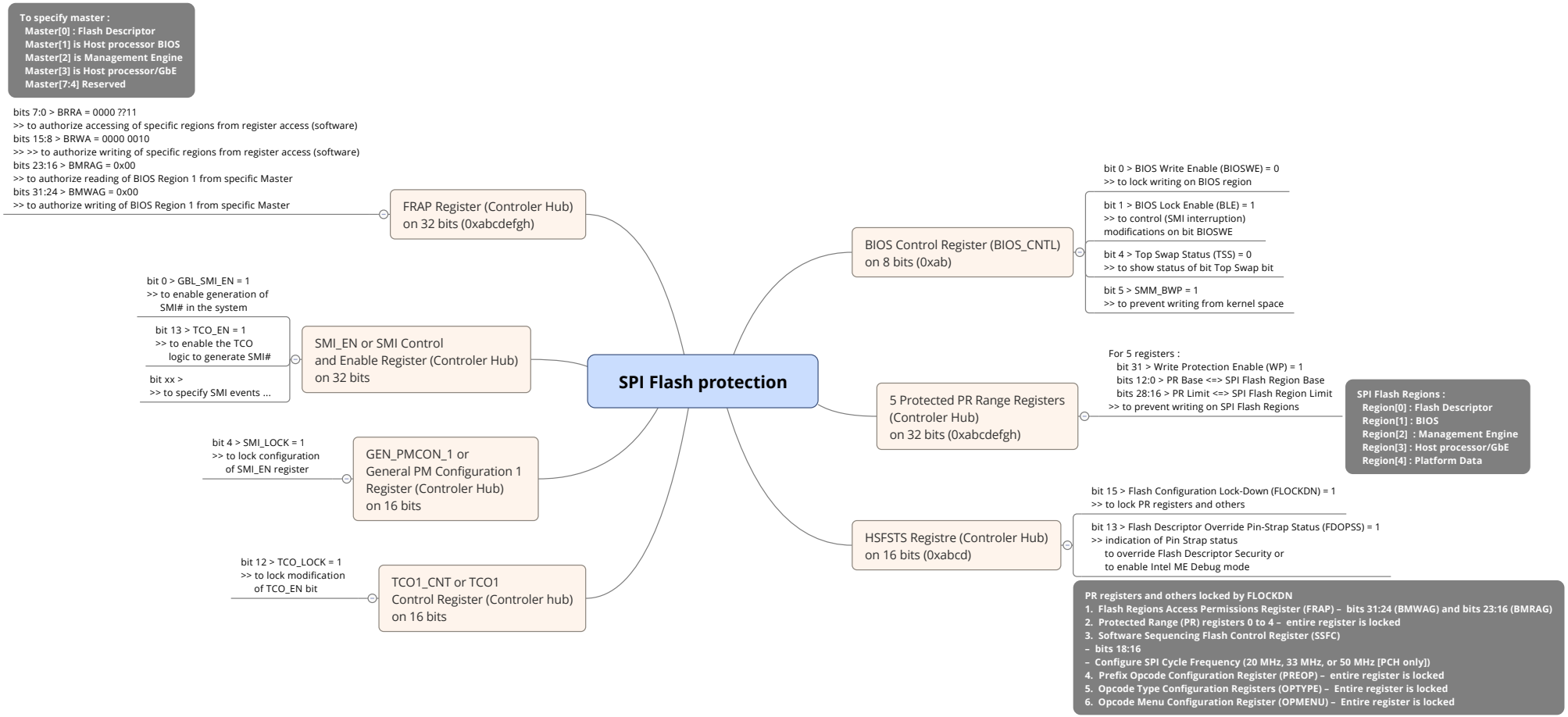
SPI Flash protection
FRAP Register (Controler Hub) on 32 bits (0xabcdefgh)
bits 7:0 > BRRA = 0000 ??11
>> to authorize accessing of specific regions from register access (software)
bits 15:8 > BRWA = 0000 0010
>> >> to authorize writing of specific regions from register access (software)
bits 23:16 > BMRAG = 0x00
>> to authorize reading of BIOS Region 1 from specific Master
bits 31:24 > BMWAG = 0x00
>> to authorize writing of BIOS Region 1 from specific Master
To specify master :
Master[0] : Flash Descriptor
Master[1] is Host processor BIOS
Master[2] is Management Engine
Master[3] is Host processor/GbE
Master[7:4] Reserved
SMI_EN or SMI Control and Enable Register (Controler Hub) on 32 bits
bit 0 > GBL_SMI_EN = 1
>> to enable generation of SMI# in the system
bit 13 > TCO_EN = 1
>> to enable the TCO logic to generate SMI#
bit xx >
>> to specify SMI events ...
GEN_PMCON_1 or General PM Configuration 1 Register (Controler Hub) on 16 bits
bit 4 > SMI_LOCK = 1
>> to lock configuration of SMI_EN register
TCO1_CNT or TCO1 Control Register (Controler hub) on 16 bits
bit 12 > TCO_LOCK = 1
>> to lock modification of TCO_EN bit
BIOS Control Register (BIOS_CNTL) on 8 bits (0xab)
bit 0 > BIOS Write Enable (BIOSWE) = 0
>> to lock writing on BIOS region
bit 1 > BIOS Lock Enable (BLE) = 1
>> to control (SMI interruption) modifications on bit BIOSWE
bit 4 > Top Swap Status (TSS) = 0
>> to show status of bit Top Swap bit
bit 5 > SMM_BWP = 1
>> to prevent writing from kernel space
5 Protected PR Range Registers (Controler Hub) on 32 bits (0xabcdefgh)
For 5 registers :
bit 31 > Write Protection Enable (WP) = 1
bits 12:0 > PR Base <=> SPI Flash Region Base
bits 28:16 > PR Limit <=> SPI Flash Region Limit
>> to prevent writing on SPI Flash Regions
SPI Flash Regions :
Region[0] : Flash Descriptor
Region[1] : BIOS
Region[2] : Management Engine
Region[3] : Host processor/GbE
Region[4] : Platform Data
HSFSTS Registre (Controler Hub) on 16 bits (0xabcd)
bit 15 > Flash Configuration Lock-Down (FLOCKDN) = 1
>> to lock PR registers and others
bit 13 > Flash Descriptor Override Pin-Strap Status (FDOPSS) = 1
>> indication of Pin Strap status to override Flash Descriptor Security or to enable Intel ME Debug mode
PR registers and others locked by FLOCKDN
1. Flash Regions Access Permissions Register (FRAP) – bits 31:24 (BMWAG) and bits 23:16 (BMRAG)
2. Protected Range (PR) registers 0 to 4 – entire register is locked
3. Software Sequencing Flash Control Register (SSFC)
– bits 18:16
– Configure SPI Cycle Frequency (20 MHz, 33 MHz, or 50 MHz [PCH only])
4. Prefix Opcode Configuration Register (PREOP) – entire register is locked
5. Opcode Type Configuration Registers (OPTYPE) – Entire register is locked
6. Opcode Menu Configuration Register (OPMENU) – Entire register is locked