



Lakefield Client Platform

SPI Programming Guide

January 2020

Revision 1.1

Intel Confidential



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

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

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

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

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

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

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

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

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

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

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

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

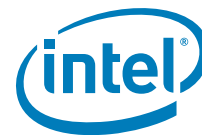
*Other names and brands may be claimed as the property of others.

Copyright © 2020, Intel Corporation. All rights reserved.



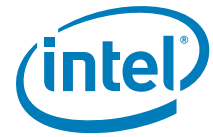
Contents

1	Introduction	9
1.1	Overview	9
1.2	Terminology	10
1.3	Reference Documents	10
2	PCH SPI Flash Architecture	12
2.1	Descriptor Mode	12
2.2	Serial Flash Discoverable Parameter (SFDP)	12
2.3	SPI Fast Read	12
2.4	Intel® Trusted Platform Module (Intel® TPM) on SPI Bus	12
2.5	Boot Flow for Lakefield PCH Family	12
2.6	Flash Regions	13
2.6.1	Flash Region Layout	13
2.6.2	Flash Region Sizes	15
2.7	Hardware Sequencing	15
3	PCH SPI Flash Compatibility Requirement	16
3.1	Lakefield PCH SPI Flash Requirements	16
3.1.1	General Requirements	16
3.1.2	Bios Requirement	17
3.1.3	Software / Firmware Requirements	17
3.1.4	JEDEC ID (Opcode 9Fh)	18
3.1.5	Multiple Page Write Usage Model	18
3.1.6	Hardware Sequencing Requirements	18
3.2	Lakefield PCH SPI AC Electrical Compatibility Guidelines	19
3.3	SPI Flash DC Electrical Compatibility Guidelines	21
4	Descriptor Overview	22
4.1	Flash Descriptor Content	23
4.1.1	Descriptor Signature and Map	24
4.1.1.1	FLVALSIG - Flash Valid Signature (Flash Descriptor Records)	24
4.1.1.2	FLMAPO - Flash Map 0 Register (Flash Descriptor Records)	24
4.1.1.3	FLMAP1 - Flash Map 1 Register (Flash Descriptor Records)	26
4.1.1.4	FLMAP2—Flash Map 2 Register (Flash Descriptor Records)	26
4.1.2	Flash Descriptor Component Section	27
4.1.2.1	FLCOMP—Flash Components Register (Flash Descriptor Records)	27
4.1.2.2	FLILL—Flash Invalid Instructions Register (Flash Descriptor Records)	30
4.1.2.3	FLILL1—Flash Invalid Instructions Register (Flash Descriptor Records)	30
4.1.3	Flash Descriptor Region Section	32
4.1.3.1	FLREG0—Flash Region 0 (Flash Descriptor) Register (Flash Descriptor Records)	32
4.1.3.2	FLREG1—Flash Region 1 (BIOS) Register (Flash Descriptor Records)	32
4.1.3.3	FLREG2—Flash Region 2 (IFWI / Intel® ME ROM Bypass) Register (Flash Descriptor Records)	33
4.1.4	Flash Descriptor Master Section	34



4.1.4.1	FLMSTR1—Flash Master 1 (Host CPU/ BIOS)	34
4.1.4.2	FLMSTR2—Flash Master 2 (Intel® ME)	34
4.1.5	PCH / CPU Softstraps	35
4.1.6	Descriptor Upper Map Section	35
4.1.6.1	FLUMAP1—Flash Upper Map 1 (Flash Descriptor Records)	35
4.1.6.2	IFWI / Intel® ME ROM Bypass Size	35
4.1.6.3	MIP - Descriptor Table	35
4.1.7	Intel® ME Vendor Specific Component Capabilities Table	36
4.1.7.1	JID0—JEDEC-ID 0 Register (Flash Descriptor Records)	36
4.1.7.2	VSCC0—Vendor Specific Component Capabilities 0 (Flash Descriptor Records)	37
4.1.7.3	JIDn—JEDEC-ID Register n (Flash Descriptor Records)	37
4.1.7.4	VSCCn—Vendor Specific Component Capabilities n (Flash Descriptor Records)	37
4.2	OEM Section	38
4.3	Region Access Control	38
4.3.1	Intel Recommended Permissions for Region Access	39
4.3.2	Overriding Region Access	39
4.4	Intel® ME Vendor-Specific Component Capabilities (Intel® ME VSCC) Table	40
4.4.1	How to Set a VSCC Entry in Intel® ME VSCC Table for Lakefield PCH Platforms	40
4.4.2	Intel® ME VSCC Table Settings for Lakefield PCH Family Systems	42
5	Serial Flash Discoverable Parameter (SFDP) Overview	43
5.1	Introduction	43
5.2	Discoverable Parameter Opcode and Flash Cycle	43
5.3	Parameter Table Supported on PCH	43
5.4	Detailed JEDEC Specification	44
6	Configuring BIOS for SPI Flash Access	45
6.1	Unlocking SPI Flash Device Protection for Lakefield PCH Platform	45
6.2	Locking SPI Flash via Status Register	46
6.3	SPI Protected Range Register Recommendations	46
6.4	Recommendations for Flash Configuration Lockdown and Vendor Component Lock Bits	46
6.4.1	Flash Configuration Lockdown	46
6.4.2	Vendor Component Lock	47
6.5	Host Vendor Specific Component Control Registers (VSCC)	47
6.6	Host VSCC Register Settings	51
7	IFWI / Intel® ME Disable for Debug/Flash Burning Purposes	52
7.1	IFWI / Intel® ME Disable	52
7.1.1	Erasing/Programming Intel® ME Region	52
8	Recommendations for SPI Flash Programming in Manufacturing Environments	53
9	Flash Descriptor PCH / PMC / CPU and Intel® ME Configuration Section	54
9.1	PCH Descriptor Record 0 (Flash Descriptor Records)	54
9.2	PCH Descriptor Record 1 (Flash Descriptor Records)	54
9.3	PCH Descriptor Record 2 (Flash Descriptor Records)	55
9.4	PCH Descriptor Record 3 (Flash Descriptor Records)	55
9.5	PCH Descriptor Record 4 (Flash Descriptor Records)	56
9.6	PCH Descriptor Record 5 (Flash Descriptor Records)	56
9.7	PCH Descriptor Record 6 (Flash Descriptor Records)	57
9.8	PCH Descriptor Record 7 (Flash Descriptor Records)	57
9.9	PCH Descriptor Record 8 (Flash Descriptor Records)	58
9.10	PCH Descriptor Record 9 (Flash Descriptor Records)	58

[illegible]



9.66	PCH Descriptor Record 65 (Flash Descriptor Records)	74
9.67	PCH Descriptor Record 66 (Flash Descriptor Records)	74
9.68	PCH Descriptor Record 67 (Flash Descriptor Records)	74
9.69	PCH Descriptor Record 68 (Flash Descriptor Records)	75
9.70	PCH Descriptor Record 69 (Flash Descriptor Records)	75
9.71	PCH Descriptor Record 70 (Flash Descriptor Records)	75
9.72	PCH Descriptor Record 71 (Flash Descriptor Records)	75
9.73	PCH Descriptor Record 72 (Flash Descriptor Records)	76
9.74	MIP Table Descriptor Record 0 (Flash Descriptor Records)	77
9.75	MIP Table Descriptor Record 1 (Flash Descriptor Records)	77
9.76	MIP Table Descriptor Record 2 (Flash Descriptor Records)	77
9.77	MIP Table Descriptor Record 3 (Flash Descriptor Records)	77
9.78	MIP Table Descriptor Record 4 (Flash Descriptor Records)	78
9.79	MIP Table Descriptor Record 5 (Flash Descriptor Records)	78
9.80	MIP Table Descriptor Record 6 (Flash Descriptor Records)	78
9.81	MIP Table Descriptor Record 7 (Flash Descriptor Records)	78
9.82	MIP Table Descriptor Record 8 (Flash Descriptor Records)	79
9.83	MIP Table Descriptor Record 9 (Flash Descriptor Records)	79
9.84	PMC Descriptor Record 0 (Flash Descriptor Records)	80
9.85	PMC Descriptor Record 1 (Flash Descriptor Records)	81
9.86	PMC Descriptor Record 2 (Flash Descriptor Records)	81
9.87	PMC Descriptor Record 3 (Flash Descriptor Records)	82
9.88	PMC Descriptor Record 4 (Flash Descriptor Records)	82
9.89	PMC Descriptor Record 5 (Flash Descriptor Records)	83
9.90	PMC Descriptor Record 6 (Flash Descriptor Records)	83
9.91	PMC Descriptor Record 7 (Flash Descriptor Records)	83
9.92	PMC Descriptor Record 8 (Flash Descriptor Records)	84
9.93	CPU Descriptor Record 0 (Flash Descriptor Records)	85
9.94	CPU Descriptor Record 1 (Flash Descriptor Records)	86
9.95	CPU Descriptor Record 2 (Flash Descriptor Records)	87
9.96	CPU Descriptor Record 2 (Flash Descriptor Records)	88
9.97	Intel® ME Descriptor Record 0 (Flash Descriptor Records)	89
9.98	Intel® ME Descriptor Record 1 (Flash Descriptor Records)	91
A	FAQ and Troubleshooting	92

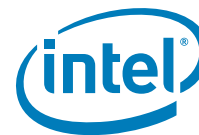


Figures

2-1 SPI Flash Layout	14
3-1 SPI Timing	20
3-2 PCH Test Load	21
4-1 Flash Descriptor (Lakefield PCH)	22
5-1 SFDP Read Instruction Sequence.....	43

Tables

1-1 Terminology	10
1-2 Reference Documents	10
3-1 SPI Timings (14 MHz)	19
3-2 SPI Timings (25 MHz)	19
3-3 SPI Timings (50 MHz)	20
4-1 Region Access Control Table Options.....	38
4-2 Recommended Read/Write Permissions	39
4-3 Recommended Read/Write Settings for Platforms	39
4-4 Jidn - JEDEC ID Portion of Intel® ME VSCC Table.....	40
4-5 Vscn - Vendor-Specific Component Capabilities Portion of the Lakefield PCH Platforms.....	40
6-1 VSCC0 - Vendor-Specific Component Capabilities Register for SPI Component 0	47
6-2 VSCC1 - Vendor Specific Component Capabilities Register for SPI Component 1	49
6-3 Description of How WSR and WEWS is Used.....	50



Revision History

Revision Number	Description	Revision Date
0.5	<ul style="list-style-type: none">Initial release	December 2017
0.51	<ul style="list-style-type: none">Based on ww50 RDL	January 2018
0.52	<ul style="list-style-type: none">Based on 04h RDL	February 2018
0.7	<ul style="list-style-type: none">Align revision number	April 2018
0.8	<ul style="list-style-type: none">Based on latest 04h RDLChanged offset 0x104 bits 0 and 1 to FIT Visible Yes	Sept 2018
0.81	<ul style="list-style-type: none">Added FLMAP3	October 2018
0.82	<ul style="list-style-type: none">Updated FLMAP2 and FLMAP3	April 2019
0.83	<ul style="list-style-type: none">Updated SPI frequency values	May 2019
1.0	<ul style="list-style-type: none">Updated revision	June 2019
1.1	<ul style="list-style-type: none">Updated I2C encoding	January 2020

§ §



1 Introduction

1.1 Overview

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

[Chapter 2, "PCH SPI Flash Architecture"](#)

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

[Chapter 3, "PCH SPI Flash Compatibility Requirement"](#)

- Overview of compatibility requirements for **Lakefield PCH** products.

[Chapter 4, "Descriptor Overview"](#)

- Overview of the descriptor and Descriptor record definition

[Chapter 5, "Serial Flash Discoverable Parameter \(SFDP\) Overview"](#)

- Overview of the SFDP definition.

[Chapter 6, "Configuring BIOS for SPI Flash Access"](#)

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

[Chapter 7, "IFWI / Intel® CSE Disable for Debug/Flash Burning Purposes"](#)

- Methods of disabling Intel Management Engine for debug purposes.

[Chapter 8, "Recommendations for SPI Flash Programming in Manufacturing Environments"](#)

- Recommendations for manufacturing environments.

[Chapter 9, "Flash Descriptor PCH / PMC / CPU and Intel® CSE Configuration Section"](#)

- Flash Descriptor PCH / CPU Soft Strap Section.

[Appendix A, "FAQ and Troubleshooting"](#)

- Frequently asked questions and Troubleshooting tips.



1.2 Terminology

Table 1-1. Terminology

Term	Description
BIOS	Basic Input-Output System
Block Media	Refers to non-serial flash block media devices (i.e. UFS, eMMC etc.)
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)
LPC	Low Pin Count Bus- bus on where legacy devices such as FWH reside
LVSCC	Lower Vendor Specific Component Capabilities
MCP	Multi-Chip package
MDTBA	MIP Descriptor Table Base Address
MIP	Master Image Profile
PCH	Platform Controller Hub
PCH-LP	Platform Controller Hub – Low Power
PMC	Power Management Controller (PCH)
SFDP	Serial Flash Discoverable Parameter
SPI	Serial Peripheral Interface – refers to serial flash memory in this document
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® ME 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® ME from VIP. The Kit MUST match the platform you intend to use the flash tools for.



Table 1-2. Reference Documents

Document	Document # / Location
<i>FW Bring Up Guide</i>	Root directory of latest Intel® CSE FW kit from VIP. The Kit MUST match the platform you intend to use the flash tools for.



2 PCH SPI Flash Architecture

2.1 Descriptor Mode

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

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

Note: Lakefield only supports Descriptor mode.

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

2.2 Serial Flash Discoverable Parameter (SFDP)

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

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

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

2.3 SPI Fast Read

Note: See ***SPI for Flash*** section of the latest Intel Platform Controller Hub Family External Design Specification (EDS) for Lakefield PCH Family for more detailed information 60-MHz support requires SPI component that meet 66-MHz timing.

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

Lakefield PCH Family supports Intel TPM on the SPI bus.

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

2.5 Boot Flow for Lakefield PCH Family

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



See [Chapter 4, “Descriptor Overview”](#) for more detailed information.

2.6 Flash Regions

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

Region	Content
0	Descriptor
1	BIOS
2	IFWI (Integrated Firmware Image) ¹

Notes:

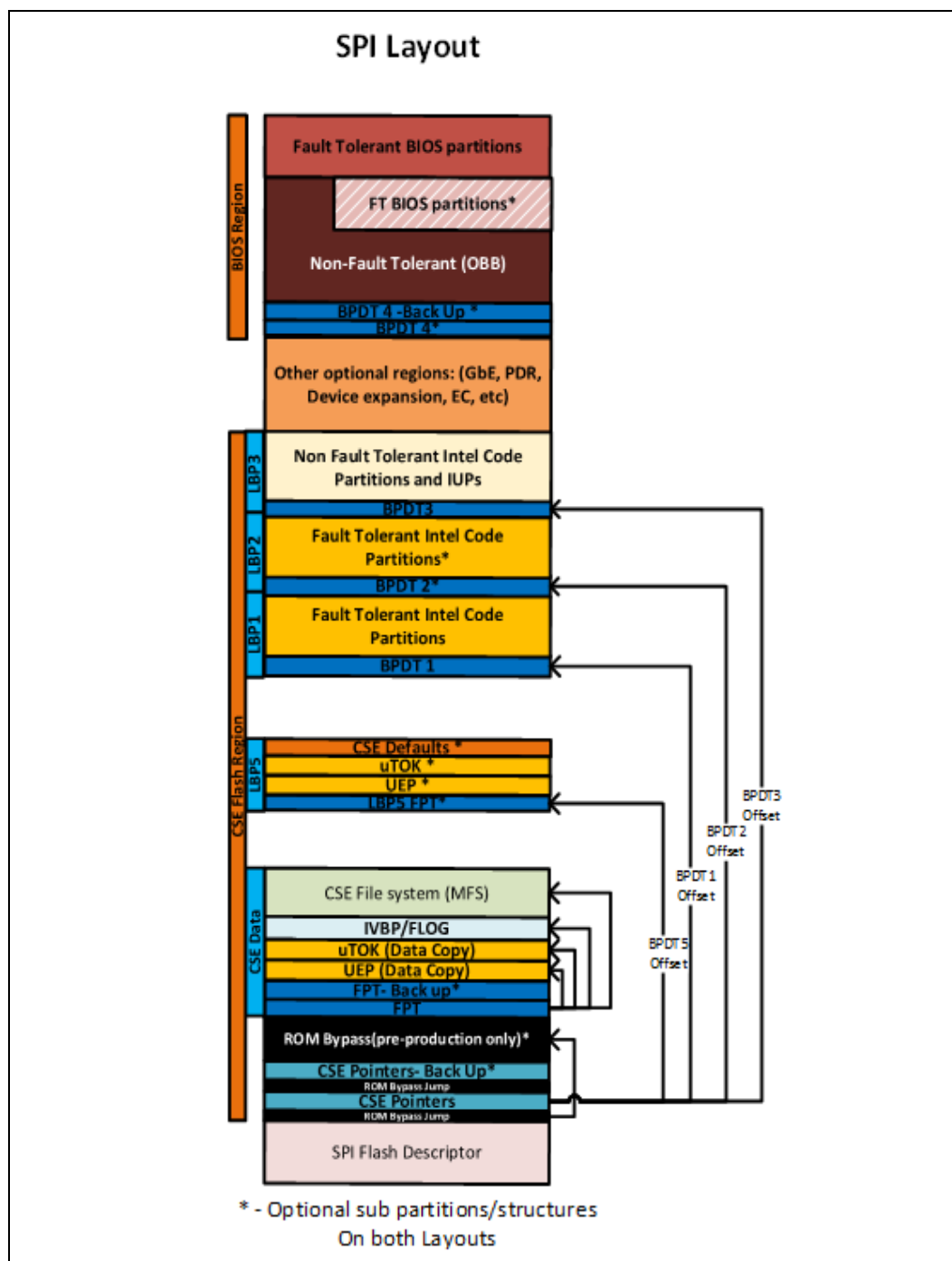
1. Also include as a part of IFWI in some instances is Intel® Management Engine (Intel® ME FW) ROM Bypass

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

2.6.1 Flash Region Layout

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

Figure 2-1. SPI Flash Layout



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

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



2.6.2 Flash Region Sizes

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

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

2.7 Hardware Sequencing

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

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

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

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

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

§ §



3 PCH SPI Flash Compatibility Requirement

3.1 Lakefield PCH SPI Flash Requirements

- Lakefield PCH Family allows for up to two SPI flash devices to store BIOS, Intel® ME FW and integrated LAN information.
 - **Intel® ME FW is required for Lakefield PCH Family-based platforms**
 - Each SPI component can support up to 64 MB (128 MB total addressable) using 26-bit addressing
- 3.3V or 1.8V SPI I/O buffer VCC
- SPI Fast Read instruction is supported at of 14 MHz, 25 MHz and 50 MHz frequencies.
- SPI Dual Output and Dual I/O Fast Read instruction is supported at frequencies of 14 MHz, 25 MHz and 50 MHz.
- SPI Quad Output and Quad I/O Fast read instruction is supported at frequencies of 14 MHz, 25 MHz and 50 MHz.

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

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

3.1.1 General Requirements

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



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

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

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

Write protection scheme must meet guidelines as defined in [SPI Flash Unlocking Requirements for Intel Management Engine](#).

SPI Flash Unlocking Requirements for Intel Management Engine

- a. Flash devices must be globally unlocked (read, write and erase access on the ME region) from power on by writing 0 to the Block Protect bits in the flash's status register to disable write protection.
- b. If the status register must be unprotected, it must use the write enable 06h instruction.
- c. Opcode 01h (write to status register) must then be used to write 0 to the Block Protect bits in the status register. If the device contains a Quad Enable bit in the status register, then firmware must perform a read-modify-write to prevent changing the state of the QE bit when writing to the status register. This must unlock the entire part. If the SPI flash's status register has non-volatile bits that must be written to, bits [5:2] of the flash's status register must be all 0h to indicate that the flash is unlocked.

3.1.2 Bios Requirement

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

3.1.3 Software / Firmware Requirements

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

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

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



3.1.4 JEDEC ID (Opcode 9Fh)

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

3.1.5 Multiple Page Write Usage Model

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

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

3.1.6 Hardware Sequencing Requirements

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

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



3.2 Lakefield PCH SPI AC Electrical Compatibility Guidelines

Table 3-1. SPI Timings (14 MHz)

Sym	Parameter	Min	Max	Units	Notes
t180a	Serial Clock Frequency - 14MHz Operation	13.06	13.73	MHz	1
t183a	Tco of SPI_MOSI with respect to serial clock falling edge at the host	-5	13	ns	
t184a	Setup of SPI_MISO with respect to serial clock falling edge at the host	16	-	ns	
t185a	Hold of SPI_MISO with respect to serial clock falling edge at the host	0	-	ns	
t186a	Setup of SPI_CS[1:0]# assertion with respect to serial clock rising edge at the host	30	-	ns	
t187a	Hold of SPI_CS[1:0]# assertion with respect to serial clock rising edge at the host	30	-	ns	
t188a	SPI_CLK High time	26.37	-	ns	2
t189a	SPI_CLK Low time	26.82	-	ns	2
Notes: 1. Typical clock frequency driven by Tiger Lake PCH Family is 17.86 MHz. 2. Measurement point for low time and high time is taken at 0.5(VccSPI).					

Table 3-2. SPI Timings (25 MHz)

Sym	Parameter	Min	Max	Units	Notes
t180b	Serial Clock Frequency - 25MHz Operation	21.83	24.81	MHz	1
t183b	Tco of SPI_MOSI with respect to serial clock falling edge at the host	-5	5	ns	
t184b	Setup of SPI_MISO with respect to serial clock falling edge at the host	8	-	ns	
t185b	Hold of SPI_MISO with respect to serial clock falling edge at the host	0	-	ns	
t186b	Setup of SPI_CS[1:0]# assertion with respect to serial clock rising edge at the host	30	-	ns	
t187b	Hold of SPI_CS[1:0]# assertion with respect to serial clock rising edge at the host	30	-	ns	
t188b	SPI_CLK High time	14.88	-	ns	2
t189b	SPI_CLK Low time	15.18	-	ns	2
Notes: 1. Typical clock frequency driven by Tiger Lake PCH Family is 25 MHz. 2. Measurement point for low time and high time is taken at 0.5(VccSPI).					



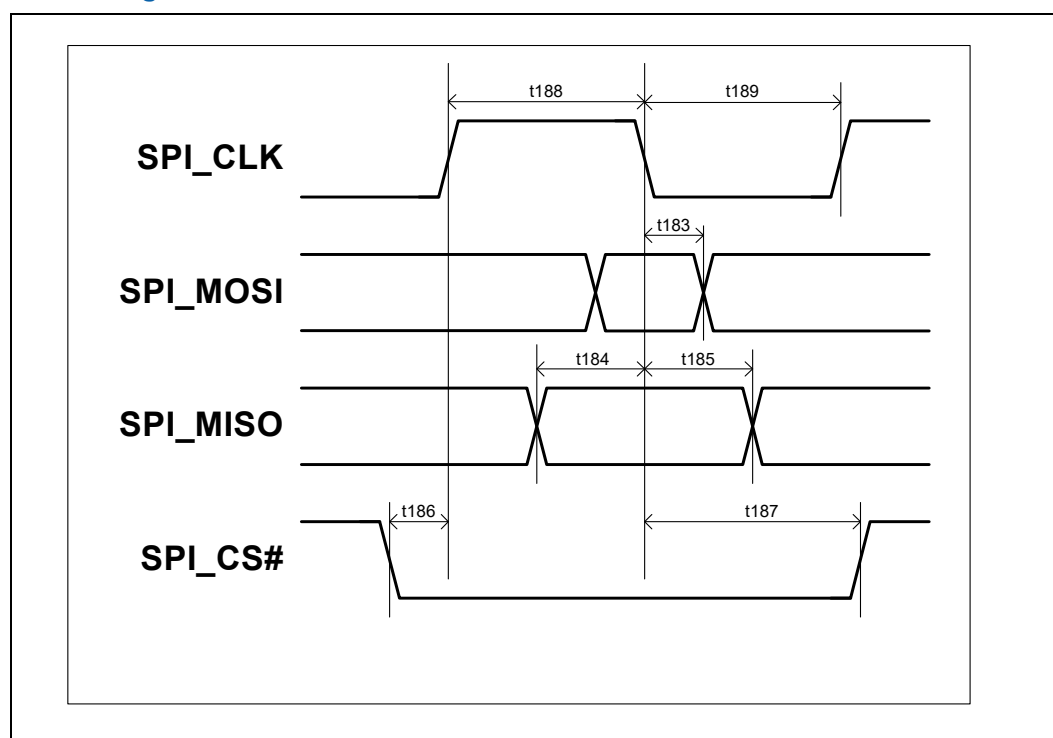
Table 3-3. SPI Timings (50 MHz)

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

Notes:

1. Typical clock frequency driven by Tiger Lake PCH Family is 50 MHz.
2. When using 50 MHz mode ensure target flash component can meet t188c and t189c specifications. Measurement should be taken at a point as close as possible to the package pin.
3. Measurement point for low time and high time is taken at 0.5(V_{ccSPI}).

Figure 3-1. SPI Timing

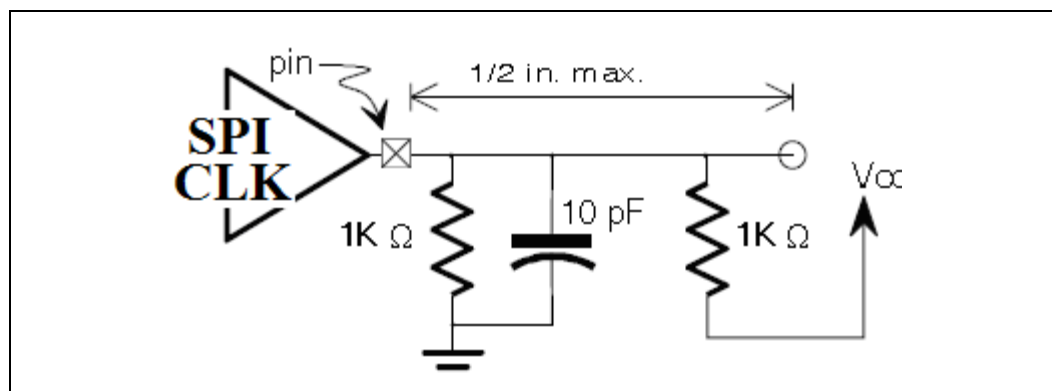


3.3 SPI Flash DC Electrical Compatibility Guidelines

Parameter	Min	Max	Units	Notes
Supply Voltage (Vcc)	3.14	3.7	V	
Input High Voltage	$0.5 \cdot V_{CC}$	$V_{CC} + 0.5$	V	
Input Low Voltage	-0.5	$0.3 \cdot V_{CC}$	V	
Output High Characteristics	$0.9 \cdot V_{CC}$	V_{CC}	V	$I_{oh} = -0.5\text{mA}$
Output Low Characteristics		$0.1 \cdot V_{CC}$		$I_{ol} = 1.5\text{mA}$
Input Leakage Current	-10	10	μA	
Output Rise Slew Rate (0.2 Vcc - 0.6 Vcc)	1	4	V/ns	1
Output Fall Slew Rate (0.6 Vcc - 0.2 Vcc)	1	4	V/ns	1

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

Figure 3-2. PCH Test Load



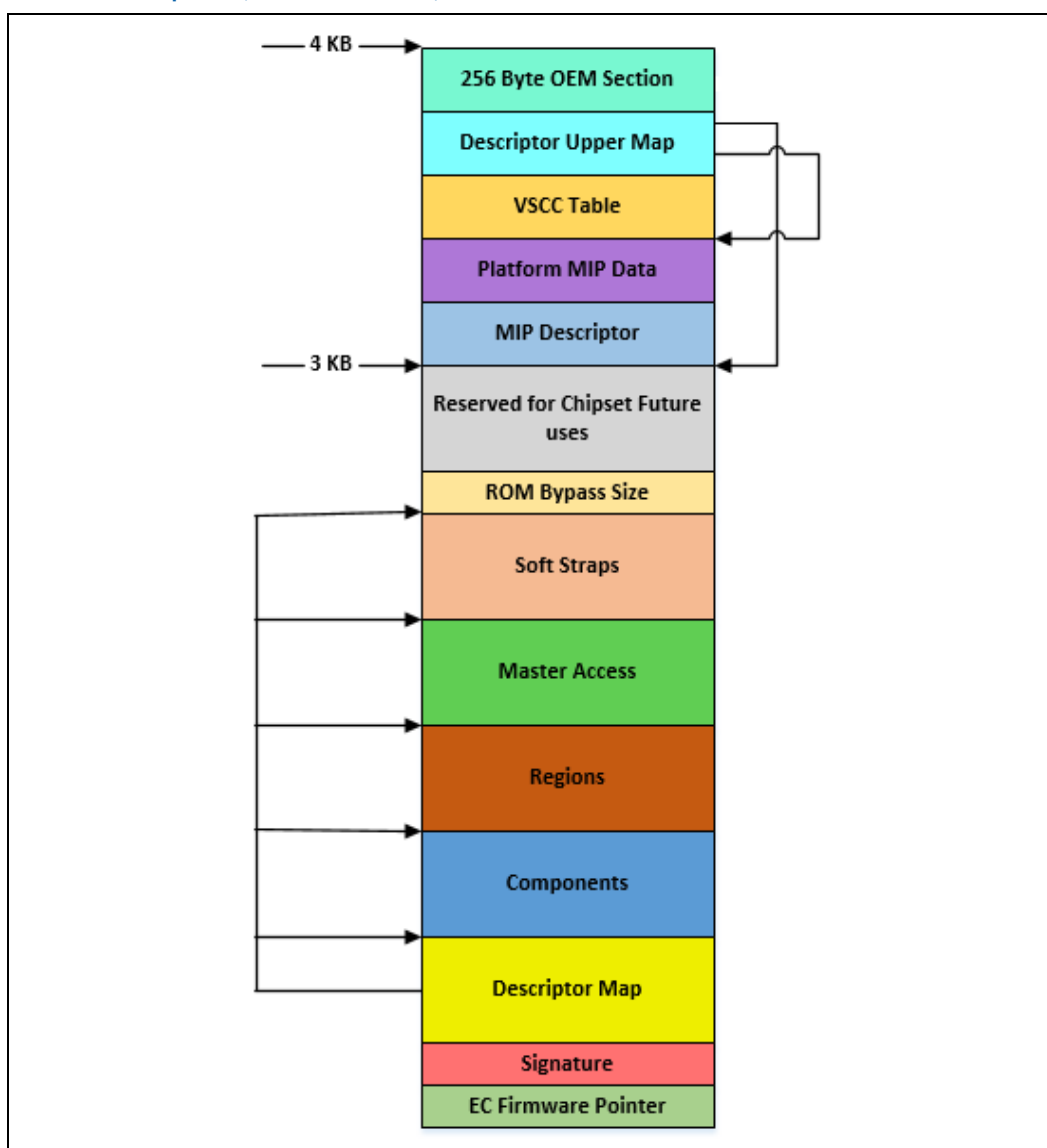
§ §

4 Descriptor Overview

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

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

Figure 4-1. Flash Descriptor (Lakefield 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® ME VSCC Table.
- The Intel® ME VSCC Table holds the JEDEC ID and the ME VSCC information for all the SPI Flash part(s) supported by the NVM image. BIOS and GbE write and erase capabilities depend on VSCC0 and VSCC1 registers in SPIBAR memory space.
- OEM Section is 256 Byte section reserved at the top of the Flash Descriptor for use by the OEM.

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

4.1 Flash Descriptor Content

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

Recommended flash descriptor map:

Region Name	Starting Address
Signature	0x10
Component FCBA	0x30
Regions FRBA	0x40
Masters FMBA	0x80
PCH Straps FPSBA	0x100
Legacy CPU Straps ¹	0x300
MDTBA	0xC00
PMC Straps	0xC14
CPU Straps	0xC38
Intel® ME Straps	0xC44
Register Init FIBA	0x340
1. The Legacy CPU Straps are for BIOS compatibility and are a duplication of the CPU Straps located 0xC38.	



4.1.1 Descriptor Signature and Map

4.1.1.1 FLVALSIG - Flash Valid Signature (Flash Descriptor Records)

Memory Address: FDBAR + 010h

Size: 32 bits

Recommended Value: 0FF0A55Ah

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

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

Memory Address: FDBAR + 014h

Size: 32 bits

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



Bits	Description	FIT Visible
9:8	<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>	No



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

Memory Address: FDBAR + 018h

Size: 32 bits

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

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

Memory Address: FDBAR + 01Ch

Size: 32 bits

Bits	Description	FIT Visible
31:24	Reg Init Length Legacy Reg Init length. Set to 0x0	No
23:16	Reserved	No
15:8	CPU Strap Length Legacy CPU Strap length. Set to 0x3	No
7:0	Flash CPU Strap Base Address Legacy CPU Strap Base Address. Set to 0x30	No

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

Memory Address: FDBAR + 020h

Size: 32 bits

Bits	Description	FIT Visible
31:21	Descriptor Major Revision ID	No
20:14	Descriptor Minor Revision ID	No
13:0	Reserved	No



4.1.2 Flash Descriptor Component Section

4.1.2.1 FLCOMP—Flash Components Register (Flash Descriptor Records)

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

Memory Address: FCBA + 000h

Size: 32 bits

Bits	Description	FIT Visible
31	Reserved	No
30	Dual Output Fast Read Support 0 : Dual Output Fast Read is not supported 1 : Dual Output Fast Read is supported Notes: 1. This setting is no longer required.	No
29:27	Read ID and Read Status Clock Frequency. 000 = Reserved 001 = 50 MHz 100 = 25 MHz 110 = 14 MHz All other Settings = Reserved Notes: 1. If more than one Flash component exists, this field must be set to the lowest common frequency of the different Flash components. 2. If setting to 48, ensure flash meets timing requirements defined in Table 3-3	Yes
26:24	Write and Erase Clock Frequency. 000 = Reserved 001 = 50 MHz 100 = 25 MHz 110 = 14 MHz All other Settings = Reserved Notes: 1. If more than one Flash component exists, this field must be set to the lowest common frequency of the different Flash components. 2. If setting to 48, ensure flash meets timing requirements defined in Table 3-3	Yes
23:21	Fast Read Clock Frequency. This field identifies the frequency that can be used with the Fast Read instruction. This field is undefined if the Fast Read Support field is '0'. 000 = Reserved 001 = 50 MHz 100 = 25 MHz 110 = 14 MHz All other Settings = Reserved Notes: 1. If more than one Flash component exists, this field must be set to the lowest common frequency of the different Flash components. 2. If setting to 48MHz, ensure flash meets timing requirements defined in Table 3-3	Yes



Bits	Description	FIT Visible
20	<p>Fast Read Support. 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>Notes: 1. If more than one Flash component exists, this field can only be set to '1' if both components support Fast Read. 2. It is strongly recommended to set this bit to 1b</p>	Yes
19:16	Reserved	No
15	<p>Quad I/O Read Enable (QIORE): 0 = Quad I/O Read is disabled 1 = Quad I/O Read is enabled</p> <p>This soft strap only has effect if Quad Output Read is discovered as supported via the SFDP If parameter table is not detected via SFDP, this bit has no effect and Quad I/O Read is controlled via the Flash Descriptor Component Section.</p>	Yes
14	<p>Quad Output Read Enable (QORE): 0 = Quad Output Read is disabled 1 = Quad Output Read is enabled</p> <p>This soft strap only has effect if Quad Output Read is discovered as supported via the SFDP If parameter table is not detected via SFDP, this bit has no effect and Quad Output Read is controlled via the Flash Descriptor Component Section.</p>	Yes
13	<p>Dual I/O Read Enable (DIORE): 0 = Dual I/O Read is disabled 1 = Dual I/O Read is enabled</p> <p>This soft strap only has effect if Dual I/O Read is discovered as supported via the SFDP If parameter table is not detected via SFDP, this bit has no effect and Dual Output I/O Read is controlled via the Flash Descriptor Component Section.</p>	Yes
12	<p>Dual Output Read Enable (DORE): 0 = Dual Output Read is disabled 1 = Dual Output Read is enabled</p> <p>This soft strap only has effect if Dual Output read is discovered as supported via the SFDP. If parameter table is not detected via SFDP, this bit has no effect and Dual Output Read is controlled via the Flash Descriptor Component Section.</p>	Yes
11:10	Reserved	No



Bits	Description	FIT Visible
9	<p>SPI Voltage Select (SPI_1p8volt_sel):</p> <p>0 = SPI supply voltage set to 3.3 volts 1 = SPI supply voltage set to 1.8 volts</p> <p>This strap sets the internal control signal on the pad for either 1.8 or 3.3 V operation.</p> <p>Note: The strap defaults to 1.8V mode before the soft straps are loaded, i.e. before the actual supply voltage is known. This is because the pad performance is slightly better when assuming 1.8V when the actual is 3.3V than vice-versa.</p>	Yes
8	Reserved	No
7:4	<p>Component 1 Density. (C1DEN) This field identifies the size of the 2nd Flash component connected directly to the PCH. If there is not 2nd Flash component, the contents of this field should be read as "1111b"</p> <p>0000 = 512 KB 0001 = 1 MB 0010 = 2 MB 0011 = 4 MB 0100 = 8 MB 0101 = 16 MB 0110 = 32 MB 0111 = 64 MB 1000 - 1110 = Reserved</p> <p>Note: This field is defaulted to "1111b" after reset Note: C1DEN field will be ignored if FLMAPO.NC bit [9:8] is set to 00 i.e. 1 component only.</p>	Yes
3:0	<p>Component 0 Density (CODEN). This field identifies the size of the 1st or only Flash component connected directly to the PCH.</p> <p>0000 = 512 KB 0001 = 1 MB 0010 = 2 MB 0011 = 4 MB 0100 = 8 MB 0101 = 16 MB 0110 = 32 MB 0111 = 64 MB 1000 - 1111 = Reserved</p> <p>Note: This field is defaulted to "0101b" (16MB) after reset.</p>	Yes



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

Memory Address: FCBA + 004h

Size: 32 bits

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

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

Memory Address: FCBA + 008h

Size: 32 bits

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



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



4.1.3 Flash Descriptor Region Section

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

Flash Regions:

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

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

Memory Address: FRBA + 000h

Size: 32 bits

Recommended Value: 00000000h

Bits	Description	FIT Visible
31	Reserved	No
30:16	Region Limit. This specifies bits 26:12 of the ending address for this Region. Notes: <ol style="list-style-type: none"> 1. Set this field to 0b. This defines the ending address of descriptor as being FFFh. 2. Region limit address Bits[11:0] are assumed to be FFFh 	No
15	Reserved	No
14:0	Region Base. This specifies address bits 26:12 for the Region Base. Note: Set this field to all 0s. This defines the descriptor address beginning at 0h.	No

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

Memory Address: FRBA + 004h

Size: 32 bits

Bits	Description	FIT Visible
31	Reserved	No
30:16	Region Limit. This specifies bits 26:12 of the ending address for this Region. Notes: <ol style="list-style-type: none"> 1. Must be set to 0000h if Intel® ME ROM Bypass region is unused (on Firmware hub) 2. Ensure BIOS region size is a correct reflection of actual BIOS image that will be used in the platform 3. Region limit address Bits[11:0] are assumed to be FFFh 	No
15	Reserved	No
14:0	Region Base. This specifies address bits 26:12 for the Region Base. Note: If the BIOS region is not used, the Region Base must be programmed to 7FFFh	No



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

Memory Address: FRBA + 008h

Size: 32 bits

Bits	Description	FIT Visible
31	Reserved	No
30:16	Region Limit. This specifies bits 26:12 of the ending address for this Region. Notes: <ol style="list-style-type: none"> Ensure size is a correct reflection of IFWI size that will be used in the platform Region limit address Bits[11:0] are assumed to be FFFh 	No
15	Reserved	No
14:0	Region Base. This specifies address bits 26:12 for the Region Base.	No

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.



4.1.4 Flash Descriptor Master Section

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

Memory Address: FMBA + 000h

Size: 32 bits

Bits	Description	FIT Visible
31:20	Master Region Write Access: Each bit [31:20] corresponds to Regions [11:0]. If the bit is set, this master can erase and write that particular region through register accesses. Note: Bit 21 and 26 are don't care as the primary master always has read/write permission to its primary region	Yes
19:8	Master Region Read Access: Each bit [19:8] corresponds to Regions [11:0]. If the bit is set, this master can read that particular region through register accesses. Note: Bit 9 and 14 are don't care as the primary master always read/write permission to its primary region.	Yes
7:4	Extended Region Write Access: Each bit [7:4] corresponds to Regions [15:12]. If the bit is set, this master can erase and write that particular region through register accesses.	Yes
3:0	Extended Region Read Access: Each bit [3:0] corresponds to Regions [15:12]. If the bit is set, this master can erase and write that particular region through register accesses.	Yes

4.1.4.2 FLMSTR2—Flash Master 2 (Intel® ME)

Memory Address: FMBA + 004h

Size: 32 bits

Bits	Description	FIT Visible
31:20	Master Region Write Access: Each bit [31:20] corresponds to Regions [11:0]. If the bit is set, this master can erase and write that particular region through register accesses. Note: Bit 22 is a don't care as the primary master always has read/write permission to its primary region	Yes
19:8	Master Region Read Access: Each bit [19:8] corresponds to Regions [11:0]. If the bit is set, this master can read that particular region through register accesses. Note: Bit 10 is a don't care as the primary master always read/write permission to its primary region.	Yes
7:4	Extended Region Write Access: Each bit [7:4] corresponds to Regions [15:12]. If the bit is set, this master can erase and write that particular region through register accesses.	Yes
3:0	Extended Region Read Access: Each bit [3:0] corresponds to Regions [15:12]. If the bit is set, this master can erase and write that particular region through register accesses.	Yes



4.1.5 PCH / CPU Softstraps

See Chapter 9, “Flash Descriptor PCH / PMC / CPU and Intel® CSE Configuration Section” for details.

4.1.6 Descriptor Upper Map Section

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

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

Memory Address: FDBAR + EFCh

Size: 32 bits

Bits	Default	Description	FIT Visible
31:16	0xC1	MIP Descriptor Table Base Address (MDTBA) . This identifies base address bits [11:4] for the Platform Configuration Data Structure in the Flash Descriptor Bits [26:12] and bits [3:0] are 0.	No
23:16	0xFF	Reserved	No
15:8	0x1	Intel® ME VSCC Table Length (VTL) . Identifies the 1s based number of DWORDS contained in the VSCC Table. Each SPI component entry in the table is 2 DWORDS long. Max recommended is 10 entries to allow for room for Platform Configuration Data (MIP)	No
7:0	0x1	Intel® ME VSCC Table Base Address (VTBA) . This identifies address bits [11:4] for the VSCC Table portion of the Flash Descriptor. Bits [26:12] and bits [3:0] are 0.	No

4.1.6.2 IFWI / Intel® ME ROM Bypass Size

Memory Address: FDBAR + C00h

Size: 32 bits

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

4.1.6.3 MIP - Descriptor Table

Memory Address: FDBAR + MDTBA

Name	Offset	Size (bytes)	Description	FIT Visible
Number of Descriptors	0x0	2	Number of MIP blocks ('n') inside this MIP structure	Yes
Size of MIP	0x2	2	Size, in bytes, of this MIP structure (including the MDT structure)	Yes
Block 0 Type	0x4	2	Type of block 0. Can be one of the following: 0 = CSE (USB 2 PHY Configuration) 1 = PMC Soft Straps 2 = Reserved Note: In order to simplify handling a new block type can be defined for each usage	Yes
Block 0 Offset	0x6	2	Offset of block 0	Yes
Block 0 Length	0x8	2	Length of block 0 in bytes	Yes



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

4.1.7 Intel® ME Vendor Specific Component Capabilities Table

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

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

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

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

4.1.7.1 J1D0—JEDEC-ID 0 Register (Flash Descriptor Records)

Memory Address: VTBA + 000h

Size: 32 bits

Bits	Description	FIT Visible
31:24	Reserved	No
23:16	SPI Component Device ID 1. This field identifies the second byte of the Device ID of the SPI Flash Component. This is the third byte returned by the Read JEDEC-ID command (opcode 9Fh).	Yes
15:8	SPI Component Device ID 0. This field identifies the first byte of the Device ID of the SPI Flash Component. This is the second byte returned by the Read JEDEC-ID command (opcode 9Fh).	Yes
7:0	SPI Component Vendor ID. This field identifies the one byte Vendor ID of the SPI Flash Component. This is the first byte returned by the Read JEDEC-ID command (opcode 9Fh).	Yes



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

Memory Address: VTBA + 004h

Size: 32 bits

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

Bits	Description	FIT Visible
31:16	Reserved	No
15:8	Erase Opcode (EO) . This field must be programmed with the Flash erase instruction opcode that corresponds to the erase size that is in BES.	No
7:5	Quad Enable Requirements (QER) 000 = Device does not have a QE bit. Device detects 1-1-4 and 1-4-4 reads based on instruction. DQ3 / HOLD# functions as hold during instruction phase. 001 = QE is bit 1 of status register 2. It is set via Write Status with two data bytes where bit 1 of the second byte is one. It is cleared via Write Status with two data bytes where bit 1 of the second byte is zero. Writing only one byte to the status register has the side effect of clearing status register 2, including the QE bit. The 100b code is used if writing one byte to the status register does not modify status register 2. 010 = QE is bit 6 of status register 1. It is set via Write Status with one data byte where bit 6 is one. It is cleared via Write Status with one data byte where bit 6 is zero. 011 = QE is bit 7 of status register 2. It is set via Write status register 2 instruction 3Eh with one data byte where bit 7 is one. It is cleared via Write status register 2 instruction 3Eh with one data byte where bit 7 is zero. The status register 2 is read using instruction 3Fh. 100 = QE is bit 1 of status register 2. It is set via Write Status with two data bytes where bit 1 of the second byte is one. It is cleared via Write Status with two data bytes where bit 1 of the second byte is zero. In contrast to the 001b code, writing one byte to the status register does not modify status register 2. 101 = QE is bit 1 of the status register 2. Status register 1 is read using Read Status instruction 05h. Status register 2 is read using instruction 35h. QE is set via Write Status instruction 01h with two data bytes where bit 1 of the second byte is one. It is cleared via Write Status with two data bytes where bit 1 of the second byte is zero. other = reserved Note: Please refer to Table note#1 below for details.	No
4:0	Reserved set to 00101b	No
Notes: 1. The manufacturers information included in the QER list are for guidance purpose. Some manufacturer devices operate as shown in the table above. Check manufacturer's data sheet for exact requirements.		

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

Memory Address: VTBA + (n*8)h

Size: 32 bits

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

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

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

Size: 32 bits

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



4.2 OEM Section

Memory Address: F00h

Size: 256 Bytes

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

4.3 Region Access Control

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

Table 4-1. Region Access Control Table Options

Master Read/Write Access		
Region (#)	CPU / BIOS	IFWI (Intel® ME)
Descriptor (0)	Read Only	Read Only
BIOS (1)	CPU / BIOS can always read from and write to BIOS region prior to EOP	Not Accessible
IFWI / Intel® Management Engine ROM Bypass (2)	Read / Write (BIOS Only)	Intel® ME can always read from and write to IFWI region
Notes: 1. The Region Access values listed above represent post manufacturing configuration only.		



4.3.1 Intel Recommended Permissions for Region Access

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

Table 4-2. Recommended Read/Write Permissions

Master Access	Descriptor Region Bit 0	BIOS Region Bit 1	IFWI / Intel® ME ROM Bypass Region Bit 2
ME read access	Y	N	Y
ME write access	N	N	Y
BIOS read access	Y	Y	Y
BIOS write access	N	Y	N

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

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

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

	ME	BIOS
Read	0b 0000 0000 0000 1101 = 0x000D	0b 0000 0000 0000 1011 = 0x00F
Write	0b 0000 0000 0000 1100 = 0x0004	0b 0000 0000 0000 1010 = 0x00A

4.3.2 Overriding Region Access

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

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

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

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

See [6.3 SPI Protected Range Register Recommendations](#) for more details.



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

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

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

Bits	Description	FIT Visible
31:24	Reserved.	No
23:16	SPI Component Device ID 1: This identifies the second byte of the Device ID of the SPI Flash Component. This is the third byte returned by the Read JEDEC-ID command (opcode 9Fh).	Yes
15:8	SPI Component Device ID 0: This identifies the first byte of the Device ID of the SPI Flash Component. This is the second byte returned by the Read JEDEC-ID command (opcode 9Fh).	Yes
7:0	SPI Component Vendor ID: This identifies the one byte Vendor ID of the SPI Flash Component. This is the first byte returned by the Read JEDEC-ID command (opcode 9Fh).	Yes

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

4.4.1 How to Set a VSCC Entry in Intel® ME VSCC Table for Lakefield PCH Platforms

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

Refer to [4.4.2 Intel® ME VSCC Table Settings for Lakefield PCH Family Systems](#).

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

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

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



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

Bits	Description	FIT Visible
7:5	Quad Enable Requirements (QER) 000 = Part does not require a Quad Enable bit to be set, either because Quad is not supported or because the manufacturer permanently enables Quad capability (e.g. Micron, Numonyx). 001 = Part requires bit 9 in status register 2 to be set to enable quad IO. Writing one byte to status register clears all bits in register 2, therefore status register writes MUST be two bytes. If the status register is unlocked and SFDP bits WSR or VSCC WSR is 1 then SPI controller cannot use the quad output, quad IO features of this part because the hardware will automatically write one byte of zeros to status register with every write/erase. (e.g. Winbond, AMIC, Spansion). 010 = Part requires bit 6 of status register 1 to be set to enable quad IO. If the status register is unlocked and SFDP WSR bit or VSCC WSR is 1 then flash controller cannot use the quad output, quad IO features of this part because the hardware will automatically write one byte of zeros to status register with every write/erase (e.g. Macronix). 011 = Part requires bit 7 of the configuration register to be set to enable Quad (e.g. Atmel). 100 = Part requires bit 9 in status register 2 to be set to enable quad IO. Writing one byte to the status register does not clear the second byte (SST/Microchip, Winbond). Note: Please refer to Table note#6 below for details.	No
4	Write Enable on Write Status (WEWS) 0 = 50h is the opcode used to unlock the status register on SPI flash if WSR (bit 3) is set to 1b. 1 = 06h is the opcode used to unlock the status register on SPI flash if WSR (bit 3) is set to 1b. Note: Please refer to Table Note #4 below for a description how this bit is used.	No
3	Write Status Required (WSR) 0 = No automatic write of 00h will be made to the SPI flash's status register) 1 = A write of 00h to the SPI flash's status register will be sent on EVERY write and erase performed by Intel® ME to the SPI flash. Note: Please refer to Table Note #5 below for a description how this bit is used.	No
2	Write Granularity (WG). 0 = 1 Byte 1 = 64 Bytes	No
1:0	Block/Sector Erase Size (BES). This field identifies the erasable sector size for all Flash components. 00 = 256 Bytes 01 = 4 K Bytes 10 = 8 K Bytes 11 = 64K Bytes	No
Notes: 1. Bit 3 (WEWS) and/or bit 4 (WSR) should not be set to '1' if there are non volatile bits in the SPI flash's status register. This may lead to premature flash wear out. 2. This is not an atomic (uninterrupted) sequence. The PCH will not wait for the status write to complete before issuing the next command, potentially causing SPI flash instructions to be disregarded by the SPI flash part. If the SPI flash component's status register is non-volatile, then BIOS should issue an atomic software sequence cycle to unlock the flash part. 3. If both bits 3 (WSR) and 4 (WEWS) are set to 1b, then sequence of 06h 01h 00h is sent to unlock the SPI flash on EVERY write and erase that Intel Management Engine firmware performs. 4. If bit 3 (WSR) is set to 1b and bit 4 (WEWS) is set to 0b then sequence of 50h 01h 00h is sent to unlock the SPI flash on EVERY write and erase that Intel Management Engine firmware performs. 5. If bit 3 (WSR) is set to 0b and bit 4 (WEWS) is set to 0b or 1b then sequence of 60h is sent to unlock the SPI flash on EVERY write and erase that Processor or Intel GbE FW performs. 6. The manufacturers information included in the QER list are for guidance purpose. Some manufacturer devices operate as shown in the table above. Check manufacturer's datasheet for exact requirements.		

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

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



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

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

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

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

4.4.2 Intel® ME VSCC Table Settings for Lakefield PCH Family Systems

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

§ §



5 Serial Flash Discoverable Parameter (SFDP) Overview

5.1 Introduction

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

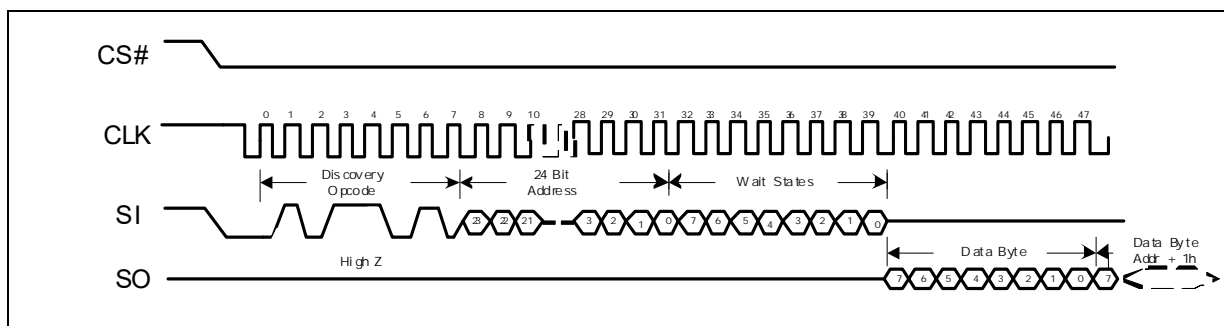
These guidelines are a standard that will allow for individual vendors to have their value add features, but will allow for a controller to discover the attributes needed to operate.

5.2 Discoverable Parameter Opcode and Flash Cycle

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

SFDP read must update at a frequency between 14 MHz and 50 MHz with a single byte of wait state.

Figure 5-1. SFDP Read Instruction Sequence



5.3 Parameter Table Supported on PCH

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

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

- Quad I/O Read
- Quad Output Read



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

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

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

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

5.4 Detailed JEDEC Specification

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

§ §



6 Configuring BIOS for SPI Flash Access

6.1 Unlocking SPI Flash Device Protection for Lakefield PCH Platform

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

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

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

Recommended flash unlocking sequence:

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

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



6.2 Locking SPI Flash via Status Register

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

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

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

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

6.3 SPI Protected Range Register Recommendations

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

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

It is strongly recommended that if Flash Descriptor Override strap (which can be checked by reading **FDOPSS (0b Flash Descriptor override is set, 1b not set) in PCH memory space (SPIBAR+4h bit 13))** is set, do not set a Protected range to cover the Intel® ME FW factory defaults. This would allow a flashing of a complete image when the Flash descriptor Override strap is set.

6.4 Recommendations for Flash Configuration Lockdown and Vendor Component Lock Bits

6.4.1 Flash Configuration Lockdown

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

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



6.4.2 Vendor Component Lock

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

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

6.5 Host Vendor Specific Component Control Registers (VSCC)

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

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

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

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

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

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



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

Bit	Description
15:8	<p>Erase Opcode (EO)— RW:</p> <p>This register is programmed with the Flash erase instruction opcode required by the vendor's Flash component. Software must program this register if the SFDP table for this component does not show 4 kByte erase capability</p> <p>This register is locked by the Vendor Component Lock (VCL) bit.</p> <p>Note: If CPPTV is 1 and the SPDP0 table shows 4k erase capability, the SFDP0 erase code is used instead of this register</p>
7:5	<p>Quad Enable Requirements (QER)</p> <p>000 = Part does not require a Quad Enable bit to be set, either because Quad is not supported or because the manufacturer permanently enables Quad capability (e.g. Micron, Numonyx).</p> <p>001 = Part requires bit 9 in status register 2 to be set to enable quad IO. Writing one byte to status register clears all bits in register 2, therefore status register writes MUST be two bytes. If the status register is unlocked and SFDP bits WSR or VSCC WSR is 1 then SPI controller cannot use the quad output, quad IO features of this part because the hardware will automatically write one byte of zeros to status register with every write/erase. (e.g. Winbond, AMIC, Spansion).</p> <p>010 = Part requires bit 6 of status register 1 to be set to enable quad IO. If the status register is unlocked and SFDP WSR bit or VSCC WSR is 1 then flash controller cannot use the quad output, quad IO features of this part because the hardware will automatically write one byte of zeros to status register with every write/erase (e.g. Macronix).</p> <p>011 = Part requires bit 7 of the configuration register to be set to enable Quad (e.g. Atmel).</p> <p>100 = Part requires bit 9 in status register 2 to be set to enable quad IO. Writing one byte to the status register does not clear the second byte (SST/Microchip, Winbond).</p> <p>Note: This register is locked by the Vendor Component Lock (VCL) bit.</p>
4	<p>Write Enable on Write Status (WEWS) — RW:</p> <p>'0' = 50h will be the opcode used to unlock the status register on the SPI flash if WSR (bit 3) is set to 1b.</p> <p>'1' = 06h will be the opcode used to unlock the status register on the SPI flash if WSR (bit 3) is set to 1b.</p> <p>This register is locked by the Vendor Component Lock (VCL) bit.</p> <p>Note: Please refer to Table 6-3 for a description of how these bits is used.</p>
3	<p>Write Status Required (WSR) — RW:</p> <p>'0' = No automatic write of 00h will be made to the SPI flash's status register.</p> <p>'1' = A write of 00h to the SPI flash's status register will be sent on EVERY write and erase to the SPI flash performed by Host and GbE.</p> <p>This register is locked by the Vendor Component Lock (VCL) bit.</p> <p>Note: Please refer to Table 6-3 for a description of how these bits is used.</p>
2	<p>Write Granularity (WG) — RW:</p> <p>0: 1 Byte</p> <p>1: 64 Byte</p> <p>This register is locked by the Vendor Component Lock (VCL) bit.</p> <p>Notes:</p> <ol style="list-style-type: none"> If more than one Flash component exists, this field must be set to the lowest common write granularity of the different Flash components If using 64 B write, BIOS must ensure that multiple byte writes do not occur over 256 B boundaries. This will lead to corruption as the write will wrap around the page boundary on the SPI flash part. This is a feature in page writable SPI flash.



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

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

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

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



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

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

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

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

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

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



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

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

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

All reserved bits should set to zeros.

6.6 Host VSCC Register Settings

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

§ §



7 IFWI / Intel® CSE Disable for Debug/Flash Burning Purposes

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

7.1 IFWI / Intel® ME Disable

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

1. HDA_SDO (Manufacturing mode jumper or Flash descriptor override jumper) asserted HIGH on the rising edge of PWROK. Power off or cold reset. Note: this is only valid as long as you do not specifically set the variable Flash Descriptor Override Pin-Strap Ignore in the Flash Image Tool to false.
2. HECI ME region unlock - There is a HECI command that allows Intel® ME FW to boot up in a temporarily disabled state and allows for a host program to overwrite the ME region.

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

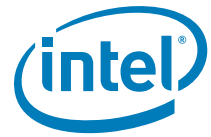
7.1.1 Erasing/Programming Intel® ME Region

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

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

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

§ §



8 Recommendations for SPI Flash Programming in Manufacturing Environments

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

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

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

§ §



9 Flash Descriptor PCH / PMC / CPU and Intel® 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.

9.1 PCH Descriptor Record 0 (Flash Descriptor Records)

Flash Address: FPSBA + 000h

Default Flash Address: 100h

Offset from 0	Bits	Description	Usage	FIT Visible
0x100	23:0	Reserved, set to '0x4'		No

9.2 PCH Descriptor Record 1 (Flash Descriptor Records)

Flash Address: FPSBA + 003h

Default Flash Address: 103h

Offset from 0	Bits	Description	Usage	FIT Visible
0x103	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



9.3 PCH Descriptor Record 2 (Flash Descriptor Records)

Flash Address: FPSBA + 004h

Default Flash Address: 104h

Offset from 0	Bits	Description	Usage	FIT Visible
0x104	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

9.4 PCH Descriptor Record 3 (Flash Descriptor Records)

Flash Address: FPSBA + 005h

Default Flash Address: 105h

Offset from 0	Bits	Description	Usage	FIT Visible
0x105	7:0	Reserved, set to '0'		No



9.5 PCH Descriptor Record 4 (Flash Descriptor Records)

Flash Address: FPSBA + 006h

Default Flash Address: 106h

Offset from 0	Bits	Description	Usage	FIT Visible
0x106	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

9.6 PCH Descriptor Record 5 (Flash Descriptor Records)

Flash Address: FPSBA + 007h

Default Flash Address: 107h

Offset from 0	Bits	Description	Usage	FIT Visible
0x107	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



9.7 PCH Descriptor Record 6 (Flash Descriptor Records)

Flash Address: FPSBA + 008h

Default Flash Address: 108h

Offset from 0	Bits	Description	Usage	FIT Visible
0x108	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

9.8 PCH Descriptor Record 7 (Flash Descriptor Records)

Flash Address: FPSBA + 009h

Default Flash Address: 109h

Offset from 0	Bits	Description	Usage	FIT Visible
0x109	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



9.9 PCH Descriptor Record 8 (Flash Descriptor Records)

Flash Address: FPSBA + 00Ah

Default Flash Address: 10Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0x10A	7:1	Reserved, set to '0'		No
	0	USB Type AB mode Select: 0 = USB Type AB connector switches based on SW event 1 = USB Type AB connector switches based on HW event	This setting configures the mode for the USB Type AB connector.	Yes

9.10 PCH Descriptor Record 9 (Flash Descriptor Records)

Flash Address: FPSBA + 00Bh

Default Flash Address: 10Bh

Offset from 0	Bits	Description	Usage	FIT Visible
0x10B	7:0	Reserved, set to '0'		No

9.11 PCH Descriptor Record 10 (Flash Descriptor Records)

Flash Address: FPSBA + 00Ch

Default Flash Address: 10Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x10C	31:0	Reserved, set to '0'		No

9.12 PCH Descriptor Record 11 (Flash Descriptor Records)

Flash Address: FPSBA + 010h

Default Flash Address: 110h

Offset from 0	Bits	Description	Usage	FIT Visible
0x110	15:0	Reserved, set to '0'		No



9.13 PCH Descriptor Record 12 (Flash Descriptor Records)

Flash Address: FPSBA + 012h

Default Flash Address: 112h

Offset from 0	Bits	Description	Usage	FIT Visible
0x112	7:0	Reserved, set to '0xff'		No

9.14 PCH Descriptor Record 13 (Flash Descriptor Records)

Flash Address: FPSBA + 013h

Default Flash Address: 113h

Offset from 0	Bits	Description	Usage	FIT Visible
0x113	7:0	Reserved, set to '0'		No

9.15 PCH Descriptor Record 14 (Flash Descriptor Records)

Flash Address: FPSBA + 014h

Default Flash Address: 114h

Offset from 0	Bits	Description	Usage	FIT Visible
0x114	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.	<p>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.</p> <p>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.</p> <p>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.</p>	Yes
	3:0	Reserved, set to '0'		No



9.16 PCH Descriptor Record 15 (Flash Descriptor Records)

Flash Address: FPSBA + 015h

Default Flash Address: 115h

Offset from 0	Bits	Description	Usage	FIT Visible
0x115	7:0	Reserved, set to '0x7'		No

9.17 PCH Descriptor Record 16 (Flash Descriptor Records)

Flash Address: FPSBA + 016h

Default Flash Address: 116h

Offset from 0	Bits	Description	Usage	FIT Visible
0x116	7:0	Reserved, set to '0x80'		No

9.18 PCH Descriptor Record 17 (Flash Descriptor Records)

Flash Address: FPSBA + 017h

Default Flash Address: 117h

Offset from 0	Bits	Description	Usage	FIT Visible
0x117	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



Offset from 0	Bits	Description	Usage	FIT Visible
0x117 (Cont)	0	Reserved, set to '0'		No

9.19 PCH Descriptor Record 18 (Flash Descriptor Records)

Flash Address: FPSBA + 018h

Default Flash Address: 118h

Offset from 0	Bits	Description	Usage	FIT Visible
0x118	7	Reserved, set to '0'		No
	6:4	Intel® Precise Touch and Stylus Controller 1 Maximum Frequency (TMF): 001 = 50MHz 011 = Reserved 100 = 25 MHz 101 = Reserved 110 = 14 MHz 111 = Reserved <i>Note:</i> 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® ME firmware will use the value in this field along with data from the Touch device's capability register to program the Intel® Precise Touch and Stylus Controller 1 Configuration Register.	Yes
	3:0	SPI Idle to Deep Power Down Timeout: Set to '0x5'	SPI Idle to Deep Power Down Timeout Default Specifies the time in microseconds that the Flash Controller waits after all activity is idle before commanding the flash devices to Deep Powerdown, time = 2^N microseconds	Yes



9.20 PCH Descriptor Record 19 (Flash Descriptor Records)

Flash Address: FPSBA + 019h

Default Flash Address: 119h

Offset from 0	Bits	Description	Usage	FIT Visible
0x119	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 = 50MHz 011 = Reserved 100 = 25 MHz 101 = Reserved 110 = 14 MHz 111 = reserved Notes: This field identifies the serial clock frequency for TPM on SPI. This field is undefined if the TPM on SPI is disabled either by soft-strap or fuse.		Yes

9.21 PCH Descriptor Record 20 (Flash Descriptor Records)

Flash Address: FPSBA + 01Ah

Default Flash Address: 11Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0x11A	7:0	Reserved, set to '0'		No

9.22 PCH Descriptor Record 21 (Flash Descriptor Records)

Flash Address: FPSBA + 01Bh

Default Flash Address: 11Bh

Offset from 0	Bits	Description	Usage	FIT Visible
0x11B	7:0	Reserved, set to '0x34'		No



9.23 PCH Descriptor Record 22 (Flash Descriptor Records)

Flash Address: FPSBA + 01Ch

Default Flash Address: 11Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x11C	31:0	Global Protected Range Default (GPRD): Set to '0x0'	Sets the default value of the GPR0 register in the SPI Flash Controller.	Yes

9.24 PCH Descriptor Record 23 (Flash Descriptor Records)

Flash Address: FPSBA + 020h

Default Flash Address: 120h

Offset from 0	Bits	Description	Usage	FIT Visible
0x120	7:0	Reserved, set to '0x20'		No

9.25 PCH Descriptor Record 24 (Flash Descriptor Records)

Flash Address: FPSBA + 021h

Default Flash Address: 121h

Offset from 0	Bits	Description	Usage	FIT Visible
0x121	7:0	Reserved, set to '0x7'		No

9.26 PCH Descriptor Record 25 (Flash Descriptor Records)

Flash Address: FPSBA + 022h

Default Flash Address: 122h

Offset from 0	Bits	Description	Usage	FIT Visible
0x122	7:0	Reserved, set to '0x40'		No

9.27 PCH Descriptor Record 26 (Flash Descriptor Records)

Flash Address: FPSBA + 023h

Default Flash Address: 123h

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



9.28 PCH Descriptor Record 27 (Flash Descriptor Records)

Flash Address: FPSBA + 024h

Default Flash Address: 124h

Offset from 0	Bits	Description	Usage	FIT Visible
0x124	7:0	Reserved, set to '0x3'		No

9.29 PCH Descriptor Record 28 (Flash Descriptor Records)

Flash Address: FPSBA + 025h

Default Flash Address: 125h

Offset from 0	Bits	Description	Usage	FIT Visible
0x125	7:0	Reserved, set to '0x1'		No

9.30 PCH Descriptor Record 29 (Flash Descriptor Records)

Flash Address: FPSBA + 026h

Default Flash Address: 126h

Offset from 0	Bits	Description	Usage	FIT Visible
0x126	7:0	Reserved, set to '0'		No

9.31 PCH Descriptor Record 30 (Flash Descriptor Records)

Flash Address: FPSBA + 027h

Default Flash Address: 127h

Offset from 0	Bits	Description	Usage	FIT Visible
0x127	7:0	Reserved, set to '0x80'		No

9.32 PCH Descriptor Record 31 (Flash Descriptor Records)

Flash Address: FPSBA + 028h

Default Flash Address: 128h

Offset from 0	Bits	Description	Usage	FIT Visible
0x128	31:0	Reserved, set to '0x3'		No



9.33 PCH Descriptor Record 32 (Flash Descriptor Records)

Flash Address: FPSBA + 02Ch

Default Flash Address: 12Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x12C	31:0	Reserved, set to '0x3'		No

9.34 PCH Descriptor Record 33 (Flash Descriptor Records)

Flash Address: FPSBA + 030h

Default Flash Address: 130h

Offset from 0	Bits	Description	Usage	FIT Visible
0x130	7:0	Reserved, set to '0'		No

9.35 PCH Descriptor Record 34 (Flash Descriptor Records)

Flash Address: FPSBA + 031h

Default Flash Address: 131h

Offset from 0	Bits	Description	Usage	FIT Visible
0x131	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



9.36 PCH Descriptor Record 35 (Flash Descriptor Records)

Flash Address: FPSBA + 032h

Default Flash Address: 132h

Offset from 0	Bits	Description	Usage	FIT Visible
0x132	7:0	Reserved, set to '0'		No

9.37 PCH Descriptor Record 36 (Flash Descriptor Records)

Flash Address: FPSBA + 033h

Default Flash Address: 133h

Offset from 0	Bits	Description	Usage	FIT Visible
0x133	7:0	Reserved, set to '0'		No

9.38 PCH Descriptor Record 37 (Flash Descriptor Records)

Flash Address: FPSBA + 034h

Default Flash Address: 134h

Offset from 0	Bits	Description	Usage	FIT Visible
0x134	7:0	Reserved, set to '0'		No

9.39 PCH Descriptor Record 38 (Flash Descriptor Records)

Flash Address: FPSBA + 035h

Default Flash Address: 135h

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

9.40 PCH Descriptor Record 39 (Flash Descriptor Records)

Flash Address: FPSBA + 036h

Default Flash Address: 136h

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



9.41 PCH Descriptor Record 40 (Flash Descriptor Records)

Flash Address: FPSBA + 037h

Default Flash Address: 137h

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

9.42 PCH Descriptor Record 41 (Flash Descriptor Records)

Flash Address: FPSBA + 038h

Default Flash Address: 138h

Offset from 0	Bits	Description	Usage	FIT Visible
0x138	7:0	Reserved, set to '0'		No

9.43 PCH Descriptor Record 42 (Flash Descriptor Records)

Flash Address: FPSBA + 039h

Default Flash Address: 139h

Offset from 0	Bits	Description	Usage	FIT Visible
0x139	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



9.44 PCH Descriptor Record 43 (Flash Descriptor Records)

Flash Address: FPSBA + 03Ah

Default Flash Address: 13Ah

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

9.45 PCH Descriptor Record 44 (Flash Descriptor Records)

Flash Address: FPSBA + 03Bh

Default Flash Address: 13Bh

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

9.46 PCH Descriptor Record 45 (Flash Descriptor Records)

Flash Address: FPSBA + 03Ch

Default Flash Address: 13Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x13C	7:0	Reserved, set to '0'		No

9.47 PCH Descriptor Record 46 (Flash Descriptor Records)

Flash Address: FPSBA + 03Dh

Default Flash Address: 13Dh

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

9.48 PCH Descriptor Record 47 (Flash Descriptor Records)

Flash Address: FPSBA + 03Eh

Default Flash Address: 13Eh

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



9.49 PCH Descriptor Record 48 (Flash Descriptor Records)

Flash Address: FPSBA + 03Fh

Default Flash Address: 13Fh

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

9.50 PCH Descriptor Record 49 (Flash Descriptor Records)

Flash Address: FPSBA + 040h

Default Flash Address: 140h

Offset from 0	Bits	Description	Usage	FIT Visible
0x140	7:0	Reserved, set to '0'		No

9.51 PCH Descriptor Record 50 (Flash Descriptor Records)

Flash Address: FPSBA + 041h

Default Flash Address: 141h

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

9.52 PCH Descriptor Record 51 (Flash Descriptor Records)

Flash Address: FPSBA + 042h

Default Flash Address: 142h

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

9.53 PCH Descriptor Record 52 (Flash Descriptor Records)

Flash Address: FPSBA + 043h

Default Flash Address: 143h

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



9.54 PCH Descriptor Record 53 (Flash Descriptor Records)

Flash Address: FPSBA + 044h

Default Flash Address: 144h

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

9.55 PCH Descriptor Record 54 (Flash Descriptor Records)

Flash Address: FPSBA + 045h

Default Flash Address: 145h

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

9.56 PCH Descriptor Record 55 (Flash Descriptor Records)

Flash Address: FPSBA + 046h

Default Flash Address: 146h

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

9.57 PCH Descriptor Record 56 (Flash Descriptor Records)

Flash Address: FPSBA + 047h

Default Flash Address: 147h

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



9.58 PCH Descriptor Record 57 (Flash Descriptor Records)

Flash Address: FPSBA + 048h

Default Flash Address: 148h

Offset from 0	Bits	Description	Usage	FIT Visible
0x148	7:0	Reserved, set to '0xf0'		No

9.59 PCH Descriptor Record 58 (Flash Descriptor Records)

Flash Address: FPSBA + 049h

Default Flash Address: 149h

Offset from 0	Bits	Description	Usage	FIT Visible
0x149	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



9.60 PCH Descriptor Record 59 (Flash Descriptor Records)

Flash Address: FPSBA + 04Ah

Default Flash Address: 14Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0x14A	7:0	Reserved, set to '0x4'		No

9.61 PCH Descriptor Record 60 (Flash Descriptor Records)

Flash Address: FPSBA + 04Bh

Default Flash Address: 14Bh

Offset from 0	Bits	Description	Usage	FIT Visible
0x14B	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

9.62 PCH Descriptor Record 61 (Flash Descriptor Records)

Flash Address: FPSBA + 04Ch

Default Flash Address: 14Ch



Offset from 0	Bits	Description	Usage	FIT Visible
0x14C	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 ME. 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
	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® ME AFS Flash Idle Reclaim Enable: 0 = AFS Flash Reclaim enabled 1 = AFS Flash Reclaim disabled	This controls enabling / disabling of Intel® ME AFS Idle flash reclaim capabilities. Note: This setting should be used for debug purposes only	Yes
	10	Intel® ME Reset Behavior: 0 = Intel® ME will attempt to boot from the next available image, if it exists 1 = Intel® ME 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



9.63 PCH Descriptor Record 62 (Flash Descriptor Records)

Flash Address: FPSBA + 050h

Default Flash Address: 150h

Offset from 0	Bits	Description	Usage	FIT Visible
0x150	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
	0	DCI BSSB over USB3 Port1 Configuration (EXI_PTSS_PORT0): 0 = BSSB is enabled on USB3 Port1 1 = BSSB is disabled on USB3 Port1	This setting determines if the USB port being used for DCI operations has BSSB (Boundary Scan Side Band) enabled. Note: For S0ix and reset flows BSSB should be enabled.	Yes

9.64 PCH Descriptor Record 63 (Flash Descriptor Records)

Flash Address: FPSBA + 051h

Default Flash Address: 151h

Offset from 0	Bits	Description	Usage	FIT Visible
0x151	7:0	Reserved, set to '0'		No

9.65 PCH Descriptor Record 64 (Flash Descriptor Records)

Flash Address: FPSBA + 052h

Default Flash Address: 152h

Offset from 0	Bits	Description	Usage	FIT Visible
0x152	7:0	Reserved, set to '0'		No



9.66 PCH Descriptor Record 65 (Flash Descriptor Records)

Flash Address: FPSBA + 053h

Default Flash Address: 153h

Offset from 0	Bits	Description	Usage	FIT Visible
0x153	7:0	Reserved, set to '0'		No

9.67 PCH Descriptor Record 66 (Flash Descriptor Records)

Flash Address: FPSBA + 054h

Default Flash Address: 154h

Offset from 0	Bits	Description	Usage	FIT Visible
0x154	7:0	Reserved, set to '0'		No

9.68 PCH Descriptor Record 67 (Flash Descriptor Records)

Flash Address: FPSBA + 055h

Default Flash Address: 155h

Offset from 0	Bits	Description	Usage	FIT Visible
0x155	7:0	Reserved, set to '0'		No

9.69 PCH Descriptor Record 68 (Flash Descriptor Records)

Flash Address: FPSBA + 056h

Default Flash Address: 156h

Offset from 0	Bits	Description	Usage	FIT Visible
0x156	7:0	Reserved, set to '0x7'		No

9.70 PCH Descriptor Record 69 (Flash Descriptor Records)

Flash Address: FPSBA + 057h

Default Flash Address: 157h

Offset from 0	Bits	Description	Usage	FIT Visible
0x157	7:0	Reserved, set to '0x68'		No



9.71 PCH Descriptor Record 70 (Flash Descriptor Records)

Flash Address: FPSBA + 058h

Default Flash Address: 158h

Offset from 0	Bits	Description	Usage	FIT Visible
0x158	31:0	Reserved, set to '0'		No

9.72 PCH Descriptor Record 71 (Flash Descriptor Records)

Flash Address: FPSBA + 05Ch

Default Flash Address: 15Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x15C	31:0	Reserved, set to '0'		No

9.73 PCH Descriptor Record 72 (Flash Descriptor Records)

Flash Address: FPSBA + 060h

Default Flash Address: 160h

Offset from 0	Bits	Description	Usage	FIT Visible
0x160	7:2	Reserved, set to '0'		No
	1	BIOS Guard protection override enable (LPC/spi_strap_prr_ts_ovr): 0 = BIOS Guard Fault Tolerant Update Capability is disabled 1 = BIOS guard Fault Tolerant Update Capability is enabled	This setting allows BIOS Guard to bypass the SPI Flash controller protections such as protected range registers and top swap. Note: For further details please review Intel® Platform Protection Technology with BIOS Guard 2.0 BIOS Specification regarding Fault Tolerant Update (FTU).	Yes
	0	TPM Over SPI Bus Enabled (TOS): 0 = TPM is not on SPI 1 = TPM is on SPI	This field identifies the frequency that should be used with the TPM on SPI. This field is undefined if the TPM on SPI is disabled by softstrap	Yes



9.74 MIP Table Descriptor Record 0 (Flash Descriptor Records)

Flash Address: MDTBA + 000h

Default Flash Address: C00h

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

9.75 MIP Table Descriptor Record 1 (Flash Descriptor Records)

Flash Address: MDTBA + 002h

Default Flash Address: C02h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC02	15:0	Size of MIP Descriptor Entry: Set to '0x50'	This setting determines the size in bytes of the MIP Descriptor Entry structure.	Yes

9.76 MIP Table Descriptor Record 2 (Flash Descriptor Records)

Flash Address: MDTBA + 004h

Default Flash Address: C04h

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

9.77 MIP Table Descriptor Record 3 (Flash Descriptor Records)

Flash Address: MDTBA + 006h

Default Flash Address: C06h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC06	15:0	MIP Descriptor Block 0 Offset: Set to '0x14h'	This setting determines the offset location of the MIP Descriptor Table Entries.	Yes



9.78 MIP Table Descriptor Record 4 (Flash Descriptor Records)

Flash Address:MDTBA + 008h

Default Flash Address: C08h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC08	15:0	MIP Descriptor Block 0 Length: Set to '0x34h'	This setting determine the length of the MIP Descriptor Block 0.	Yes

9.79 MIP Table Descriptor Record 5 (Flash Descriptor Records)

Flash Address:MDTBA + 00Ah

Default Flash Address: C0Ah

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

9.80 MIP Table Descriptor Record 6 (Flash Descriptor Records)

Flash Address:MDTBA + 00Ch

Default Flash Address: C0Ch

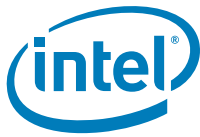
Offset from 0	Bits	Description	Usage	FIT Visible
0xC0C	15:0	MIP Descriptor Block 1 Type: Set to '0'	This setting determines what the data type is for the MIP Descriptor.	Yes

9.81 MIP Table Descriptor Record 7 (Flash Descriptor Records)

Flash Address:MDTBA + 00Eh

Default Flash Address: C0Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0xC0E	15:0	MIP Descriptor Block 1 Offset: Set to '0x48h'	This setting determines the offset location of the MIP Descriptor Table Entries.	Yes



9.82 MIP Table Descriptor Record 8 (Flash Descriptor Records)

Flash Address: MDTBA + 010h

Default Flash Address: C10h

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

9.83 MIP Table Descriptor Record 9 (Flash Descriptor Records)

Flash Address: MDTBA + 012h

Default Flash Address: C12h

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



9.84 PMC Descriptor Record 0 (Flash Descriptor Records)

Flash Address: MDTBA + 014h

Default Flash Address: C14h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC14	31:28	Reserved, set to '0'		No
	27	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



Offset from 0	Bits	Description	Usage	FIT Visible
0xC14 (cont)	18:16	Over-Clocking WDT Self-Start Enable (OC_WDT_SS_EN): 0x0 = Over-Clocking WDT disabled 0x1 = Over-Clocking WDT 3 second timeout 0x2 = Over-Clocking WDT 5 second timeout 0x3 = Over-Clocking WDT 10 second timeout 0x4 = Over-Clocking WDT 15 second timeout 0x5 = Over-Clocking WDT 30 second timeout 0x6 = Over-Clocking WDT 45 second timeout 0x7 = Over-Clocking WDT 60 second timeout	This setting affects whether the Over-Clocking WDT is enabled to automatically start on Host power cycle.	Yes
	15:12	Reserved, set to '0'		No
	11:10	tPCH46 Timing: 00 = 1 ms 01 = Reserved 10 = 5 ms 11 = 2 ms	tPch46: PROCPWRGD and SYS_PWROK high to SUS_STAT# deassertion. Refer to EDS for details.	Yes
	9:8	tPCH45 Timing: 00 = 100 ms 01 = 50 ms 10 = 5 ms 11 = 1 ms	tPCH45: PCH clock output stable to PROCPWRGD high. Refer to EDS for details.	Yes
	7:0	Reserved, set to '0x74'		No

9.85 PMC Descriptor Record 1 (Flash Descriptor Records)

Flash Address:MDTBA + 018h

Default Flash Address: C18h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC18	31:8	Reserved, set to '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

9.86 PMC Descriptor Record 2 (Flash Descriptor Records)

Flash Address:MDTBA + 01Ch

Default Flash Address: C1Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0xC1C	31:0	Reserved, set to '0x7fcd7410'		No



9.87 PMC Descriptor Record 3 (Flash Descriptor Records)

Flash Address: MDTBA + 020h

Default Flash Address: C20h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC20	31:0	Reserved, set to '0x107fff0'		No

9.88 PMC Descriptor Record 4 (Flash Descriptor Records)

Flash Address: MDTBA + 024h

Default Flash Address: C24h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC24	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



9.89 PMC Descriptor Record 5 (Flash Descriptor Records)

Flash Address: MDTBA + 028h

Default Flash Address: C28h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC28	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 = Fast Plus	This setting determines the communication speed over the I2C interface.	Yes

9.90 PMC Descriptor Record 6 (Flash Descriptor Records)

Flash Address: MDTBA + 02Ch

Default Flash Address: C2Ch

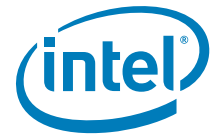
Offset from 0	Bits	Description	Usage	FIT Visible
0xC2C	31:0	Reserved, set to '0'		No

9.91 PMC Descriptor Record 7 (Flash Descriptor Records)

Flash Address: MDTBA + 030h

Default Flash Address: C30h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC30	31:0	Reserved, set to '0'		No



9.92 PMC Descriptor Record 8 (Flash Descriptor Records)

Flash Address: MDTBA + 034h

Default Flash Address: C34h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC34	31:15	Reserved, set to '0'		No
	14:8	Reserved, set to '0x64'		No
	7:0	Reserved, set to '0'		No



9.93 CPU Descriptor Record 0 (Flash Descriptor Records)

Flash Address: MDTBA + 038h

Default Flash Address: C38h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC38	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



9.94 CPU Descriptor Record 1 (Flash Descriptor Records)

Flash Address: MDTBA + 03Ch

Default Flash Address: C3Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0xC3C	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 purposes 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 purposes only.	Yes
	11:6	Flex Ratio: '0x0'	This setting controls the maximum processor non-turbo ratio. Note: This strap is intended for debugging purposes 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 purposes 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 purposes 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 purposes only. See BIOS Spec for more details on enabling / disabling Hyper threading	Yes



9.95 CPU Descriptor Record 2 (Flash Descriptor Records)

Flash Address: MDTBA + 040h

Default Flash Address: C40h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC40	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



9.96 CPU Descriptor Record 2 (Flash Descriptor Records)

Flash Address: MDTBA + 044h

Default Flash Address: C44h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC44	31:0	Reserved, set to '0'		No



9.97 Intel® ME Descriptor Record 0 (Flash Descriptor Records)

Flash Address: MDTBA + 048h

Default Flash Address: C48h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC48	31:0	Reserved, set to '0'		No



9.98 Intel® ME Descriptor Record 1 (Flash Descriptor Records)

Flash Address: MDTBA + 04Ch

Default Flash Address: C4Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0xC4C	31:24	Reserved, set to '0'		No
	23:16	Early USB DbC Intel® ME Boot Stall Enable: 0 = Intel® ME Boot Stall not enabled 1 = Intel® ME Boot Stall enabled	This setting enables a delay during Intel® ME FW bring-up to allow USB DCI to be established and Early DbC arbitration to be granted.	Yes
	15:8	USB Connector's Associated USB3 Port enable: 0x0 = USB3 Port 1 DbC enabled 0x1 = USB3 Port 2 DbC enabled 0x2 = USB3 Port 3 DbC enabled 0x3 = USB3 Port 4 DbC enabled 0x4 = USB3 Port 5 DbC enabled 0x5 = USB3 Port 6 DbC enabled 0xff = No USB3 ports are assigned to DbC All other values are Reserved	This setting determines which USB3 port goes to the target USB2 ports connector for Early DbC debugging.	Yes
	7:0	USB2 DbC port enable: 0x0 = USB2 Port 1 DbC enabled 0x1 = USB2 Port 2 DbC enabled 0x2 = USB2 Port 3 DbC enabled 0x3 = USB2 Port 4 DbC enabled 0x4 = USB2 Port 5 DbC enabled 0x5 = USB2 Port 6 DbC enabled 0x6 = USB2 Port 7 DbC enabled 0x7 = USB2 Port 8 DbC enabled 0x8 = USB2 Port 9 DbC enabled 0x9 = USB2 Port 10 DbC enabled 0xff = No USB2 ports are assigned to DbC All other values are Reserved	This setting determines which USB2 ports are enabled for Early DbC debugging.	Yes





A FAQ and Troubleshooting

A.1 FAQ

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

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

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

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

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

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

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

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

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

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

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

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

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

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



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

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

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

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

A.2 Troubleshooting

Q: I'm seeing the following error:

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

--- Flash Devices Found ---

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

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

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

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

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

Q: What does following FPT error message mean?

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

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



Q: What does following FPT error message mean?

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

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

Q: What does following FPT error message mean?

Error: There is no supported SPI flash device installed.

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

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

--- Flash Devices Found ---

SPI 1234 ID:0x123456 Size: 4096KB (32768Kb)

Device ID: 0xFFFF not supported.

Error 405: There is no supported SPI flash device installed

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

See [6.4 Recommendations for Flash Configuration Lockdown and Vendor Component Lock Bits](#) for Opcodes required for FPT operation.

§ §