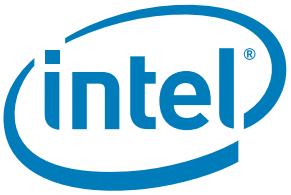


Intel® 6 Series Express Chipset SPI Programming Guide

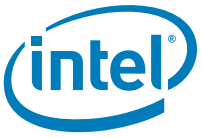
Application Note

July 2010

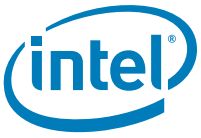
Revision 0.82

Intel Confidential

Document Number: 445780



Contents



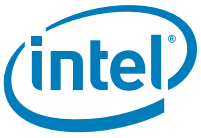
Figures

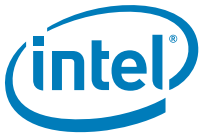
Tables

Revision History

Document Number	Revision Number	Description	Revision Date
	0.7	• Initial release.	January 2010
	0.8	• Updated Straps • Corrected	March 2010
445780	0.81	• Fixed formatting Errors	March 2010
	0.82	• Added necessary descriptor information to change processor features • Corrected language on Dual input fast read • Added SMBus Fast mose for SMLINK0 • Updated Serial Flash requirements for ME	July 2010

§ §





1 Introduction

1.1 Overview

This manual is intended for Original Equipment Manufacturers and software vendors to clarify various aspects of programming Serial Flash on PCH family based platforms. The current scope of this document is PCH for only.

Chapter 2, “PCH Serial Flash Architecture”

Overview of Serial Flash, Non-Descriptor vs. Descriptor, Flash Layout, and PCH compatible Serial Flash.

Chapter 3, “PCH Serial Flash Compatibility Requirements”

Overview of compatibility requirements for PCH products.

Chapter 4, “Flash Descriptor”

Overview of the descriptor and Descriptor record definition.

Chapter 5, “Configuring BIOS/GbE for Serial Flash Access”

Describes how to configure BIOS/GbE for Serial Flash access.

Chapter 6, “Serial Flash Discovery Parameters (SFDP) Rev 1.1”

Describes SFDP specification for Serial Flash(SPI) parts. This is a way to standardize discovery of information such as VSCC and serial flash features.

1.2 Terminology

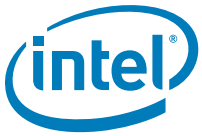
Table 1-1. Terminology

Term	Description
BIOS	Basic Input-Output System
CRB	Customer Reference Board
FPT	Flash Programming Tool - programs the Serial Flash
FIT	Flash Image Tool – creates a flash image from separate binaries
FW	Firmware
FWH	Firmware Hub – LPC based flash where BIOS may reside
Intel® AMT	Intel® Active Management Technology
GbE	Intel Integrated 1000/100/10
HDCP	High bandwidth Digital Content Protection
PCH	PCH Chipset. Platform Controller Hub
Intel® ME Firmware	Intel firmware that adds functionality such as Intel® Active Management Technology and Intel® QST, Intel Anti-Theft Technology, , etc.
Intel PCH	Intel Platform Controller Hub
Intel PCHn family	All PCHn derivatives including PCHn (desktop) and PCHnM (mobile)
Intel® QST	Intel® Quiet System Technology - Embedded hardware and firmware solution that allows for algorithmic relationship between system cooling fans and temperature monitors so as to reduce noise without losing thermal efficiency
LPC	Low Pin Count Bus- bus on where legacy devices such a FWH reside
SPI	Serial Peripheral Interface – refers to serial flash memory in this document
VSCC	Vendor Specific Component Capabilities
LVSCC	Lower Vendor Specific Component Capabilities
UVSCC	Upper Vendor Specific Component Capabilities

1.3 Reference Documents

Table 1-2. Reference Documents

Document	Document No./Location
PCH *External Design Specification (EDS)*	Contact Intel field representative
Intel® Flash Image Tool (FIT)	\System Tools\Flash Image Tool of latest Intel® ME kit from VIP/ARMS. The Kit MUST match the platform you intend to use the flash tools for.
Intel® Flash Programming Tool (FPT)	\System Tools\Flash Programming Tool of latest Intel® ME from VIP/ ARMS. The Kit MUST match the platform you intend to use the flash tools for.
FW Bring Up Guide	Root directory of latest Intel ME kit from VIP/ARMS. The Kit MUST match the platform you intend to use the flash tools for.



§ §

2 PCH Serial Flash Architecture

PCH SPI interface consists of clock (CLK), MOSI (Master Out Slave In) MISO (Master In Slave Out) and up to two active low chip selects (CSX#) on PCH.

PCH can support serial flash devices up to 16 Mbytes per chip select. PCH can support frequencies of both 20 MHz, 33 MHz, and 50 MHz.

2.1 Non-Descriptor vs. Descriptor Mode

Serial Flash on PCH has two operational modes: descriptor and non-descriptor. **PCH supports descriptor mode only.**

Non-descriptor mode is not supported in due to all PCH platforms requiring Intel ME FW.

Descriptor mode supports up to two Serial flashes, and allows for integrated LAN support, as well as Intel® ME firmware to share a single flash. There is also additional security for reads and writes to the flash. Hardware sequencing, heterogeneous flash space, Intel integrated LAN, Intel® ME firmware on Serial Flash, require descriptor mode. Descriptor mode requires the Serial Flash to be hooked up **directly** to the PCH's SPI bus.

See **SPI Supported Feature Overview** of the latest *External Design Specification (EDS)* for PCH for more detailed information.

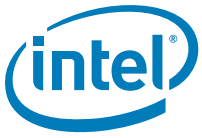
2.2 Boot Destination Options

2.2.1 Boot Flow for PCH

When booting from Global Reset the PCH SPI controller will look for a descriptor signature on the Serial Flash device on Chip Select 0 at address 0x10. The descriptor fetch is triggered by whichever comes first, the assertion of MEPWROK or deassertion of LAN_RST#. If the signature is present and valid, then the PCH controller will boot in Descriptor mode. It will load up the descriptor into corresponding registers in the PCH. If the signature is NOT present the PCH will boot in non descriptor mode where integrated LAN and all Intel Management Firmware will be disabled. Whether there is a valid descriptor or not, the PCH will look to the BIOS boot straps to determine the location of BIOS for host boot.

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

If LPC is chosen as the BIOS boot destination, then the PCH will fetch the reset vector on top of the firmware hub flash device.



If SPI is chosen as the BIOS destination, it will either fetch the reset vector on top of the Serial Flash device on chip select 0, or if the PCH is in descriptor mode it will determine the location of BIOS through the base address that is defined in the Serial Flash descriptor.

See Chapter 4, "Flash Descriptor" and for more detailed information.

2.3 Flash Regions

Flash Regions only exist in Descriptor mode. The controller can divide the Serial Flash in up to five separate regions.

Region	Content
0	Descriptor
1	BIOS
2	ME – Intel® Management Engine Firmware
3	GbE – Location for Integrated LAN firmware and MAC address
4	PDR – Platform Data Region

The descriptor (Region 0) must be located in the first sector of component 0 (offset 0x10). Descriptor and ME regions are required for all PCH based platforms

If Regions 0, 2, 3 or 4 are defined they must be on SPI. BIOS can be on either FWH or SPI. The BIOS that will load on boot will be set by Boot BIOS destination straps.

There are three masters can access the five regions: Host CPU, integrated LAN, and Intel® ME.

2.3.1 Flash Region Sizes

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

The Flash Descriptor requires one block. GbE requires two separate blocks. The amount of actual flash space consumed for the above regions are dependent on the erase granularity of the flash part. BIOS size will determine how small of a flash part can be used for the platform.

Table 2-1. Region Size vs. Erase Granularity of Flash Components

Regions	Size with uniform 4 KB blocks
Descriptor	4 KB
GbE	8 KB
Platform Data Region	Varies by platform
BIOS	Varies by platform
ME	Varies by platform and configuration

2.4 Hardware vs. Software Sequencing

Hardware and Software sequencing are the two methods the PCH uses communicates with the flash via programming registers for each of the three masters.

When utilizing software sequencing, BIOS needs to program the OPTYPE and OPMENU registers respectively with the opcode it needs. It also defines how the system should use each opcode. If the system needs a new opcode that has not been defined, then BIOS can overwrite the OPTYPE and OPMENU register and define new functionality as long as the FLOCKDN bits have not been set.

FPT as well as some BIOS implementation use software sequencing.

Hardware sequencing has a predefined list of opcodes with only the erase opcode being programmable. This mode is only available if the descriptor is present and valid. Intel® ME Firmware and Integrated LAN FW, and integrated LAN drivers all must use HW sequencing, so BIOS must properly set up the PCH to account for this. The Host VSCC registers and Management Engine VSCC table have to be correctly configured for BIOS, GbE and Intel® ME Firmware to have read/write access to SPI.

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

§ §

3 PCH Serial Flash Compatibility Requirements

3.1 PCH Serial Flash Requirements

PCH allows for up to two Serial Flash devices to store BIOS, Intel® ME Firmware and security keys for Platform Data Region and integrated LAN information.

Intel® ME FW is required for all PCH based platforms!

3.1.1 SPI-based BIOS Requirements

- Erase size capability of: 4 KBytes.
- Serial flash device must ignore the upper address bits such that an address of FFFFFFh aliases to the top of the flash memory.
- SPI Compatible Mode 0 support: Clock phase is 0 and data is latched on the rising edge of the clock.
- If the device receives a command that is not supported or incomplete (less than 8 bits), the device must discard the cycle gracefully without any impact on the flash content.
- An erase command (page, sector, block, chip, etc.) must set all bits inside the designated area (page, sector, block, chip, etc.) to 1 (Fh).
- Status Register bit 0 must be set to 1 when a write, erase or write to status register is in progress and cleared to 0 when a write or erase is NOT in progress.
- Devices requiring the Write Enable command must automatically clear the Write Enable Latch at the end of Data Program instructions.
- Byte write must be supported. The flexibility to perform a write between 1 byte to 64 bytes is recommended.
- ~~Serial Flash parts that do not meet Hardware sequencing command set requirements may work in BIOS only platforms via software sequencing.~~

3.1.2 Integrated LAN Firmware Serial Flash Requirements

A serial flash device that will be used for system BIOS and Integrated LAN or Integrated LAN only must meet all the SPI Based BIOS Requirements plus:

·Must support 3.1.8 Hardware Sequencing Requirements

·4 KBytes erase capability must be supported.

3.1.2.1 Serial Flash Unlocking Requirements for Integrated LAN

BIOS must ensure there is no Serial 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 Intel® Management Engine (Intel® ME) Firmware Serial Flash Requirements

Intel Management Firmware must meet the Serial Flash based BIOS Requirements plus:

- 3.1.6 JEDEC ID (Opcode 9Fh)
- 3.1.7 Multiple Page Write Usage Model
- 3.1.8 Hardware Sequencing Requirements
- Flash part must be uniform 4 KB erasable block throughout the entire part
- Write protection scheme must meet guidelines as defined in 3.1.3.1 Serial Flash Unlocking Requirements for Management Engine.
- If less than 256 bytes are written to a page, no data outside of the target write address will be affected, even in the case of unexpected power loss.
  - Example: If there bytes 0-63 are being programmed and if a power loss occurs during the operation. Bytes 64-255 in the page will be unaffected
- 4 KB erase cannot cause affect data anywhere else in the flash array other than the cell affected, even during power loss.

3.1.3.1 Serial Flash Unlocking Requirements for Management Engine

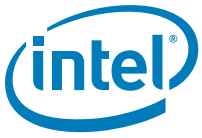
Flash devices must be globally unlocked (read, write and erase access on the ME region) from power on by writing 00h to the flash's status register to disable write protection.

If the status register must be unprotected, it must use the enable write status register command 50h or write enable 06h.

Opcode 01h (write to status register) must then be used to write a single byte of 00h into the status register. This must unlock the entire part. If the Serial 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.

If there is no need to execute a write enable on the status register, then opcodes 06h and 50h must be ignored.

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 5.1 Unlocking Serial Flash Device Protection for PCH Platforms and 5.2 Locking Serial Flash via Status Register for more information about flash based write/erase protection.



3.1.4 Single Input, Dual Output Fast Read (Optional)

The PCH supports the functionality of a dual output fast read. Opcode and address phase are shifted in serially to the serial flash SI (Serial In) pin. Data is read out after 8 clocks (dummy bits or wait states) from the both the SI and SO pin effectively doubling the throughput of each fast read output. In order to enable this functionality, both Single Input Dual Output Fast Read Supported (FCBA bit 30) and Fast Read (FCBA bit 20) supported must be set to 1b.

3.1.5 Serial Flash Discoverable Parameters(SFDP) (Recommended)

As serial flash the number features keeps growing, the need for correct, accurate configuration increases. A new method of determining configuration information is Serial Flash Discoverable Parameters (SFDP). Information such as VSCC values and flash attributes can be queried directly from the flash parts. The discoverable parameter read opcode behaves like a fast read command. The opcode is 5Ah and the address cycle is 24 bits long. After the opcode 5Ah is clocked in, there are 24 bit of address clocked in. There will then be eight clocks (8 wait states) before valid data is clocked out. SFDP is a capability of the flash part, please confirm with target flash vendor to see if it is supported.

As serial flash the number features keeps growing, the need for correct, accurate configuration increases. A new method of determining configuration information is Serial Flash Discoverable Parameters (SFDP). Information such as VSCC values and flash attributes can be read directly from the flash parts. The discoverable parameter read opcode behaves like a fast read command. The opcode is 5Ah and the address cycle is 24 bits long. After the opcode 5Ah is clocked in, there are 24 bit of address clocked in. There will then be eight clocks (8 wait states) before valid data is clocked out. SFDP is a capability of the flash part, please confirm with target flash vendor to see if there it is supported.

3.1.6 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 devicPCHe 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.

3.1.7 Multiple Page Write Usage Model

Intel platforms have firmware usage models 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 ME firmware multiple page write usage models apply to sequential and non-sequential data writes.

Flash parts must support the writing of a single bytes 1024 times in a single 256 Byte page without an erase cycle without flash corruption.

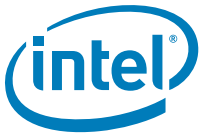
In some scenarios, will write zeros bytes of zeros over existing zeros. Flash parts must support writing of zero over zero 32 times for a byte without flash corruption.

3.1.8 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.

Table 3-1. Opcodes requirmed by Hardware Sequencing

Commands	OPCODE	Notes
Write to Status Register	01h	Writes a byte to Serial 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 Serial Flash's status register
Write Enable	06h	
Fast Read	0Bh	
Single Input Dual Output Fast Read	3Bh	Optional, See Section 3.1.4 for more information
Enable Write to Status Register	50h or 06h	Enables a bit in the status register to allow an update to the status register
Erase	Programmable	4 Kbyte erase
Chip Erase	C7h and/or 60	
JEDEC ID	9Fh	See Section 3.1.6 for more information



3.2 PCH SPI AC Electrical Compatibility Guidelines

Table 3-2. SPI Timings (20 MHz)

Sym	Parameter	Min	Max	Units	Notes
t180a	Serial Clock Frequency - 20MHz Operation	17.06	18.73	MHz	1
t183a	Tco of SPI_MOSI with respect to serial clock falling edge at the host	-5	13	ns	
t184a	Setup of SPI_MISO with respect to serial clock falling edge at the host	16	-	ns	
t185a	Hold of SPI_MISO with respect to serial clock falling edge at the host	0	-	ns	
t186a	Setup of SPI_CS[1:0]# assertion with respect to serial clock rising edge at the host	30	-	ns	
t187a	Hold of SPI_CS[1:0]# assertion with respect to serial clock rising edge at the host	30	-	ns	
t188a	SPI_CLK High time	26.37	-	ns	2
t189a	SPI_CLK Low time	26.82	-	ns	2

Notes:
1. Typical clock frequency driven by PCH is 17.86 MHz
2. Measurement point for low time and high time is taken at .5(VccME3_3)

Table 3-3. SPI Timings (33 MHz)

Sym	Parameter	Min	Max	Units	Notes
t180b	Serial Clock Frequency - 33MHz Operation	29.83	32.81	MHz	1
t183b	Tco of SPI_MOSI with respect to serial clock falling edge at the host	-5	5	ns	
t184b	Setup of SPI_MISO with respect to serial clock falling edge at the host	8	-	ns	
t185b	Hold of SPI_MISO with respect to serial clock falling edge at the host	0	-	ns	
t186b	Setup of SPI_CS[1:0]# assertion with respect to serial clock rising edge at the host	30	-	ns	
t187b	Hold of SPI_CS[1:0]# assertion with respect to serial clock rising edge at the host	30	-	ns	
t188b	SPI_CLK High time	14.88	-	ns	2
t189b	SPI_CLK Low time	15.18	-	ns	2

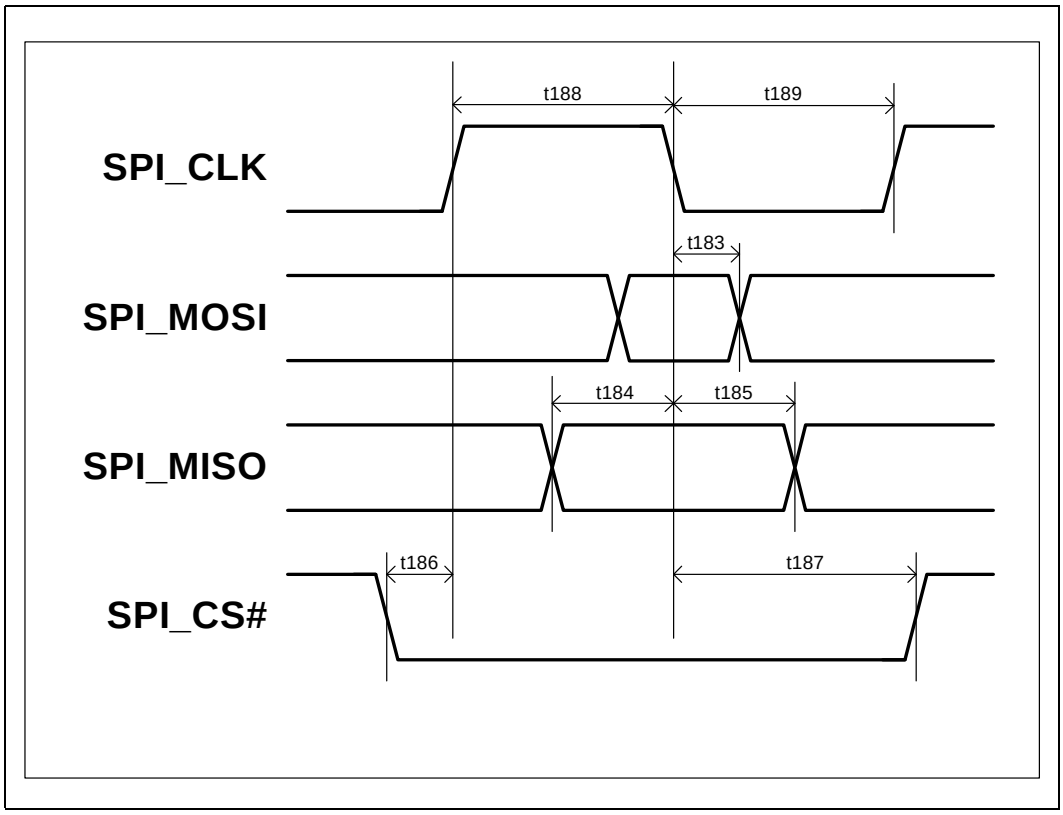
Notes:
1. Typical clock frequency driven by PCH is 31.25 MHz
2. Measurement point for low time and high time is taken at .5(VccME3_3)

Table 3-4. SPI Timings (50 MHz)

Sym	Parameter	Min	Max	Units	Notes
t180c	Serial Clock Frequency - 50MHz 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	7.1	-	ns	2, 3
t189c	SPI_CLK Low time	11.17	-	ns	2, 3

1. Typical clock frequency driven by PCH is 50 MHz. This frequency is not available for ES1 samples.
2. When using 50 MHz mode ensure target flash component can meet t188c and t189c specifications.
3. Measurement point for low time and high time is taken at .5(VccME3_3)

Figure 3-1. SPI Timings



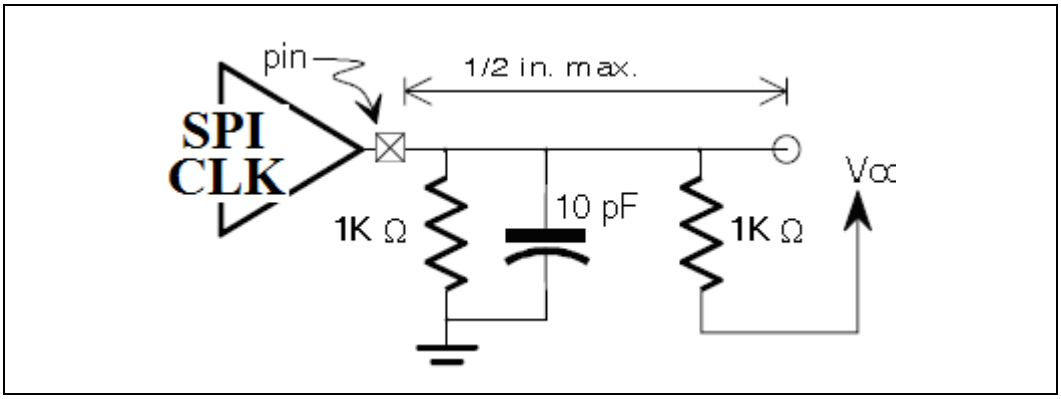
3.3 Serial Flash DC Electrical compatibility guidelines

Parameter	Min	Max	Units	Note
Supply Voltage (Vcc)	3.14	3.7	V	
Input High Voltage	0.5*VCC	VCC+0.5	V	
Input Low Voltage	-0.5	0.3*VCC	V	
Output High Characteristics	0.9*VCC	VCC	V	Ioh = -0.5mA
Output Low Characteristics		0.1*VCC		Iol = 1.5mA
Input Leakage Current	-10	10	uA	
Output Rise Slew Rate (0.2Vcc - 0.6Vcc)	1	4	V/ns	1
Output Fall Slew Rate (0.6Vcc - 0.2Vcc)	1	4	V/ns	1

Notes:

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

Figure 3-2. PCH Test Load



§ §

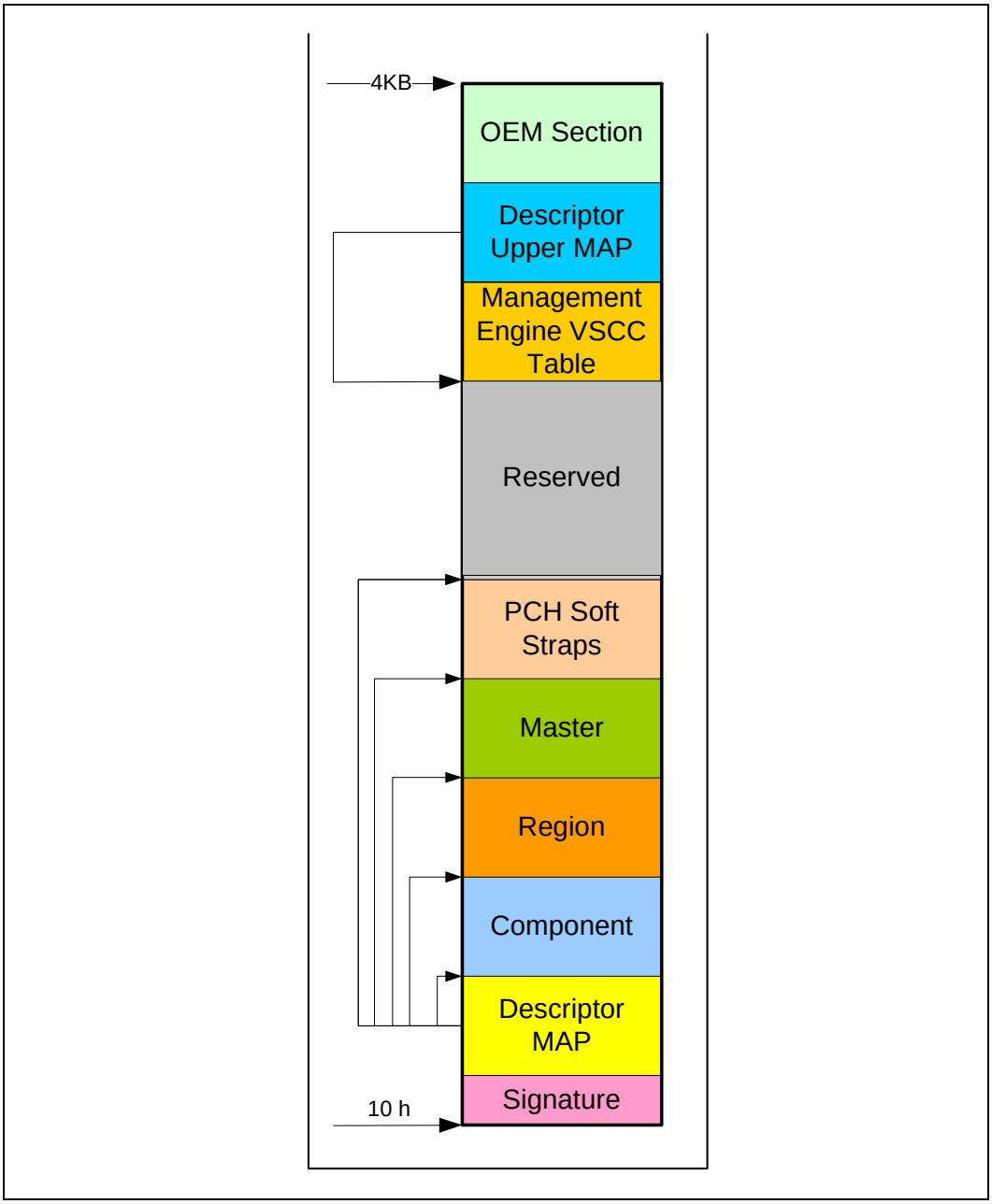
4 Flash Descriptor

The Flash Descriptor is a data structure that is programmed on the Serial Flash part on 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 Serial 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.

The descriptor has 9 basic parts:

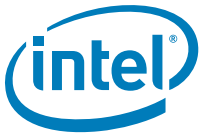
Figure 4-1. Flash Descriptor



- 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 Serial Flashpart(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, ME and GbE 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 Serial Flash part(s) supported by the NVM image. This table is NOT used by Intel® ME Ignition FW only. BIOS and GbE write and erase capabilities depend on LVSCC and UVSCC 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 *PCH 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 Serial Flash device on chip select 0.

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
31:0	**Flash Valid Signature.** This field identifies the Flash Descriptor sector as valid. If the contents at this location contain 0FF0A55Ah, then the Flash Descriptor is considered valid and it will operate in Descriptor Mode, else it will operate in Non-Descriptor Mode.

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

Memory Address:FDBAR + 014h Size:32 bits

Bits	Description
31:27	Reserved
26:24	**Number Of Regions (NR).** This field identifies the total number of Flash Regions. This number is 0's based, so a setting of all 0's indicates that the only Flash region is region 0, the Flash Descriptor region.
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. ***Note:*** Set this value to 04h. This will define FRBA as 40h.
15:10	Reserved
9:8	**Number Of Components (NC)**. This field identifies the total number of Flash Components. Each supported Flash Component requires a separate chip select. 00 = 1 Component 01 = 2 Components All other settings = Reserved
7:0	**Flash Component Base Address (FCBA)**. This identifies address bits [11:4] for the Component portion of the Flash Descriptor. Bits [24:12] and bits [3:0] are 0. ***Note:*** Set this value to 03h. This will define FCBA as 30h

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

Memory Address:FDBAR + 018h Size:32 bits

Recommended Value:12100206h

Bits	Description
31:24	**PCH Strap Length (ISL).** 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. ***Note:*** This field **MUST** be set to 12h
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. ***Note:*** Set this field to 10h. This will define FPSBA to 100h
15:10	Reserved
9:8	**Number Of Masters (NM).** This field identifies the total number of Flash Masters. ***Note:*** Set this field to 10b
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. ***Note:*** Set this field to 06h. This will define FMBA as 60h

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

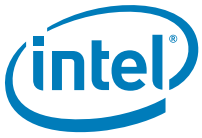
Memory Address:FDBAR + 01Ch Size:32 bits
Recommended Value:00000120h

Bits	Description
31:16	Reserved
15:08	**PROC Strap Length (PSL).** Identifies the 1's based number of Dwords of Processor Straps to be read, up to 255 DWs (1KB) max. A setting of all 0's indicates there are no Processor DW straps. ***Note:*** Set this field to 01h
7:0	**Flash Processor Strap Base Address (FPSBA).** This identifies address bits [11:4] for the Processor Strap portion of the Flash Descriptor. Bits [24:12] and bits [3:0] are 0. ***Note:*** Set this field to 20h. This will define FPSBA as 200h

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

Memory Address:FDBAR + 020h Size:32 bits

Bits	Description
31:0	Reserved



4.1.2 Flash Descriptor Component Section

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

4.1.2.1 FLCOMP—Flash Components Record (Flash Descriptor Records)

Memory Address:FCBA + 000h Size: 32 bits
Default Address: 30h

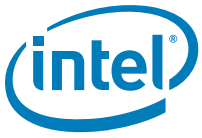
Bits	Description
31	Reserved
30	**Single Input Dual Output Fast Read Support**: 0 = Single Input, Dual Output Fast Read opcode is **NOT** supported by serial flash on the platform 1 = Single Input, Dual Output Fast Read opcode is supported by serial flash on the platform ***Notes:*** 1. If more than one Flash component exists, this field must be set to the lowest common frequency of the different Flash components 2. Only opcode supported for single input Dual Output Fast Read by PCH is 3Bh opcode 3. Fast read behavior is a combination of this bit and Fast read support as to which read operation will be used for direct reads and Hardware Sequencing Reads. Both **Single Input Dual Output Fast Read Support** and **Fast Read Support** have to be set to 1 in order to get Single Input Dual Output Fast Read Support to work.
29:27	**Read ID and Read Status Clock Frequency**. 000 = 20 MHz 001 = 33 MHz 100 = 50 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 50 MHz, ensure flash meets timing requirements defined in Table 3-4
26:24	**Write and Erase Clock Frequency**. 000 = 20 MHz 001 = 33 MHz 100 = 50 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 50 MHz, ensure flash meets timing requirements defined in Table 3-4
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 = 20 MHz 001 = 33 MHz 100 = 50 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 50 MHz, ensure flash meets timing requirements defined in Table 3-4

Bits	Description
20	**Fast Read Support**. 0 = Fast Read is not Supported 1 = Fast Read is supported ***Notes:*** 1. If the Fast Read Support bit is a '1', all Direct Read or Hardware Sequencing reads are "Fast Read" or "Single Input Dual Output Fast Read" depending on how the 2. Reads to the Flash Descriptor always use the Read command independent of the setting of this bit. 3. If more than one Flash component exists, this field can only be set to '1' if both components support Fast Read. 4. It is strongly recommended to set this bit to 1b
19:17	**Read Clock Frequency**. 000 = 20 MHz All other Settings = Reserved ***Note:*** If more than one Flash component exists, this field must be set to the lowest common frequency of the different Flash components.
16:6	Reserved
5:3	**Component 2 Density.** 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 are unused. 000 = 512 KB 001 = 1 MB 010 = 2 MB 011 = 4 MB 100 = 8 MB 101 = 16 MB 111 = Reserved
2:0	**Component 1 Density.** This field identifies the size of the 1st or only Flash component connected directly to the PCH. 000 = 512 KB 001 = 1 MB 010 = 2 MB 011 = 4 MB 100 = 8 MB 101 = 16 MB 111 = Reserved ***Note:*** If using a flash part smaller than 512 KB, use the 512 KB setting.

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

Memory Address:FCBA + 004h Size: 32 bits
Default Address: 34h

Bits	Description
31:24	**Invalid Instruction 3**. See definition of Invalid Instruction 0



Bits	Description
23:16	**Invalid Instruction 2**. See definition of Invalid Instruction 0
15:8	**Invalid Instruction 1**. See definition of Invalid Instruction 0
7:0	**Invalid Instruction 0**. Op-code 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. Op-codes programmed in the Software Sequencing Opcode Menu Configuration and Prefix-Opcode Configuration are not affected by the values in this field.

4.1.2.3 FLPB—Flash Partition Boundary Record (Flash Descriptor Records)

Memory Address:FCBA + 008h Size: 32 bits
Default Address: 38h

Bits	Description
31:13	Reserved
12:0	**Flash Partition Boundary Address (FPBA)**. This register specifies Flash Boundary Address bits[24:12] that logically divides the flash space into two partitions, a lower and an upper partition. The lower and upper partitions can support Serial Flashparts with different attributes between partitions that are defined in the LVSCC and UVSCC. ***Notes:*** 1. All flash space in each partition must have the same in the VSCC attributes, even if it spans between different flash parts. 2. If this field is set to all 0s, then there is only one partition, the upper partition, and the entire address space has uniform erasable sector sizes, write granularity, and write state required settings. The FPBA must reside on an erasable sector boundary. If set to all zeros, then only UVSCC register value is used (with the exception of the VCL bit).

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 Serial Flash.

Flash Regions:

- If a particular region is not using Serial 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 FFFh and the Region Limit to 000h 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
Default Address: 40h
Recommended Value:00000000h

Bits	Description
31:29	Reserved
28:16	**Region Limit.** This specifies bits 24:12 of the ending address for this Region. ***Notes:*** 1. Set this field to 0b. This defines the ending address of descriptor as being FFFh 2. Region limit address Bits[11:0] are assumed to be FFFh
15:13	Reserved
12:0	**Region Base.** This specifies address bits 24:12 for the Region Base. ***Note:*** Set this field to all 0s. This defines the descriptor address beginning at 0h.

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

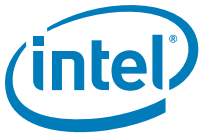
Memory Address:FRBA + 004h Size: 32 bits
Default Address: 44h

Bits	Description
31:29	Reserved
28:16	**Region Limit.** This specifies bits 24:12 of the ending address for this Region. ***Notes:*** 1. Must be set to 0000h if BIOS 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
15:13	Reserved
12:0	**Region Base.** This specifies address bits 24:12 for the Region Base. ***Note:*** If the BIOS region is not used, the Region Base must be programmed to FFFh

4.1.3.3 FLREG2—Flash Region 2 (Intel ME) Register (Flash Descriptor Records)

Memory Address:FRBA + 008h Size: 32 bits
Default Address: 48h

Bits	Description
31:29	Reserved
28:16	**Region Limit.** This specifies bits 24:12 of the ending address for this Region. ***Note:*** Ensure size is a correct reflection of actual Intel ME firmware size that will be used in the platform ***Note:*** Region limit address Bits[11:0] are assumed to be FFFh
15:13	Reserved
12:0	**Region Base.** This specifies address bits 24:12 for the Region Base.



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

Memory Address:FRBA + 00Ch Size: 32 bits
Default Address: 4Ch

Bits	Description
31:29	Reserved
28:16	**Region Limit.** This specifies bits 24:12 of the ending address for this Region. ***Notes:*** 1. The maximum Region Limit is 128KB above the region base. 2. If the GbE region is not used, the Region Limit must be programmed to 0000h 3. Region limit address Bits[11:0] are assumed to be FFFh
15:13	Reserved
12:0	**Region Base.** This specifies address bits 24:12 for the Region Base. ***Note:*** If the GbE region is not used, the Region Base must be programmed to FFFh

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

Memory Address:FRBA + 010h Size: 32 bits
Default Address: 50h

Bits	Description
31:29	Reserved
28:16	**Region Limit.** This specifies bits 24:12 of the ending address for this Region. ***Notes:*** 1. If PDR Region is not used, the Region Limit must be programmed to 0000h 2. Ensure BIOS region size is a correct reflection of actual BIOS image that will be used in the platform 3. Region limit address Bits[11:0] are assumed to be FFFh
15:13	Reserved
12:0	**Region Base.** This specifies address bits 24:12 for the Region Base. ***Note:*** If the Platform Data region is not used, the Region Base must be programmed to 1FFFh

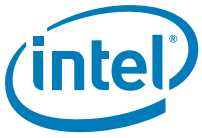
4.1.4 Flash Descriptor Master Section

See 4.3 Region Access Control for more detail on how to properly set this section.

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

Memory Address:FMBA + 000h Size:32 bits
Default Address: 60h

Bits	Description
31:29	Reserved ***Note:*** This field shoud be set to 111b if all regions of flash are open to all masters in pre-production environments. See 4.3.1 Intel Recommended Permissions for Region Access for more details.
28	**Platform Data Region Write Access**. If the bit is set, this master can erase and write that particular region through register accesses.
27	**GbE Region Write Access**. If the bit is set, this master can erase and write that particular region through register accesses.
26	**Intel ME Region Write Access**. If the bit is set, this master can erase and write that particular region through register accesses.
25	**Host CPU/BIOS Master Region Write Access**. If the bit is set, this master can erase and write that particular region through register accesses. Bit 25 is a don't care as the primary master always has read/write permissions to it's primary region
24	**Flash Descriptor Region Write Access**. If the bit is set, this master can erase and write that particular region through register accesses.
23:21	Reserved ***Note:*** This field shoud be set to 111b if all regions of flash are open to all masters in pre-production environments. See 4.3.1 Intel Recommended Permissions for Region Access for more details.
20	**Platform Data Region Read Access**. If the bit is set, this master can read that particular region through register accesses.
19	**GbE Region Read Access**. If the bit is set, this master can read that particular region through register accesses.
18	**Intel ME Region Read Access**. If the bit is set, this master can read that particular region through register accesses.
17	**Host CPU/BIOS Master Region Read Access**. If the bit is set, this master can read that particular region through register accesses. Bit 17 is a don't care as the primary master always has read/write permissions to it's primary region
16	**Flash Descriptor Region Read Access**. If the bit is set, this master can read that particular region through register accesses.
15:0	**Requester ID**. This is the Requester ID of the Host processor. This must be set to 0000h.



4.1.4.2 FLMSTR2—Flash Master 2 (Intel® ME) (Flash Descriptor Records)

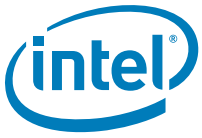
Memory Address:FMBA + 004h Size:32 bits
Default Address: 64h

Bits	Description
31:29	Reserved ***Note:*** This field shoud be set to 111b if all regions of flash are open to all masters in pre-production environments. See 4.3.1 Intel Recommended Permissions for Region Access for more details.
28	**Platform Data Region Write Access**. If the bit is set, this master can erase and write that particular region through register accesses.
27	**GbE Region Write Access**. If the bit is set, this master can erase and write that particular region through register accesses.
26	**Intel ME Master Region Write Access**. If the bit is set, this master can erase and write that particular region through register accesses. Bit 26 is a don't care as the primary master always has read/write permissions to it's primary region
25	**Host CPU/BIOS Region Write Access**. If the bit is set, this master can erase and write that particular region through register accesses.
24	**Flash Descriptor Region Write Access**. If the bit is set, this master can erase and write that particular region through register accesses.
23:21	Reserved ***Note:*** This field shoud be set to 111b if all regions of flash are open to all masters in pre-production environments. See 4.3.1 Intel Recommended Permissions for Region Access for more details.
20	**Platform Data Region Read Access**. If the bit is set, this master can read that particular region through register accesses.
19	**GbE Region Read Access**. If the bit is set, this master can read that particular region through register accesses.
18	**Intel ME Master Region Read Access**. If the bit is set, this master can read that particular region through register accesses. Bit 18 is a don't care as the primary master always has read/write permissions to it's primary region
17	**Host CPU/BIOS Region Read Access**. If the bit is set, this master can read that particular region through register accesses.
16	**Flash Descriptor Region Read Access**. If the bit is set, this master can read that particular region through register accesses.
15:0	**Requester ID**. This is the Requester ID of the Intel Management Engine. This must be set to 0000h.

4.1.4.3 FLMSTR3—Flash Master 3 (GbE) (Flash Descriptor Records)

Memory Address:FMBA + 008h Size: 32 bits
Default Address: 68h

Bits	Description
31:29	Reserved ***Note:*** This field shoud be set to 111b if all regions of flash are open to all masters in pre-production environments. See 4.3.1 Intel Recommended Permissions for Region Access for more details.
28	**Platform Data Region Write Access**. If the bit is set, this master can erase and write that particular region through register accesses.
27	**GbE Master Region Write Access**. If the bit is set, this master can erase and write that particular region through register accesses. Bit 27 is a don't care as the primary master always has read/write permissions to it's primary region
26	**Intel ME Region Write Access**. If the bit is set, this master can erase and write that particular region through register accesses.
25	**Host CPU/BIOS Region Write Access**. If the bit is set, this master can erase and write that particular region through register accesses.
24	**Flash Descriptor Region Write Access**. If the bit is set, this master can erase and write that particular region through register accesses.
23:21	Reserved ***Note:*** This field shoud be set to 111b if all regions of flash are open to all masters in pre-production environments. See 4.3.1 Intel Recommended Permissions for Region Access for more details.
20	**Platform Data Region Read Access**. If the bit is set, this master can read that particular region through register accesses.
19	**GbE Master Region Read Access**. If the bit is set, this master can read that particular region through register accesses. Bit 19 is a don't care as the primary master always has read/write permissions to it's primary region
18	**Intel ME Region Read Access**. If the bit is set, this master can read that particular region through register accesses.
17	**Host CPU/BIOS Region Read Access**. If the bit is set, this master can read that particular region through register accesses.
16	**Flash Descriptor Region Read Access**. If the bit is set, this master can read that particular region through register accesses.
15:0	**Requester ID**. This is the Requester ID of the GbE. This must be set to 0118h.



4.1.5 PCH Softstraps

See Appendix A, “APPENDIX A - Descriptor Configuration” for Record descriptions and listings

4.1.6 Processor SoftStraps

Memory Address: FDBAR + **FPSBA** Size: 32 bits
Default Address: 200h

Bits	Default	Description
31:0	0	Reserved

4.1.7 Descriptor Upper Map Section

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

Memory Address:FDBAR + EFCh Size: 32 bits

Bits	Default	Description
31:16	0	Reserved
15:8	1	**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.
7:0	1	**Intel ME VSCC Table Base Address (VTBA).** This identifies address bits [11:4] for the VSCC Table portion of the Flash Descriptor. Bits [24:12] and bits [3:0] are 0. **NOTE:** VTBA should be above the offset for PROCSTRP0 and below FLUMAP1. It is recommended that this address is set based on the anticipated maximum number of different flash parts entries.

4.1.8 Intel® ME Vendor Specific Component Capabilities Table

Entries in this table allow support for a Serial Flash part for Intel Management Engine capabilities including Intel® Active Management Technology, Intel® Quiet System Technology. BIOS will still need to set up the proper VSCC registers for BIOS and Integrated Gigabit Ethernet usage.

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

See 4.4 Intel® Management Engine (Intel® ME) Vendor-Specific Component Capabilities Tablefor information on how to program individual entries.

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

Memory Address:VTBA + 000h Size: 32 bits

Bits	Description
31:24	Reserved
23:16	**SPI Component Device ID 1.** This field identifies the second byte of the Device ID of the Serial Flash Component. This is the third byte returned by the Read JEDEC-ID command (opcode 9Fh).
15:8	**SPI Component Device ID 0.** This field identifies the first byte of the Device ID of the Serial Flash Component. This is the second byte returned by the Read JEDEC-ID command (opcode 9Fh).
7:0	**SPI Component Vendor ID.** This field identifies the one byte Vendor ID of the Serial Flash Component. This is the first byte returned by the Read JEDEC-ID command (opcode 9Fh).

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

Memory Address:VTBA + 004h Size: 32 bits

Note: In this table “Lower” applies to characteristics of all flash space below the Flash Partition Boundary Address (FPBA). “Upper” applies to characteristics of all flash space above the FPBA.

Bits	Description
31:24	**Lower Erase Opcode (LEO).** This field must be programmed with the Flash erase instruction opcode that corresponds to the erase size that is in LBES.
23:21	Reserved
20	**Lower Write Enable on Write Status (LWEWS)**. ‘0’ = 50h will be the opcode used to unlock the status register on Serial Flash if **LWSR** (bit 3) is set to 1b. ‘1’ = 06h will be the opcode used to unlock the status register on Serial Flash if **LWSR** (bit 3) is set to 1b. **NOTES:** 1.Bit 19 (**LWEWS**) and/or bit 20 (**LWSR**) should not be set to ‘1’ if there are non volatile bits in the Serial 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 Serial Flash instructions to be disregarded by the Serial Flash part. If the Serial 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 19 (**LWSR)** and 20 (**LWEWS**) are set to 1b, then sequence of 06h 01h 00h is sent to unlock the Serial Flash on EVERY write and erase that Intel Management Engine firmware performs. 4.If bit 19 (**LWSR)** is set to 1b and bit 20 (**LWEWS**) is set to 0b then sequence of 50h 01h 00h is sent to unlock the Serial Flash on EVERY write and erase that Intel Management Engine firmware performs.

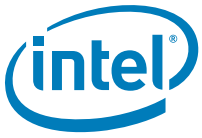
Bits	Description
19	**Lower Write Status Required (LWSR)**. 0 = No automatic write of 00h will be made to the Serial Flash's status register) 1 = A write of 00h to the Serial Flash's status register will be sent on EVERY write and erase performed by Intel ME to the Serial Flash. **NOTES:** 1.Bit 19 (**LWEWS**) and/or bit 20 (**LWSR**) should not be set to '1' if there are non volatile bits in the Serial 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 Serial Flash instructions to be disregarded by the Serial Flash part. If the Serial 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 19 (**LWSR)** and 20 (**LWEWS**) are set to 1b, then sequence of 06h 01h 00h is sent to unlock the Serial Flash on EVERY write and erase that Intel Management Engine firmware performs. 4.If bit 19 (**LWSR)** is set to 1b and bit 20 (**LWEWS**) is set to 0b then sequence of 50h 01h 00h is sent to unlock the Serial Flash on EVERY write and erase that Intel Management Engine firmware performs.
18	**Lower Write Granularity (LWG)**. 0 = 1 Byte 1 = 64 Byte
17:16	**Lower Block/Sector Erase Size (LBES)**. This field identifies the erasable sector size for all Flash space below the flash partition boundary address. Valid Bit Settings: 00 = 256 Byte 01 = 4 KB 10 = 8 KB 11 = 64 KB
15:8	**Upper Erase Opcode (UEO)**. This field must be programmed with the Flash erase instruction opcode that corresponds to the erase size that is in LBES.
7:5	Reserved

Bits	Description
4	**Upper Write Enable on Write Status (UWEWS)**. '0' = 50h will be the opcode used to unlock the status register on Serial Flash if **UWSR** (bit 3) is set to 1b. '1' = 06h will be the opcode used to unlock the status register on Serial Flash if **UWSR** (bit 3) is set to 1b. **NOTES:** 1.Bit 3 (**UWEWS**) and/or bit 4 (**UWSR**) should not be set to '1' if there are non volatile bits in the Serial 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 Serial Flash instructions to be disregarded by the Serial Flash part. If the Serial 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 (**UWSR)** and 4 (**UWEWS**) are set to 1b, then sequence of 06h 01h 00h is sent to unlock the Serial Flash on EVERY write and erase that Intel Management Engine firmware performs. 4.If bit 3 (**UWSR)** is set to 1b and bit 4 (**UWEWS**) is set to 0b then sequence of 50h 01h 00h is sent to unlock the Serial Flash on EVERY write and erase that Intel Management Engine firmware performs.
3	**Upper Write Status Required (UWSR)**. 0 = No automatic write of 00h will be made to the Serial Flash's status register) 1 = A write of 00h to the Serial Flash's status register will be sent on EVERY write and erase performed by Intel ME to the Serial Flash. **NOTES:** 1.Bit 3 (**UWEWS**) and/or bit 4 (**UWSR**) should not be set to '1' if there are non volatile bits in the Serial 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 Serial Flash instructions to be disregarded by the Serial Flash part. If the Serial 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 (**UWSR)** and 4 (**UWEWS**) are set to 1b, then sequence of 06h 01h 00h is sent to unlock the flash on EVERY write and erase that Intel Management Engine firmware performs. 4.If bit 3 (**UWSR)** is set to 1b and bit 4 (**UWEWS**) is set to 0b then sequence of 50h 01h 00h is sent to unlock the Serial Flash on EVERY write and erase that Intel Management Engine firmware performs
2	**Upper Write Granularity (UWG)**. 0 = 1 Byte 1 = 64 Bytes
1:0	**Upper Block / Sector Erase Size (UBES)**. 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

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

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

Note: "n" is an integer denoting the index of the Intel ME VSCC table.



Bits	Description
31:24	Reserved
23:16	**SPI Component Device ID 1.** This field identifies the second byte of the Device ID of the Serial Flash Component. This is the third byte returned by the Read JEDEC-ID command (opcode 9Fh).
15:8	**SPI Component Device ID 0.** This field identifies the first byte of the Device ID of the Serial Flash Component. This is the second byte returned by the Read JEDEC-ID command (opcode 9Fh).
7:0	**SPI Component Vendor ID.** This field identifies the one byte Vendor ID of the Serial Flash Component. This is the first byte returned by the Read JEDEC-ID command (opcode 9Fh).

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

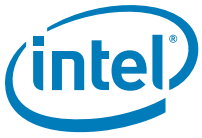
Memory Address:VTBA + 004h + (n*8)hDefault Value: Size: 32 bits

Note: "n" is an integer denoting the index of the Intel ME VSCC table.

Note: In this table "Lower" applies to characteristics of all flash space below the Flash Partition Boundary Address (FPBA). "Upper" applies to characteristics of all flash space above the FPBA.

Bits	Description
31:24	**Lower Erase Opcode (LEO).** This field must be programmed with the Flash erase instruction opcode that corresponds to the erase size that is in LBES.
23:21	Reserved
20	**Lower Write Enable on Write Status (LWEWS)**. '0' = 50h will be the opcode used to unlock the status register on Serial Flash if **LWSR** (bit 3) is set to 1b. '1' = 06h will be the opcode used to unlock the status register on Serial Flash if **LWSR** (bit 3) is set to 1b. **NOTES:** 1.Bit 19 (**LWEWS**) and/or bit 20 (**LWSR**) should not be set to '1' if there are non volatile bits in the Serial 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 Serial Flash instructions to be disregarded by the Serial Flash part. If the Serial 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 19 (**LWSR)** and 20 (**LWEWS**) are set to 1b, then sequence of 06h 01h 00h is sent to unlock the Serial Flash on EVERY write and erase that Intel Management Engine firmware performs. 4.If bit 19 (**LWSR)** is set to 1b and bit 20 (**LWEWS**) is set to 0b then sequence of 50h 01h 00h is sent to unlock the Serial Flash on EVERY write and erase that Intel Management Engine firmware performs.

Bits	Description
19	**Lower Write Status Required (LWSR)**. 0 = No automatic write of 00h will be made to the Serial Flash's status register) 1 = A write of 00h to the Serial Flash's status register will be sent on EVERY write and erase performed by Intel ME to the Serial Flash. **NOTES:** 1.Bit 19 (**LWEWS**) and/or bit 20 (**LWSR**) should not be set to '1' if there are non volatile bits in the Serial 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 Serial Flash instructions to be disregarded by the Serial Flash part. If the Serial 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 19 (**LWSR)** and 20 (**LWEWS**) are set to 1b, then sequence of 06h 01h 00h is sent to unlock the Serial Flash on EVERY write and erase that Intel Management Engine firmware performs. 4.If bit 19 (**LWSR)** is set to 1b and bit 20 (**LWEWS**) is set to 0b then sequence of 50h 01h 00h is sent to unlock the Serial Flash on EVERY write and erase that Intel Management Engine firmware performs.
18	**Lower Write Granularity (LWG)**. 0 = 1 Byte 1 = 64 Byte
17:16	**Lower Block/Sector Erase Size (LBES)**. This field identifies the erasable sector size for all Flash space below the flash partition boundary address. Valid Bit Settings: 00 = 256 Byte 01 = 4 KB 10 = 8 KB 11 = 64 KB
15:8	**Upper Erase Opcode (UEO)**. This field must be programmed with the Flash erase instruction opcode that corresponds to the erase size that is in LBES.
7:5	Reserved
4	**Upper Write Enable on Write Status (UWEWS)**. '0' = 50h will be the opcode used to unlock the status register on Serial Flash if **UWSR** (bit 3) is set to 1b. '1' = 06h will be the opcode used to unlock the status register on Serial Flash if **UWSR** (bit 3) is set to 1b. **NOTES:** 1.Bit 3 (**UWEWS**) and/or bit 4 (**UWSR**) should not be set to '1' if there are non volatile bits in the Serial 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 Serial Flash instructions to be disregarded by the Serial Flash part. If the Serial 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 (**UWSR)** and 4 (**UWEWS**) are set to 1b, then sequence of 06h 01h 00h is sent to unlock the Serial Flash on EVERY write and erase that Intel Management Engine firmware performs. 4.If bit 3 (**UWSR)** is set to 1b and bit 4 (**UWEWS**) is set to 0b then sequence of 50h 01h 00h is sent to unlock the Serial Flash on EVERY write and erase that Intel Management Engine firmware performs.



Bits	Description
3	**Upper Write Status Required (UWSR)**. 0 = No automatic write of 00h will be made to the Serial Flash's status register) 1 = A write of 00h to the Serial Flash's status register will be sent on EVERY write and erase performed by Intel ME to the Serial Flash. **NOTES:** 1.Bit 3 (**UWEWS**) and/or bit 4 (**UWSR**) should not be set to '1' if there are non volatile bits in the Serial 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 Serial Flash instructions to be disregarded by the Serial Flash part. If the Serial 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 (**UWSR)** and 4 (**UWEWS**) are set to 1b, then sequence of 06h 01h 00h is sent to unlock the flash on EVERY write and erase that Intel Management Engine firmware performs. 4.If bit 3 (**UWSR)** is set to 1b and bit 4 (**UWEWS**) is set to 0b then sequence of 50h 01h 00h is sent to unlock the Serial Flash on EVERY write and erase that Intel Management Engine firmware performs
2	**Upper Write Granularity (UWG)**. 0 = 1 Byte 1 = 64 Bytes
1:0	**Upper Block / Sector Erase Size (UBES)**. 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

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

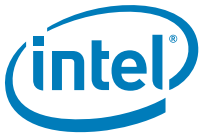
Refer to the **FLMSTR1**, **FLMSTR2** and **FLMSTR3** sections of *Intel PCH External Design Specification (EDS)* for register information for each master.

Table 4-1. Example Flash Master Register

Bits	Description
31:29	Reserved, must be zero.
28	**Platform Data Region Write Access:** If the bit is set, this master can erase and write that particular region through register accesses.
27	**GbE Region Write Access:** If the bit is set, this master can erase and write that particular region through register accesses.
26	**ME Region Write Access:** If the bit is set, this master can erase and write that particular region through register accesses.
25	**Host CPU/BIOS Master Region Write Access:** If the bit is set, this master can erase and write that particular region through register accesses.
24	**Flash Descriptor Region Write Access:** If the bit is set, this master can erase and write that particular region through register accesses.
23:21	Reserved, must be zero.
20	**Platform Data Region Read Access:** If the bit is set, this master can read that particular region through register accesses.
19	**GbE Region Read Access:** If the bit is set, this master can read that particular region through register accesses.
18	**ME Region Read Access:** If the bit is set, this master can read that particular region through register accesses.
17	**Host CPU/BIOS Master Region Read Access:** If the bit is set, this master can read that particular region through register accesses.
16	**Flash Descriptor Region Read Access:** If the bit is set, this master can read that particular region through register accesses.
15:0	**Requester ID:** This field is different for each master: Host CPU/BIOS = 0000h, ME= 0000h, GbE = 0118h .

Table 4-2. Region Access Control Table Options

Master Read/Write Access			
Region (#)	CPU and BIOS	ME/MCH	GbE Controller
Descriptor (0)	Read / Write	Read / Write	Read / Write
BIOS (1)	CPU and BIOS can always read from and write to BIOS region	Read / Write	Read / Write
ME (2)	Read / Write	ME can always read from and write to ME region	Read / Write
GbE (3)	Read / Write	Read / Write	GbE software can always read from and write to GbE region
PDR (4)	Read / Write	Read / Write	Read / Write



NOTES:
1. Descriptor and PDR regions are not masters, so they will not have Master R/W access.
2. Descriptor should NOT have write access by any master in production systems.
3. PDR region should only have read and/or write access by CPU/Host. GbE and ME should NOT have access to PDR region.

4.3.1 Intel Recommended Permissions for Region Access

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

Table 4-3. Recommended Read/Write Settings for Platforms Using Intel® ME Firmware

Master Access	Descriptor Region Bit 0	ME Region Bit 2	GbE Region Bit 3	BIOS Region Bit 1	PDR Region Bit 4
ME read access	Y	Y	Y	N	N
ME write access	N	Y	Y	N	N
GbE read access	N	N	Y	N	N
Master Access	**Descriptor Region Bit 0**	**ME Region Bit 2**	**GbE Region Bit 3**	**BIOS Region Bit 1**	**PDR Region Bit 4**
GbE write access	N	N	Y	N	N
BIOS read access	Y	N	Y	Y	‡
BIOS write access	N	N	Y	Y	‡

NOTES:
1. ‡ = Host access to PDR is the discretion of the customer. Implementation of PDR is optional

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.

Table 4-4. Recommended Read/Write Settings for Platforms Using Intel® ME Firmware (Cont'd)

	ME	GbE	BIOS
Read	0b 0000 1101 = 0x0d	0b 0000 1000 = 0x08	0b 000‡ 1011 = 0x‡B
Write	0b 0000 1100 = 0x0c	0b 0000 1000 = 0x08	0b 000‡ 1010 = 0x‡A

NOTES:
1. ‡ = Value dependent on if PDR is implemented and if Host access is desired.

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 GPIO33 low 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.exe 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 writablewriteable/readable.

See 5.3 SPI Protected Range Register Recommendations for more details

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

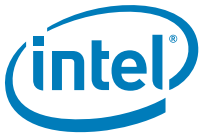
The Intel® ME VSCC Table defines how the Intel® ME will communicate with the installed Serial Flash. This table is defined in the descriptor and is the responsibility of who puts together the NVM image. LVSCC and/or UVSCC registers are defined in memory space and must be set by BIOS. This table must define every flash part that is intended to be used. The size (number of max entries) of the table is defined in 4.1.7.1 FLUMAP1—Flash Upper Map 1 (Flash Descriptor Records). Each Table entry is made of two parts: the JEDEC ID and VSCC setting.

4.4.1 How to Set a JEDEC ID Portion of Intel® ME VSCC Table Entry

Table 4-5. Jidn - JEDEC ID Portion of Intel® ME VSCC Table

Bits	Description
31:24	Reserved.
23:16	**SPI Component Device ID 1:** This identifies the second byte of the Device ID of the Serial Flash Component. This is the third byte returned by the Read JEDEC-ID command (opcode 9Fh).
15:8	**SPI Component Device ID 0:** This identifies the first byte of the Device ID of the Serial Flash Component. This is the second byte returned by the Read JEDEC-ID command (opcode 9Fh).
7:0	**SPI Component Vendor ID:** This identifies the one byte Vendor ID of the Serial Flash Component. This is the first byte returned by the Read JEDEC-ID command (opcode 9Fh).

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



4.1.7.1 FLUMAP1—Flash Upper Map 1 (Flash Descriptor Records) thru 4.1.8.4 VSCCn—Vendor Specific Component Capabilities n (Flash Descriptor Records)

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

Lower VSCC (bits 31:16) needs to be programmed in instances where the Flash Partition Boundary is not 0x0. When using an asymmetric flash component (part with two different sets of attributes based on address) a Flash Partition Boundary will need to be used. This includes if the system is intended to support both symmetric AND asymmetric Serial Flash parts. If all flash parts that will be used on this system are not asymmetric, and if all flash space has all the same attributes (not the same vendor or family), then only UVSCC (bits 15:0) needs to be populated.

It is advised that you program both LVSCC and UVSCC in order to support the widest range of flash components.

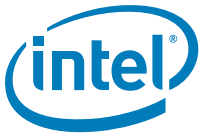
Refer to 4.4.3 Example Intel® ME VSCC Table Settings for PCH Systems.

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

Table 4-6. Vsccn – Vendor-Specific Component Capabilities Portion of the PCH Platforms

Bits	Description
31:24	**Lower Erase Opcode (LEO).** This field must be programmed with the Flash erase instruction opcode that corresponds to the erase size that is in LBES.
23:21	Reserved
20	**Lower Write Enable on Write Status (LWEWS).** '0' = 50h will be the opcode used to unlock the status register on Serial Flash if **LWSR** (bit 3) is set to 1b. '1' = 06h will be the opcode used to unlock the status register on Serial Flash if **LWSR** (bit 3) is set to 1b. **NOTES:** 1. Bit 19 (**LWEWS**) and/or bit 20 (**LWSR**) should not be set to '1' if there are non volatile bits in the Serial 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 Serial Flash instructions to be disregarded by the Serial Flash part. If the Serial 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 19 (**LWSR**) and 20 (**LWEWS**) are set to 1b, then sequence of 06h 01h 00h is sent to unlock the Serial Flash on EVERY write and erase that Intel Management Engine firmware performs. 4. If bit 19 (**LWSR**) is set to 1b and bit 20 (**LWEWS**) is set to 0b then sequence of 50h 01h 00h is sent to unlock the Serial Flash on EVERY write and erase that Intel Management Engine firmware performs.

Bits	Description
19	**Lower Write Status Required (LWSR)**. 0 = No automatic write of 00h will be made to the Serial Flash's status register) 1 = A write of 00h to the Serial Flash's status register will be sent on EVERY write and erase performed by Intel ME to the Serial Flash. **NOTES:** 1.Bit 19 (**LWEWS**) and/or bit 20 (**LWSR**) should not be set to '1' if there are non volatile bits in the Serial 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 Serial Flash instructions to be disregarded by the Serial Flash part. If the Serial 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 19 (**LWSR)** and 20 (**LWEWS**) are set to 1b, then sequence of 06h 01h 00h is sent to unlock the Serial Flash on EVERY write and erase that Intel Management Engine firmware performs. 4.If bit 19 (**LWSR)** is set to 1b and bit 20 (**LWEWS**) is set to 0b then sequence of 50h 01h 00h is sent to unlock the Serial Flash on EVERY write and erase that Intel Management Engine firmware performs.
18	**Lower Write Granularity (LWG)**. 0 = 1 Byte 1 = 64 Byte
17:16	**Lower Block/Sector Erase Size (LBES)**. This field identifies the erasable sector size for all Flash space below the flash partition boundary address. Valid Bit Settings: 00 = 256 Byte 01 = 4 KB 10 = 8 KB 11 = 64 KB
15:8	**Upper Erase Opcode (UEO)**. This field must be programmed with the Flash erase instruction opcode that corresponds to the erase size that is in LBES.
7:5	Reserved



Bits	Description
4	**Upper Write Enable on Write Status (UWEWS)**. '0' = 50h will be the opcode used to unlock the status register on Serial Flash if **UWSR** (bit 3) is set to 1b. '1' = 06h will be the opcode used to unlock the status register on Serial Flash if **UWSR** (bit 3) is set to 1b. **NOTES:** 1.Bit 3 (**UWEWS**) and/or bit 4 (**UWSR**) should not be set to '1' if there are non volatile bits in the Serial 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 Serial Flash instructions to be disregarded by the Serial Flash part. If the Serial 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 (**UWSR)** and 4 (**UWEWS**) are set to 1b, then sequence of 06h 01h 00h is sent to unlock the Serial Flash on EVERY write and erase that Intel Management Engine firmware performs. 4.If bit 3 (**UWSR)** is set to 1b and bit 4 (**UWEWS**) is set to 0b then sequence of 50h 01h 00h is sent to unlock the Serial Flash on EVERY write and erase that Intel Management Engine firmware performs.
3	**Upper Write Status Required (UWSR)**. 0 = No automatic write of 00h will be made to the Serial Flash's status register) 1 = A write of 00h to the Serial Flash's status register will be sent on EVERY write and erase performed by Intel ME to the Serial Flash. **NOTES:** 1.Bit 3 (**UWEWS**) and/or bit 4 (**UWSR**) should not be set to '1' if there are non volatile bits in the Serial 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 Serial Flash instructions to be disregarded by the Serial Flash part. If the Serial 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 (**UWSR)** and 4 (**UWEWS**) are set to 1b, then sequence of 06h 01h 00h is sent to unlock the flash on EVERY write and erase that Intel Management Engine firmware performs. 4.If bit 3 (**UWSR)** is set to 1b and bit 4 (**UWEWS**) is set to 0b then sequence of 50h 01h 00h is sent to unlock the Serial Flash on EVERY write and erase that Intel Management Engine firmware performs
2	**Upper Write Granularity (UWG)**. 0 = 1 Byte 1 = 64 Bytes

Bits	Description
1:0	**Upper Block/Sector Erase Size (UBES)**. 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

Upper and Lower Erase Opcode (**LEO/UEO**) and **Upper and Lower Block/Sector Erase Size** (**LBSES/UBSES**) should be set based on the flash part and the firmware on the platform. For Intel® ME enabled platforms this should be 4 KB.

Either **Upper and Lower Write Status Required (LWSR and UWSR) or Upper Write Enable on Write Status (LWEWS and UWEWS)** 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 **LWSR/UWSR** bit to 1b and **LWEWS/UWEWS** to 0b if the Enable Write Status Register opcode (50h) is needed to unlock the status register. Opcodes sequence sent to Serial Flash will bit 50h 01h 00h.
- Set the **LWEWS/UWEWS** bit AND **LWSR/UWSR** bit to 1b if write enable (06h) will unlock the status register. Opcodes sequence sent to Serial Flash will bit 06h 01h 00h.
- **LWSR/UWSR or LWEWS/UWEWS 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 5.1 Unlocking Serial Flash Device Protection for PCH Platforms and 5.2 Locking Serial Flash via Status Register for more information.

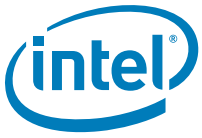
Erase Opcode (**EO**) and Block/Sector Erase Size (**BES**) should be set based on the flash part and the firmware on the platform.

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 23:21 and 7:5 are reserved and should set to all zeros.

4.4.3 Example Intel® ME VSCC Table Settings for PCH Systems

Below is a table that provides general guidelines for BIOS VSCC settings for different Serial Flash devices. These settings are not part recommendations, nor are they an indication these parts are supported on Intel platforms. Flash parts may change



opcodes and architectures so please refer to the respective flash datasheet and flash vendor to confirm.

Please refer to 4.4.2 How to Set a VSCC Entry in Intel® ME VSCC Table for PCH Platforms for requirements and how the below values were derived.

Vendor/ Family	Jedec Vendor ID	ME VSCC Table Entry	Upper Flash Erase	Lower Flash Erase	Notes
Atmel* AT25DFxxx or AT26DFxxx1	0x1F	0x20152015, or 0x201D201D	4 KB	4 KB	1, 4, 5
Macronix* MX25L	0xC2	0x20052005	4 KB	4 KB	1, 4
SST* 25VF	0xBF	0x20092009 or 0x200D200D	4 KB	4 KB	1,2,6~~4~~
Numonyx* / ST Micro* M25PE/PF/PX	0x20	0x20052005	4 KB	4 KB	1,3,4
Winbond* W25X / W25Q	0xEF	0x20052005	4 KB	4 KB	1,4

NOTES:

1. Upper 2 bytes of ME VSCC Table Entry is not necessary to program if Flash Partition Boundary is zero and flash is not asymmetric. For example: 0x00002005 instead of 0x20052005.
2. SST* is a registered trademark of Silicon Storage Technology, Inc.
3. Verify the Erase granularity as it may change with revision of flash part. 256 B erase is not supported in any Intel® ME Firmware.
4. Using 0x20012001, 0x20192019 or 0x20112011 will result in slower Intel® ME Firmware performance.
5. Both values are valid.
6. Use 0x200D200D if the flash part supports 256 Byte (page) write. The parts parts that only support single byte MUST use 0x20092009

§ §

5 Configuring BIOS/GbE for Serial Flash Access

5.1 Unlocking Serial Flash Device Protection for PCH Platforms

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.

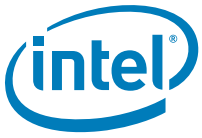
All the Serial Flash devices that meet the Serial Flash requirements in the *Intel PCH External Design Specification (EDS)* will be unlocked by writing a 00h to the Serial Flash's status register. This command must be done via an atomic software sequencing to account for differences in flash architecture. 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 *Intel PCH External Design Specification (EDS)* more detailed information.



5.2 Locking Serial 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 Serial 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 Serial Flash protection in multiple master systems such as Management Engine firmware and/or integrated GbE. BIOS must ensure that any flash based protection will only apply to BIOS region only. It should not affect ~~not~~ 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.

5.3 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 Ignition 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 Ignition FW factory defaults. This would allow a flashing of a complete image when the Flash descriptor Override strap is set.

5.4 Software Sequencing Opcode Recommendations

It is strongly recommended that the "9Fh" JEDEC ID be used instead of "90h" or "AB". The JEDEC ID Council ensures that every Serial Flash model is unique. There are flash vendors that have flash parts of different sizes that report out the same value using the "90h" opcode.

Intel utilities such as the Flash Programming tool will incorrectly detect the flash part in the system and it may lead to undesired program operation.

Intel Flash Programming tool requires the following software sequencing opcodes to be programmed in the OPMENU and corresponding OPTYPE register.

It is strongly recommended that you do not program opcodes write enable commands into the OPMENU definition. These should be programmed in the PREOP register.

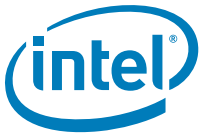
Order of the opcodes is not important, but the OPMENU and OPTYPE do have to correspond. see **OPTYPE— Opcode Type Configuration Register OPMENU- Opcode Menu Configuration Register** in the *Intel PCH External Design Specification (EDS)*.

Table 5-1. Recommended opcodes for FPT operation

Function	OPMENU	OPTYPE
Write to Status Register	0x01	'01'
Program Data	0x02	'11'
Read Data	0x03	'10'
Read Status Register	0x05	'00'
4 KB Erase	0x20	'11'
JEDEC ID	0x9F	'00'
Serial Flash Discovery Parameters (SFDP)	0x5A	'10'

Table 5-2. Recommended opcodes for FPT operation

Function	PREOP
Write Enable	0x06
Enable Status Register Write	0x50



5.5 Recommendations for Flash Configuration Lockdown and Vendor Component Lock Bits

5.5.1 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 Serial Flash Programing Registers** section in the *Intel PCH External Design Specification (EDS)*.

5.5.2 Vendor Component Lock

It is strongly recommended that BIOS sets the **Vendor Component Lock (VCL)** bits. These bits are located in the BIOS/GbE LVSCC registers. VCL applies the lock to both LVSCC and UVSCC even if LVSCC 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 Serial Flash functionality.

Refer to **LVSCC— Lower Vendor Specific Component Capabilities Register** in the *Intel PCH External Design Specification (EDS)* for more information.

5.6 Host Vendor Specific Component Control Registers (LVSCC and UVSCC) for PCH Family Systems

LVSCC and UVSCC are memory mapped registers are used by the PCH when BIOS or Integrate LAN reads, programs or erases the Serial Flash via Hardware sequencing.

All Serial Flash address space above or equal to the Flash Partition Boundary Address (FPBA) that is in the Flash Partition Boundary Register (FLPB) utilizes the UVSCC register for flash access. All Serial Flash address space below what is defined as the Flash Partition Boundary Address (FPBA) uses the LVSCC register for flash access.

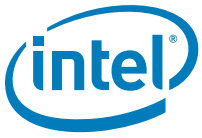
If Serial Flash space has only one set of attributes, UVSCC needs to be set. In addition, the Flash Partition Boundary Address in the FLPB in the descriptor must be set to all 0's. The bit definitions for UVSCC and LVSCC are identical, they just apply to different areas of Serial Flash space.

Refer to **LVSCC— Lower Vendor Specific Component Capabilities Register** and **UVSCC— Upper Vendor Specific Component Capabilities Register** in the *Intel PCH External Design Specification (EDS)*.

See text below the tables for explanation on how to determine LVSCC and UVSCC register values.

Table 5-3. LVSCC - Lower Vendor-Specific Component Capabilities Register

Bit	Description
31:24	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. ***Notes:*** 1. This bit applies to both UVSCC and LVSCC registers. 2. All bits locked by (**VCL)** will remained locked until a global reset.
22:16	Reserved
15:8	**Lower Erase Opcode (LEO)**— RW: This register is programmed with the Flash erase instruction opcode required by the vendor's Flash component. This register is locked by the Vendor Component Lock (**VCL**) bit.
7:5	Reserved
4	**Lower Write Enable on Write Status (LWEWS)** — RW: '0' = 50h will be the opcode used to unlock the status register on the Serial Flash if **LWSR** (bit 3) is set to 1b. '1' = 06h will be the opcode used to unlock the status register on the Serial Flash if **LWSR** (bit 3) is set to 1b. This register is locked by the Vendor Component Lock (VCL) bit. **NOTES**: 1.Bit 3 (**LWEWS**) and/or bit 4 (**LWSR**) should not be set to 1b if there are non volatile bits in the Serial Flash device'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 Serial Flash instructions to be disregarded by the flash part. If the SPI 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 (**LWSR)** and 4 (**LWEWS**) are set to 1b, then sequence of 06h 01h 00h is sent to unlock the flash on EVERY write and erase that Processor or Intel GbE FW performs. 4.If bit 3 (**LWSR)** is set to 1b and bit 4 (**LWEWS**) is set to 0b then sequence of 50h 01h 00h is sent to unlock the Serial Flash on EVERY write and erase that Processor or Intel GbE FW performs.



Bit	Description
3	**Lower Write Status Required (LWSR)** — RW: '0' = No automatic write of 00h will be made to the Serial Flash's status register. '1' = A write of 00h to the Serial Flash's status register will be sent on EVERY write and erase to the Serial Flash performed by Host and GbE. This register is locked by the Vendor Component Lock (**VCL**) bit. **NOTES:** 1. Bit 3 (**LWEWS**) and/or bit 4 (**LWSR**) should not be set to '1' if there are non volatile bits in the Serial 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 Serial Flash instructions to be disregarded by the Serial Flash part. If the Serial 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 (**LWSR)** and 4 (**LWEWS**) are set to 1b, then sequence of 06h 01h 00h is sent to unlock the flash on EVERY write and erase that Processor or Intel GbE FW performs. 4. If bit 3 (**LWSR)** is set to 1b and bit 4 (**LWEWS**) is set to 0b then sequence of 50h 01h 00h is sent to unlock the Serial Flash on EVERY write and erase that Processor or Intel GbE FW performs.
2	**Lower Write Granularity (LWG) —** RW**:** 0: 1 Byte 1: 64 Byte This register is locked by the Vendor Component Lock (**VCL**) bit. **NOTES:** 1. If more than one Flash component exists, this field must be set to the lowest common write granularity of the different Flash components 2. If using 64 B write, BIOS must ensure that multiple byte writes do not occur over 256 B boundaries. This will lead to corruption as the write will wrap around the page boundary on the Serial Flash part. This is a feature in page writable Serial Flash.
1:0	**Lower Block/Sector Erase Size (LBES)—** RW: This field identifies the erasable sector size for all Flash components. Valid Bit Settings: 00: 256 Byte 01: 4 KByte 10: 8 KByte 11: 64 K This register is locked by the Vendor Component Lock (**VCL**) bit. Hardware takes no action based on the value of this register. The contents of this register are to be used only by software and can be read in the HSFSTS.BERASE register in both the BIOS and the GbE program registers if FLA is less than FPBA.

Lower Erase Opcode (**LEO**) and **Lower Block/Sector Erase Size** (**LBSES**) should be set based on the flash part and the firmware image on the platform.

Either **Lower Write Status Required (LWSR) OR Lower Write Enable on Write Status (LWEWS)** 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 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.

- Set the **LWSR** bit to 1b and **LWEWS** to 0b if the Enable Write Status Register opcode (50h) is needed to unlock the status register. Opcodes sequence sent to Serial Flash will bit 50h 01h 00h.
- Set the **LWEWS** bit AND **LWSR** bit to 1b if write enable (06h) will unlock the status register. Opcodes sequence sent to Serial Flash will bit 06h 01h 00h.
- **LWSR or LWEWS 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 5.1 Unlocking Serial Flash Device Protection for PCH Platforms and 5.2 Locking Serial Flash via Status Register for more information.
- **Lower Write Granularity (LWG)** 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.

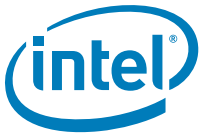
Vendor Component Lock (VCL) should remain unlocked during development, but locked in shipping platforms. When **VCL** and **FLOCKDN** are set, it is possible that you may not be able to use in system programming methodologies including Intel Flash Programming Tool if programmed improperly. It will require a system reset to unlock this register and BIOS not to set this bits. See 5.5 Recommendations for Flash Configuration Lockdown and Vendor Component Lock Bits for more details.

Bit ranges 31:24 and 22:16 and 7:5 are reserved and should set to all zeros.

See below table for explanation on how to set bits.

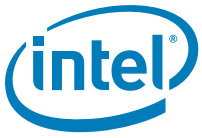
Table 5-4. UVSCC - Upper Vendor-Specific Component Capabilities Register

Bit	Description
31:16	Reserved



Bit	Description
15:8	**Upper Erase Opcode (UEO)**— RW: This register is programmed with the Flash erase instruction opcode required by the vendor's Flash component. This register is locked by the Vendor Component Lock (**VCL**) bit.
7:5	Reserved
4	**Upper Write Enable on Write to Status (UWEWS)** — RW: '0' = 50h will be the opcode used to unlock the status register if **UWSR** (bit 3) is set to 1b. '1' = 06h will be the opcode used to unlock the status register if **UWSR** (bit 3) is set to 1b. This register is locked by the Vendor Component Lock (**VCL**) bit. **NOTES**: 1.Bit 3 (**UWEWS**) and/or bit 4 (**UWSR**) should not be set to 1b if there are non volatile bits in the Serial Flash device'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 Serial Flash instructions to be disregarded by the flash part. If the SPI 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 (**UWSR)** and 4 (**UWEWS**) are set to 1b, then sequence of 06h 01h 00h is sent to unlock the flash on EVERY write and erase that Processor or Intel GbE FW performs. 4.If bit 3 (**UWSR)** is set to 1b and bit 4 (**UWEWS**) is set to 0b then sequence of 50h 01h 00h is sent to unlock the Serial Flash on EVERY write and erase that Processor or Intel GbE FW performs.

Bit	Description
3	**Upper Write Status Required (UWSR)** — RW: '0' = No automatic write of 00h will be made to the Serial Flash's status register '1' = A write of 00h to the Serial Flash's status register will be sent on EVERY write and erase to the Serial Flash performed by Host and GbE. This register is locked by the Vendor Component Lock (**VCL**) bit. **NOTES:** 1. Bit 3 (**UWEWS**) and/or bit 4 (**UWSR**) should not be set to '1' if there are non volatile bits in the Serial 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 Serial Flash instructions to be disregarded by the Serial Flash part. If the Serial 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 (**UWSR)** and 4 (**UWEWS**) are set to 1b, then sequence of 06h 01h 00h is sent to unlock the flash on EVERY write and erase that Processor or Intel GbE FW performs. 4. If bit 3 (**UWSR)** is set to 1b and bit 4 (**UWEWS**) is set to 0b then sequence of 50h 01h 00h is sent to unlock the Serial Flash on EVERY write and erase that Processor or Intel GbE FW performs
2	**Upper Write Granularity (UWG) —** RW**:** 0: 1 Byte 1: 64 Byte This register is locked by the Vendor Component Lock (**VCL**) bit. If more than one Flash component exists, this field must be set to the lowest common write granularity of the different Flash components. If using 64 B write, BIOS must ensure that multiple byte writes do not occur over 256 B boundaries. This will lead to corruption as the write will wrap around the page boundary on the Serial Flash part. This is a feature in page writeable Serial Flash.
1:0	**Upper Block/Sector Erase Size (UBES)—** RW: This field identifies the erasable sector size for all Flash components. Valid Bit Settings: 00: 256 Byte 01: 4 KByte 10: 8 KByte 11: 64 K This register is locked by the Vendor Component Lock (**VCL**) bit. Hardware takes no action based on the value of this register. The contents of this register are to be used only by software and can be read in the HSFSTS.BERASE register in both the BIOS and the GbE program registers if FLA is less than FPBA.



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

Either **Upper Write Status Required (UWSR) or Upper Write Enable on Write Status (UWEWS)** 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 Serial 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.

- Set the **UWSR** bit to 1b and **UWEWS** to 0b if the Enable Write Status Register opcode (50h) is needed to unlock the status register. Opcodes sequence sent to Serial Flash will bit 50h 01h 00h.
- Set the **UWEWS** bit AND **UWSR** bit to 1b if write enable (06h) will unlock the status register. Opcodes sequence sent to Serial Flash will bit 06h 01h 00h.
- **UWSR or UWEWS 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 5.1 Unlocking Serial Flash Device Protection for PCH Platforms and 5.2 Locking Serial Flash via Status Register for more information.

Upper Write Granularity (UWG) 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.**Bit ranges 31:16 and 7:5** are reserved and should set to all zeros.

5.7 Example Host VSCC Register Settings for PCH Systems

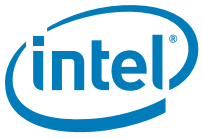
Below is a table that provides general guidelines for BIOS VSCC settings for different Serial Flash devices. These settings are not part recommendations, nor are they an indication these parts are supported on Intel platforms. Flash parts may change opcodes and architectures so please refer to the respective flash datasheet and flash vendor to confirm.

Please refer to 3 PCH Serial Flash Compatibility Requirements and **5.4 Software Sequencing Opcode Recommendations, 5.6 Host Vendor Specific Component Control Registers (LVSCC and UVSCC) for PCH Family Systems for requirements and how the below values were derived.

Vendor/Family	Jedec Vendor ID	UVSCC	LVSCC	Upper Flash Erase	Lower Flash Erase	Notes
Atmel* AT25DFxxx or AT26DFxxx1	0x1F	0x2015 (mbw), 0x2011 (sbw) or 0x201D (mbw), 0x2019 (sbw)	0x802015 (mbw), 0x802011 (sbw) or 0x80201D (mbw), 0x802019, (sbw)	4 KB	4 KB	1,5,6,7, 8
Macronix* MX25L	0xC2	0x2005 (mbw) or 0x2001 (sbw)	0x802005 (mbw) or 0x802001 (sbw)	4 KB	4 KB	1,5,6,8
SST* 25VF	0xBF	0x2009 (sbw) or 0x200D (mbw)	0x802009	4 KB	4 KB	1,2,6,9
Numonyx* / ST Micro* 25PE/PF/PX	0x20	0x2005 (mbw) or 0x2001 (sbw)	0x802005 (mbw) or 0x802001 (sbw)	4 KB	4 KB	1,3,5,6,8
Winbond* W25X / W25Q	0xEF	0x2005 (mbw) or 0x2001 (sbw)	0x802005 (mbw) or 0x802001 (sbw)	4 KB	4 KB	1,5,6,8

NOTES:

1. It is not necessary to program LVSCC if the Flash Partition boundary is 0x0.
2. SST* is a registered trademark of Silicon Storage Technology, Inc.
3. Verify the Erase granularity as it may change with different revisions of flash part. 256 B erase is not supported in any Intel® ME Firmware.
4.
5. Use sbw setting if BIOS does not prevent the writing across 256 Byte page boundaries with multiple byte writes.
6. It is strongly recommended to set bit 23 of LVSCC on shipping platforms. See 5.5.2 Vendor Component Lock for more details.

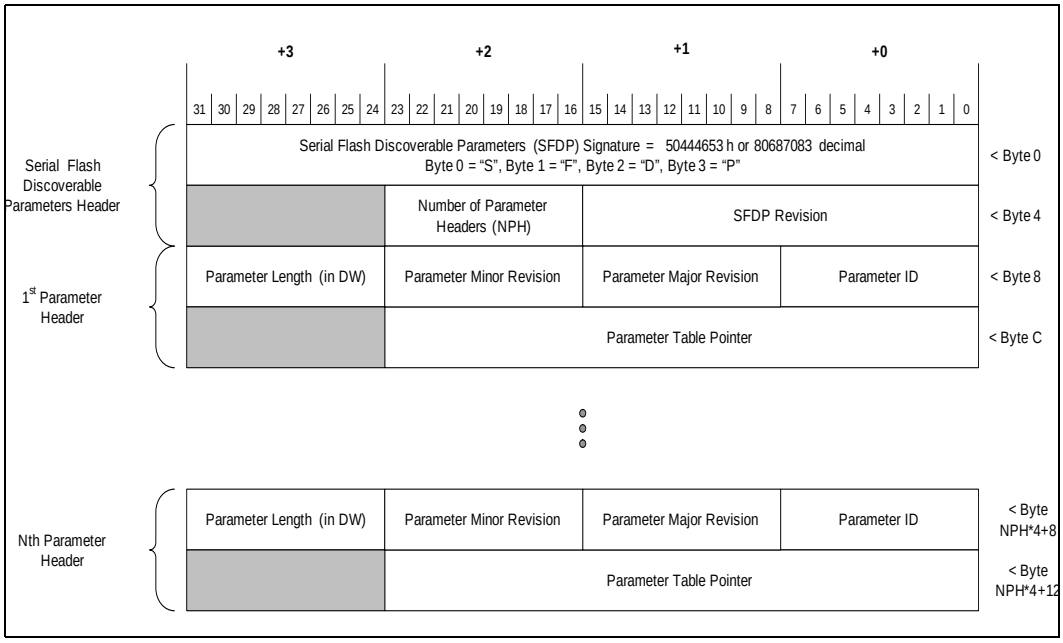


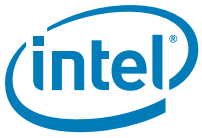
7. When using values of 0x2015, 0x2011, 0x802015, and/or 0x802011 you must unlock the status register. See 5.1 Unlocking Serial Flash Device Protection for PCH Platforms for details
8. mbw = multiple byte write capable. sbw = single byte write capable.
9. Not all SST* parts support multiple byte write. Please ensure the target flash parts support before using multiple byte write capable VSCC message (0x200D200D).

6 Serial Flash Discovery Parameters (SFDP) Rev 1.1

6.1 Specification

6.1.1 Serial Flash Discoverable Parameters Data Structure





6.1.2 SDFP Data Structure

6.1.2.1 Offset 0h: SFDPSIG – Serial Flash Discoverable Parameters Signature

Bit	Description
31:00	Serial Flash Discoverable Parameters (SFDP) Signature: When performing the Discoverable Parameter Read to this address, this will let a controller know that this is valid information. If the contents at this location do not return the expected value, then the Discoverable Parameters are assumed to be un-programmed or corrupted and is not usable. Signature[31:00]: 50444653h

6.1.2.2 Offset 4h: SFPDREV – SFPD Revision

Bit	Description
15:08	Serial Flash Discoverable Parameters (SFDP) Revision: 8 bits for Major revisions. Major revisions are changes that reorganize or add parameters that are locations that are NOT currently Reserved. Major revisions would require code (BIOS/firmware) or hardware change to get previously defined discoverable parameters. Note: Major Revision starts at 01h

07:00	Serial Flash Discoverable Parameters (SFDP) Revision: 8 bits for Minor revision Minor revisions are changes that add discoverable parameters is existing Reserved locations. This field should be set to 01h Minor revisions are changes that add parameters in existing Reserved locations, or clarifications to existing fields. Minor revisions do NOT change overall structure of SFDP. Note: Minor Revision starts at 00h

6.1.2.3 Offset 6h: NPH - Number of Parameter Headers

Bit	Description
15:08	Reserved
07:00	**Number of Parameter Headers (NPH):** Defines the number of parameter headers in the SFDP data structure. This number is 0's based, so 0 = 1 parameter header

6.1.2.4 Offset 8h: Parameter ID(0):Serial Flash Basic properties

Bit	Description
31:24	**Parameter ID(0):Serial Flash Basic Length:** This field defines how many Dwords are in the ParameterID(0) field. ***Note:*** If this Parameter is unimplemented then this must be set to 00h

23:16	**Parameter ID(0):Serial Flash Basic Major revisions:** 8 bits for Major revisions. Major revisions are changes that reorganize or add parameters that are locations that are NOT currently Reserved. Major revisions would require code (BIOS/firmware) or hardware change to get previously defined discoverable parameters. ***Note:*** Note: Major Revision starts at 01h
15:08	**Parameter ID(0):Serial Flash Basic Minor revisions:** 8 bits for Minor revision ~~Minor revisions are changes that add discoverable parameters to existing Reserved locations.~~ Minor revisions are changes that add parameters in existing Reserved locations, or clarifications. Minor revisions do NOT change overall structure of SFDP. ***Note:*** Note: Minor Revision starts at 00h
07:00	**Parameter ID(0) ID Number:** ~~Serial Flash Basic properties: This field must be programmed to 0x0. Parameters must be programmed in increasing order.~~Manufacturer JEDEC ID number: This field must be programmed with manufacturer JEDEC ID number. Note: Intel ID is 89h. The PCH controller will be looking for Parameter ID # 89h for the appropriate configuration information

6.1.2.5 Offset Ch: Parameter ID(0):Serial Flash Basic properties Address

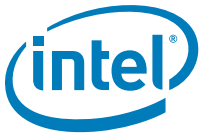
Bit	Description
31:24	Reserved
23:00	**PIDADD(0): Address of Parameter ID(0) Table:** This is a 24 bit address that will define where Parameter ID(0) is in the Discoverable Parameter array.

6.1.2.6 Offset 10h: Parameter ID(1): Serial Flash properties

Bit	Description
31:24	**Parameter ID(1):Serial Flash Length:** This field defines how many Dwords are in the ParameterID(1) field. ***Note:*** If this Parameter is unimplemented then this must be set to 00h
23:16	**Parameter ID(1): Serial Flash properties: Major revisions:** 8 bits for Major revisions. Major revisions are changes that reorganizes or add parameters that are locations that are NOT currently Reserved. Major revisions would require code (BIOS/firmware) or hardware change to get previously defined discoverable parameters. ***Note:*** Major Revision starts at 01h
15:08	**Parameter ID(1): Serial Flash properties Minor revisions:** 8 bits for Minor revision ~~Minor revisions are changes that add discoverable parameters to existing Reserved locations.~~Minor revisions are changes that add parameters in existing Reserved locations, or clarifications. Minor revisions do NOT change overall structure of SFDP. ***Note:*** Minor Revision starts at 00h
07:00	**Parameter ID(1) ID Number:** Manufacturer JEDEC ID number: This field must be programmed with manufacturer JEDEC ID numberSerial Flash properties: This field must be programmed to 0x1. Parameters must be programmed in increasing order.

6.1.2.7 Offset 14h: Parameter ID(1):Serial Flash Properties Address

Bit	Description
31:24	Reserved



23:00	**PIDADD(1): Address of Parameter ID(1) Table:** This is a 24 bit address that will define where Parameter ID(1) is in the Discoverable Parameter array.

6.1.2.8 Offset (8*(NPH) + 0x8)h: Parameter ID(N): Serial Flash Parameter ID(N) properties

Bit	Description
31:24	**Parameter ID(N):Serial Flash Parameter ID(N) Length:** This field defines how many Dwords are in the ParameterID(N) field. ***Note:*** If this Parameter is unimplemented then this must be set to 00h
23:16	**Parameter ID(N): Serial Flash Parameter ID(N) properties: Major revisions:** 8 bits for Major revisions. Major revisions are changes that reorganize or add parameters that are locations that are NOT currently Reserved. Major revisions would require code (BIOS/firmware) or hardware change to get previously defined discoverable parameters. ***Note:*** Major Revision starts at 01h
15:08	**Parameter ID(N): Serial Flash Parameter ID(N) properties Minor revisions:** 8 bits for Minor revision ~~Minor revisions are changes that add discoverable parameters to existing Reserved locations.~~Minor revisions are changes that add parameters in existing Reserved locations, or clarifications. Minor revisions do NOT change overall structure of SFDP. ***Note:*** Minor Revision starts at 00h
07:00	**Parameter ID(N) ID Number:** Manufacturer JEDEC ID number: This field must be programmed with manufacturer JEDEC ID number. Serial Flash Parameter ID(N) properties: This field must be programmed to 0xN. Parameters must be programmed in increasing order.

6.1.2.9 Offset (8*(NPH) + 0xC)h: Parameter ID(N):Serial Flash Parameter ID(N) properties Address

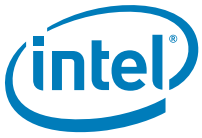
Bit	Description
31:24	Reserved
23:00	**PIDADD(N): Address of Parameter ID(N) Table:** This is a 24 bit address that will define where Parameter ID(N) is in the Discoverable Parameter array.

6.1.3 ParameterID(0) Flash Basics

The ParameterID(0) describes general behavior of the flash component.

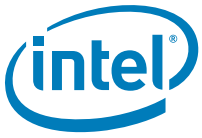
6.1.3.1 Offset PIDADD(0): Parameter ID(0) properties

Bit	Description
31:23	Reserved
22	Supports Single Input Address Quad Output Fast Read: Device supports single input address phase, Quad output data phase fast read. 0: Single Input Address Quad Output Fast Read NOT supported. 1: Single Input Address Quad Output Fast Read supported. All dummy bits and mode bits shifting in '0' (after opcode+address, before valid data out) will NOT enter any execute in place mode, or mode that will skip opcode.
21	Supports Quad Input Address Quad Output Fast Read: Device supports Quad input address phase, Quad output data phase fast read. 0: Quad Input Address Quad Output Fast Read NOT supported. 1: Quad Input Address Quad Output Fast Read supported. All dummy bits and mode bits shifting in '0' (after opcode+address, before valid data out) will NOT enter any execute in place mode, or mode that will skip opcode.



Bit	Description
20	Supports Dual Input Address Dual Output Fast Read: Device supports Dual input address phase, dual output data phase fast read. 0: Dual Input Address Dual Output Fast Read NOT supported. 1: Dual Input Address Dual Output Fast Read supported. All dummy bits and mode bits shifting in '0' (after opcode+address, before valid data out) will NOT enter any execute in place mode, or mode that will skip opcode.
19	Supports Dual Transfer Rate Clocking: 0: Dual Transfer Rate Clocking NOT supported 1: Dual Transfer Rate Clocking supported All dummy bits and mode bits shifting in '0' (after opcode+address, before valid data out) will NOT enter any execute in place mode, or mode that will skip opcode.
18:17	Number of bytes used in addressing for flash array read, write and erase: 00: 3 bytes, or 24 bit addressing 01: 4 bytes, or 32 bit addressing 10: Reserved 11: Reserved **Note:** All flash under 128 Mb in size should use 00 for this value for 24 bit addressing. This field refers to the number of address bits/bytes that are clocked in for any command requiring an address in the flash array. Examples: Read, Fast Read, Write, 4 Kilo Byte Erase.
16	Supports Single Input Address Dual Output Fast read: Device supports single input address phase, dual output data phase fast read with 8 bits of wait states. 0: Single Input Address Dual Output Fast Read NOT supported. 1: Single Input Address Dual Output Fast Read supported. **Note:** This bit should only be set to '1' if the Opcode for Single Input Address Dual Output Data is 3Bh.
15:08	**4 Kilo Byte Erase Opcode :** **Note:** If 4 Kilo Byte erase is not supported then enter FFh.
07:05	Reserved

Bit	Description
04	Write Enable Opcode Select for Writing to Volatile Status Register: 0: 50h is the Opcode that is written to the status register when bit 3 is set to 1. 1: 06h is the Opcode that is written to the status register when bit 3 is set to 1. **Note**: If target flash register is non-Volatile, then bits 3 and 4 must be set to 0b.
03	Write Enable Command Required for Writing to Volatile Status Register: 0: Target flash has non-volatile status bit and does not require status register to be written on every power on to allow writes and erases. 1: Target flash requires a status register is requires a 00h to be written to the status register in order to allow writes and erases. **Note**: If target flash register is non-Volatile, then bits 3 and 4 must be set to 0b.
02	Write Granularity: 0: 1 Byte – Use this setting for single byte programmable devices 1: 64 Byte – Use this setting for page programmable devices. **Note:** These must support 64 Byte writes.
01:00	**Block/Sector Erase Sizes:** Identifies the erase granularity for all Flash Components. 00: Reserved 01: 4 Kilo Byte Erase 10: Reserved 11: 64 Kilo Byte Erase (Should only be set if 4 Kilo Byte erase is unavailable)



6.1.3.2 Offset PIDADD(0) + 4h: Parameter ID(0) properties

Bit	Description
31:00	**Flash Size in bits.** Example: 00FFFFFFh = 16 Mega bits

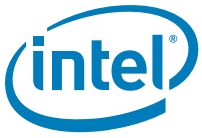
6.1.3.3 Offset PIDADD(0) + 8h: Parameter ID(0) properties

Bit	Description
31:24	**Single Input Address Quad Output Fast Read Opcode:** Opcode for Single input address phase, Quad output data phase fast read.
23:21	**Single Input Address Quad Output Fast Read Number of Mode Bits:** If Mode bits are not supported, enter 000b in this field **Note:** This field should be counted in clocks (cycles of CLK) not number of bits received by the serial flash. **Example:** If 4 mode bits are needed with a single input address phase command, this field would be 100b
20:16	**Single Input Address Quad Output Fast Read Number of Wait states (dummy bits) needed before valid output:** If dummy bits/wait states are not supported, enter 00000b in this field **Note:** This field should be counted in clocks (cycles of CLK). **Example:** If 8 bits are needed with a single input address phase command, this field would be 01000b
15:8	**Quad Input Address Quad Output Fast Read Opcode:** Opcode for Quad input address phase, Quad output data phase fast read

Bit	Description
7:5	**Quad Input Address Quad Output Fast Read Opcode Number of Mode Bits:** If Mode bits are not supported, enter 000b in this field **Note:** This field should be counted in clocks (cycles of CLK) not number of bits received by the serial flash. **Example:** If 8 mode bits are needed with a quad input address phase command, this field would be 010b
4:0	**Quad Input Address Quad Output Fast Read Opcode Number of Wait states (dummy bits) needed before valid output:** If dummy bits/wait states are not supported, enter 00000b in this field **Note:** This field should be counted in clocks (cycles of CLK). **Example:** If 16 bits are needed with a quad input address phase command, this field would be 00100b

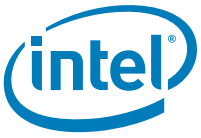
6.1.3.4 Offset PIDADD(0) + Ch: Parameter ID(0) properties

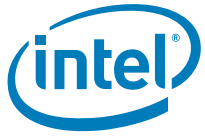
Bits	Description
31:24	**Dual Input Address Dual Output Fast Read Opcode:** Opcode for Dual input address phase, Dual output data phase fast read.
23:21	**Dual Input Address Dual Output Fast Read Number of Mode Bits:** If Mode bits are not supported, enter 000b in this field **Note:** This field should be counted in clocks (cycles of CLK) not number of bits received by the serial flash. **Example:** If 8 mode bits are needed with a dual input address phase command, this field would be 100b



Bits	Description
20:16	**Dual Input Address Dual Output Fast Read Number of Wait states (dummy bits) needed before valid output:** If dummy bits/wait states are not supported, enter 00000b in this field **Note:** This field should be counted in clocks (cycles of CLK). **Example:** If 8 bits are needed with a dual input address phase command, this field would be 00100b
15:8	**Single Input Address Dual Output Fast Read Opcode:** Opcode for Single input address phase, Dual output data phase fast read
7:5	**Single Input Address Dual Output Fast Read Opcode Number of Mode Bits:** If Mode bits are not supported, enter 000b in this field **Note:** This field should be counted in clocks (cycles of CLK) not number of bits received by the serial flash. **Example:** If 4 mode bits are needed with a single input address phase command, this field would be 100b
4:0	**Single Input Address Dual Output Fast Read Opcode Number of Wait states (dummy bits) needed before valid output:** This field should be programmed with 01000b for 8 bits of dummy cycle. **Note:** If dummy bits for this this opcode is not 01000b, then PIDADD(0) bit 16 (Supports Single Input, Dual Output fast must NOT be set to '1')

§ §





A APPENDIX A - Descriptor Configuration

A.1 Flash Descriptor PCH Soft Strap 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.

Only default values that will be provided are for softstraps that are reserved.

A.2 PCHSTRP0—Strap 0 Record (Flash Descriptor Records)

Flash Address: FPSBA + 000h Size:32 bits
Default Flash Address: 100h

Bits	Description	Usage
31	Reserved, set to '0'	
30:29	**BIOS Boot-Block size (BBBS):** Sets BIOS boot-block size 00: 64 KB. Invert A16 if Top Swap is enabled (Default) 01: 128 KB. Invert A17 if Top Swap is enabled 10: 256 KB. Invert A18 if Top Swap is enabled 11: 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 Boot block size. This value has to be determined by how BIOS implements Boot-Block.	BIOS Boot-Block size deals with a BIOS recovery mechamism. It allows for the system to use alternate code in order to boot a platform based upon the **Top Swap** (GPIO[55] pulled low during the rising edge of **PWROK**.) strap being asserted. **Top Swap** inverts an address on access to SPI and firmware hub, so the processor believes its fetches the alternate boot block instead of the original boot-block. The size of the boot-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. If BIOS is located on firmware hub, then this value must be set to '00'. Refer to **Boot-Block Update Scheme** in the latest revision of Patsburg EDS. ***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.
28:25	Reserved, set to '0'	
24	**DMI RequesterID Check Disable (DMI_REQID_DIS):** The primary purpose of this strap is to support environments with multiple processors that each have a different RequesterID that can each access to Serial Flash. 0 = DMI RequesterID Checks are enabled 1 = DMI RequesterID Checks are disabled. No Requester ID checking is done on accesses from DMI.	This bit is only applicable for platforms that contain multiple processor sockets. If multiple processors need to access Serial Flash then this bit would need to set to '1'. Platforms that have a single processor socket set to '0'

Bits	Description	Usage
23:22	Reserved, set to '0'	
21	**LinkSec Disable (LINKSEC_DIS)** 0 = LinkSec is Enabled 1 = LinkSec is Disabled ***Notes:*** 1. If not using Intel integrated wired LAN or if disabling it, then set to '1' 2. If using Intel integrated wired LAN solution **AND** the use of Linksec is desired set to '0'.	LinkSec is a hop-by-hop network security solution. It provides Layer 2 encryption and authenticity/integrity protection for packets traveling between LinkSec-enabled nodes of the network. The key components that need to support this functionality are the server, client and switch network interface devices. If not using Intel's integrated wired solution, then this field must be set to '1'. ***Note:*** This setting is not the same for all designs, is dependent on the board design. The platform hardware designer can determine the setting for this
20	**LAN PHY Power Control GPIO12 Select (LANPHYPC_GP12_SEL):** 0 = GPIO12 default is General Purpose (GP) output 1 = GPIO12 is used in native mode as LAN_PHY_PWR_CTRL ***Notes:*** 1. If not using Intel integrated wired LAN or if disabling it, then set to '0' 2. If using Intel integrated wired LAN solution **AND** if GPIO12 is routed to LAN_DISABLE_N on the Intel PHY, this bit should be set to '1'.	If using Intel integrated wired LAN solution **AND** if GPIO12 is routed to LAN_DISABLE_N on the Intel PHY, this bit must be set to '1'. If GPIO12 is routed not routed to LAN_DISABLE_N on the Intel PHY, this bit must be set to '0'. If not using Intel integrated wired LAN or if disabling it, this bit must be set to '0' ***Note:*** This setting is not the same for all designs, is dependent on the board design. The platform hardware designer can determine the setting for this.
19:16	Reserved, set to '0'	
15:14	**SMLink0 Frequency (SML0FRQ):** These bits determine the physical bus speed supported by the HW. ~~Must be programmed to 01b (100 kHz)~~Must be programmed to 11b (SMBus Fast Mode). All other values reserved.	Fast Mode will be the only supported speed of SMLink0 interface. Speed on this bus will between 300 KHz and 350 KHz. Speed is dependent on board topology and layout.
13:12	**Intel ME SMBus Frequency (SMB0FRQ):** The value of these bits determine the physical bus speed supported by the HW. Must be programmed to 01b (100 kHz)	100 kHz will be the only supported speed of the Intel ME SMBus interface.
11:10	**SMLink1 Frequency (SML1FRQ) Frequency:** The value of these bits determine the physical bus speed supported by the HW. Must be programmed to 01b (100 kHz). All other values reserved.	100 kHz will be the only supported speed of the SMLink1 interface.

Bits	Description	Usage
9	**SMLink1 Enable (SML1_EN):** Configures if SMLink1 segment is enabled 0 = Disabled 1 = Enabled ***Note:*** This must be set to '1' platforms that use PCH SMBus based thermal reporting.	This bit must be set to '1' if using the PCH's Thermal reporting. If setting this bit to '0', there must be an external solution that gathers temperature information from PCH and processor. ***Note:*** This setting is not the same for all designs, is dependent on the board design. The setting of this field must be determined by the BIOS developer and the platform hardware designer.
8	**SMLink0 Enable (SML0_EN):** Configures if SMLink0 segment is enabled 0 = Disabled 1 = Enabled ***Notes:*** 1. This bit MUST be set to '1' when utilizing Intel integrated wired LAN. 2. The Intel PHY SMBus controller must be routed to this SMLink 0 Segment. 3. If not using Intel integrated wired LAN solution or if disabling it, then this segment must be set to '0'.M	This bit MUST be set to '1' when utilizing Intel integrated wired LAN. The Intel PHY SMBus controller must be routed to this SMLink 0 Segment. If not using Intel integrated wired LAN solution or if disabling it, then this segment must be disabled (set to '0'). ***Note:*** This setting is not the same for all designs, is dependent on the board design. The setting of this field must be determined by the BIOS developer and the platform hardware designer.
7	**Intel ME SMBus Select (SMB_EN):** Configures if the ME SMBus segment is enabled 0 = Disabled 1 = Enabled ***Note:*** This bit MUST be set to '1'.	This bit must always be set to '1'.
6:2	Reserved, set to '0'	
1	**Chipset Configuration Softstrap 1**: Must be set to 1b.	
0	Reserved, set to '0'	

A.3 PCHSTRP1—Strap 1 Record (Flash Descriptor Records)

Flash Address: FPSBA + 004h Default Value: 0000000Fh Size:32 bits
Default Flash Address: 104h

Bits	Description	Usage
31:94	Reserved, set to '0'	
8	**Chipset Configuration Softstrap 2**: Must be set to 1b.	
7:4		
3:0	**Chipset Configuration Softstrap 3**: Must be set to Fh.	

A.4 PCHSTRP2—Strap 2 Record (Flash Descriptor Records)

Flash Address: FPSBA + 008h Size:32 bits
Default Flash Address: 108h

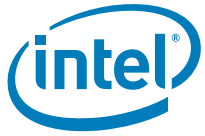
Bits	Description	Usage
31:25	**Intel® ME SMBus I²C Address (MESMI2CA):** Defines 7 bit Intel® ME SMBus I²C target address ***Note:*** This field is only used for testing purposes	This address is only used by Intel® ME FW for testing purposes. If **MESMI2CEN (PCHSTRP2 bit 24)** is set to 1 then the address used in this field must be non-zero and not conflict with any other devices on the segment.
24	**Intel® ME SMBus I²C Address Enable (MESMI2CEN):** 0 = Intel® ME SMBus I²C Address is disabled 1 = Intel® ME SMBus I²C Address is enabled ***Note:*** This field is only used for testing purposes on Intel® ME Ignition FW	This field should only be set to '1' for testing purposes
23:17	**Intel® ME SMBus** MCTP **Address (MESMMCTPA):** Defines 7 bit Intel® ME SMBus MCTP target address ***Note:*** This field is only used for testing purposes on Intel® ME Ignition FW.	This address is used by Intel® ME Anti-Theft Technology . If **MESMI2CEN (PCHSTRP2 bit 24)** is set to 1 then the address used in this field must be non-zero and not conflict with any other devices on the segment.

Bits	Description	Usage
16	**Intel® ME SMBus** MCTP **Address Enable (MESMMCTPAEN):** 0 = Intel® ME SMBus MCTP Address is disabled 1 = Intel® ME SMBus MCTP Address is enabled ***Note:*** This field is only used for testing purposes on Intel® ME Ignition FW	This field should only be set to '1' for testing purposes on platforms that use Intel® ME Ignition FW.
15:9	**Intel® ME SMBus Alert Sending Device (ASD) Address (MESMASDA):** Intel ME SMBus Controller ASD Target Address. ***Note:*** This field is only applicable if there is an ASD attached to SMBus and using Intel® AMT	If **MESMASDEN(PCHSTRP2 bit 8)** is set to '1' there must be a valid address for ASD. The address must be determined by the BIOS developer based on the requirements below. A valid address must be: • Non-zero value • Must be a unique address on the Host SMBus segment • Be compatible with the master on SMBus - For example, if the ASD address the master that needs write thermal information to an address "xy"h. Then this field must be set to "xy"h.
8	**Intel® ME SMBus Alert Sending Device (ASD) Address Enable (MESMASDEN):** 0 = Intel® ME SMBus ASD Address is disabled 1 = Intel® ME SMBus ASD Address is enabled ***Note:*** This field is only applicable if there is an ASD attached to SMBus and using Intel® AMT	This bit must only be set to '1' when there is an ASD (Alert Sending Device) attached to Host SMBus. This is only applicable in platforms using Intel® AMT. ***Note:*** This setting is not the same for all designs, is dependent on the board design. The setting of this field must be determined by the BIOS developer and the platform hardware designer.
7:0	Reserved, set to '0'	

A.5 PCHSTRP3—Strap 3 Record (Flash Descriptor Records)

Flash Address: FPSBA + 00Ch Default Value: 00000000h Size:32 bits
Default Flash Address: 10Ch

Bits	Description	Usage
31:0	Reserved, set to '0'	



A.6 PCHSTRP4—Strap 4 Record (Flash Descriptor Records)

Flash Address: FPSBA + 010h Size:32 bits
Default Flash Address: 110h

Bits	Description	Usage
31:24	Reserved, set to '0'	
23:17	**GbE PHY SMBus Address:** This is the 7 bit SMBus address the PHY uses to accept SMBus cycles from the MAC. ***Note:*** This field must be programmed to 64h.	This is the Intel PHY's SMBus address. This field must be programmed to 64h. GbE PHY SMBus Address and GbE MAC address have to be programmed to 64h and 70h in order to ensure proper arbitration of SMBus communication between the Intel integrated MAC and PHY.
16	Reserved, set to '0'	
15:9	**GbE MAC SMBus Address:** This is the 7 bit SMBus address uses to accept SMBus cycles from the PHY. ***Note:*** This field must be programmed to 70h.	This is the Intel integrated wired MAC's SMBus address. This field must be programmed to 70h. GbE PHY SMBus Address and GbE MAC address have to be programmed to 64h and 70h in order to ensure proper arbitration of SMBus communication between the Intel integrated MAC and PHY.

Bits	Description	Usage
8	**Gbe MAC SMBus Address Enable (GBEMAC_SMBUS_ADDR_EN):** 0 = Disable 1 = Enable ***Notes:*** 1. This bit MUST be set to '1' when utilizing Intel integrated wired LAN. 2. If not using Intel integrated wired LAN solution or if disabling it, then this segment must be set to '0'.	This bit must be set to '1' if Intel integrated wired LAN solution is used. If not using, or if disabling Intel integrated wired LAN solution, then this field must be set to '0'.
7:2	Reserved, set to '0'	
01:00	**Intel PHY Connectivity (PHYCON[1:0]):** This field determines if Intel wired PHY is connected to SMLink0 00: No Intel wired PHY connected 10: Intel wired PHY on SMLink0 All other values Reserved ***Notes:*** 1. This bit MUST be set to '10' when utilizing Intel integrated wired LAN. 2. If not using, or if disabling Intel integrated wired LAN solution, then this segment must be set to 00b.	This field must be set to "10" if Intel integrated wired LAN solution is used. If not using, or if disabling Intel integrated wired LAN solution, then field must be set to "00".

A.7 PCHSTRP5—Strap 5 Record (Flash Descriptor Records)

Flash Address: FPSBA + 014h Default Value: 00000000h Size:32 bits
Default Flash Address: 114h

Bits	Description	Usage
31:0	Reserved, set to '0'	

A.8 PCHSTRP6—Strap 6 Record (Flash Descriptor Records)

Flash Address: FPSBA + 018h Default Value: 00000000h Size:32 bits
Default Flash Address: 118h

Bits	Description	Usage
31:0	Reserved, set to '0'	

A.9 PCHSTRP7—Strap 7 Record (Flash Descriptor Records)

Flash Address: FPSBA + 01Ch Default Value: 00000000h Size:32 bits
Default Flash Address: 11Ch

Bits	Description	Usage
31:0	**Intel ME SMBus Subsystem Vendor and Device ID** (MESMA2UDID): MESMAUDID[15:0] - Subsystem Vendor ID MESMAUDID[31:16] - Subsystem Device ID The values contained in MESMAUDID[15:0] and MESMAUDID[31:16] are provided as bytes 8-9 and 10-11 of the data payload to an external master when it initiates a Directed GET UDID Block Read Command to the Alert Sending Device ASD's address.	This bit must only be set to '1' when there is an ASD (Alert Sending Device) attached to SMBus and when **MESMASDEN(PCHSTRP2 bit 8)** is set to '1'. This is only applicable in platforms using Intel® AMT. Set this if you want to add a 4 byte payload to an external master when a GET UDID Block read command is made to Intel ME SMBus ASD's address.

A.10 PCHSTRP8—Strap 8 Record (Flash Descriptor Records)

Flash Address: FPSBA + 020h Size:32 bits
Default Flash Address: 120hs

Bits	Description	Usage
31:0	Reserved, set to '0'	

A.11 PCHSTRP9—Strap 9 Record (Flash Descriptor Records)

Flash Address: FPSBA + 024h Size:32 bits
Default Flash Address: 124h

Bits	Description	Usage
31:23	Reserved, set to '0'.	
22	**PCHHOT# or SML1AlERT# Select (PCHHOT#_SML1ALERT#_SEL)** This strap determines the native mode operation of GPIO74 0 = SML1ALERT# is the native functionality of GPIO74 1 = PCHHOT# is the native functionality of GPIO74	**PCHHOT#** is used to indicate the PCH temperature out of bounds condition to an external agent such as BMC or EC, when PCH temperature is greater than value programmed by BIOS.
21:15	Reserved, set to '0'.	

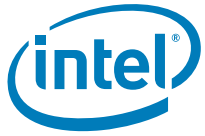
Bits	Description	Usage
14	**Subtractive Decode Agent Enable (SUB_DECODE_EN)** 0 = Disables PCH PCIe ports from Subtractive Decode Agent 1 = Enables PCH's PCIe ports to behave as a subtractive decode agent ***Note:*** If connecting a PCI bridge chip to the PCH that requires the PCH to behave as a subtractive decode agent, then set this bit to '1'.	Set this bit to '1' if there is a PCI bridge chip connected to the PCH, that requires subtractive decode agent. Set to '0' if the platform has no PCI bridge chip. ***Note:*** This setting is not the same for all designs, is dependent on the board design. The setting of this field must be determined by the platform hardware designer.
13:12	Reserved, set to '0'	
11	**Intel PHY Over PCI Express* Enable (PHY_PCIE_EN):** 0 = Intel integrated wired MAC/PHY communication is not enabled over PCI Express*. 1 = The PCI Express* port selected by the **PHY_PCIEPORT_SEL** soft strap to be used by Intel PHY ***Note:*** This bit must be "1" if using Intel integrated wired LAN solution.	This bit MUST be set to '1' if using Intel integrated wired LAN solution. If not using, or if disabling Intel integrated wired LAN solution then set this to '0'.
10:8	**Intel PHY PCIe* Port Select (PHY_PCIEPORTSEL):** Sets the default PCIe* port to use for Intel integrated wired PHY. 000: Port 1 001: Port 2 010: Port 3 011: Port 4 100: Port 5 101: Port 6 110: Port 7 111: Port 8 ***Note:*** This field only applies when **PHY_PCIE_EN** = '1'. Set to 000b when **PHY_PCIE_EN** is set to '0'	This field tells the PCH which PCI Express* port an Intel PHY is connected. If PHY_PCIE_EN is ='0', then this field is ignored. ***Note:*** This setting is not the same for all designs, is dependent on the board design. The platform hardware designer or schematic review can determine what PCIe* Port the Intel wired PHY is routed.
7	**Chipset Configuration Softstrap 4** Set to'1'b	
6	**DMI and Intel® Flexible Display Interface (FDI) Reversal (DMILR).** 0 = DMI Lanes 0 - 3 are not reversed. 1 = DMI Lanes 0 - 3 are reversed.	This field is used only when DMI Lanes are reversed on the layout. This usually only is done on layout constrained boards where reversing lanes help routing. ***Note:*** This setting is dependent on the board design. The platform hardware designer must determine if DMI needs lane reversal.

Bits	Description	Usage
5	**PCIe* Lane Reversal 2 (PCIELR2).** This bit lane reversal behavior for PCIe Port 5 if configured as a x4 PCIe* port. 0 = PCIe Lanes 4-7 are not reversed. 1 = PCIe Lanes 4-7 are reversed when Port 5 is configured as a 1x4. ***Note:*** This field only is in effect if PCIEPCS2 is set to '11'b.	If configuring PCIe* port 5 as a x4 PCIe* bus, reversing the lanes of this port is done via this strap. 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.
4	**PCIe* Lane Reversal 1 (PCIELR1).** This bit lane reversal behavior for PCIe* Port 1 if configured as a x4 PCIe port. 0 = PCIe Lanes 0-3 are not reversed. 1 = PCIe Lanes 0-3 are reversed when Port 1 is configured as a 1x4. ***Note:*** This field only is in effect if PCIEPCS1 is set to '11'b.	If configuring PCIe* port 5 as a x4 PCIe* bus, reversing the lanes of this port is done via this strap. 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 can determine if this port needs lane reversal
3:2	**PCI Express* Port Configuration Strap 2 (PCIEPCS2).** These straps set the default value of the PCI Express port Configuration 2 register covering PCIe ports 5-8. 11: 1x4 Port 5 (x4), Ports 6-8 (disabled) 10: 2x2 Port 5 (x2), Port 7 (x2), Ports 6, 8 (disabled) 01: 1x2, 2x1 Port 5 (x2), Port 6 (disabled), Ports 7, 8 (x1) 00: 4x1Ports 5-8 (x1) ***Note:*** ~~x2 configurations are not supported on desktop platforms~~	Setting of this field depend on what PCIe* ports 5-8 configurations are desired by the board manufacturer. Only the x4 configuration ("11") has the option of lane reversal if PCIELR2 is set to '1'. ***Note:*** This field must be determined by the PCI Express* port requirements of the design. The platform hardware designer must determine this setting.
1:0	**PCI Express* Port Configuration Strap 1 (PCIEPCS1).** These straps set the default value of the PCI Express* Port Configuration 1 register covering PCIe ports 1-4. 11: 1x4Port 1 (x4), Ports 2-4 (disabled) 10: 2x2 Port 1 (x2), Port 3 (x2), Ports 2, 4 (disabled) 01: 1x2, 2x1 Port 1 (x2), Port 2 (disabled), Ports 3, 4 (x1) 00: 4x1Ports 1-4 (x1) ***Note:*** ~~x2 configurations are not supported on desktop platforms~~	Setting of this field depend on what PCIe* ports 1-4 configurations are desired by the board manufacturer. Only the x4 configuration ("11") has the option of lane reversal if PCIELR1 is set to '1'. ***Note:*** This field must be determined by the PCI Express* port requirements of the design. The platform hardware designer must determine this setting.

A.12 PCHSTRP10—Strap 10 Record (Flash Descriptor Records)

Flash Address: FPSBA + 028h Size: 32 bits
Default Flash Address: 128h

Bits	Description	Usage
31:25	Reserved, set to '0'	
24	**ME Debug LAN Emergency Mode** 0 = ME Debug LAN Emergency Mode Disable 1 = Enables LAN Emergency mode of ME Debug ***Note:*** Default for production platforms should be '0'	ME Debug LAN emergency mode is enabled when setting this softstrap On this mode, a default "send all-events" setting will take place. This bit should be set to '1' if it is desired to capture events with the Intel LAN interface with the ME Debug tool. This bit should be set to '0' for production platforms. **Note:** ME Debug messaging is halted when descriptor flash permissions are locked to Intel recommended values.
23	**Deep SX Enable (Deep_SX_EN)** 0 = Deep SX is NOT supported on the platform 1 = Deep SX is supported on the platform	Deep SX refers to two low power states that are referred to Deep S4 and Deep S5. See Cougar Point EDS for more details. ***Note:*** This setting is dependent on the board design. The platform hardware designer can determine if Deep SX is supported on this platform.
22	**Integrated Clocking Controller (ICC) Profile Selection (ICC_PRO_SEL)** 0 = ICC Profile will be provided by BIOS 1 = ICC Profile selected by Softstraps (**ICC_SEL**)	This field determines what mechanism will select the ICC profile. This way a customer can decide how the profile section will be made. To set the clock profile select in a pre-manufacturing environment by setting the ICC profile in softstraps, this bit would have to be set to '1'. **ICC_SEL** would also have to be properly set. To have BIOS manage the clock profile selection, then this bit would have to be set to '0'. **ICC_SEL** would be ignored.
21	**Intel ME Reset Capture on CL_RST1#: (MER_CL1)** 0 = PCH Signal **CL_RST1#** does NOT assert when Intel ME performs a reset. 1 = PCH Signal **CL_RST1#** asserts when Intel ME resets. ***Notes:*** 1. Signal CL_RST1# is only present on mobile PCH	This field requires proper Intel Management Engine Firmware and descriptor. When this field is set to '1', Intel Management Engine will assert a the **CL_RST1#** when it resets. When set to '0', Intel ME does not reflect this reset.



Bits	Description	Usage
20:18	**Integrated Clocking Configuration Select (ICC_SEL)** Select the clocking parameters that the platform will boot with. 000 - Config '0' - <default> 001 - Config '1' 010 - Config '2' 011 - Config '3' 100 - Config '4' 101 - Config '5' 110 - Config '6' 111 - Config '7'	This field chooses the set of clock parameters that are used on the target platform. Its is recommended to set this field to '111' if you will change the value on the manufacturing line to minimize programming time.
17:16	Reserved, set to '0'	
15:9	**ME Debug SMBus Emergency Mode Address (MDSMBE_ADD):** SMBUS address used for ME Debug status writes. If this field is 00h, the default address, 38h, is used.	This field is only used for testing purposes.
8	**ME Debug SMBus Emergency Mode Enable (MDSMBE_EN):** 0 = Disable Intel ME Debug status writes 1 = Enable Intel ME Debug status writes over SMBUS using the address set by MMADDR.	This field is only used for testing purposes. When this bit is enabled, you will see writes on SMBus to address 38h bits address (70h bit shifted), or value is specified in **MMADDR. MMADDR** specifies address bits 7:1 of the target addres.
7:2	Reserved, set to '0'	
1	**ME Boot Flash (ME_Boot_Flash).** 0 = Intel Management Engine will boot from ROM, then flash 1 = Intel Management Engine will boot from flash ***Note:*** This field should only be set to '1b' if the Intel ME binary loaded in the platfrom has a ME ROM Bypass image	This bit must be set to 0 for production PCH based platforms. This bit will only be set to '1' in order to work around issues in pre-production hardware and Intel ME FW.
0	Reserved, set to '0'	

A.13 PCHSTRP11—Strap 11 Record (Flash Descriptor Records)

Flash Address: FPSBA + 02Ch Size:32 bits
Default Flash Address: 12Ch

Bits	Description	Usage
31:25	**SMLink1 I2C* Target Address (SML1I2CA)** Defines the 7 bit I2C target address for PCH Thermal Reporting on SMLink1. ***Notes:*** 1. This field is not active unless SML1I2CAEN is set to '1'. 2. This address MUST be set if there is a device on the SMLink1 segment that will use thermal reporting supplied by PCH. 3. If SML1I2CAEN ='1' then this field must be a valid 7 bit, non-zero address that does not conflict with any other devices on SMLink1 segment. 4. This address can be different for every design, ensure BIOS developer supplies the address.	When **SML1I2CAEN(PCHSTRP11 bit 24)** ='1', there needs to be a valid I^2C address in this field. This address used here is design specific. The BIOS developer and/or platform hardware designer must supply an address with the criteria below. A valid address must be: • Non-zero value • Must be a unique address on the SMLink1 segment • Be compatible with the master on SMLink1 - For example, if the I^2C address the master that needs write thermal information to a address "xy"h. Then this filed must be to "xy"h.
24	**SMLink1 I^2C Target Address Enable (SML1I2CAEN)** 0 = SMLink1 I^2C Address is disabled 1 = SMLink1 I^2C Address is enabled ***Notes:*** 1. This bit MUST set to '1' if there is a device on the SMLink1 segment that will use PCH thermal reporting. 2. This bit MUST be set to '0' if PCH thermal reporting is not used.	This bit must be set in cases where SMLink1 has a master that requires SMBus based Thermal Reporting that is supplied by the PCH. Some examples of this master could be an Embedded Controller, a BMC, or any other SMBus Capable device that needs Processor and/or PCH temperature information. If no master on the SMLink1 segment is capable of utilizing thermal reporting, then this field must be set to '0'. ***Note:*** This setting is not the same for all designs, is dependent on the board design. The setting of this field must be determined by the BIOS developer and the platform hardware designer.
23:8	Reserved, set to '0'	
7:1	**SMLink1 GP Address (SML1GPA):** SMLink1 controller General Purpose Target Address (7:1) ***Notes:*** 1. This field is not active unless **SML1GPAEN** is set to '1'. 2. This address MUST be set if there is a device on the SMLink1 segment that will use SMBus based PCH thermal reporting. 3. If **SML1GPAEN** ='1' then this field must be a valid 7 bit, non-zero address that does not conflict with any other devices on SMLink1 segment.	When **SML1GPAEN** ='1', there needs to be a valid GP address in this field. This address used here is design specific. The BIOS developer and/or platform hardware designer must supply an address with the criteria below. A valid address must be: • Non-zero value • Must be a unique address on the SMLink1 segment • Be compatible with the master on SMLink1 - For example if the GP address the master that needs read thermal information from a certain address, then this filed must be set accordingly.

Bits	Description	Usage
0	**SMLink1 GP Address Enable(SML1GPAEN):** SMLink1 controller General Purpose Target Address Enable 0 = SMLink1 GP Address is disabled 1 = SMLink1 GP Address is enabled ***Notes:*** 1. This bit MUST set to '1' if there is a device on the SMLink1 segment that will use SMBus based PCH thermal reporting. 2. This bit MUST be set to '0' if PCH thermal reporting is not used.	This bit must be set in cases where SMLink1 has a master that requires SMBus based Thermal Reporting that is supplied by the PCH. Some examples of this master could be an Embedded Controller, a BMC, or any other SMBus Capable device that needs Processor or PCH temperature information. If no master on the SMLink1 segment is capable of utilizing thermal reporting, then this field must be set to '0'. ***Note:*** This setting is not the same for all designs, is dependent on the board design. The setting of this field must be determined by the BIOS developer and the platform hardware designer.

A.14 PCHSTRP12—Strap 12 Record (Flash Descriptor Records)

Flash Address: FPSBA + 030h Default Value: 00000000h Size:32 bits
Default Flash Address: 130h

Bits	Description	Usage
31:0	Reserved, set to '0'	

A.15 PCHSTRP13—Strap 13 Record (Flash Descriptor Records)

Flash Address: FPSBA + 034h Default Value: 00000000h Size:32 bits
Default Flash Address: 134h

Bits	Description	Usage
31:0	Reserved, set to '0'	

A.16 PCHSTRP14—Strap 14 Record (Flash Descriptor Records)

Flash Address: FPSBA + 038h Default Value: 00000000h Size:32 bits
Default Flash Address: 138h

Bits	Description	Usage
31:0	Reserved, set to '0'	

A.17 PCHSTRP15—Strap 15 Record (Flash Descriptor Records)

Flash Address: FPSBA + 03Ch Size: 32 bits
Default Flash Address: 13Ch
Recommended Value:

Bits	Description	Usage
31:16	Reserved, set to '0'	
15	**SLP_LAN#/GPIO29 Select (SLP_LAN#_GP29_SEL)** 0 = GPIO29 can only used only as SLP_LAN# for Intel integrated LAN solution. 1 = GPIO29 is available for GPIO configuration ***Notes:*** 1. This must be set to '0' if the platform is using Intel's integrated wired LAN solution. 2. Set to '1' only if GPIO29 needs to be available for target platform design **AND** if Intel integrated wired LAN solution is **NOT** used.	This strap will allow the usage of GPIO29, which is not available when the Intel integrated LAN functionality is not set. If there is no Intel integrated LAN AND there is a need of GPIO29. Then set this bit to '1'. If Intel integrated LAN is used, then this bit must be set to '0'.
14	**SMLink1 Thermal Reporting Select (SMLINK1_THERM_SEL)** 0 = Intel ME FW will collect temperature from the processor, PCH and DIMMs. It will be available for polling on SMLink1 1 = PCH temperature (1 byte of data) will be available for polling out on SMLink1. Processor and DIMMs temperature monitoring will require an external device.	
13:10	Reserved, set to '0'	
9:8	**Chipset Configuration Softstrap 5** Set to'11'b	
7	Reserved, set to '0'	
6	**Intel integrated wired LAN Enable(IWL_EN)** 0 = Disable Intel integrated wired LAN Solution 1 = Enable Intel integrated wired LAN Solution ***Notes:*** 1. This must be set to '1' if the platform is using Intel's integrated wired LAN solution. 2. Set to '0' if not using Intel integrated wired LAN solution or if disabling it.	This must be set to '1' if the platform is using Intel's integrated wired LAN solution. This must be set to '0' if not using Intel's integrated wired LAN solution or if disabling it.
5:0	**Chipset Configuration Softstrap 6** Set to'111110'b	

A.18 PCHSTRP16—Strap 16 Record (Flash Descriptor Records)

Flash Address: FPSBA + 040h Size: 32 bits
Default Flash Address: 140h
Recommended Value:

Bits	Description	Usage
31:0	Reserved, set to '0'	

A.19 PCHSTRP17—Strap 17 Record (Flash Descriptor Records)

Flash Address: FPSBA + 044h Size: 32 bits
Default Flash Address: 144h
Recommended Value:

Bits	Description	Usage
31:2	Reserved, set to '0'	
1	**Chipset Configuration Softstrap 7** Set to '1b'	
0	**Integrated Clock Mode Select** 0 = Full Integrated Clock Mode (default) 1 = Buffered Through Clock Mode	

A.20 Softstrap Step through

General questions help in setting softstraps and certain other descriptor values.For All configurations the following must be set.

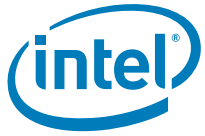
Name	Location	Value
SMB_EN	PCHSTRP0[7]	1b

1. **Does the target plaform use the Intel integrated wired LAN solution?**
   a. If Yes,

Name	Location	Value
SML0_EN	PCHSTRP0[8]	1b
GBEPHY_SMBUS_ADDR	PCHSTRP4[23:17]	64h
GBEMAC_SMBUS_ADDR	PCHSTRP4[15:9]	70h
GBE_SMBUS_ADDR_EN	PCHSTRP4[8]	1b
PHYCON[1:0]	PCHSTRP4[1:0]	10b
PHY_PCIE_EN	PCHSTRP9[11]	1b
SLP_LAN#_GP29_SEL	PCHSTRP15[15]	0b
IWL_EN	PCHSTRP15[6]	1b

- i. What PCIe* port is the Intel PHY attached? Note: Intel CRBs use port 6.

Name	Location	Value
PHY_PCIEPORTSEL	PCHSTRP9[10:8]	000b: Port 1, 001b: Port 2, 010b: Port 3, 011b: Port 4, 100b: Port 5, 101b: Port 6, 110b: Port 7, 111b: Port 8



- ii. Is the signal GPIO12 from the PCH routed to the signal LAN_DISABLE_N on the Intel wired PHY?
  1. If yes:

Name	Location	Value
LANPHYPC_GP12_SEL	PCHSTRP0[20]	1b

  2. If no:

Name	Location	Value
LANPHYPC_GP12_SEL	PCHSTRP0[20]	0b

iii. Is LinkSec Disabled
  1. If yes (default):

Name	Location	Value
LINKSEC_DIS	PCHSTRP0[21]	1b

  2. If no:

Name	Location	Value
LINKSEC_DIS	PCHSTRP0[21]	0b

b. If No, then set all LAN Disabled softstraps

Name	Location	Value
LINKSEC_DIS	PCHSTRP0[21]	1b
LANPHYPC_GP12_SEL	PCHSTRP0[20]	0b
SML0_EN	PCHSTRP0[8]	0b
GBE_SMBUS_ADDR_EN	PCHSTRP4[8]	0b
PHYCON[1:0]	PCHSTRP4[1:0]	00b
PHY_PCIE_EN	PCHSTRP9[11]	0b
SLP_LAN#_GP29_SEL	PCHSTRP15[15]	1b
IWL_EN	PCHSTRP15[6]	0b

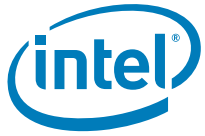
2. Are DMI Lanes reversed on target design?

a. If Yes:

Name	Location	Value
DMILR	PCHSTRP9[6]	1b

b. If No:

Name	Location	Value
DMILR	PCHSTRP9[6]	0b



3. How should PCIe* Lanes 1-4 on the target plaform be configured?

a. 1x4: Port 1 (x4), Ports 2-4 (disabled)

Name	Location	Value
PCIEPCS1	PCHSTRP9[1:0]	11b

i. If 1X4, is PCIe lane 1 reversed?

1. If Reversed:

Name	Location	Value
PCIELR1	PCHSTRP9[4]	1b

2. If NOT Reversed:

Name	Location	Value
PCIELR1	PCHSTRP9[4]	0b

b. 2x2: 2x2 Port 1 (x2), Port 3 (x2), Ports 2, 4 (disabled) (Not for Desktop)

Name	Location	Value
PCIEPCS1	PCHSTRP9[1:0]	10b

c. 1x2, 2x1 Port 1 (x2), Port 2 (disabled), Ports 3, 4 (x1) (Not for Desktop)

Name	Location	Value
PCIEPCS1	PCHSTRP9[1:0]	01b

d. 4x1: Ports 1-4 (x1)

Name	Location	Value
PCIEPCS1	PCHSTRP9[1:0]	00b

4. How should PCIe* Lanes 5-8 on the target plaform be configured?

a. 1x4 – one 4 lane PCIe port

Name	Location	Value
PCIEPCS2	PCHSTRP9[3:2]	11b

i. Is PCIe* lane 5 reversed?

1. If Reversed:

Name	Location	Value
PCIELR2	PCHSTRP9[5]	1b

2. If NOT Reversed:

Name	Location	Value
PCIELR2	PCHSTRP9[5]	0b

b. 2x2: Port 5 (x2), Port 7 (x2), Ports 6, 8 (disabled) (Not for Desktop)

Name	Location	Value
PCIEPCS2	PCHSTRP9[3:2]	10b

c. 1x2, 2x1: Port 5 (x2), Port 6 (disabled), Ports 7, 8 (x1) (Not for Desktop)

Name	Location	Value
PCIEPCS2	PCHSTRP9[3:2]	01b

d. 4x1: Ports 5-8 (x1)

Name	Location	Value
PCIEPCS2	PCHSTRP9[3:2]	00b

5. Is there a third party device connected to SMLink1 that will gather Thermal Reporting Data on the target platform?

a. If Yes,

Name	Location	Value
SM1_EN	PCHSTRP0[9]	1b
SML1I2CA	PCHSTRP11[31:25]	See PCHSTRP11[31:25] usage
SML1I2CAEN	PCHSTRP11[24]	1b
SML1GPA	PCHSTRP11[7:1]	See PCHSTRP11[7:1] usage
SML1GPEN	PCHSTRP11[0]	1b

i. If thermal data to be collected is PCH only

Name	Location	Value
SMLINK1_THERM_SEL	PCHSTRP15[14]	1b

ii. If thermal data is to Processor, and PCH

Name	Location	Value
SMLINK1_THERM_SEL	PCHSTRP15[14]	0b

b. If No,

Name	Location	Value
SM1_EN	PCHSTRP0[9]	0b
SML1I2CA	PCHSTRP11[31:25]	00h
SML1I2CAEN	PCHSTRP11[24]	0b
SML1GPA	PCHSTRP11[7:1]	00h
SML1GPEN	PCHSTRP11[0]	0b
SMLINK1_THERM_SEL	PCHSTRP15[14]	0b

6. What is the size of the boot BIOS block on the target platform? Note: Value must be determined by BIOS developer.

a. If 64 KB,

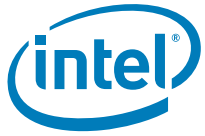
Name	Location	Value
BBBS	PCHSTRP0[30:29]	00b

b. If 128 KB,

Name	Location	Value
BBBS	PCHSTRP0[30:29]	01b

c. If 256 KB,

Name	Location	Value
BBBS	PCHSTRP0[30:29]	10b



7. **Is there an alert sending device (ASD) on Host SMBus on the target platform? NOTE: this is only valid for Intel® AMT enabled platforms**

   a. If Yes,

Name	Location	Value
MESMASDA	PCHSTRP2[15:9]	See PCHSTRP2[15:9] usage
MESMASDEN	PCHSTRP2[8]	1b
MESMA2UDID	PCHSTRP7[31:0]	See PCHSTRP7 usage

   b. If No,

Name	Location	Value
MESMASDA	PCHSTRP2[15:9]	00h
MESMASDEN	PCHSTRP2[8]	0b
MESMA2UDID	PCHSTRP7[31:0]	00000000h

8. **Are there multiple processors in the target system?**

   a. If no,

Name	Location	Value
DMI_REQID_DIS	PCHSTRP0[24]	0b

   b. If yes,

Name	Location	Value
DMI_REQID_DIS	PCHSTRP0[24]	1b

9. **Enable Intel ME Debug Options. Including Logging for Intel MDDD (Intel ME Memory-attached Debug Disaplay Device), Intel MESSDC (ME SMBus Debug Console) ? Note: All production systems must have logging disabled.**

If yes.

Name	Location	Value
ME_DEBUG_EN	PCHSTRP10[24]	1b
MDSMBE_ADD	PCHSTRP10[15:9]	38h
MDSMBE_EN	PCHSTRP10[8]	1b

c. If No, **NOTE:** All production platforms **MUST** disable Options.

Name	Location	Value
ME_DEBUG_EM	PCHSTRP10[24]	0b
MDSMBE_ADD	PCHSTRP10[15:9]	00h
MDSMBE_EN	PCHSTRP10[8]	0b

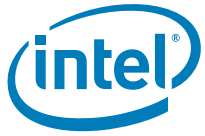
10. What is the desired native functionality of GPIO74?

i. If **SML1Alert#**

Name	Location	Value
PCHHOT#_SML1ALERT#_SEL	PCHSTRP9[22]	0b

ii. If **PCHHOT#,**

Name	Location	Value
PCHHOT#_SML1ALERT#_SEL	PCHSTRP9[22]	1b



11. Is the platform power state "Deep SX" supported?

i. If Yes,

Name	Location	Value
Deep_SX_EN	PCHSTRP10[23]	1b

ii. If No,

Name	Location	Value
Deep_SX_EN	PCHSTRP10[23]	0b

12. **Does the platform have a PCI bridge chip that requires a subtractive decode agent? Note:** If your platform doesn't support PCI set this to no. If using a Desktop/Server PCH that supports PCI interface and do NOT require an external PCi bridge chip then set this to no.

i. If Yes,

Name	Location	Value
SUB_DECODE_EN	PCHSTRP09[14]	1b

ii. If No,

Name	Location	Value
SUB_DECODE_EN	PCHSTRP09[14]	0b

§ §