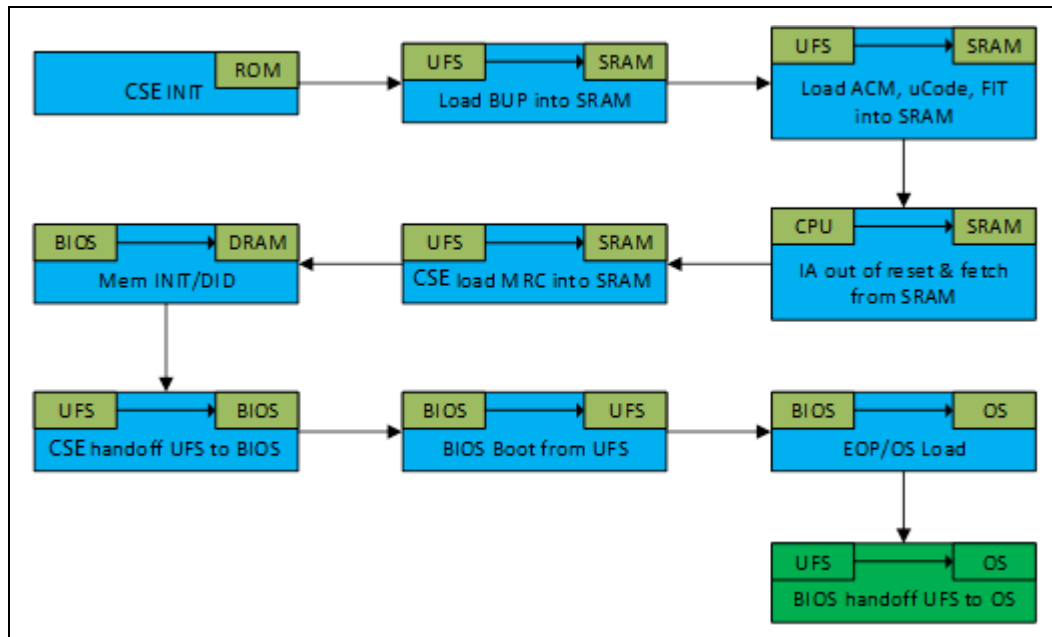
2.3 Boot Flow when booting from UFS NVM

This chapter provides high level overview of general platform boot from UFS.

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

Since UFS controller is single headed, only one master can access the UFS NVM. On Lakefield platform Intel®CSE, OS and BIOS require UFS NVM access during boot and during run time. Intel®CSE have access to UFS NVM when platform comes out of reset. Once DRAM is initialized, UFS NVM access is transferred to BIOS. Intel®CSE 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 Intel®CSE 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_User-Guide for more detail.

Please see partitioning recommendation in the table below:

Table 2-1. Lakefield UFS Partitions

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



Partition	Size	Use	Comments
RPMB	4MB	Replay protected partition: Provisioned by Intel®CSE and used for Intel®CSE file system, PTT storage and UEFI variable storage	Vendor created - Provisioned with platform specific key by Intel®CSE 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®CSE code and data. This is unlike SPI, which prevents host SW from accessing Intel®CSE code and data, assuming the flash descriptor is programmed correctly.

At the EOM:

- Intel®CSE will derive a key unique to the chipset and program this key into UFS.
- After provisioning of the key is done, Intel®CSE will initiate data migration from Temp Data Partition (LUN6) into RPMB partition. Once migration is done, Intel®CSE 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®CSE 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
RPMB/LBP5	Block settings Descriptor
LBP4	BIOS Region/Non Fault Tolerant Region/OBB
LBP3	IUP – Independent Updatable Partitions
LBP2/1	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	

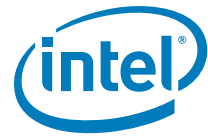
2.4.1 Flash Region Layout

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
Signature	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").
Descriptor Count	4	2	Number of BPDT entries following this header
Version	6	1	Version of this BPDT structure. '1' - Layout 2.0 and 1.6 '2' - Layout 1.7
BPDT Configuration	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
CRC32 Checksum	8	4	CRC32 checksum of entire BPDT structure (Header and Entries)
IFWI Version	12	4	Version of the particular IFWI build as marked by the build server
Intel® FIT tool version	16	8	Major/Minor/Build/Hotfix version of the Intel® FIT tool that was used to stitch the image. Not used by firmware

Lakefield 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®CSE will take BPDT address and subtract Top Swap size to find it.

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



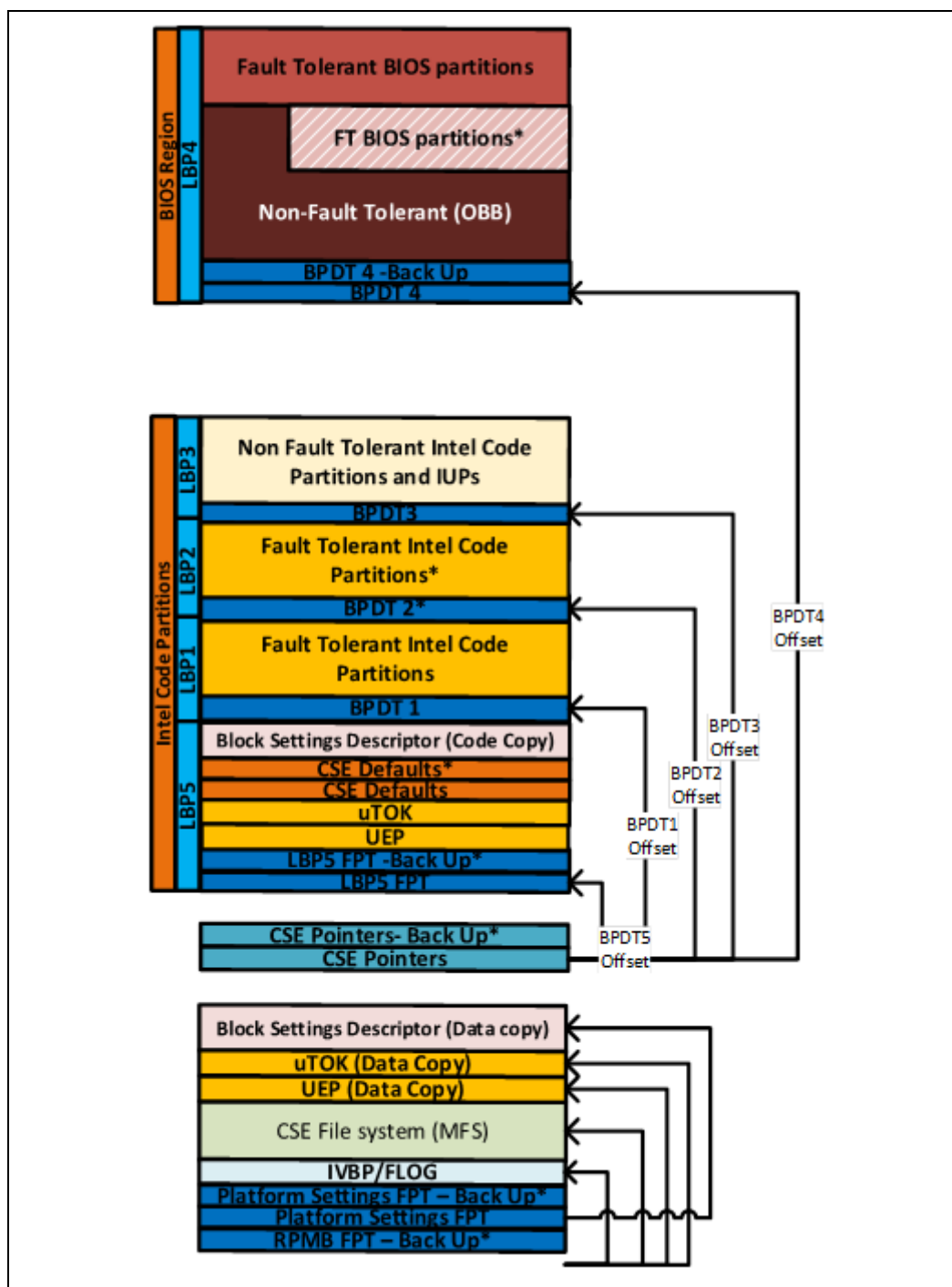
2.4.2 Platform Settings

The same SPI Flash descriptor structure will be used on UFS NVM with the structure maintained under LBP5. On 1st boot, Intel®CSE 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 Lakefield Firmware Requirements

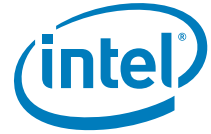
The user shall configure the logical units of the UFS device according to the following guidelines:

- 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®CSE needs.
- LUN6 should be reserved for temporary data storage. Data will be stored in LUN6 until after EOM. At EOM, Intel®CSE will perform binding between PCH and UFS after which data will be located at RPMB.
- RPMB size should at least accommodate Intel®CSE and BIOS needs for storage (RPMB for example could be as small as 128KB while Intel®CSE 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 Lakefield 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.



3 Descriptor Overview

The same SPI Flash descriptor structure will be used on UFS NVM with the structure maintained under LBP5. On 1st boot, Intel®CSE will pull this platform settings structure to LUN6 and then at EOM to RPMB, in order to provide the same security bar as SPI flash w/o a need for signing.

Descriptor settings that on SPI based platforms are consumed directly by SPI controller, such as SPI region map, master access control, SPI descriptor validity marker, SPI SFDP table, etc. are not used when in UFS. In UFS image those settings will be set by Intel®FIT to default values.

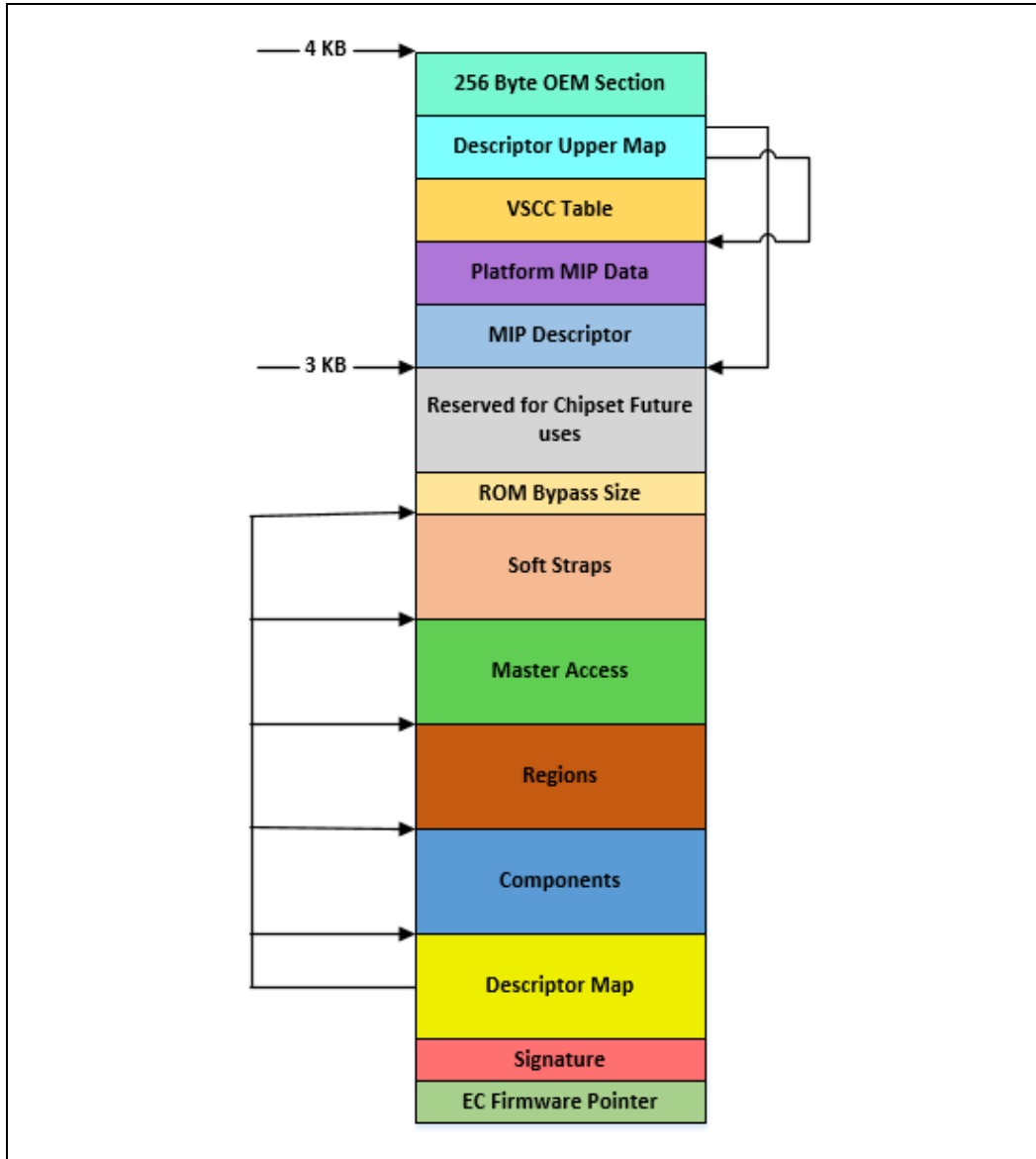
OEM Signature and Soft straps will be in the same location as on SPI. Signing and Soft straps will be identical for UFS and SPI.

On platforms with SPI boot media, the Descriptor defines the layout of the flash as well as configuration parameters for the PCH, while with UFS it contains only the configuration data.

The maximum size of the Flash Descriptor is 4 K Bytes, this is maintained the same as in SPI.



Figure 3-1. Flash Descriptor (Lakefield PCH)



- EC Firmware Pointer is not present in UFS.
- The Flash signature at the bottom of the flash (offset 10h) must be 0FF0A55Ah in order to be in Descriptor mode. Maintained for UFS same as for SPI.
- The Descriptor map has pointers to the descriptor sections as well as the size of each. Maintained for UFS same as for SPI.
- The Component section is not present in UFS.
- The Region section is not present in UFS.
- The Master region is not present in UFS.
- PCH chipset soft strap sections contain PCH configurable parameters. Maintained for UFS same as for SPI.



- The Reserved region is for future chipset usage.
- The Descriptor Upper Map determines the length and base address of the Intel® CSE VSCC Table and the MIP Descriptor. Maintained for UFS same as for SPI.
- The Intel® CSE VSCC Table is not present in UFS.
- Platform MIP data contains actual MIP strap information for PMC, CPU and Intel® CSE.
- OEM Section is 256 Byte section reserved at the top of the Flash Descriptor for use by the OEM. Maintained for UFS same as for SPI.

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.

On platforms with UFS boot media, Descriptor base address is known to Intel® CSE from Flash Partitioning Table (FPT) of Data partition (LBP5 / LUN6 / RPMB)

Recommended flash descriptor map:

Region Name	Starting Address Offset
Signature	0x10
Component FCBA	0x30
Regions FRBA	0x40
Masters FMBA	0x80
PCH Straps FPSBA	0x100
MDTBA	0xC00
PMC Straps	0xC14
CPU Straps	0xC38
Intel® CSE Straps	0xC48
Register Init FIBA	0x340



3.1.1 Descriptor Signature and Map

3.1.1.1 FLVALSIG - Flash Valid Signature (Flash Descriptor Records)

Memory Address: Base Descriptor Address in Data Partition + 010h

Size: 32 bits

Recommended Value: 0FF0A55Ah

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

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

Memory Address: Base Descriptor Address in Data Partition + 014h

Size: 32 bits

Bits	Description	Present in UFS
31:27	Reserved	Yes
26:24	Reserved	Yes
23:16	Flash Region Base Address (FRBA). This identifies address bits [11:4] for the Region portion of the Flash Descriptor. Bits [24:12] and bits [3:0] are 0. Set this value to 04h. This will define FRBA as 40h.	Yes
15:13	Reserved	Yes
12	Fingerprint sensor on shared flash/TPM SPI bus 0 = No fingerprint sensor is connected to CS1 1 = Fingerprint sensor is connected to CS1 and acting as a flash device Note: Hardware does not use this field. This value must be read directly from flash. It's not available via Host FDOC/FDOD registers.	Yes
11	Touch on dedicated SPI bus 0 = No Touch device is connected to the dedicated Touch SPI bus 1 = Touch device is connected to the dedicated Touch SPI bus Note: Hardware does not use this field. This value must be read directly from flash. It's not available via Host FDOC/FDOD registers.	Yes
10	Touch on shared flash/TPM SPI bus 0 = No Touch device is connected to CS1 1 = Touch device is connected to CS1 and acting as a flash device Note: Hardware does not use this field. This value must be read directly from flash. It's not available via Host FDOC/FDOD registers.	Yes



Bits	Description	Present in UFS
9:8	<p>Number Of Components (NC). 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>Note: With the introduction of DnX mode support, the flash controller ignores this descriptor field. It determines the number of attached flash components by virtue of SFDP discovery. Software may still use this field, therefore it must be properly initialized.</p>	Yes
7:0	<p>Flash Component Base Address (FCBA). This identifies address bits [11:4] for the Component portion of the Flash Descriptor. Bits [24:12] and bits [3:0] are 0.</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: Base Descriptor Address in Data Partition + 018h

Size: 32 bits

Bits	Description	Present in UFS
31:24	PCH Strap Length (PSL). Identifies the 1s based number of Dwords of PCH Straps to be read, up to 255 DWs (1KB) max. A setting of all 0's indicates there are no PCH DW straps. This field MUST be set to 55h	Yes
23:16	Flash PCH Strap Base Address (FPSBA). This identifies address bits [11:4] for the PCH Strap portion of the Flash Descriptor. Bits [24:12] and bits [3:0] are 0. Set this field to 10h. This will define FPSBA to 100h	Yes
15:11	Reserved	Yes
10:8	Number Of Masters (NM). This field identifies the total number of Flash Masters. Note: This field is not used by the Flash Controller.	Yes
7:0	Flash Master Base Address (FMBA). This identifies address bits [11:4] for the Master portion of the Flash Descriptor. Bits [24:12] and bits [3:0] are 0. Set this field to 08h. This will define FMBA as 80h	Yes

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

Memory Address: Base Descriptor Address in Data Partition + 01Ch

Size: 32 bits

Bits	Description	Present in UFS
31:0	Reserved	Yes

3.1.2 Flash Descriptor Component Section

This section of the Flash Descriptor is used to identify the different SPI Flash Components and their capabilities. Not present in UFS.

3.1.3 Flash Descriptor Region Section

This section of the Flash Descriptor is used to identify the different Regions of the NVM image on the SPI flash. Not present in UFS.



3.1.4 Flash Descriptor Master Section

This section of the Flash Descriptor is used to identify hardware security settings for the flash, granting read/write permissions for each region and identifying each master. Not present in UFS.

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 Intel® CSE to find SPI VSCC information and MIP data.

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

Memory Address: Base Descriptor Address in Data Partition + EFCh

Size: 32 bits

Bits	Default	Description	Present in UFS
31:16	0xC1	MIP Descriptor Table Base Address (MDTBA) . This identifies base address bits [11:4] for the Platform Configuration Data Structure in the Flash Descriptor Bits [26:12] and bits [3:0] are 0.	Yes
23:16	0xFF	Reserved	Yes
15:8	0x1	Intel® CSE VSCC Table Length (VTL) . Identifies the 1s based number of DWORDS contained in the VSCC Table. Each SPI component entry in the table is 2 DWORDS long. Max recommended is 10 entries to allow for room for Platform Configuration Data (MIP)	Yes
7:0	0x1	Intel® CSE VSCC Table Base Address (VTBA) . This identifies address bits [11:4] for the VSCC Table portion of the Flash Descriptor. Bits [26:12] and bits [3:0] are 0.	Yes

3.1.6.2 IFWI / Intel® CSE ROM Bypass Size

Memory Address: Base Descriptor Address in Data Partition + C00h

Size: 32 bits

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

3.1.6.3 MIP - Descriptor Table

Memory Address: Base Descriptor Address in Data Partition + MDTBA

Name	Offset	Size (bytes)	Description	Present in UFS
Number of Descriptors	0x0	2	Number of MIP blocks ('n') inside this MIP structure	Yes



Name	Offset	Size (bytes)	Description	Present in UFS
Size of MIP	0x2	2	Size, in bytes, of this MIP structure (including the MDT structure)	Yes
Block 0 Type	0x4	2	Type of block 0. Can be one of the following: 0 = CSE (USB 2 PHY Configuration) 1 = PMC Soft Straps 2 = Reserved Note: In order to simplify handling a new block type can be defined for each usage	Yes
Block 0 Offset	0x6	2	Offset of block 0	Yes
Block 0 Length	0x8	2	Length of block 0 in bytes	Yes
Block 0 Reserved	0xA	2	Must be 0	Yes
Block 1 Type	0xC	2	See Block 0 type	Yes
Block 1 Offset	0xE	2	Offset of block 1	Yes
Block 1 Length	0x10	2	Length of block 1 in bytes	Yes
Block 1 Reserved	0x12	2	Must be 0	Yes
.....				Yes
Block 'n' Type		2	See Block 0 type	Yes
Block 'n' Offset		2	Offset of block 'n'	Yes
Block 'n' Length		2	Length of block 'n' in bytes	Yes
Block 'n' Reserved		2	Must be 0	Yes

3.1.7 Intel® CSE Vendor Specific Component Capabilities Table

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

This part of the descriptor is not present in UFS.

3.2 OEM Section

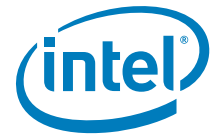
Memory Address: F00h

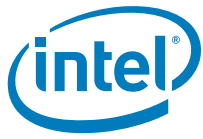
Size: 256 Bytes

256 Bytes are reserved at the top of the Flash Descriptor for use by the OEM. The 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.







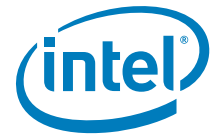


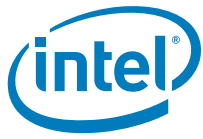














4 UFS PCH / PMC / CPU and Intel® CSE Configuration Section

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 '0x4'		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 '0'		No
	6:4	OPI Link Width (OPDMI_LW): 0x0 = 1 Lane 0x1 = 2 Lanes 0x2 = 4 Lanes 0x3 = 8 Lanes	This setting configures the OPI Link Width. For further details see the Ice Lake PCH EDS. Note: This strap and OPI Link Width (OPDMI_LW_DMI) must match the same lane configuration for proper platform operation.	Yes
	3:0	OPI Link Speed (OPDMI_TLS): 0x2 = 2 GT/s Link Speed 0x3 = 4 GT/s Link Speed	This strap must be configured when setting OPI Link Speed Strap (OPDMI_STRP). Note: This strap and the OPI Link Speed Strap (OPDMI_STRP) and (OPDMI_TLS_DMI) 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
0x4104	7:3	Reserved, set to '0'		No
	1	XHCI Port 2 Ownership Strap (XHC_PORT2_OWNERSHIP_STRAP): Strap to decide XHCI Port 2 Ownership between XHCI/PCIe/CSI. 0x0 = XHC Port 2 configured as XHC 0x1 = XHC Port 2 configured as Non-XHC	This strap must also be configured when setting the USB3 / PCIe Combo Port 1 (FIA/LOSL1) . Note: When USB3 / PCIe Combo Port 1 (FIA/LOSL1) configured as USB3 this setting needs to be set to 0x0. When USB3 / PCIe Combo Port 1 (FIA/LOSL1) is configured as PCIe this setting needs to be set to 0x1.	Yes
	0	XHCI Port 1 Ownership Strap (XHC_PORT1_OWNERSHIP_STRAP): Strap to decide XHCI Port 1 Ownership between XHCI/PCIe/CSI. 0x0 = XHC Port 1 configured as XHC 0x1 = XHC Port 1 configured as Non-XHC	This strap must also be configured when setting the USB3 / PCIe Combo Port 0 (FIA/LOSL0). Note: When USB3 / PCIe Combo Port 0 (FIA/LOSL0) configured as USB3 this setting needs to be set to 0x0. When USB3 / PCIe Combo Port 0 (FIA/LOSL0) is configured as PCIe this setting needs to be set to 0x1.	Yes

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	USB3 Port 2 Speed Select: 0 = Port 2 is configured as USB3.1 Gen2 1 = Port 2 is configured as USB3.1 Gen1	This setting determines the USB3 Port 2 speed capabilities.	Yes
	0	USB3 Port 1 Speed Select: 0 = Port 1 is configured as USB3.1 Gen2 1 = Port 1 is configured as USB3.1 Gen1	This setting determines the USB3 Port 1 speed capabilities.	Yes

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	Reserved, set to '0'		No
	1	USB3 Port 2 Initialization Speed Select: 0 = Port 2 will boot as USB 3.1 Gen1 and carry on LBPM if USB 3.1 Gen2 is enabled 1 = Port 2 will boot as USB 3.1 Gen2 and skip LBPM	This setting determines USB3 Port 2 speed during platform power-up.	Yes
	0	USB3 Port 1 Initialization Speed Select: 0 = Port 1 will boot as USB 3.1 Gen1 and carry on LBPM if USB 3.1 Gen2 is enabled 1 = Port 1 will boot as USB 3.1 Gen2 and skip LBPM	This setting determines USB3 Port 1 speed during platform power-up.	Yes

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	USB3 Port 2 Connector Type Select: 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. Note: This Strap and USB3 Port 2 Connector Type Select Aux must match for proper operation.	Yes
	3:0	USB3 Port 1 Connector Type Select: 0x0 = USB Port 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. Note: This Strap and USB3 Port 1 Connector Type Select Aux must match for proper operation.	Yes

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	USB2 Port 2 Connector Type Select: 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	USB2 Port 1 Connector Type Select: 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	Reserved, set to '0'		No
	0	USB Type AB mode Select: 0 = USB Type AB connector switches based on SW event 1 = USB Type AB connector switches based on HW event	This setting configures the mode for the USB Type AB connector.	Yes

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	Reserved, set to '0'		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 '0xff'		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	Top Swap Block size (TSBS): 000 = 64 KB. Invert A16 if Top Swap is enabled 001 = 128 KB. Invert A17 if Top Swap is enabled 010 = 256 KB. Invert A18 if Top Swap is enabled 011 = 512 KB. Invert A19 if Top Swap is enabled 100 = 1 MB. Invert A20 if Top Swap is enabled 101 - 111: Reserved. Notes: 1. This setting is dependent on BIOS architecture and can be different per design. The BIOS developer for the target platform has to determine this value. 2. If FWH is set as Boot BIOS destination then PCH only supports 64 KB Top Swap block size. This value has to be determined by how BIOS implements Boot-Block. 3. Intel Client chipset supports top swap block size of up to 256 KB. TS block sizes of greater than 256KB are not supported.	This allows for the system to use alternate code in order to boot a platform based upon the Top Swap (GPIO66/SDIO_D0 pulled low during the rising edge of PWROK .) strap being asserted. Top Swap inverts an address on access to SPI and firmware hub, so the processor fetches the alternate Top Swap block instead of the original boot-block. The size of the Top Swap block and setting of this field must be determined by the BIOS developer. If this is not set correctly, then BIOS boot-block recovery mechanism will not work. Note: This setting is not the same for all designs, is dependent on the architecture of BIOS. The setting of this field must be determined by the BIOS developer.	Yes
	3:0	Reserved, set to '0'		No



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 '0x7'		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 '0x80'		No

4.18 PCH Record 17 (UFS Flash Records)

Platform Setting Offset + 117h

Default Address: 4117h



Offset from 0	Bits	Description	Usage	FIT Visible
0x4117	7:6	SPI Maximum write and erase Resume to Suspend intervals: 0x0 = 128us 0x1 = 256us 0x2 = 512us 0x3 = No Ceiling	This setting specifies the maximum value for the write and erase Resume to Suspend intervals.	Yes
	5	SPI Out of Order operation Enable: 0 = Out or Order operation Enabled 1 = Out of Order operation Disabled	When this setting is enabled priority operations may be issued while waiting for write / erase operations to complete on the flash device. When this setting is disabled all write / erase type operations in order.	Yes
	4	SPI Suspend / Resume Enable: 0 = Enable suspend / resume 1 = Disable suspend / resume	When this setting is enabled writes and erases may be suspended to allow a read to be issued on the flash device. When this setting is disabled no transaction will be allowed to the busy flash device.	Yes
	3:1	SPI Resume Holdoff Delay: 0x0 = 0us 0x1 = 2us 0x2 = 4us 0x3 = 6us 0x4 = 8us 0x5 = 10us 0x6 = 12us 0x7 = 14us	Specifies the time after the completion of a pri_op before the flash controller sends the resume instruction. If a new pri_op is eligible to be issued prior to the end of this delay time then the pri_op is issued and the timer is re-initialized to tRHD. 3-bit field encodes count with range 0-7. tRHD = count * 2us.	Yes
0x4117 (Cont)	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
0x4118	7	Reserved, set to '0'		No
	6:4	Intel® Precise Touch and Stylus Controller 1 Maximum Frequency (TMF): 000 = 120MHz 001 = 60MHz 010 = 48MHz 011 = Reserved 100 = 30 MHz 101 = Reserved 110 = 17 MHz 111 = Reserved Note: The listed frequencies are approximate.	This field allows the OEM to set an upper limit on the frequency for Touch transactions on Intel® Precise Touch and Stylus Controller 1. Intel® CSE firmware will use the value in this field along with data from the Touch device's capability register to program the Intel® Precise Touch and Stylus Controller 1 Configuration Register.	Yes
	3:0	SPI Idle to Deep Power Down Timeout: Set to '0x5'	SPI Idle to Deep Power Down Timeout Default Specifies the time in microseconds that the Flash Controller waits after all activity is idle before commanding the flash devices to Deep Powerdown, time = 2^N microseconds	Yes

4.20 PCH Record 19 (UFS Flash Records)

Platform Setting Offset + 119h

Default Address: 4119h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4119	7:3	Reserved, set to '0x10'		No
	2:0	SPI TPM Clock Frequency (STCF): This field is defined with a broad range to support both SOC and PCH implementations. The listed frequencies are approximate. 000 = Reserved 001 = Reserved 010 = 48MHz 011 = Reserved 100 = 30 MHz 101 = Reserved 110 = 17 MHz 111 = reserved Notes: This field identifies the serial clock frequency for TPM on SPI. This field is undefined if the TPM on SPI is disabled either by soft-strap or fuse.		Yes

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 '0x34'		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	Global Protected Range Default (GPRD): Set to '0x0'	Sets the default value of the GPR0 register in the SPI Flash Controller.	Yes

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 '0x20'		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 '0x7'		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 '0x40'		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 '0x3'		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 '0x1'		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 '0x80'		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 '0x3'		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 '0x3'		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	PCIe Controller 1 (Port 1-4): Straps to set the default value of the PCI Express Port Configuration 1 register covering PCIe ports 1-4. 00 = 4x1 01 = 1x2, 2x1 10 = 2x2 11 = 1x4 NOTE: Refer to EDS for PCIe supported port configurations.	Setting of this field depend on what PCIe ports 1-4 configurations are desired by the board manufacturer. NOTE: This field must be determined by the PCI Express port requirements of the design. The platform hardware designer must determine this setting.	Yes
	2	PCIe Controller 1 Lane Reversal: 0 = PCIe Lanes are not reversed. 1 = PCIe Lanes are reversed. Note: 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. Note: This setting is dependent on the board design. The platform hardware designer must determine if this port needs lane reversal.	Yes
	1:0	Reserved, set to '0'		No

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	PCIe Controller 2 (Port 5-8): 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 NOTE: Refer to EDS for PCIe supported port configurations.	Setting of this field depend on what PCIe ports 5-8 configurations are desired by the board manufacturer. NOTE: This field must be determined by the PCI Express port requirements of the design. The platform hardware designer must determine this setting.	Yes
	2	PCIe Controller 2 Lane Reversal: 0 = PCIe Lanes are not reversed. 1 = PCIe Lanes are reversed. Note: Refer to EDS supported Lane reversal configuration.	This bit controls lane reversal behavior for PCIe Controller 2. PCI Express port lane reversal can be done to aid in the laying out of the board. Note: This setting is dependent on the board design. The platform hardware designer must determine if this port needs lane reversal.	Yes
	1:0	Reserved, set to '0'		No

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 + 141h

Default Address: 4141h



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 + 142h

Default Address: 4142h

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 + 143h

Default Address: 4143h

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 + 144h

Default Address: 4144h

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 + 145h

Default Address: 4145h

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 + 146h

Default Address: 4146h



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 + 147h

Default Address: 4147h

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 + 148h

Default Address: 4148h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4148h	7:0	Reserved, set to '0xf0'		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	OPI Link Width (OPDMI_LW_DMI): 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. Note: This strap and OPI Link Width (OPDMI_LW) must match the same lane configuration for proper platform operation.	Yes
	3:0	OPI Link Speed (OPDMI_TLS_DMI): 0x2 = 2 GT/s Link Speed 0x3 = 4 GT/s Link Speed	This strap must be configured when setting OPI Link Speed Strap (OPDMI_STRP). Note: This strap and the OPI Link Speed Strap (OPDMI_STRP) and (OPDMI_TLS) 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 + 14Ah

Default Address: 414Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0x414Ah	7:0	Reserved, set to '0x4'		No

4.61 PCH Record 60 (UFS Flash Records)

Platform Setting Offset + 14Bh

Default Address: 414Bh

Offset from 0	Bits	Description	Usage	FIT Visible
0x414B	7:6	Reserved, set to '0x3'		No
	5:3	Reserved, set to '0'		No
	2:1	OPI Link Voltage (OPD_LVO): 0 = 0.95 Volts 1 = 0.85 Volts 2 = 1.05 Volts	This strap must be configured when setting OPI Link Speed strap (OPD_LVO_STRP). Note: This strap and the OPI Link Speed strap (OPD_LVO_STRP) must match the same voltage configuration setting for proper platform operation function. This setting configures the OPI Link Voltage. For further details see Ice Lake PCH EDS.	Yes
	0	Reserved, set to '0'		No

4.62 PCH Record 61 (UFS Flash Records)

Platform Setting Offset + 14Ch

Default Address: 414Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x414Ch	31	Reserved, set to '0x1'		No
	30	Intel® Trace Hub Soft Enable: 0 = ROM Tracing Soft Disable 1 = ROM Tracing Soft Enable	This soft strap enables ROM based tracing in the CSE. Note: Only applicable if Intel® Trace Hub Debug Messages strap is also enabled	Yes
	29:22	Reserved, set to '0'		
	21	Intel® Trace Hub - Emergency Mode: 0 = ROM Tracing Emergency mode disabled 1 = ROM Tracing Emergency mode enabled	This option enables ROM Tracing in the base platform image.	Yes



Offset from 0	Bits	Description	Usage	FIT Visible
0x414Ch (Cont)	20	Deep Sx Enable (Deep_SX_EN): 0 = Deep Sx is not supported on the platform 1 = Deep Sx is supported on the platform	This requires the target platform to support Deep Sx state Note: When configuring Deep Sx you must also set DEEPSX_PLT_CFG_SS .	Yes
	19:18	Reserved, set to '0'		No
	17	Direct Connect Interface (DCI) Enabled: 0 = DCI Disabled 1 = DCI Enabled		Yes
	16	Reserved, set to '0'		Yes
	15:12	Reserved, set to '0'		No
	11	Intel® CSE AFS Flash Idle Reclaim Enable: 0 = AFS Flash Reclaim enabled 1 = AFS Flash Reclaim disabled	This controls enabling / disabling of Intel® CSE AFS Idle flash reclaim capabilities. Note: This setting should be used for debug purposes only	Yes
	10	Intel® CSE Reset Behavior: 0 = Intel® CSE will attempt to boot from the next available image, if it exists 1 = Intel® CSE will halt		
	9:1	Reserved, set to '0'		No
	0	Firmware ROM Bypass Enable Softstrap: 0 = ROM Bypass disabled 1 = ROM Bypass enabled	Firmware ROM Bypass Enable Softstrap.	Yes

4.63 PCH Record 62 (UFS Flash Records)

Platform Setting Offset + 150h

Default Address: 4150h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4150h	7:5	Reserved, set to '0'		No
	4	DCI BSSB over USB3 Port2 Configuration (EXI_PTSS_PORT4): 0 = BSSB is enabled on USB3 Port2 1 = BSSB is disabled on USB3 Port2	This setting determines if the USB port being used for DCI operations has BSSB (Boundary Scan Side Band) enabled. Note: For S0ix and reset flows BSSB should be enabled.	Yes
	3	Reserved, set to '0'		No
	2	DCI BSSB over GPIO Configuration (EXI_PTSS_PORT2): 0 = BSSB is enabled over GPIO 1 = BSSB is disabled over GPIO	This setting enables BSSB (Boundary Scan Side Band) over GPIO for DCI operations. Note: If this setting is enabled the DCI Port1 Configuration also needs to be enabled. Note: For S0ix and reset flows BSSB should be enabled.	Yes
	1	Reserved, set to '0'		No



Offset from 0	Bits	Description	Usage	FIT Visible
0x4150h (Cont)	0	DCI BSSB over USB3 Port1 Configuration (EX1_PTSS_PORT0): 0 = BSSB is enabled on USB3 Port1 1 = BSSB is disabled on USB3 Port1	This setting determines if the USB port being used for DCI operations has BSSB (Boundary Scan Side Band) enabled. Note: For S0ix and reset flows BSSB should be enabled.	Yes

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	Reserved, set to '0'		No

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	Reserved, set to '0'		No

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 '0x7'		No

4.70 PCH Record 69 (UFS Flash Records)

Platform Setting Offset + 157h

Default Address: 4157h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4157	7:0	Reserved, set to '0x68'		No

4.71 PCH Record 70 (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 71 (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 72 (UFS Flash Records)

Platform Setting Offset + 160h

Default Address: 4160h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4160	7:2	Reserved, set to '0'		No
	1	BIOS Guard protection override enable (LPC/spi_strap_prr_ts_ovr): 0 = BIOS Guard Fault Tolerant Update Capability is disabled 1 = BIOS guard Fault Tolerant Update Capability is enabled	This setting allows BIOS Guard to bypass the SPI Flash controller protections such as protected range registers and top swap. Note: For further details please review Intel® Platform Protection Technology with BIOS Guard 2.0 BIOS Specification regarding Fault Tolerant Update (FTU).	Yes
	0	TPM Over SPI Bus Enabled (TOS): 0 = TPM is not on SPI 1 = TPM is on SPI	This field identifies the frequency that should be used with the TPM on SPI. This field is undefined if the TPM on SPI is disabled by softstrap	Yes

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	Number of MIP Table Descriptor Entries: Set to '0x2'	This setting determines the total number of MIP Table Descriptor entries present in the SPI image.	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	Size of MIP Descriptor Entry: Set to '0x50'	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	MIP Descriptor Block 0: Set to '0x1'	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	MIP Descriptor Block 0 Offset: Set to '0x14h'	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	MIP Descriptor Block 0 Length: Set to '0x34h'	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	MIP Descriptor Block 1 Type: 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	MIP Descriptor Block 1 Offset: 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	MIP Descriptor Block 1 Length: Set to '0x8h'	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	Reserved, set to '0'		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	Reserved, set to '0'		No
	27	Intel® Trace Hub Debug Messages Enable: 0 = PCH Tracing debug messages Disabled 1 = PCH Tracing debug messages Enabled	This setting enables debug messages on the Intel® Trace Hub. Note: You will also need to set the Intel® Trace Hub Soft Enable to "Enabled"	Yes
	26	Reserved, set to '0'		No
	25	Power Reporting Enable (THERM_PWR_REP_DIS): 0 = Power Reporting is enabled. 1 = Power Reporting is completely disabled, regardless of the settings in the Thermal Power Reporting configuration registers. Note: When this setting is disabled the once-per-second timer interrupt associated with this feature must not be turned on.	This bit, when set, causes the PMC FW to completely turn off the Power Reporting feature. Note: A once-per-second timer interrupt is enabled which triggers firmware to report power and temperature information as enabled by configuration registers.	Yes
	24	PCIe* Power Stable Timer (tPCH33 timer): 0 = tPCH33 timer is disabled 1 = PCH will count 99ms from PWROK assertion before PLTRST# is de-asserted.	Board dependent. Default is disabled, Platform is required to ensure timing of PWROK and SYS_PWROK in such a way that it satisfies the PCIe timing requirement of power stable to reset de-assertion.	Yes
	23	Reserved, set to '0'		No
	22:21	APWROK Timing (APWROK_TIMING): 00 = 2 ms 01 = 4 ms 10 = 8 ms 11 = 16 ms	This soft strap determines the time between the SLP_A# pin de-asserting and the APWROK timer expiration.	Yes
	20	DeepSx Platform Configuration (DEEPSX_PLT_CFG_SS): 0 =The platform does not support DeepSx. 1 =The platform supports DeepSx		Yes
	19	Reserved, set to '0'		No
	18:16	Over-Clocking WDT Self-Start Enable (OC_WDT_SS_EN): 0x0 = Over-Clocking WDT disabled 0x1 = Over-Clocking WDT 3 second timeout 0x2 = Over-Clocking WDT 5 second timeout 0x3 = Over-Clocking WDT 10 second timeout 0x4 = Over-Clocking WDT 15 second timeout 0x5 = Over-Clocking WDT 30 second timeout 0x6 = Over-Clocking WDT 45 second timeout 0x7 = Over-Clocking WDT 60 second timeout	This setting affects whether the Over-Clocking WDT is enabled to automatically start on Host power cycle.	Yes
	15:12	Reserved, set to '0'		No



Offset from 0	Bits	Description	Usage	FIT Visible
0x4C14h (cont)	11:10	tPCH46 Timing: 00 = 1 ms 01 = Reserved 10 = 5 ms 11 = 2 ms	tPch46: PROCPWRGD and SYS_PWROK high to SUS_STAT# deassertion. Refer to EDS for details.	Yes
	9:8	tPCH45 Timing: 00 = 100 ms 01 = 50 ms 10 = 5 ms 11 = 1 ms	tPCH45: PCH clock output stable to PROCPWRGD high. Refer to EDS for details.	Yes
	7:0	Reserved, set to '0x74'		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 '0xfe0082'		No
	7	Integrated Sensor Hub Supported: 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 '0x7fcd7410'		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 '0x107fff0'		No



4.88 PMC Record 4 (UFS Flash Records)

Platform Setting Offset + C24h

Default Address: 4C24h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4C24	31:17	Reserved, set to '0xe0'		No
	16:11	Reserved, set to '0'		No
	10:9	OPI Link Voltage Strap (OPD_LVO_STRP): 0x0 = 0.85 Volts 0x1 = 0.95 Volts 0x2 = 1.05 Volts	This strap must be configured when setting OPI Link Voltage strap (OPD_LVO). Note: This strap and the OPI Link Voltage strap (OPD_LVO) must match the same voltage configuration setting for proper platform operation function.	No
	8	OPI Link Speed Strap (OPDMI_STRP): 0x0 = 2 / GT/s Link Speed 0x1 = 4 / GT/s Link Speed	This strap must be configured when setting OPI Link Speed strap (OPDMI_TLS). Note: This strap and the OPI Link Speed strap (OPDMI_TLS_DMI) and (OPDMI_TLS_DMI) must match the same GT configuration setting for proper platform operation function.	No
	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
0x4C28	31:26	Reserved, set to '0x1e'		No
	25	Boot Media Sx Reset Policy: 0 = BM_Reset# Asserted 1 = BM_Reset# Not Asserted	This setting determine that behavior of Boot Media Sx Reset.	Yes
	24	Boot Media Second Reset Policy: 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 '0xc0001'		No
	1:0	I2C Communication Speed: 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	CPU Strap Length (CPUSL): Identifies the 1's based number of Dwords of Processor Straps to be read, up to 31 DWs (1KB) max. A setting of all 0's indicates there are no Processor DW straps. Set this field to 0x3		No
	26:0	Reserved, set to '0'		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	Reserved, set to '0x1'		No
	30:16	Reserved, set to '0'		No
	17	Encrypted Debug Enable: 0 = Encrypted Debug Enabled 1 = Encrypted Debug Disabled	This setting determines if encrypted debugging is enabled Note: This strap is intended for debugging purposes only.	Yes
	14:15	Reserved, set to '0'		No
	13	JTAG Power Disable: 0 = Disable JTAG Power for C10 and deeper states 1 = Enable JTAG Power for C10 and deeper states	This setting determines if JTAG power will be maintained on C10 or lower power states. Note: This strap is intended for debugging purposed only.	Yes
	12	Processor Boot Max Non-Turbo Frequency: 0 = Disable Boot Non-Turbo Max Frequency 1 = Enable Boot Non-Turbo Max Frequency	This setting determines if the processor will operate at maximum Non-Turbo frequency at power-on and boot. Note: This strap is intended for debugging purposed only.	Yes
	11:6	Flex Ratio: '0x0'	This setting controls the maximum processor non-turbo ratio. Note: This strap is intended for debugging purposed only. See BIOS Spec for more details on maximum processor non-turbo ratio configuration.	Yes
	5	BIST Initialization: 0 = Disable BIST at Reset 1 = Enable BIST at Reset	This setting determines if BIST will be run at platform reset after BIOS requested actions. Note: This strap is intended for debugging purposed only.	Yes
	4:1	Number of Active Cores: 0x0 = All Cores active 0x1 = One core active 0x2 = Two cores active 0x3 = Three cores active 0x4 = Four cores active 0x5 = Five cores active 0x6 = Six cores active 0x7 = Seven cores active 0x8 = Eight cores active	This setting controls the number of active processor cores. Note: This strap is intended for debugging purposed only. See BIOS Spec for more details on enabling / disabling processor cores.	Yes
	0	Disable Hyper threading: 0 = Enable Hyper Threading 1 = Disable Hyper Threading	This setting control enabling / disabling of Hyper threading. Note: This strap is intended for debugging purposed only. See BIOS Spec for more details on enabling / disabling Hyper threading	Yes



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

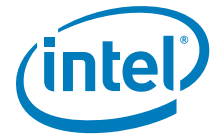


4.96 CPU Record 3 (UFS Flash Records)

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® CSE Record 0 (UFS Flash Records)

Platform Setting Offset + C48h

Default Address: 4C48h

Offset from 0	Bits	Description	Usage	FIT Visible
0x4C48	31:0	Reserved, set to '0'		No



4.98 Intel® CSE Record 1 (UFS Flash Records)

Platform Setting Offset + C4Ch

Default Address: 4C4Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x4C4Ch	31:24	Reserved, set to '0'		No
	23:16	Early USB DbC Intel® CSE Boot Stall Enable: 0 = Intel® CSE Boot Stall not enabled 1 = Intel® CSE Boot Stall enabled	This setting enables a delay during Intel® CSE FW bring-up to allow USB DCI to be established and Early DbC arbitration to be granted.	Yes
	15:8	USB Connector's Associated USB3 Port enable: 0x0 = USB3 Port 1 DbC enabled 0x1 = USB3 Port 2 DbC enabled 0x2 = USB3 Port 3 DbC enabled 0x3 = USB3 Port 4 DbC enabled 0x4 = USB3 Port 5 DbC enabled 0x5 = USB3 Port 6 DbC enabled 0xff = No USB3 ports are assigned to DbC All other values are Reserved	This setting determines which USB3 port goes to the target USB2 ports connector for Early DbC debugging.	Yes
	7:0	USB2 DbC port enable: 0x0 = USB2 Port 1 DbC enabled 0x1 = USB2 Port 2 DbC enabled 0x2 = USB2 Port 3 DbC enabled 0x3 = USB2 Port 4 DbC enabled 0x4 = USB2 Port 5 DbC enabled 0x5 = USB2 Port 6 DbC enabled 0x6 = USB2 Port 7 DbC enabled 0x7 = USB2 Port 8 DbC enabled 0x8 = USB2 Port 9 DbC enabled 0x9 = USB2 Port 10 DbC enabled 0xff = No USB2 ports are assigned to DbC All other values are Reserved	This setting determines which USB2 ports are enabled for Early DbC debugging.	Yes