Advanced x86:
BIOS and System Management Mode Internals
Flash Descriptor

Xeno Kovah && Corey Kallenberg

LegbaCore, LLC

All materials are licensed under a Creative Commons “Share Alike” license.

http://creativecommons.org/licenses/by-sa/3.0/

You are free:

to Share — to copy, distribute and transmit the work

to Remix — to adapt the work

Under the following conditions:

Attribution — You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).

Share Alike — If you alter, transform, or build upon this work, you may distribute the resulting work only under the same, similar or a compatible license.

Attribution condition: You must indicate that derivative work
"Is derived from John Butterworth & Xeno Kovah’s ’Advanced Intel x86: BIOS and SMM’ class posted at http://opensecuritytraining.info/IntroBIOS.html”

SPI Regions

Required

Required

Region	Content
0	Flash Descriptor
1	BIOS
2	Intel Management Engine
3	Gigabit Ethernet
4	Platform Data

Added in ICH9

- Intel has left room for additional regions
- The only ones required are the Flash Descriptor region and the BIOS region
- They are not listed in the order in which they will appear on the flash chip:
  - Flash Descriptor will always be first, as listed, but BIOS will always be last so it ends at 4 GB of memory address space

Determining SPI Regions

FREG0—Flash Region 0 (Flash Descriptor) Register (SPI Memory Mapped Configuration Registers)

Memory Address:  + 54h Attribute: RO
Default Value: 00000000h Size: 32 bits

This register is only applicable when SPI device is in descriptor mode.

Bit	Description
31:29	Reserved
28:16	**Region Limit (RL)** — RO. This specifies address bits 24:12 for the Region 0 Limit. The value in this register is loaded from the contents in the Flash Descriptor.FLREG0.Region Limit
15:13	Reserved
12:0	**Region Base (RB) / Flash Descriptor Base Address Region (FDBAR)** — RO. This specifies address bits 24:12 for the Region 0 Base The value in this register is loaded from the contents in the Flash Descriptor.FLREG0.Region Base

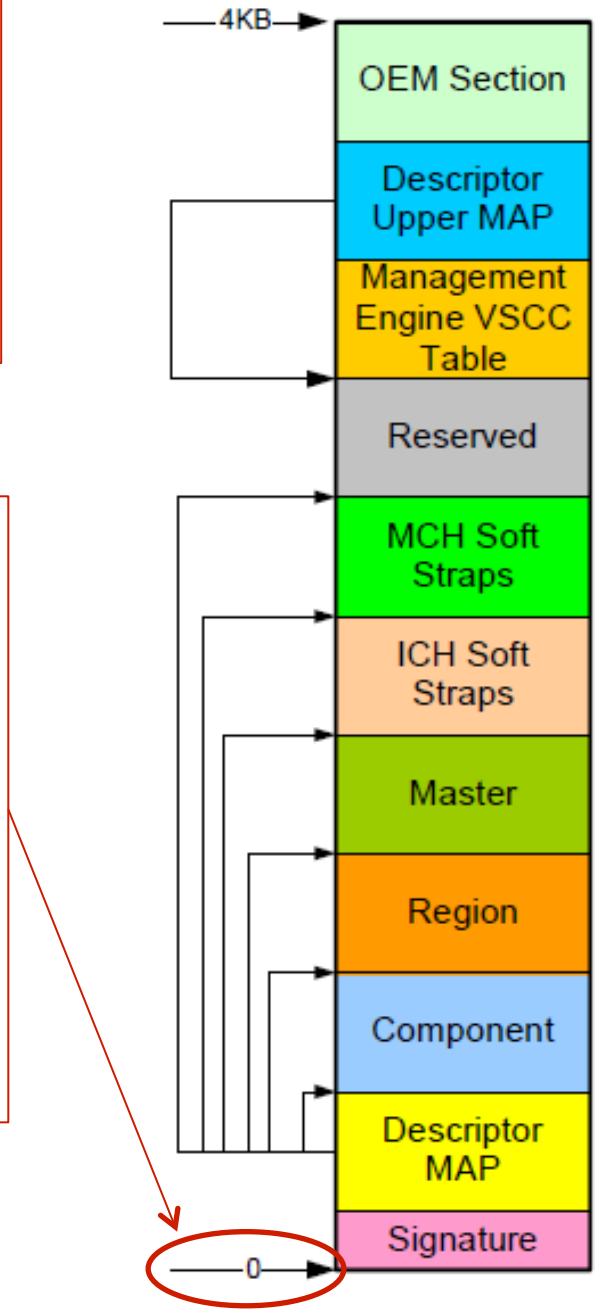
- You can determine the regions on your flash by reading the FREG(n) registers in the SPI Base Address Registers (SPIBAR  + {54 to 64h})
- FREG0 to FREG4, each 32 bits
- If the Base is higher than the limit, the region is unused

Flash Descriptor

- Defines most (but not all) of the flash protection that are supported by the Controller Hub
  - Not defined in flash descriptor:
    - BIOS Range Write Protection
    - SMI# Global Write protection (described elsewhere)
    - Logically OR'd together, if either are set then access is blocked
- Must be written during the manufacturing process and set to Read-Only when it leaves the manufacturer, per Intel
  - Sometimes (rarely) the Flash Descriptor itself is left open and thus vulnerable

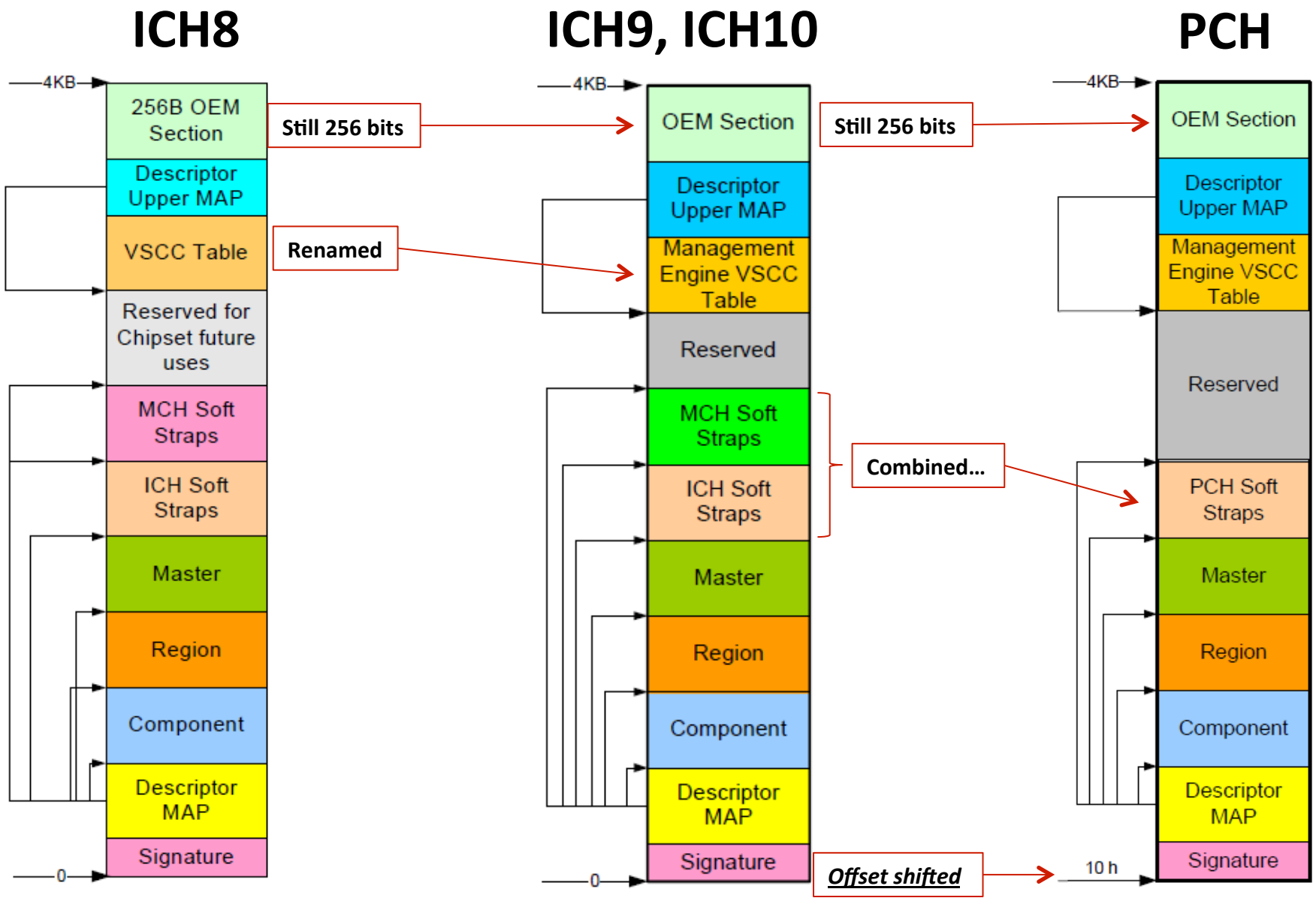
- This "Flash Descriptor" structure is what's read by the ICH/PCH in order to populate and expose the information via RO registers (like FREG0) in SPIBAR

- **Signature 0FF0A55Ah** denotes the device has a valid descriptor and is therefore operating in Descriptor mode.
- Signature offset is located at 0 on ICH8, ICH9, and ICH10
- In PCH it has been moved to 0x10 and bytes 0 thru 0x0F are Reserved



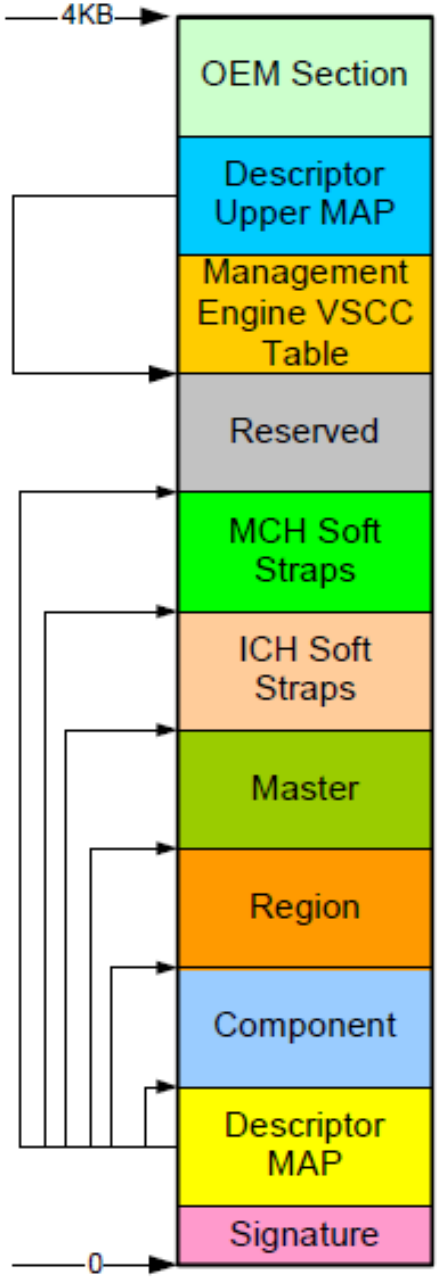
Pictured: ICH 10 Flash Descriptor

Evolution of the Flash Descriptor from ICH to PCH



ICH 8, 9, 10 are identical

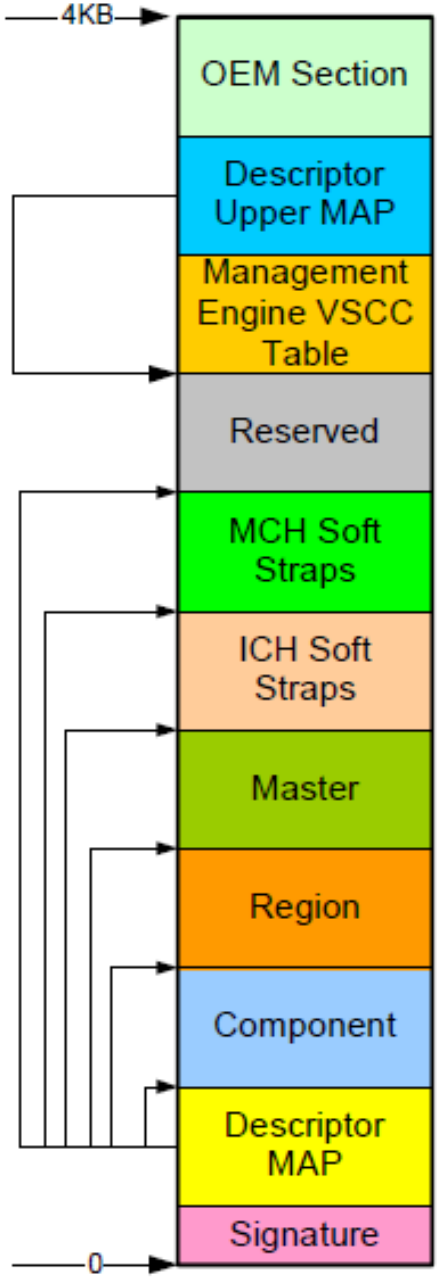
- The registers of the Flash Descriptor used to be documented fully in the I/O Controller Hub datasheets.
- In the Platform Controller Hub datasheets, however, the Descriptor offsets and registers are no longer described.
- For this reason, we will use the image of the flash descriptor as taken from ICH10.



ICH10 used as example

- When describing the protection mechanisms provided by the flash descriptor, I'll point out how they differ between ICH revisions where applicable
- Remember, this isn't an exercise in memorization but in acquiring new awareness and understanding, with that you can fill in details as they change in the future.
- The functionality described will be present, even if the offsets change in the future.

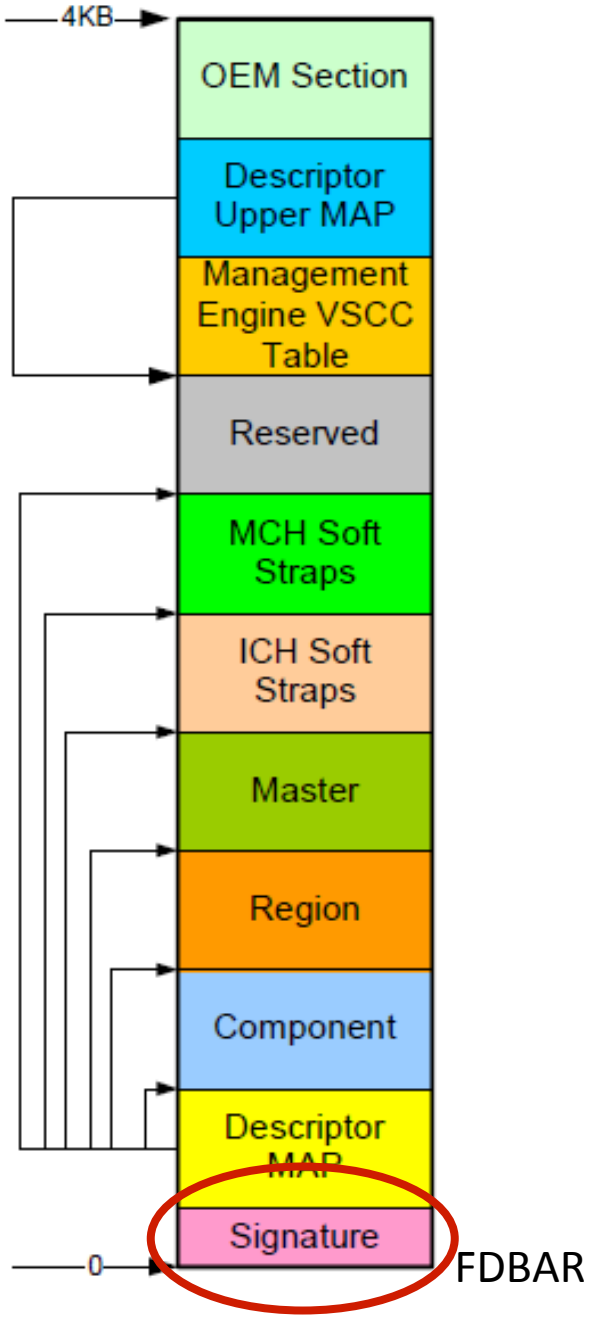
- Note: FDBAR is *not* a memory base address register. When you see later references to offsets from FDBAR, you're dealing in flash linear address offsets (so you need to be careful because FDBAR will differ depending on whether you're running an ICH (0) or PCH (0x10))



ICH10 used as example

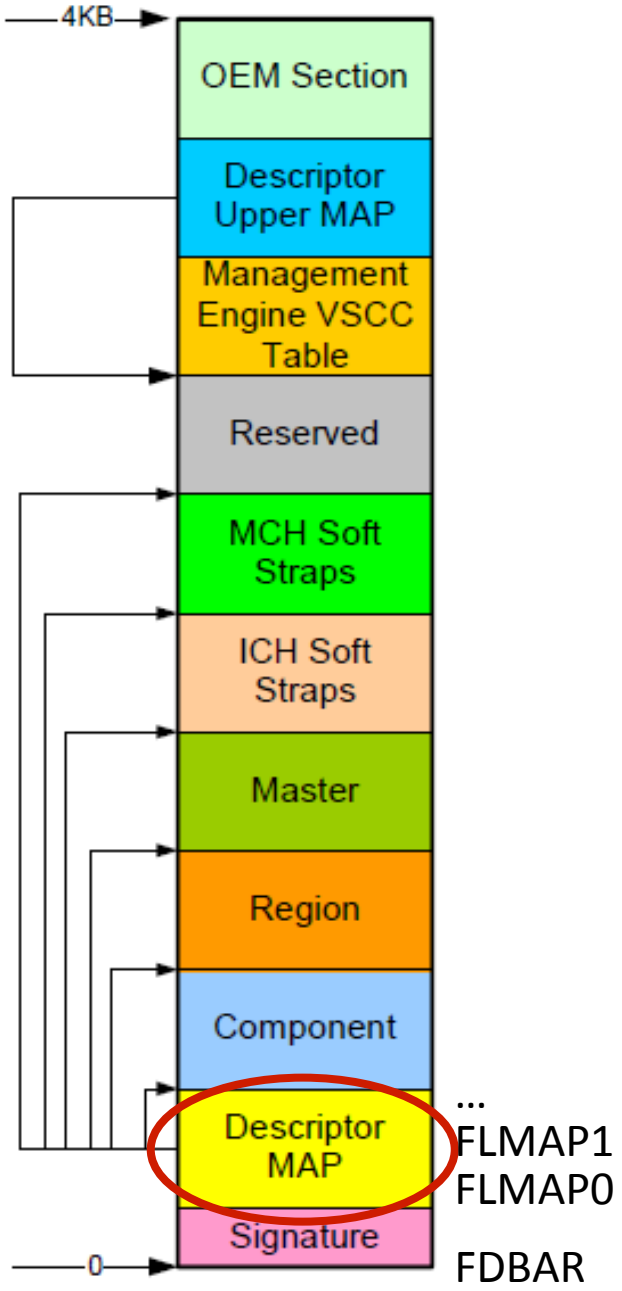
Signature

- Signature 0FF0A55Ah identifies a valid flash descriptor
- A valid flash descriptor indicates the SPI flash is operating in Descriptor mode
- PCH and Management Engine each require a valid flash descriptor
- Located at FDBAR + 0000h
  - FDBAR defined in bits 12:0 in FREG0 (located in SPIBAR)
- Signature offset is located at 0 on ICH8, ICH9, and ICH10
- In PCH it has been moved to 0x10 and bytes 0 thru 0x0F are Reserved



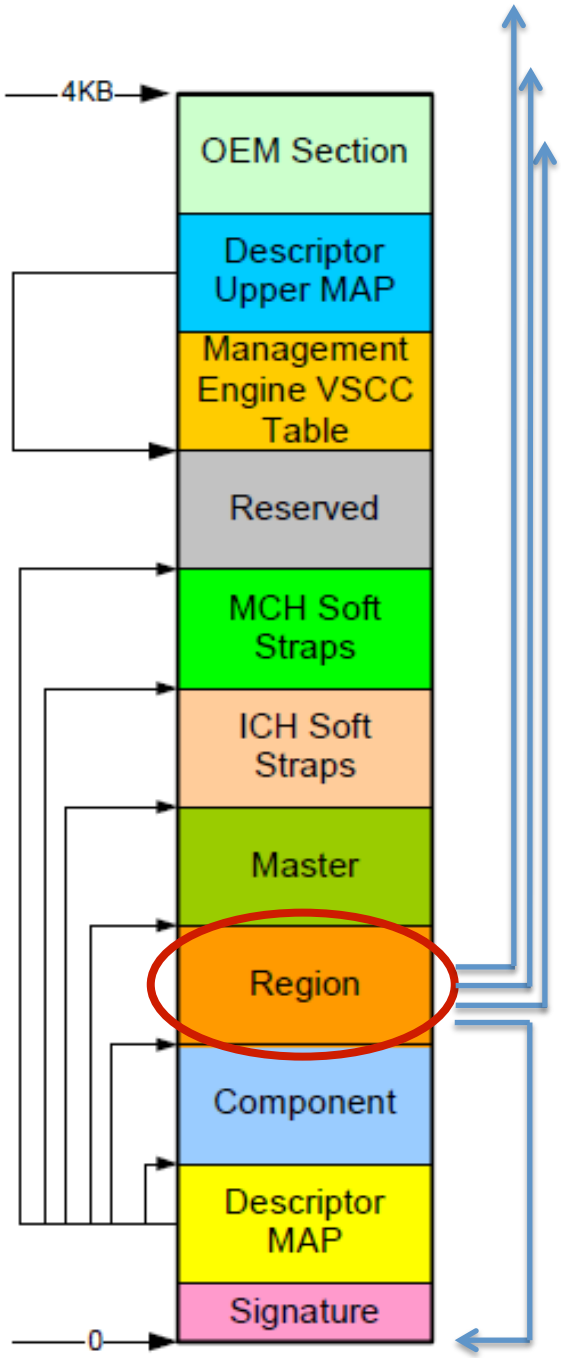
Descriptor Map

- Describes the data structure of the Flash Descriptor
- number of sections in the descriptor
- pointers to these sections as well as the size of each section
- # of physical SPI flash chips present



Region

- Identifies the different regions of the SPI Flash (BIOS, Mgt Eng, etc.)
  - Not to be confused with defining the flash descriptor map.
- Each FLREG register (0-4) has a base and a limit, each corresponding to the range of that particular region
  - FLREG0 = Flash Descriptor
  - FLREG1 = BIOS
  - FLREG2 = ME
  - FLREG3 = GbE
  - FLREG4 = Platform Data
- Disabled/unused regions will have a base of 1FFFh and a limit of 0000h
  - Can determine what regions are active
  - If BIOS region is inactive, then the BIOS is located on the FWH



Keeping it straight

- FLREG0-4 are what's in the Flash Descriptor. The data from the Descriptor is then exposed through FREG0-4 registers.

FREG0—Flash Region 0 (Flash Descriptor) Register (SPI Memory Mapped Configuration Registers)

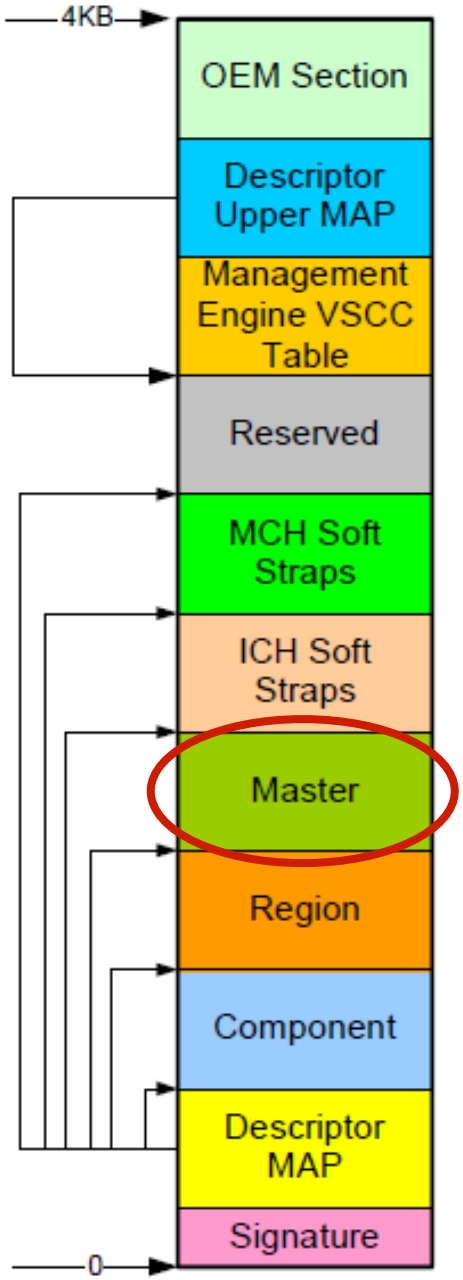
Memory Address: + 54h Attribute: RO
Default Value: 00000000h Size: 32 bits

This register is only applicable when SPI device is in descriptor mode.

Bit	Description
31:29	Reserved
28:16	**Region Limit (RL)** — RO. This specifies address bits 24:12 for the Region 0 Limit. The value in this register is loaded from the contents in the Flash Descriptor.FLREG0.Region Limit
15:13	Reserved
12:0	**Region Base (RB) / Flash Descriptor Base Address Region (FDBAR)** — RO. This specifies address bits 24:12 for the Region 0 Base The value in this register is loaded from the contents in the Flash Descriptor.FLREG0.Region Base

Master

- Defines the Read/Write capabilities that each Flash Master has with respect to each of the SPI regions, including the flash descriptor
- Each SPI Master has a register that defines these permissions called the Flash Master register
  - Permissions apply only to register access



Flash Master Permissions

- Register layout is identical for each of the three masters
- Register location and layout is also identical across ICH8, ICH9, ICH10
- Appears to be identical on PCH as well*

Should never be set anywhere!

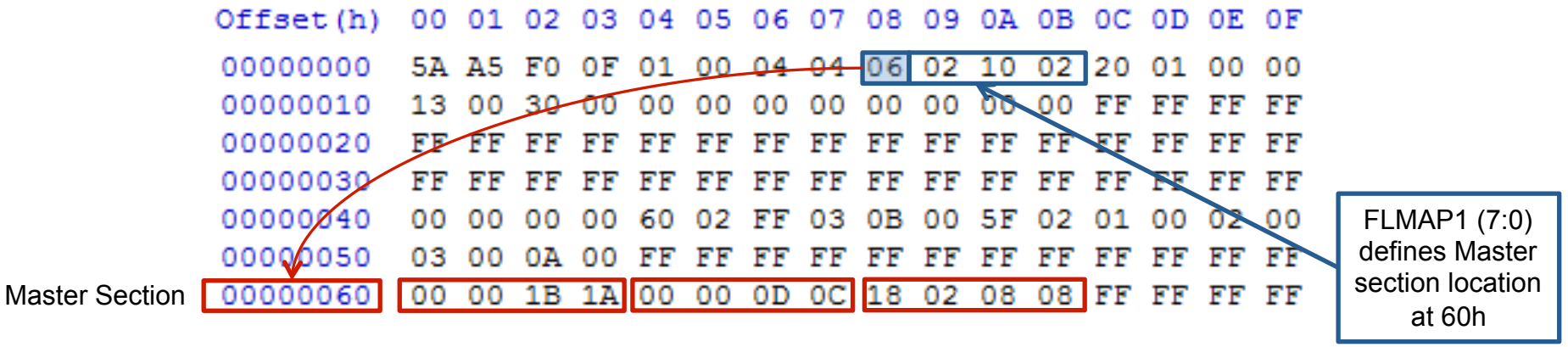
Bits	Description
31:29	Reserved, must be zero
28	**Platform Data Region Write Access.** If the bit is set, this master can erase and write that particular region through register accesses.
27	**GbE Region Write Access.** If the bit is set, this master can erase and write that particular region through 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. 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, 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. 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.

*Based on John's analysis of SPI serial flash dumps

Flash Master Permissions

- The requestor ID of the master attempting to access a region must match that of the defined requestor ID
  - 2-Byte value
  - CPU and ME must have requestor ID's of 0h
  - GbE must have a requestor ID of 0218h
- Each master will always have Read/Write permission to its own region
  - CPU/BIOS will always be able to read the BIOS region of the SPI flash, and so on.
  - This is by default and hardcoded by Intel

Example: FLMSTR meanings



- Based on analysis of the Descriptor Map (FLMAP offset 8h), we have identified that the Master section begins at offset 60h of the Serial Flash (06h is left-shifted 4 bits).
  - FLMAP = 12100206h (bits 7:0 define Flash Master location)
- FLMSTR1 (CPU/BIOS) = 1A1B0000h
- FLMSTR2 (Mgt Engine) = 0C0D0000h
- FLMSTR3 (GbE) = 08080218h

*HxD doesn't let you view the words in 32- bit format (with little-endian interpretation)

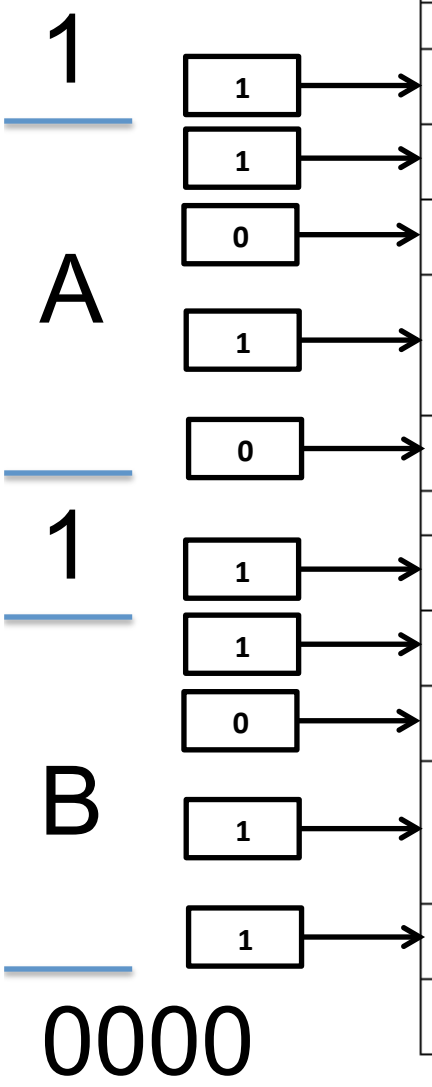
FLMSTR1 (CPU/BIOS)

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00000000	5A	A5	F0	0F	01	00	04	04	06	02	10	02	20	01	00	00
00000010	13	00	30	00	00	00	00	00	00	00	00	00	FF	FF	FF	FF
00000020	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
00000030	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
00000040	00	00	00	00	60	02	FF	03	0B	00	5F	02	01	00	02	00
00000050	03	00	0A	00	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
Master Section 00000060	00	00	1B	1A	00	00	0D	0C	18	02	08	08	FF	FF	FF	FF

- FLMSTR1 (CPU/BIOS) = 1A1B0000h
- Therefore CPU/BIOS has the following privileges:
- Write (bits 28:24)
  - Can write to the Platform Data region of SPI Flash
  - Can write to the BIOS region of SPI Flash
  - Can write to the GbE region of SPI Flash
- Read (bits 20:16)
  - Can read the Flash Descriptor of SPI flash
  - Can read the BIOS region of SPI flash
  - Can read the GbE region of SPI flash

***Note: The FLMAP0 register defines 03h + 1 SPI regions, therefore there is no Platform Data region on this SPI flash.**

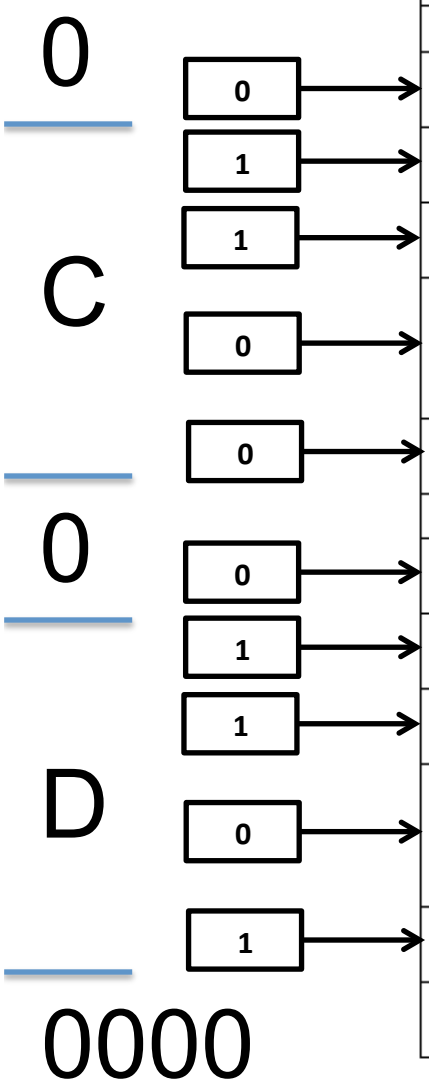
CPU/BIOS Permissions = 1A1B0000h



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. 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, 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. 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.

***Note: The FLMAP0 register defines 03h + 1 SPI regions, therefore there is no Platform Data region on this SPI flash.**

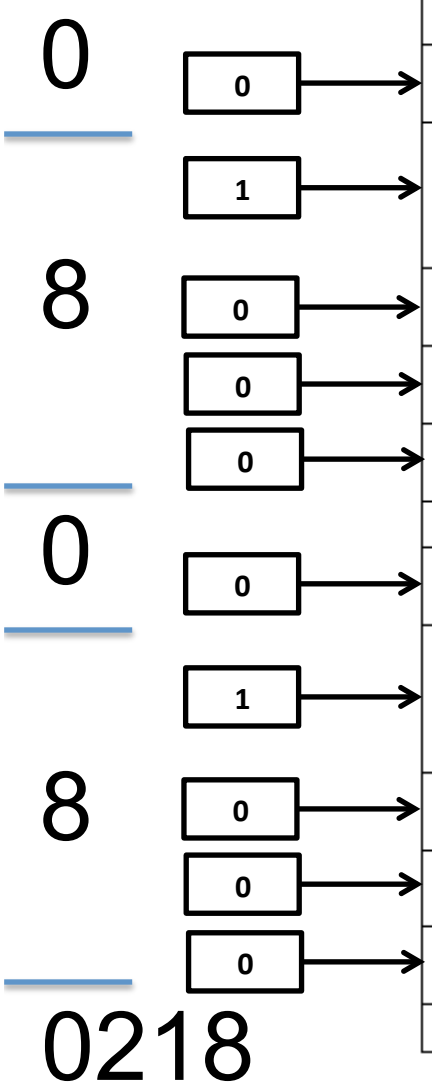
ME Permissions = 0C0D0000h



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. 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, 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. 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.

***Note: The FLMAP0 register defines 03h + 1 SPI regions, therefore there is no Platform Data region on this SPI flash.**

GbE Permissions = 08080218h



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 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	**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, 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 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	**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 0218h.

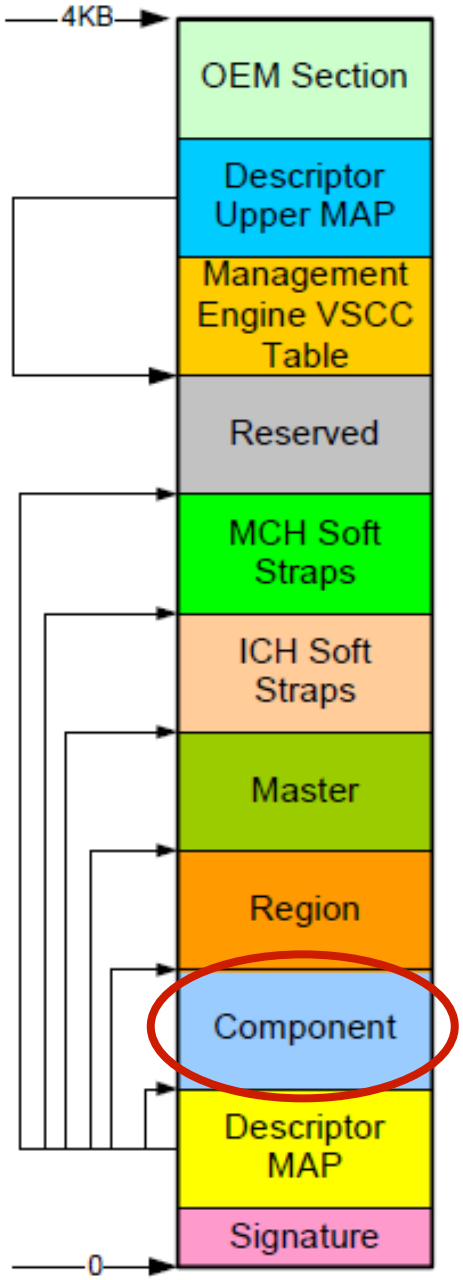
***Note: Requestor ID 0218h is required on ICH8, ICH9, and ICH10 systems, in PCH this is 0118h**

Backup

- Deferred due to lack of time/importance for our purposes
- Included for completeness

Component

- Identifies the different flash chips themselves and their capabilities
- Read/Write/Erase clock frequencies
- Even if there are 2 SPI chips, there is still just a single component section
- The component section contains the Flash Invalid Instructions Register which says which instructions will be blocked from execution by the hardware



FLILL—Flash Invalid Instructions Register (Flash Descriptor Registers)

Memory Address: + 004h Default Value: h
Size: 32 bits

Bits	Description
31:24	**Invalid Instruction 3**. See definition of Invalid Instruction 0
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 invalid instruction in the 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 allowed o use any of the Invalid Instructions listed in this register.

- Defines opcodes that will be prevented from running on the chip by the flash controller hardware
- Chip Erase (opcode 0xC7 is a good one to block)
- FLILL register is constant across ICH8, ICH9, ICH10 and appears to be the same on PCH*
  - Same location (FCBA + 004h), same bit meanings

*Based purely on my analysis of BIOS dumps on machines running PCH

Note on SPI Instructions (opcodes)

- Each ICH/PCH datasheet defines a minimal set of SPI commands that a chip must support
  - H/W Sequencing
  - Interoperability with Intel platform
- This table can serve a reference to identify any opcodes that are listed in the FLILL register
- However, each serial flash device may have unique capabilities and commands

Commands	Opcode
Write to Status Register	01h
Program Data	02h
Read Data	03h
Write Disable	04h
Read Status	05h
Write Enable	06h
Fast Read	0Bh
Enable Write to Status Register	50h or 06h
Erase	Program mable
Full Chip Erase	C7h
JEDEC ID	9Fh

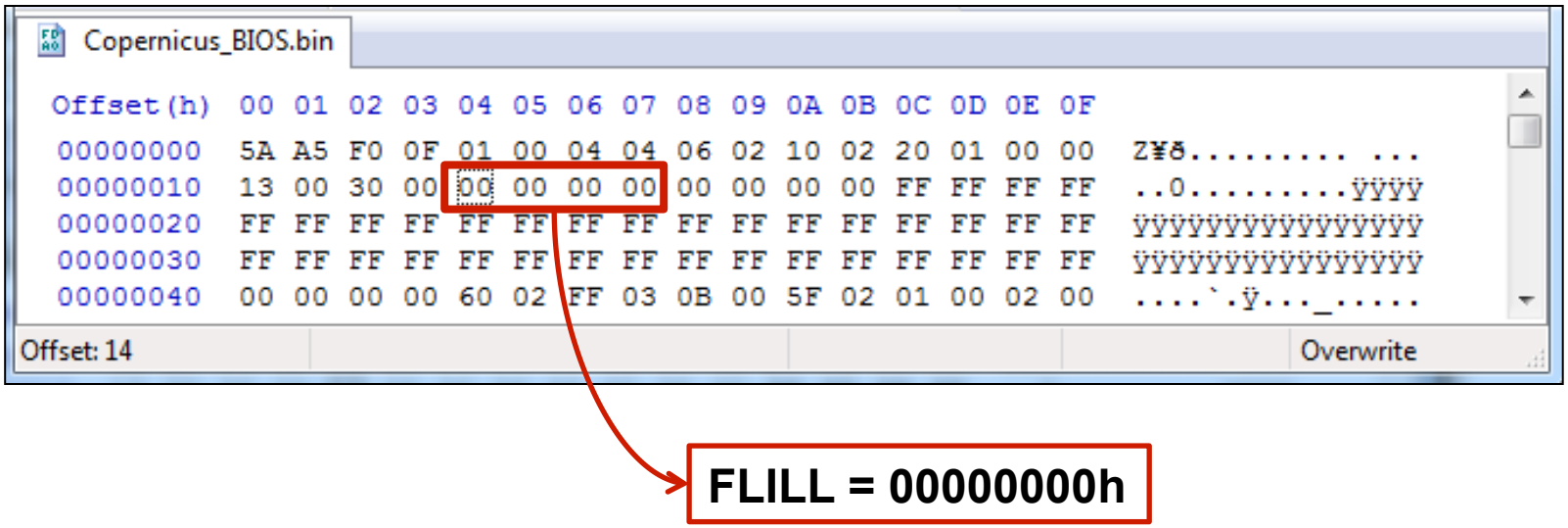
ICH 10 Required Opcodes

*Write Enable looks interesting doesn't it? A future Advanced course goes into SPI Programming

- Supported opcodes on an Atmel AT25DF321A SPI Serial Flash
- Taken straight from Atmel's datasheet
- Supports more than the minimum set required by Intel
- Notice it supports more than one Chip Erase command
- FLILL register must be filled out with these opcodes in mind, not just those that Intel lists

Command	Opcode	
Read Commands		
Read Array	0Bh	0000 1011
Read Array (Low Frequency)	03h	0000 0011
Program and Erase Commands		
Block Erase (4-KBytes)	20h	0010 0000
Block Erase (32-KBytes)	52h	0101 0010
Block Erase (64-KBytes)	D8h	1101 1000
Chip Erase	60h	0110 0000
	C7h	1100 0111
Byte/Page Program (1 to 256 Bytes)	02h	0000 0010
Protection Commands		
Write Enable	06h	0000 0110
Write Disable	04h	0000 0100
Protect Sector	36h	0011 0110
Unprotect Sector	39h	0011 1001
Global Protect/Unprotect	Use Write Status Register command	
Read Sector Protection Registers	3Ch	0011 1100
Status Register Commands		
Read Status Register	05h	0000 0101
Write Status Register	01h	0000 0001
Miscellaneous Commands		
Read Manufacturer and Device ID	9Fh	1001 1111
Deep Power-Down	B9h	1011 1001
Resume from Deep Power-Down	ABh	1010 1011

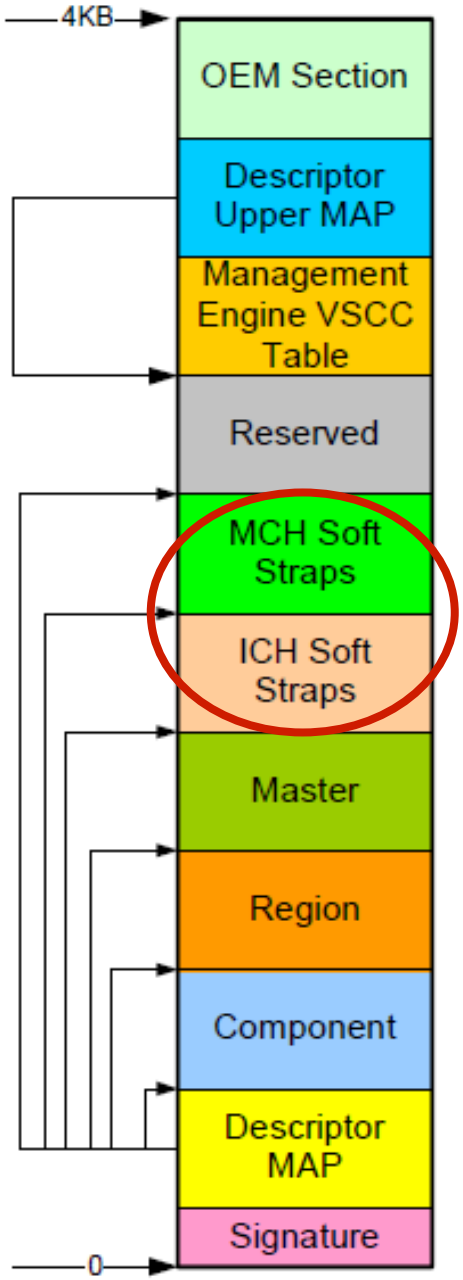
http://www.atmel.com/Images/doc3633.pdf



- Looking at the Flash Invalid Instructions Register from the Copernicus BIOS dump, we can see that none are defined
- Although only 4 opcodes can be black-listed here, it's still a setting that should be used
- And the SPI Flash vendor's datasheet should be taken into account when defining forbidden opcodes
- I don't recall any other source that has provided this recommendation

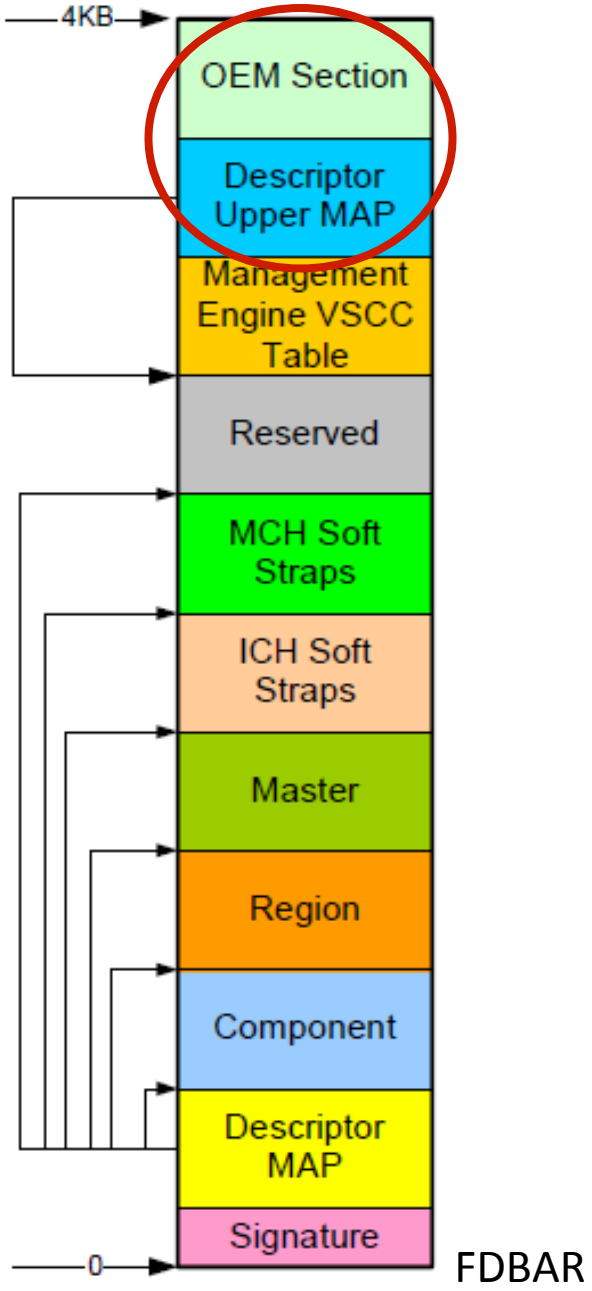
Soft Straps

- First implemented in ICH8
  - In PCH, both regions are combined into a single PCH Soft Straps section
- Soft Strap data is read out of the SPI device prior to de-asserting a reset (power-on, in layman's terms)
- Configure specific functions within the chipset before the BIOS or any other software can intervene
- The specific details regarding the implementation of Soft Straps are located in Intel's confidential SPI programming guides



OEM Section and Descriptor Upper MAP

- OEM Section
  - *CH does not read the OEM information
  - 256 bytes (ICH8, ICH9, ICH10, and PCH (up thru 8-series PCH[1])
- Descriptor Upper MAP
  - Describes the Base and length of the Management Vendor Specific Component Capabilities (VSCC) Table
  - Base address is at FDBAR + EFCh (ICH8, ICH9, ICH10, and PCH[2])
    - Recall FDBAR is offset 10h on the flash chip on PCH, 0h on all others

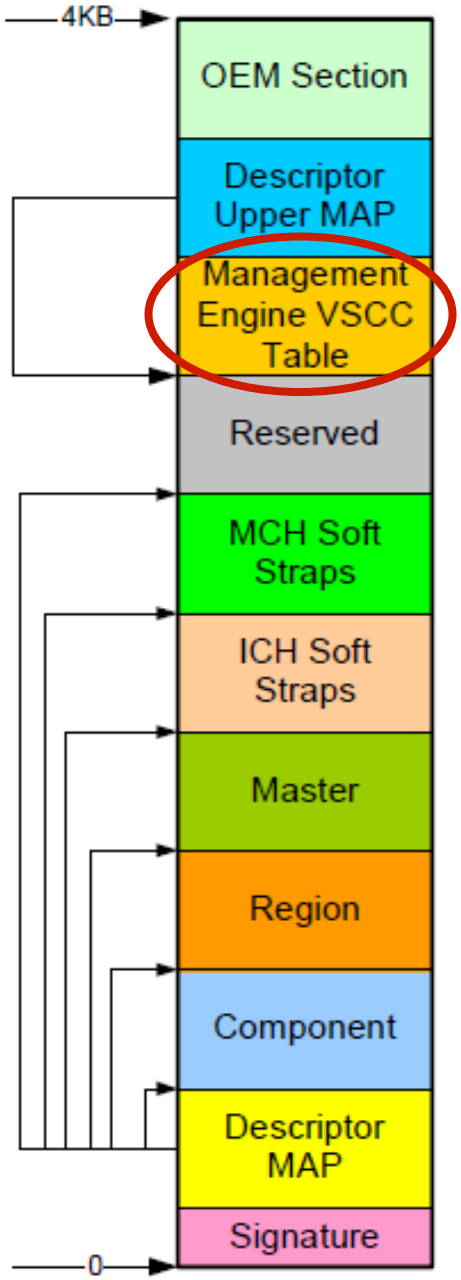


[1] Most recent PCH at the time of this writing

[2] Based on my analysis of BIOS binaries

Management Engine VSCC* Table

- Contains the JEDEC ID of the Flash Chip
  - Identifies the Vendor and Device ID of the SPI serial flash
- Describes the different attributes an SPI partition can have (Upper or Lower)
  - Based on the value defined in the FPBA flash descriptor register in the Master section
  - If SPI is defined as having one single partition, then only the attributes defined for the Upper partition are used.



*VSCC = Vendor Specific Component Capabilities