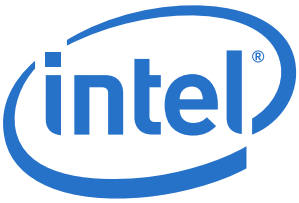


10th Generation Intel® Processor Families

Datasheet, Volume 2 of 2

Supporting 10th Generation Intel® Core™ Processor Families, Intel® Pentium® Processors, Intel® Celeron® Processors for U/Y Platforms, formerly known as Ice Lake

April 2020

Revision 002

Document Number: 341078-002

Contents

1 Introduction 7

2 Processor Configuration Register Definitions and Address Ranges 8

2.1 Register Terminology 8
2.2 PCI Devices and Functions 9
2.3 System Address Map 10
2.4 DOS Legacy Address Range 12
2.4.1 DOS Range (0h – 9_FFFFh) 13
2.4.2 Legacy Video Area (A_0000h – B_FFFFh) 13
2.4.3 Programmable Attribute Map (PAM) (C_0000h – F_FFFFh) 14
2.5 Lower Main Memory Address Range (1 MB – TOLUD) 15
2.5.1 ISA Hole (15 MB –16 MB) 16
2.5.2 1 MB to TSEGMB 16
2.5.3 TSEG 16
2.5.4 Protected Memory Range (PMR) - (Programmable) 16
2.5.5 DRAM Protected Range (DPR) 17
2.5.6 Pre-allocated Memory 17
2.6 PCI Memory Address Range (TOLUD – 4 GB) 17
2.6.1 APIC Configuration Space (FEC0_0000h – FECF_FFFFh) 20
2.6.2 HSEG (FEDA_0000h – FEDB_FFFFh) 20
2.6.3 MSI Interrupt Memory Space (FEE0_0000h – FEEF_FFFFh) 20
2.6.4 High BIOS Area 20
2.7 Upper Main Memory Address Space (4 GB to TOUUD) 21
2.7.1 Top of Memory (TOM) 21
2.7.2 Top of Upper Usable DRAM (TOUUD) 21
2.7.3 Top of Low Usable DRAM (TOLUD) 21
2.7.4 TSEG_BASE 21
2.7.5 Memory Re-claim Background 22
2.7.6 Indirect Accesses to MCHBAR Registers 22
2.7.7 Memory Remapping 23
2.7.8 Hardware Remap Algorithm 23
2.8 PCI Express* Configuration Address Space 23
2.9 Graphics Memory Address Ranges 23
2.9.1 IOBAR Mapped Access to Device 2 MMIO Space 24
2.9.2 Trusted Graphics Ranges 24
2.10 System Management Mode (SMM) 24
2.11 SMM and VGA Access Through GTT TLB 24
2.12 Intel® Management Engine (Intel® ME) Stolen Memory Accesses 25
2.13 I/O Address Space 25
2.13.1 PCI Express* I/O Address Mapping 26
2.14 Direct Media Interface (DMI) Interface Decode Rules 26
2.14.1 DMI Accesses to the Processor that Cross Device Boundaries 27
2.14.2 Traffic Class (TC) / Virtual Channel (VC) Mapping Details 27
2.15 PCI Express* Interface Decode Rules 30
2.15.1 TC/VC Mapping Details 30
2.16 Legacy VGA and I/O Range Decode Rules 31
2.17 I/O Mapped Registers 35

3 Host Bridge and DRAM Controller (D0:F0) 36

3.1 Host Bridge/DRAM Registers (D0:F0) 36
3.2 Memory Controller (MCHBAR) Registers 80

3.3 Power Management (MCHBAR) Registers 127
3.4 Host Controller (MCHBAR) Registers 166
3.5 Direct Media Interface BAR (DMIBAR) Registers 171
3.6 REGBAR Registers 189
3.7 PCI Express Egress Port BAR (PXPEPBAR) Registers 211
3.8 VTDPVC0BAR Registers 231

4 Processor Graphics (D2:F0) 268
4.1 Processor Graphics Registers (D2:F0) 268
4.2 Graphics VT BAR (GFXVTBAR) Registers 322

5 Dynamic Power Performance Management Registers (D4:F0) 376
5.1 Vendor ID (VID_0_4_0_PCI) — Offset 0h 376
5.2 Device ID (DID_0_4_0_PCI) — Offset 2h 377
5.3 PCI Command (PCICMD_0_4_0_PCI) — Offset 4h 377
5.4 PCI Status (PCISTS_0_4_0_PCI) — Offset 6h 378
5.5 Revision ID (RID_0_4_0_PCI) — Offset 8h 380
5.6 Class Code (CC_0_4_0_PCI) — Offset 9h 380
5.7 Extended Class Code (CC_0_4_0_NOPI_PCI) — Offset Ah 381
5.8 Cache Line Size Register (CLS_0_4_0_PCI) — Offset Ch 381
5.9 Master Latency Timer (MLT_0_4_0_PCI) — Offset Dh 382
5.10 Header Type (HDR_0_4_0_PCI) — Offset Eh 382
5.11 Built In Self Test (BIST_0_4_0_PCI) — Offset Fh 382
5.12 Thermal Controller Base Address (TMBAR_0_4_0_PCI) — Offset 10h 383
5.13 Subsystem Vendor ID (SVID_0_4_0_PCI) — Offset 2Ch 384
5.14 Subsystem ID (SID_0_4_0_PCI) — Offset 2Eh 384
5.15 Capability Pointer (CAPPOINT_0_4_0_PCI) — Offset 34h 385
5.16 Interrupt Line Register (INTRLINE_0_4_0_PCI) — Offset 3Ch 385
5.17 Interrupt Pin Register (INTRPIN_0_4_0_PCI) — Offset 3Dh 386
5.18 Minimum Guaranteed (MINGNT_0_4_0_PCI) — Offset 3Eh 386
5.19 Maximum Latency (MAXLAT_0_4_0_PCI) — Offset 3Fh 387
5.20 Device Enable (DEVEN_0_4_0_PCI) — Offset 54h 387
5.21 Capabilities A (CAPID0_A_0_4_0_PCI) — Offset E4h 389
5.22 Capabilities B (CAPID0_B_0_4_0_PCI) — Offset E8h 391

6 Image Processing Unit Registers (D5:F0) 394
6.1 Vendor ID and Device ID (VID_DID) — Offset 0h 394
6.2 Command and Status (PCICMD_PCISTS) — Offset 4h 395
6.3 Revision ID and Class Code (RID_CC) — Offset 8h 396
6.4 Cache Line Size, Master Latency Timer, Header Type and BIST (CLS_MLT_HT_BIST) — Offset Ch 397
6.5 ISPMMADR LSB (ISPMMADR_LOW) — Offset 10h 398
6.6 ISPMMADR MSB (ISPMMADR_HIGH) — Offset 14h 398
6.7 Subsystem Vendor ID and Subsystem ID (SVID_SID) — Offset 2Ch 399
6.8 Capabilities Pointer (CAPPOINT) — Offset 34h 399
6.9 Interrupt Properties (INTR) — Offset 3Ch 399
6.10 PCIe Capabilities (PCIECAPHDR_PCIECAP) — Offset 70h 400
6.11 Device Capabilities (DEVICECAP) — Offset 74h 401
6.12 Device Capabilities and Control (DEVICECTL_DEVICESTS) — Offset 78h 402
6.13 MSI Capabilities and MSI Control (MSI_CAPID) — Offset ACh 402
6.14 MSI Address Low (MSI_ADDRESS_LO) — Offset B0h 403
6.15 MSI Address High (MSI_ADDRESS_HI) — Offset B4h 404
6.16 MSI Data (MSI_DATA) — Offset B8h 404
6.17 Power Management Capabilities (PMCAP) — Offset D0h 405
6.18 Power Management Control and Status (PMCS) — Offset D4h 405
6.19 IPUVTDBAR Base Address Register (IPUVTDBAR_LOW) — Offset F0h 406

6.20 IPUVTDBAR Base Address Register (IPUVTDBAR_HIGH) — Offset F4h 407

7 Gauss Newton Algorithm Registers (D8:F0) 408

7.1 Vendor & Device ID (IDENTIFICATION) — Offset 0h 409
7.2 Device Control (DCTRL) — Offset 4h 409
7.3 Device Status (DSTS) — Offset 6h 410
7.4 Revision ID & Class Codes (RID_DLCO) — Offset 8h 412
7.5 Cache Line Size (CLS) — Offset Ch 412
7.6 Header Type (HTYPE) — Offset Eh 413
7.7 Built-in Self Test (BIST) — Offset Fh 413
7.8 GNA Base Address Low (GNABAL) — Offset 10h 414
7.9 GNA Base Address High (GNABAH) — Offset 14h 415
7.10 Sub System Vendor Identifiers (SSVI) — Offset 2Ch 415
7.11 Sub System Identifiers (SSI) — Offset 2Eh 416
7.12 Capabilities Pointers (CAPP) — Offset 34h 416
7.13 Interrupt Line (INTL) — Offset 3Ch 417
7.14 Interrupt Pin Register (INTP) — Offset 3Dh 417
7.15 Min Grant And Min Latency Register (MINGNTLAT) — Offset 3Eh 418
7.16 Override Configuration Control (OVRCFGCTL) — Offset 40h 418
7.17 Message Signaled Interrupt Capability ID (MSICAPID) — Offset 90h 419
7.18 Message Signaled Interrupt Message Control (MC) — Offset 92h 420
7.19 Message Signaled Interrupt Message Address (MA) — Offset 94h 420
7.20 Message Signaled Interrupt Message Data (MD) — Offset 98h 421
7.21 D0i3 Capability ID (D0I3CAPID) — Offset A0h 421
7.22 D0i3 Capability (D0I3CAP) — Offset A2h 422
7.23 D0i3 Vendor Extended Capability Register (D0I3VSEC) — Offset A4h 422
7.24 D0i3 SW LTR Pointer Register (D0I3SWLTRPTR) — Offset A8h 423
7.25 D0i3 DevIdle Pointer Register (D0I3DEVIDLEPTR) — Offset ACh 423
7.26 D0i3 DevIdle Power On Latency (D0I3DEVIDLEPOL) — Offset B0h 424
7.27 D0i3 Power Control Enables Register (PCE) — Offset B2h 425
7.28 Power Management Capability ID (PMCAPID) — Offset DCh 425
7.29 Power Management Capability (PMCAP) — Offset DEh 426
7.30 Power Management Control Status (PMCS) — Offset E0h 427
7.31 FLR Capability ID (FLRCAPID) — Offset F0h 428
7.32 FLR Capability Length And Version (FLRMISC) — Offset F2h 428
7.33 FLR Control Register (FLRCTL) — Offset F4h 429
7.34 FLR Status Register (FLRSTS) — Offset F5h 429

8 Type C Subsystem (TCSS) 430

8.1 Thunderbolt DMA Device Registers (D13:F2-3) 430
8.2 USB Host Controller (xHCI) Registers (D13:F0) 448
8.3 USB Host Controller MBAR Registers (D13:F0) 472
8.4 USB Device Controller (xDCI) Configuration Registers (D13:F1) 581
8.5 Thunderbolt PCI Express* Controller Registers (D7:F0-3) 594

Revision History

Revision Number	Description	Revision Date
001	• Initial release	August 2019
002	• Updated revision description	April 2020

§ §

1 Introduction

This is Volume 2 of the Intel® 10th Generation Core Datasheet. Volume 2 provides register information for the processor.

Refer #341077 for the Intel® 10th Generation Core Datasheet, Volume 1 of 2.

The processor contains one or more PCI devices within a single physical component. The configuration registers for these devices are mapped as devices residing on the PCI Bus assigned for the processor socket. This document describes these configuration space registers or device-specific control and status registers only.

§ §

2 Processor Configuration Register Definitions and Address Ranges

This chapter describes the processor configuration register, I/O, memory address ranges and Model Specific Registers (MSRs). The chapter provides register terminology. PCI Devices and Functions are described.

2.1 Register Terminology

Table below lists the register-related terminology and access attributes that are used in this document. Register Attribute Modifiers table provides the attribute modifiers.

Table 2-1. Register Attributes and Terminology

Item	Description
RO	**Read Only:** These bits can only be read by software, writes have no effect. The value of the bits is determined by the hardware only.
RW	**Read / Write:** These bits can be read and written by software.
RW1C	**Read / Write 1 to Clear:** These bits can be read and cleared by software. Writing a '1' to a bit will clear it, while writing a '0' to a bit has no effect. Hardware sets these bits.
RW0C	**Read / Write 0 to Clear:** These bits can be read and cleared by software. Writing a '0' to a bit will clear it, while writing a '1' to a bit has no effect. Hardware sets these bits.
RW1S	**Read / Write 1 to Set:** These bits can be read and set by software. Writing a '1' to a bit will set it, while writing a '0' to a bit has no effect. Hardware clears these bits.
RsvdP	**Reserved and Preserved:** These bits are reserved for future RW implementations and their value should not be modified by software. When writing to these bits, software should preserve the value read. When SW updates a register that has RsvdP fields, it should read the register value first so that the appropriate merge between the RsvdP and updated fields will occur.
RsvdZ	**Reserved and Zero:** These bits are reserved for future RW1C implementations. Software should use 0 for writes.
WO	**Write Only:** These bits can only be written by software, reads return zero.
RC	**Read Clear:** These bits can only be read by software, but a read causes the bits to be cleared. Hardware sets these bits.
RSW1C	**Read Set / Write 1 to Clear:** These bits can be read and cleared by software. Reading a bit will set the bit to '1'. Writing a '1' to a bit will clear it, while writing a '0' to a bit has no effect.
RCW	**Read Clear / Write:** These bits can be read and written by software, but a read causes the bits to be cleared.

Table 2-2. Register Attribute Modifiers (Sheet 1 of 2)

Attribute Modifier	Applicable Attribute	Description
S	RO (w/ -V)	**Sticky:** These bits are only re-initialized to their default value by a "Power Good Reset" (Cold Reset).
	RW	
	RW1C	
	RW1S	

Table 2-2. Register Attribute Modifiers (Sheet 2 of 2)

Attribute Modifier	Applicable Attribute	Description
-K	RW	**Key**: These bits control the ability to write other bits (identified with a 'Lock' modifier)
-L	RW	**Lock**: Hardware can make these bits "Read Only" using a separate configuration bit or other logic.
	WO	
-O	RW	**Once**: After reset, these bits can only be written by software once, after which they become "Read Only".
	WO	
-FW	RO	**Firmware Write**: The value of these bits can be updated by processor hardware mechanisms that may be firmware dependent.
-V	RO	**Variant**: The value of these bits can be updated by hardware.

2.2 PCI Devices and Functions

The processor contains multiple PCI devices. The configuration registers for these devices are mapped as devices residing on PCI Bus 0.

- Device 0: Host Bridge / DRAM Controller / LLC Controller 0 – Logically this device appears as a PCI device residing on PCI bus 0. Device 0 contains the standard PCI header registers, PCI Express* base address register, DRAM control (including thermal/throttling control), configuration for the DMI, and other processor specific registers.
- Device 2: Processor Graphics – Logically, this device appears as a PCI device residing on PCI Bus 0. Device 2 contains the configuration registers for 3D, 2D, and display functions. In addition, Device 2 is located in two separate physical locations – Processor Graphics (GT) and Display Engine.
- Device 4: Dynamic Power Performance Management (DPPM) - Logically, this device appears as a PCI device residing on PCI Bus 0. Device 4 contains the configuration registers for the DPPM device.
- Device 5: Image Processing Unit (IPU) – Logically, this device appears as a PCI device residing on PCI Bus 0. Device 5 contains the configuration registers for the Image Processing Unit.
- Device 7: Thunderbolt™ PCIe* Controllers – Logically this device appears as a "virtual" PCI-to-PCI bridge residing on PCI bus 0, and is compliant with the *PCI-to-PCI Bridge Architecture Specification, Revision 1.2*. Device 7 is a multi-function device consisting of up to 4 functions (0, 1, 2, 3). Device 7 contains the standard PCI-to-PCI bridge registers and the standard PCI Express*/PCI configuration registers.
  - Device 7 is closely associated with device 13.
- Device 8: Gauss Newton Algorithm Device (GNA) – Logically, this device appears as a PCI device residing on PCI Bus 0. Device 8 contains the configuration registers for the Gauss Newton Algorithm Device.
- Device 9: Intel® Trace Hub. Logically, this device appears as a PCI device residing on PCI Bus 0. Device 9 contains the configuration registers for the Trace Hub device. Trace Hub documentation can be found at https://software.intel.com/sites/default/files/managed/f3/47/intel-trace-hub-developers-manual-v2.pdf
- Device 13: USB-C Device – Logically, this device appears as a PCI device residing on PCI Bus 0. Device 13 contains the following functions:

— Function 0: USB-C SuperSpeed Host Controller.
— Function 1: USB-C SuperSpeed Device Controller.
— Functions 2, 3: Thunderbolt™ DMA Controllers.

Table 2-3. Processor PCI Devices and Functions

Description	Device	Function
HOST and DRAM Controller	0	0
Processor Graphics	2	0
Dynamic Power Performance Management	4	0
Image Processing Unit	5	0
Thunderbolt™ PCI Express* Controllers	7	0,1,2,3
Gauss Newton Algorithm Device	8	0
Trace Hub	9	0
USB Host Controller	13	0
USB Device Controller	13	1
Thunderbolt™ DMA	13	2,3

From a configuration standpoint, the DMI is logically PCI bus 0. As a result, all devices internal to the processor and the PCH appear to be on PCI Bus 0.

Note: Some devices are not present in every model of the processor.

Note: PCI Express* (PCIe*) and DMI do not apply to U/Y Processors.

2.3 System Address Map

The processor supports 512 GB (39 bits) of addressable memory space and 64 KB+3 of addressable I/O space.

This section focuses on how the memory space is partitioned and how the separate memory regions are used. I/O address space has simpler mapping and is explained towards the end of this chapter.

The processor supports PCIe* port upper prefetchable base/limit registers. This allows the PCIe* bridges to claim Memory Mapped I/O (MMIO) accesses above 32 bit. Addressing of greater than 4 GB is allowed on both the DMI Interface or PCIe* interfaces. DRAM capacity is limited by the number of address pins available. There is no hardware lock to prevent more memory from being inserted than is addressable.

In the following sections, it is assumed that all of the compatibility memory ranges reside on the DMI Interface. The exception to this rule is VGA ranges, which may be mapped to PCI Express*, DMI, or to the Processor Graphics device (Processor Graphics). The processor does not remap APIC or any other memory spaces above TOLUD (Top of Low Usable DRAM). The TOLUD register is set to the appropriate value by BIOS. The remapbase/remaplimit registers remap logical accesses bound for addresses above 4 GB onto physical addresses that fall within DRAM.

The Address Map includes a number of programmable ranges that are not configured using standard PCI BAR configuration:

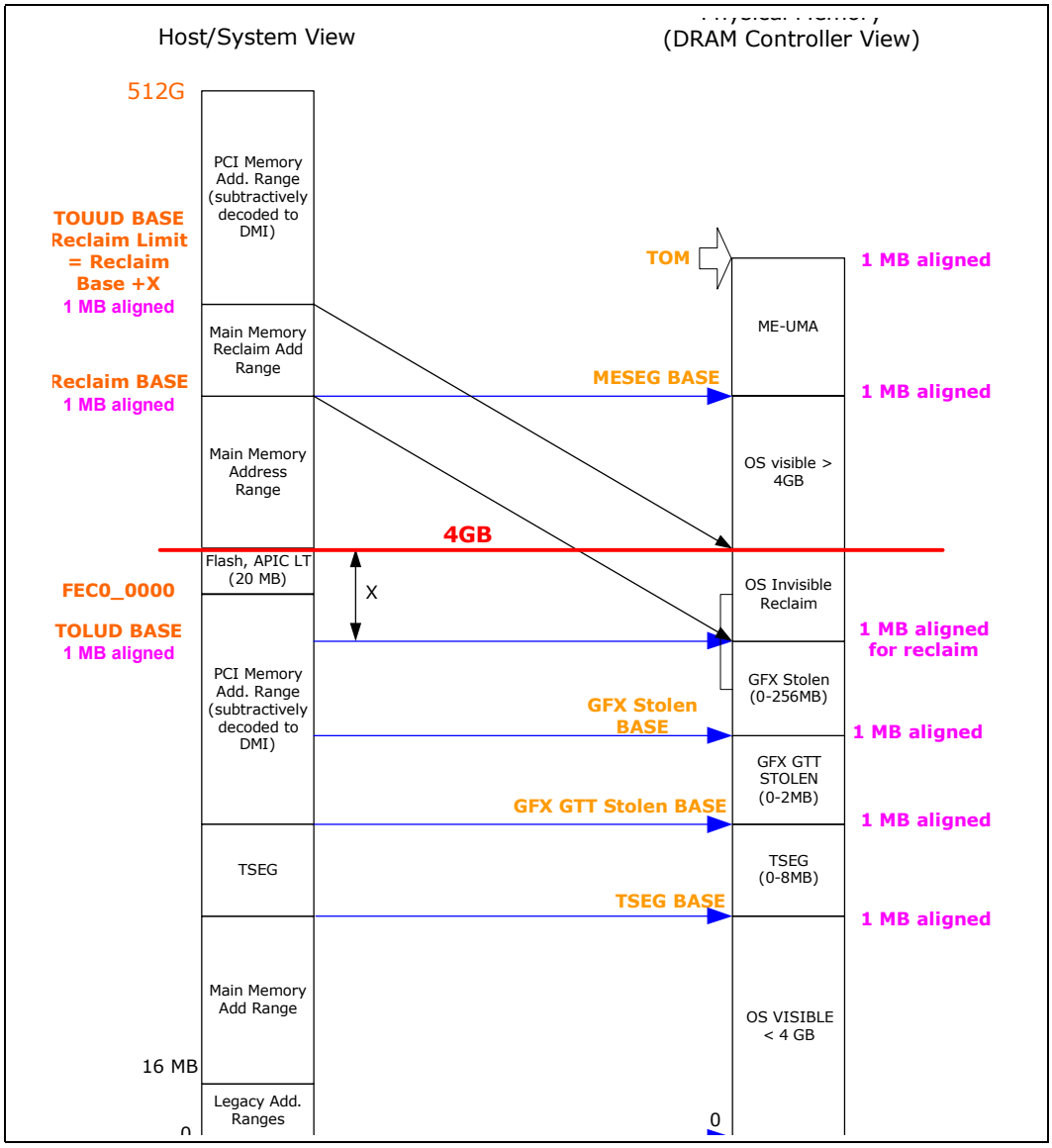
- Device 0:

  - PXPEPBAR – Memory mapped range for PCIe* egress port registers. (4 KB window).
  - MCHBAR – Host Memory Mapped Configuration (memory subsystem and power management registers). (64 KB window)
  - DMIBAR – This window is used to access registers associated with the processor/PCH Serial Interconnect (DMI) register memory range. (4 KB window).
  - VTDPVC0BAR - Memory mapped range for VT-d configuration
  - GFXVTBAR - Memory mapped range for VT configuration of the processor graphics device (4KB window).
  - REGBAR - Memory mapped range for System Agent registers (16MB window).
  - GGC.GMS – Graphics Mode Select. Main memory that is pre-allocated to support the Processor Graphics device in VGA (non-linear) and Native (linear) modes. (0 – 512 MB options).
  - GGC.GGMS – GTT Graphics Memory Size. Main memory that is pre-allocated to support the Processor Graphics Translation Table. (0 – 2 MB options).
- For all other PCI devices within the processor that expose PCI configuration space, the behavior is according to PCI specification.

The rules for the above programmable ranges are:

1. For security reasons, the processor positively decodes (FFE0_0000h to FFFF_FFFFh) to DMI. This ensures the boot vector and BIOS execute off the PCH.
2. ALL of these ranges should be unique and NON-OVERLAPPING. It is the BIOS or system designer's responsibility to limit memory population so that adequate PCI, PCI Express*, High BIOS, PCI Express* Memory Mapped space, and APIC memory space can be allocated.
3. In the case of overlapping ranges with memory, the memory decode will be given priority. This is an Intel® Trusted Execution Technology (Intel® TXT) requirement. It is necessary to get Intel® TXT protection checks, avoiding potential attacks.
4. There are NO Hardware Interlocks to prevent problems in the case of overlapping memory ranges.
5. Accesses to overlapped ranges may produce indeterminate results.
6. Peer-to-peer write cycles are allowed below the Top of Low Usable memory (register TOLUD) for DMI Interface to PCI Express* VGA range writes. Peer-to-peer cycles to the Processor Graphics VGA range are not supported.

Figure 2-1. System Address Range Example



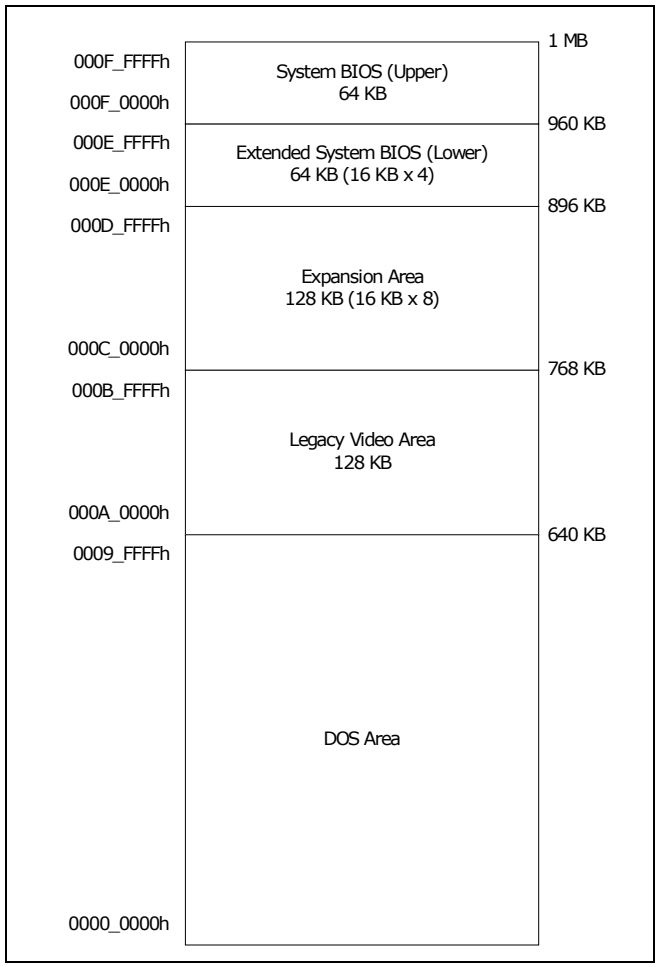
2.4 DOS Legacy Address Range

The memory address range from 0 to 1 MB is known as Legacy Address. This area is divided into the following address regions:

- 0 – 640 KB - DOS Area
- 640 – 768 KB - Legacy Video Buffer Area
- 768 – 896 KB in 16 KB sections (total of 8 sections) – Expansion Area
- 896 – 960 KB in 16 KB sections (total of 4 sections) – Extended System BIOS Area
- 960 KB – 1 MB Memory, System BIOS Area

The area between 768 KB – 1 MB is also collectively referred to as PAM (Programmable Address Memory). All accesses to the DOS and PAM ranges from any device are sent to DRAM. However, access to the legacy video buffer area is treated differently.

Figure 2-2. DOS Legacy Address Range



2.4.1 DOS Range (0h – 9_FFFFh)

The DOS area is 640 KB (0000_0000h – 0009_FFFFh) in size and is always mapped to the main memory.

2.4.2 Legacy Video Area (A_0000h – B_FFFFh)

The same address region is used for both Legacy Video Area.

- Legacy Video Area: The legacy 128 KB VGA memory range, frame buffer, at 000A_0000h – 000B_FFFFh, can be mapped to Processor Graphics (Device 2), to PCI Express* (Device 1, 6), and/or to the DMI Interface.
- Monochrome Adapter (MDA) Range: Legacy support for monochrome display adapter

Note: The legacy video area is not available for SMM use.

2.4.2.1 Legacy Video Area

The legacy 128 KB VGA memory range, frame buffer at 000A_0000h – 000B_FFFFh, can be mapped to Processor Graphics (Device 2), to PCI Express* (Device 1, 6), and/or to the DMI Interface.

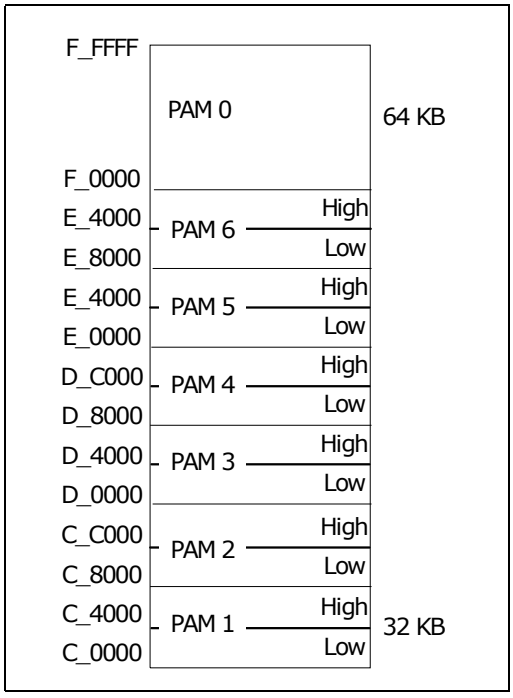
2.4.2.2 Monochrome Adapter (MDA) Range

Legacy support requires the ability to have a second graphics controller (monochrome) in the system. The monochrome adapter may be mapped to Processor Graphics (Device 2), to PCI Express* (Device 1, 6), and/or to the DMI Interface.

2.4.3 Programmable Attribute Map (PAM) (C_0000h – F_FFFFh)

PAM is a legacy BIOS ROM area in MMIO. It is overlaid with DRAM and used as a faster ROM storage area. It has a fixed base address (000C_0000h) and fixed size of 256 KB. The 13 sections from 768 KB to 1 MB comprise what is also known as the PAM Memory Area. Each section has Read enable and Write enable attributes.

Figure 2-3. PAM Region Space



The PAM registers are mapped in Device 0 configuration space.

- ISA Expansion Area (C_0000h – D_FFFFh)
- Extended System BIOS Area (E_0000h – E_FFFFh)
- System BIOS Area (F_0000h – F_FFFFh)

The processor decodes the Core request, then routes to the appropriate destination (DRAM or DMI).

Snooped accesses from devices to this region are snooped on processor Caches.

Graphics translated requests to this region are not allowed. If such a mapping error occurs, the request will be routed to C_0000h. Writes will have the byte enables de-asserted.

2.5 Lower Main Memory Address Range (1 MB – TOLUD)

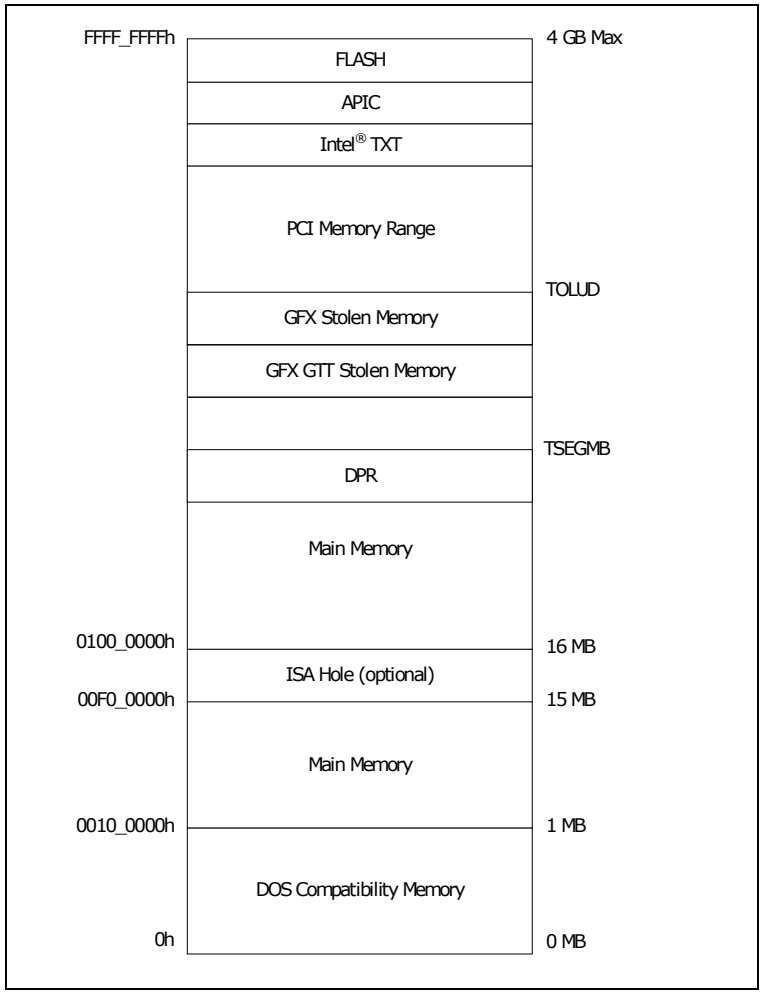
This address range extends from 1 MB to the top of Low Usable physical memory that is permitted to be accessible by the processor (as programmed in the TOLUD register). The processor will route all addresses within this range to the DRAM unless it falls into the optional TSEG, optional ISA Hole or optional Processor Graphics stolen memory.

This address range is divided into two sub-ranges:

- 1 MB to TSEGMB
- TSEGMB to TOULUD

TSEGMB indicates the TSEG Memory Base address.

Figure 2-4. Main Memory Address Range



2.5.1 ISA Hole (15 MB –16 MB)

The ISA Hole (starting at address F0_0000h) is enabled in the Legacy Access Control Register in Device 0 configuration space. If no hole is created, the processor will route the request to DRAM. If a hole is created, the processor will route the request to DMI.

Graphics translated requests to the range will always route to DRAM.

2.5.2 1 MB to TSEGMB

Processor access to this range will be directed to memory with the exception of the ISA Hole (when enabled).

2.5.3 TSEG

For processor initiated transactions, the processor relies on correct programming of SMM Range Registers (SMRR) to enforce TSEG protection.

TSEG is below Processor Graphics stolen memory, which is at the Top of Low Usable physical memory (TOLUD). BIOS will calculate and program the TSEG BASE in Device 0 (TSEGMB), used to protect this region from DMA access. Calculation is:

TSEGMB = TOLUD – DSM SIZE – GSM SIZE – TSEG SIZE

SMM-mode processor accesses to TSEG always access the physical DRAM.

When the extended SMRAM space is enabled, processor accesses without SMM attribute or without write-back attribute to the TSEG range are handled as invalid accesses.

Non-processor originated accesses such as PCI Express*, DMI or processor graphics to enabled SMM space are handled as invalid cycle type with reads and writes to location C_0000h and byte enables turned off for writes.

2.5.4 Protected Memory Range (PMR) - (Programmable)

For robust and secure launch of the MVMM, the MVMM code and private data need to be loaded to a memory region protected from bus master accesses. Support for protected memory region is required for DMA-remapping hardware implementations on platforms supporting Intel® TXT, and is optional for non-Intel® TXT platforms. Since the protected memory region needs to be enabled before the MVMM is launched, hardware should support enabling of the protected memory region independently from enabling the DMA-remapping hardware.

As part of the secure launch process, the SINIT-AC module verifies the protected memory regions are properly configured and enabled. Once launched, the MVMM can setup the initial DMA-remapping structures in protected memory (to ensure they are protected while being setup) before enabling the DMA-remapping hardware units.

To optimally support platform configurations supporting varying amounts of main memory, the protected memory region is defined as two non-overlapping regions:

- **Protected Low-memory Region**: This is defined as the protected memory region below 4 GB to hold the MVMM code/private data, and the initial DMA-remapping structures that control DMA to host physical addresses below 4 GB. DMA-

remapping hardware implementations on platforms supporting Intel® TXT are required to support protected low-memory region 5.

- **Protected High-memory Region**: This is defined as a variable sized protected memory region above 4 GB, enough to hold the initial DMA-remapping structures for managing DMA accesses to addresses above 4 GB. DMA-remapping hardware implementations on platforms supporting Intel® TXT are required to support protected high-memory region 6, if the platform supports main memory above 4 GB.

Once the protected low/high memory region registers are configured, bus master protection to these regions is enabled through the Protected Memory Enable register. For platforms with multiple DMA-remapping hardware units, each of the DMA-remapping hardware units should be configured with the same protected memory regions and enabled.

2.5.5 DRAM Protected Range (DPR)

This protection range only applies to DMA accesses and GMADR translations. It serves a purpose of providing a memory range that is only accessible to processor streams. The range just below TSEGMB is protected from DMA accesses.

The DPR range works independently of any other range, including the PMRC checks in Intel VT-d. It occurs post any Intel VT-d translation. Therefore, incoming cycles are checked against this range after the Intel VT-d translation and faulted if they hit this protected range, even if they passed the Intel VT-d translation.

The system will set up:

- 0 to (TSEG_BASE – DPR size – 1) for DMA traffic
- TSEG_BASE to (TSEG_BASE – DPR size) as no DMA.

After some time, software could request more space for not allowing DMA. It will get some more pages and make sure there are no DMA cycles to the new region. DPR size is changed to the new value. When it does this, there should not be any DMA cycles going to DRAM to the new region.

All upstream cycles from 0 to (TSEG_BASE – 1 – DPR size), and not in the legacy holes (VGA), are decoded to DRAM.

2.5.6 Pre-allocated Memory

Voids of physical addresses that are not accessible as general system memory and reside within the system memory address range (< TOLUD) are created for SMM-mode, legacy VGA graphics compatibility, and GFX GTT stolen memory. **It is the responsibility of BIOS to properly initialize these regions**.

2.6 PCI Memory Address Range (TOLUD – 4 GB)

Top of Low Usable DRAM (TOLUD) – TOLUD is restricted to 4 GB memory (1MB granularity), but the System Agent may support up to a much higher capacity, which is limited by DRAM.

This address range from the top of low usable DRAM (TOLUD) to 4 GB is normally mapped to the DMI Interface.

Device 0 exceptions are:

1. Addresses decoded to the egress port registers (PXPEPBAR)
2. Addresses decoded to the memory mapped range for Host Memory Mapped Configuration Space registers (MCHBAR)
3. Addresses decoded to the registers associated with the PCH Serial Interconnect (DMI) register memory range. (DMIBAR)

For each PCI Express* port, there are two exceptions to this rule:

4. Addresses decoded to the PCI Express* Memory Window defined by the MBASE, MLIMIT registers are mapped to PCI Express*.
5. Addresses decoded to the PCI Express* prefetchable Memory Window defined by the PMBASE, PMLIMIT registers are mapped to PCI Express*.

In Processor Graphics configurations, there are exceptions to this rule:

6. Addresses decode to the Processor Graphics translation window (GMADR)
7. Addresses decode to the Processor Graphics translation table or Processor Graphics registers. (GTTMMADR)

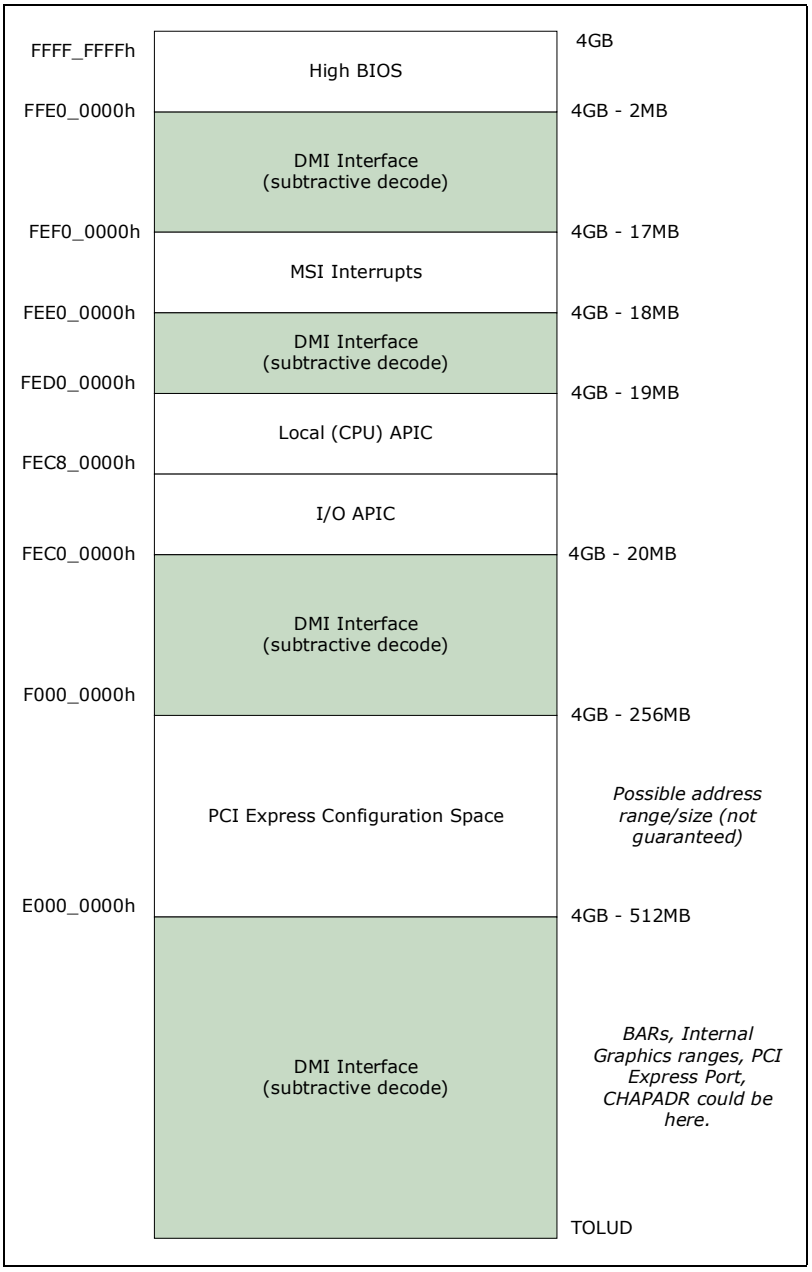
In an Intel VT enable configuration, there are exceptions to this rule:

8. Addresses decoded to the memory mapped window to Graphics Intel® VT remap engine registers (GFXVTBAR)
9. Addresses decoded to the memory mapped window to PEG/DMI VC0 Intel® VT remap engine registers (VTDPVC0BAR)
10. TCm accesses (to Intel ME stolen memory) from PCH do not go through Intel® VT remap engines.

Some of the MMIO Bars may be mapped to this range or to the range above TOUUD.

There are sub-ranges within the PCI memory address range defined as APIC Configuration Space, MSI Interrupt Space, and High BIOS address range. The exceptions listed above for Processor Graphics and the PCI Express* ports ***should NOT overlap with these ranges***.

Figure 2-5. PCI Memory Address Range



2.6.1 APIC Configuration Space (FEC0_0000h – FECF_FFFFh)

This range is reserved for APIC configuration space. The I/O APIC(s) usually reside in the PCH portion of the chipset, but may also exist as stand-alone components like PXH.

The IOAPIC spaces are used to communicate with IOAPIC interrupt controllers that may be populated in the system. Since it is difficult to relocate an interrupt controller using plug-and-play software, fixed address decode regions have been allocated for them. Processor accesses to the default IOAPIC region (FEC0_0000h to FEC7_FFFFh) are always forwarded to DMI.

The processor optionally supports additional I/O APICs behind the PCI Express* "Graphics" port. When enabled using the APIC_BASE and APIC_LIMIT registers (mapped PCI Express* Configuration space offset 240h and 244h), the PCI Express* port(s) will positively decode a subset of the APIC configuration space.

Memory requests to this range would then be forwarded to the PCI Express* port. This mode is intended for the entry Workstation/Server SKU of the PCH, and would be disabled in typical Desktop systems. When disabled, any access within the entire APIC Configuration space (FEC0_0000h to FECF_FFFFh) is forwarded to DMI.

2.6.2 HSEG (FEDA_0000h – FEDB_FFFFh)

This decode range is not supported on this processor platform.

2.6.3 MSI Interrupt Memory Space (FEE0_0000h – FEEF_FFFFh)

Any PCI Express* or DMI device may issue a Memory Write to 0FEEx_xxxxh. This Memory Write cycle does not go to DRAM. The system agent will forward this Memory Write along with the data to the processor as an Interrupt Message Transaction.

2.6.4 High BIOS Area

For security reasons, the processor will positively decode this range to DMI. This positive decode ensures any overlapping ranges will be ignored. This ensures that the boot vector and BIOS execute off the PCH.

The top 2 MB (FFE0_0000h – FFFF_FFFFh) of the PCI Memory Address Range is reserved for System BIOS (High BIOS), extended BIOS for PCI devices, and the A20 alias of the system BIOS.

The processor begins execution from the High BIOS after reset. This region is positively decoded to DMI. The actual address space required for the BIOS is less than 2 MB. However, the minimum processor MTRR range for this region is 2 MB; thus, the full 2 MB should be considered.

2.7 Upper Main Memory Address Space (4 GB to TOUUD)

The maximum main memory size supported is 64 GB total DRAM memory.

A hole between TOLUD and 4 GB occurs when main memory size approaches 4 GB or larger. As a result, TOM and TOUUD registers and REMAPBASE/REMAPLIMIT registers become relevant.

The remap configuration registers exist to remap lost main memory space. The greater than 32-bit remap handling will be handled similar to other MCHs.

Upstream read and write accesses above 39-bit addressing will be treated as invalid cycles by PEG and DMI.

2.7.1 Top of Memory (TOM)

The "Top of Memory" (TOM) register reflects the total amount of populated physical memory. This is NOT necessarily the highest main memory address (holes may exist in main memory address map due to addresses allocated for memory mapped IO above TOM).

The TOM was used to allocate the Intel® Management Engine (Intel® ME) stolen memory. The Intel® ME stolen size register reflects the total amount of physical memory stolen by the Intel® ME. The Intel® ME stolen memory is located at the top of physical memory. The Intel® ME stolen memory base is calculated by subtracting the amount of memory stolen by the Intel® ME from TOM.

2.7.2 Top of Upper Usable DRAM (TOUUD)

The Top of Upper Usable DRAM (TOUUD) register reflects the total amount of addressable DRAM. If remap is disabled, TOUUD will reflect TOM minus Intel® ME stolen size. If remap is enabled, then it will reflect the remap limit. When there is more than 4 GB of DRAM and reclaim is enabled, the reclaim base will be the same as TOM minus Intel® ME stolen memory size to the nearest 1 MB alignment.

2.7.3 Top of Low Usable DRAM (TOLUD)

TOLUD register is restricted to 4 GB memory (A[31:20]), but the processor can support up to 64 GB, limited by DRAM pins. For physical memory greater than 4 GB, the TOLUD register helps identify the address range between the 4 GB boundary and the top of physical memory. This identifies memory that can be directly accessed (including remap address calculation) that is useful for memory access indication and early path indication. TOLUD can be 1 MB aligned.

2.7.4 TSEG_BASE

The “TSEG_BASE” register reflects the total amount of low addressable DRAM, below TOLUD. BIOS will calculate memory size and program this register; thus, the system agent has knowledge of where (TOLUD) – (Gfx stolen) – (Gfx GTT stolen) – (TSEG) is located. I/O blocks use this minus DPR for upstream DRAM decode.

2.7.5 Memory Re-claim Background

The following are examples of Memory Mapped IO devices that are typically located below 4 GB:

- High BIOS
- TSEG
- GFX stolen
- GTT stolen
- XAPIC
- Local APIC
- MSI Interrupts
- Mbase/Mlimit
- Pmbase/PMlimit
- Memory Mapped IO space that supports only 32B addressing

The processor provides the capability to re-claim the physical memory overlapped by the Memory Mapped IO logical address space. The MCH re-maps physical memory from the Top of Low Memory (TOLUD) boundary up to the 4 GB boundary to an equivalent sized logical address range located just below the Intel ME stolen memory.

2.7.6 Indirect Accesses to MCHBAR Registers

Similar to prior chipsets, MCHBAR registers can be indirectly accessed using:

- Direct MCHBAR access decode:
  - — Cycle to memory from processor
  - — Hits MCHBAR base, AND
  - — MCHBAR is enabled, AND
  - — Within MMIO space (above and below 4 GB)
- GTTMMADR (10000h – 13FFFh) range -> MCHBAR decode:
  - — Cycle to memory from processor, AND
  - — Device 2 (Processor Graphics) is enabled, AND
  - — Memory accesses for device 2 is enabled, AND
  - — Targets GFX MMIO Function 0, AND
  - — MCHBAR is enabled or cycle is a read. If MCHBAR is disabled, only read access is allowed.
- MCHTMBAR -> MCHBAR (Thermal Monitor)
  - — Cycle to memory from processor, AND
  - — Targets MCHTMBAR base
- IOBAR -> GTTMMADR -> MCHBAR.
  - — Follows IOBAR rules. Refer GTTMMADR information above as well.

2.7.7 Memory Remapping

An incoming address (referred to as a logical address) is checked to view if it falls in the memory re-map window. The bottom of the re-map window is defined by the value in the REMAPBASE register. The top of the re-map window is defined by the value in the REMAPLIMIT register. An address that falls within this window is re-mapped to the physical memory starting at the address defined by the TOLUD register. The TOLUD register should be 1 MB aligned.

2.7.8 Hardware Remap Algorithm

The following pseudo-code defines the algorithm used to calculate the DRAM address to be used for a logical address above the top of physical memory made available using re-claiming.

```
IF (ADDRESS_IN[38:20] >= REMAP_BASE[35:20]) AND
(ADDRESS_IN[38:20] <= REMAP_LIMIT[35:20]) THEN
    ADDRESS_OUT[38:20] = (ADDRESS_IN[38:20] - REMAP_BASE[35:20]) +
0000000b & TOLUD[31:20]
    ADDRESS_OUT[19:0] = ADDRESS_IN[19:0]
```

2.8 PCI Express* Configuration Address Space

PCIEXBAR is located in Device 0 configuration space. The processor detects memory accesses targeting PCIEXBAR. BIOS should assign this address range such that it will not conflict with any other address ranges.

2.9 Graphics Memory Address Ranges

The integrated memory controller can be programmed to direct memory accesses to the Processor Graphics when addresses are within any of the ranges specified using registers in MCH Device 2 configuration space.

- The Graphics Memory Aperture Base Register (GMADR) is used to access graphics memory allocated using the graphics translation table.
- The Graphics Translation Table Base Register (GTTADR) is used to access the translation table and graphics control registers. This is part of the GTTMMADR register.

These ranges can reside above the Top-of-Low-DRAM and below High BIOS and APIC address ranges. They should reside above the top of memory (TOLUD) and below 4 GB so they do not take any physical DRAM memory space.

Alternatively, these ranges can reside above 4 GB, similar to other BARs that are larger than 32 bits in size.

GMADR is a Prefetchable range in order to apply USWC attribute (from the processor point of view) to that range. The USWC attribute is used by the processor for write combining.

2.9.1 IOBAR Mapped Access to Device 2 MMIO Space

Device 2, Processor Graphics, contains an IOBAR register. If Device 2 is enabled, Processor Graphics registers or the GTT table can be accessed using this IOBAR. The IOBAR is composed of an index register and a data register.

MMIO_Index: MMIO_INDEX is a 32-bit register. A 32-bit (all bytes enabled) I/O write to this port loads the offset of the MMIO register or offset into the GTT that needs to be accessed. An I/O Read returns the current value of this register. I/O read/write accesses less than 32 bits in size (all bytes enabled) will not target this register.

MMIO_Data: MMIO_DATA is a 32-bit register. A 32-bit (all bytes enabled) I/O write to this port is re-directed to the MMIO register pointed to by the MMIO-index register. An I/O read to this port is re-directed to the MMIO register pointed to by the MMIO-index register. I/O read/write accesses less than 32 bits in size (all bytes enabled) will not target this register.

The result of accesses through IOBAR can be:

- Accesses directed to the GTT table. (that is, route to DRAM)
- Accesses to Processor Graphics registers with the device.
- Accesses to Processor Graphics display registers now located within the PCH. (that is, route to DMI).

Note: GTT table space writes (GTTADR) are supported through this mapping mechanism.

This mechanism to access Processor Graphics MMIO registers should NOT be used to access VGA I/O registers that are mapped through the MMIO space. VGA registers should be accessed directly through the dedicated VGA I/O ports.

2.9.2 Trusted Graphics Ranges

Trusted graphics ranges are NOT supported.

2.10 System Management Mode (SMM)

The Core handles all SMM mode transaction routing. The processor does not allow I/O devices access to the CSEG/TSEG/HSEG ranges.

DMI Interface and PCI Express* masters are Not allowed to access the SMM space.

Table 2-4. SMM Regions

SMM Space Enabled	Transaction Address Space	DRAM Space (DRAM)
TSEG (T)	(TOLUD – STOLEN – TSEG) to TOLUD – STOLEN	(TOLUD – STOLEN – TSEG) to TOLUD – STOLEN

2.11 SMM and VGA Access Through GTT TLB

Accesses through GTT TLB address translation SMM DRAM space are not allowed. Writes will be routed to memory address 000C_0000h with byte enables de-asserted and reads will be routed to Memory address 000C_0000h. If a GTT TLB translated address hits VGA space, an error is recorded.

PCI Express* and DMI Interface originated accesses are **never** allowed to access SMM space directly or through the GTT TLB address translation. If a GTT TLB translated address hits enabled SMM DRAM space, an error is recorded.

PCI Express* and DMI Interface write accesses through the GMADR range will not be snooped. Only PCI Express* and DMI assesses to GMADR linear range (defined using fence registers) are supported. PCI Express* and DMI Interface tileY and tileX writes to GMADR are not supported. If, when translated, the resulting physical address is to enable SMM DRAM space, the request will be remapped to address 000C_0000h with de-asserted byte enables.

PCI Express* and DMI Interface read accesses to the GMADR range are not supported. Therefore, there are no address translation concerns. PCI Express* and DMI Interface reads to GMADR will be remapped to address 000C_0000h. The read will complete with UR (unsupported request) completion status.

GTT fetches are always decoded (at fetch time) to ensure fetch is not in SMM (actually, anything above base of TSEG or 640 KB - 1 MB). Thus, the fetches will be invalid and go to address 000C_0000h. This is not specific to PCI Express* or DMI; it also applies to processor or Processor Graphics engines.

2.12 Intel® Management Engine (Intel® ME) Stolen Memory Accesses

There are two ways to validly access Intel® ME stolen memory:

- PCH accesses mapped to VCm will be decoded to ensure only Intel® ME stolen memory is targeted. These VCm accesses will route non-snooped directly to DRAM. This is the means by which the Intel® ME (located within the PCH) is able to access the Intel® ME stolen range.
- The display engine is allowed to access Intel® ME stolen memory as part of Intel® KVM technology flows. Specifically, display-initiated HHP reads (for displaying a Intel® KVM technology frame) and display initiated LP non-snoop writes (for display writing an Intel® KVM technology captured frame) to Intel® ME stolen memory are allowed.

2.13 I/O Address Space

The system agent generates either DMI Interface or PCI Express* bus cycles for all processor I/O accesses that it does not claim. The Configuration Address Register (CONFIG_ADDRESS) and the Configuration Data Register (CONFIG_DATA) are used to generate PCI configuration space access.

The processor allows 64K+3 bytes to be addressed within the I/O space. The upper three locations can be accessed only during I/O address wrap-around.

A set of I/O accesses are consumed by the Processor Graphics device if it is enabled. The mechanisms for Processor Graphics I/O decode and the associated control is explained in following sub-sections.

The I/O accesses are forwarded normally to the DMI Interface bus unless they fall within the PCI Express* I/O address range as defined by the mechanisms explained below. I/O writes are NOT posted. Memory writes to PCH or PCI Express* are posted. The PCI Express* devices have a register that can disable the routing of I/O cycles to the PCI Express* device.

The processor responds to I/O cycles initiated on PCI Express* or DMI with an UR status. Upstream I/O cycles and configuration cycles should never occur. If one does occur, the transaction will complete with an UR completion status.

I/O reads that lie within 8-byte boundaries but cross 4-byte boundaries are issued from the processor as one transaction. The reads will be split into two separate transactions. I/O writes that lie within 8-byte boundaries but cross 4-byte boundaries will be split into two transactions by the processor.

2.13.1 PCI Express* I/O Address Mapping

The processor can be programmed to direct non-memory (I/O) accesses to the PCI Express* bus interface when processor initiated I/O cycle addresses are within the PCI Express* I/O address range. This range is controlled using the I/O Base Address (IOBASE) and I/O Limit Address (IOLIMIT) registers in Device 1 Functions 0, 1, 2 configuration space.

Address decoding for this range is based on the following concept. The top 4 bits of the respective I/O Base and I/O Limit registers correspond to address bits A[15:12] of an I/O address. For the purpose of address decoding, the device assumes that the lower 12 address bits A[11:0] of the I/O base are zero and that address bits A[11:0] of the I/O limit address are FFFh. This forces the I/O address range alignment to a 4 KB boundary and produces a size granularity of 4 KB.

The processor positively decodes I/O accesses to PCI Express* I/O address space as defined by the following equation:

```
I/O_Base_Address ≤ processor I/O Cycle Address ≤ I/O_Limit_Address
```

The effective size of the range is programmed by the plug-and-play configuration software and it depends on the size of I/O space claimed by the PCI Express* device.

The processor also forwards accesses to the Legacy VGA I/O ranges according to the settings in the PEG configuration registers BCTRL (VGA Enable) and PCICMD (IOAE), unless a second adapter (monochrome) is present on the DMI Interface/PCI (or ISA). The presence of a second graphics adapter is determined by the MDAP configuration bit. When MDAP is set to 1, the processor will decode legacy monochrome I/O ranges and forward them to the DMI Interface. The I/O ranges decoded for the monochrome adapter are 3B4h, 3B5h, 3B8h, 3B9h, 3BAh, and 3BFh.

The PEG I/O address range registers defined above are used for all I/O space allocation for any devices requiring such a window on PCI-Express.

The PCICMD register can disable the routing of I/O cycles to PCI Express*.

2.14 Direct Media Interface (DMI) Interface Decode Rules

Note: DMI does not apply to U/Y Processors.

All “SNOOP semantic” PCI Express* transactions are kept coherent with processor caches.

All "Snoop not required semantic" cycles reference the main DRAM address range. PCI Express* non-snoop initiated cycles are not snooped.

The processor accepts accesses from the DMI Interface to the following address ranges:

- All snoop memory read and write accesses to Main DRAM including PAM region (except stolen memory ranges, TSEG, A0000h – BFFFFh space)
- Write accesses to enabled VGA range, MBASE/MLIMIT, and PMBASE/PMLIMIT will be routed as peer cycles to the PCI Express* interface.
- Write accesses above the top of usable DRAM and below 4 GB (not decoding to PCI Express* or GMADR space) will be treated as master aborts.
- Read accesses above the top of usable DRAM and below 4 GB (not decoding to PCI Express*) will be treated as unsupported requests.
- Reads and accesses above the TOUUD will be treated as unsupported requests on VC0.

DMI Interface memory read accesses that fall between TOLUD and 4 GB are considered invalid and will master abort. These invalid read accesses will be reassigned to address 000C_0000h and dispatch to DRAM. Reads will return unsupported request completion. Writes targeting PCI Express* space will be treated as peer-to-peer cycles.

There is a known usage model for peer writes from DMI to PEG. A video capture card can be plugged into the PCH PCI bus. The video capture card can send video capture data (writes) directly into the frame buffer on an external graphics card (writes to the PEG port). As a result, peer writes from DMI to PEG should be supported.

I/O cycles and configuration cycles are not supported in the upstream direction. The result will be an unsupported request completion status.

2.14.1 DMI Accesses to the Processor that Cross Device Boundaries

The processor does not support transactions that cross device boundaries. This should not occur because PCI Express* transactions are not allowed to cross a 4 KB boundary.

For reads, the processor will provide separate completion status for each naturally-aligned 64-byte block or, if chaining is enabled, each 128-byte block. If the starting address of a transaction hits a valid address, the portion of a request that hits that target device (PCI Express* or DRAM) will complete normally.

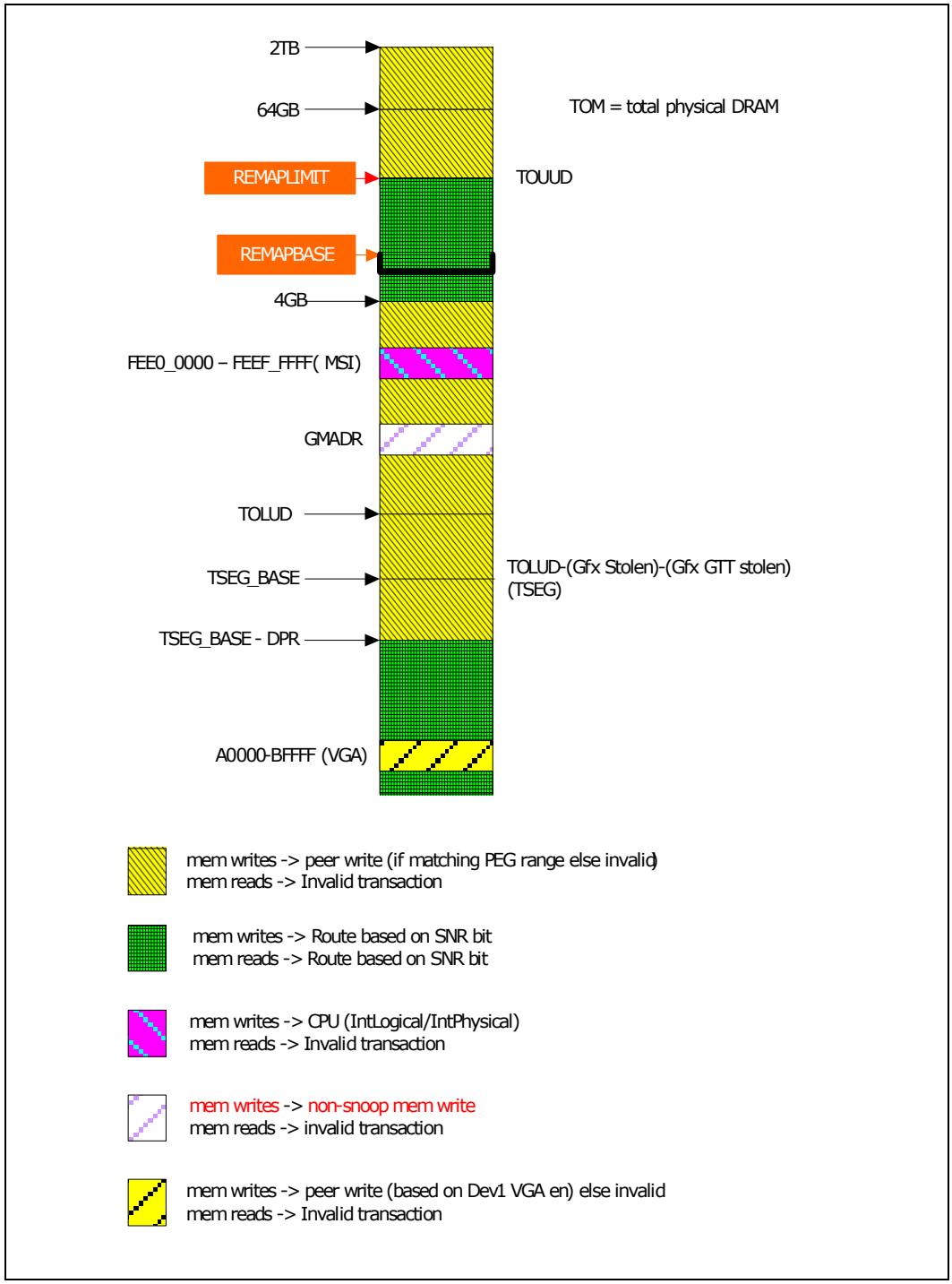
If the starting transaction address hits an invalid address, the entire transaction will be remapped to address 000C_0000h and dispatched to DRAM. A single unsupported request completion will result.

2.14.2 Traffic Class (TC) / Virtual Channel (VC) Mapping Details

- VC0 (enabled by default)
  - — Snoop port and Non-snoop Asynchronous transactions are supported.

  - Internal Graphics GMADR writes can occur. These writes will NOT be snooped regardless of the snoop not required (SNR) bit.
  - Processor Graphics GMADR reads (unsupported).
  - Peer writes can occur. The SNR bit is ignored.
  - MSI can occur. These will route and be sent to the cores as Intlogical/ IntPhysical interrupts regardless of the SNR bit.
  - VLW messages can occur. These will route and be sent to the cores as VLW messages regardless of the SNR bit.
  - MCTP messages can occur. These are routed in a peer fashion.
- VC1 (Optionally enabled)
  - Supports non-snoop transactions only. (Used for isochronous traffic). The PCI Express* Egress port (PXPEPBAR) should also be programmed appropriately.
  - The snoop not required (SNR) bit should be set. Any transaction with the SNR bit not set will be treated as an unsupported request.
  - MSI and peer transactions are treated as unsupported requests.
  - No "pacer" arbitration or TWRR arbitration will occur. Never remaps to different port. (PCH takes care of Egress port remapping). The PCH meters TCm Intel® ME accesses and Intel® High Definition Audio (Intel® HD Audio) TC1 access bandwidth.
  - Processor Graphics GMADR writes and GMADR reads are not supported.
- VCm accesses
  - VCm access only map to Intel® ME stolen DRAM. These transactions carry the direct physical DRAM address (no redirection or remapping of any kind will occur). This is how the PCH Intel® ME accesses its dedicated DRAM stolen space.
  - DMI block will decode these transactions to ensure only Intel® ME stolen memory is targeted, and abort otherwise.
  - VCm transactions will only route non-snoop.
  - VCm transactions will not go through VTd remap tables.
  - The remapbase/remaplimit registers to not apply to VCm transactions.

Figure 2-6. Example: DMI Upstream VC0 Memory Map



2.15 PCI Express* Interface Decode Rules

All "SNOOP semantic" PCI Express* transactions are kept coherent with processor caches. All "Snoop not required semantic" cycles should reference the direct DRAM address range. PCI Express* non-snoop initiated cycles are not snooped. If a "Snoop not required semantic" cycle is outside of the address range mapped to system memory, then it will proceed as follows:

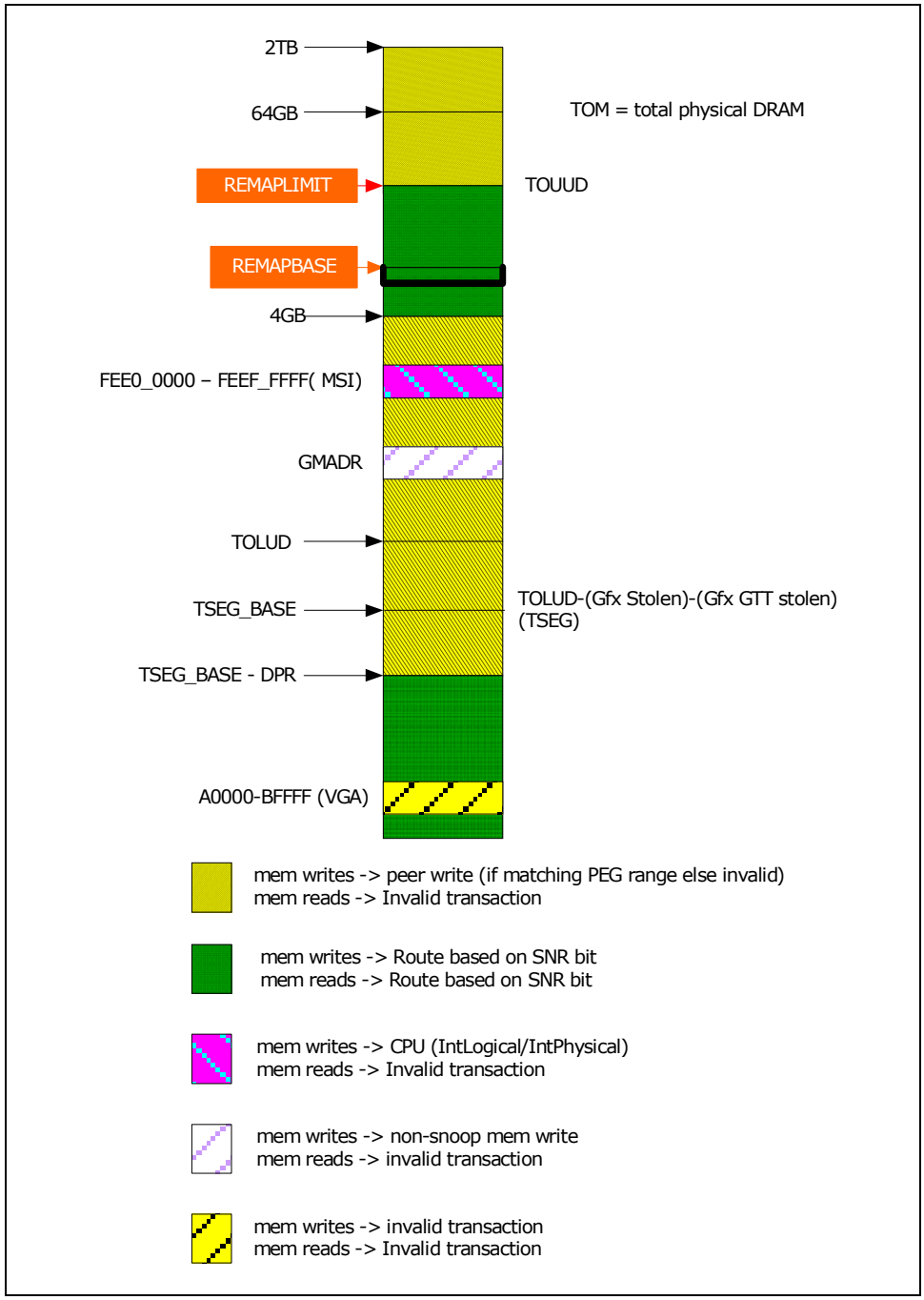
- Reads: Sent to DRAM address 000C_0000h (non-snooped) and will return "unsuccessful completion".
- Writes: Sent to DRAM address 000C_0000h (non-snooped) with byte enables all disabled Peer writes from PEG to DMI are not supported.

If PEG bus master enable is not set, all reads and writes are treated as unsupported requests.

2.15.1 TC/VC Mapping Details

- VC0 (enabled by default)
  - Snoop port and Non-snoop Asynchronous transactions are supported.
  - Processor Graphics GMADR writes can occur. Unlike FSB chipsets, these will NOT be snooped regardless of the snoop not required (SNR) bit.
  - Processor Graphics GMADR reads (unsupported).
  - Peer writes are only supported between PEG ports. PEG to DMI peer write accesses are NOT supported.
  - MSI can occur. These will route to the cores (IntLogical/IntPhysical) regardless of the SNR bit.
- VC1 is not supported.
- VCm is not supported.

Figure 2-7. PEG Upstream VC0 Memory Map



2.16 Legacy VGA and I/O Range Decode Rules

The legacy 128 KB VGA memory range 000A_0000h – 000B_FFFFh can be mapped to Processor Graphics (Device 2), PCI Express* (Device 1 Functions), and/or to the DMI interface depending on the programming of the VGA steering bits. Priority for VGA

mapping is constant in that the processor always decodes internally mapped devices first. Internal to the processor, decode precedence is always given to Processor Graphics. The processor always positively decodes internally mapped devices, namely the Processor Graphics. Subsequent decoding of regions mapped to either PCI Express* port or the DMI Interface depends on the Legacy VGA configurations bits (VGA Enable and MDAP).

For the remainder of this section, PCI Express* can refer to either the device 1 port functions.

VGA range accesses will always be mapped as UC type memory.

Accesses to the VGA memory range are directed to Processor Graphics depend on the configuration. The configuration is specified by:

- Processor Graphics controller in Device 2 is enabled (DEVEN.D2EN bit 4)
- Processor Graphics VGA in Device 0 Function 0 is enabled through register GGC bit 1.
- Processor Graphics's memory accesses (PCICMD2 04h – 05h, MAE bit 1) in Device 2 configuration space are enabled.
- VGA compatibility memory accesses (VGA Miscellaneous Output register – MSR Register, bit 1) are enabled.
- Software sets the proper value for VGA Memory Map Mode register (VGA GR06 Register, bits 3:2). Refer the following table for translations.

Table 2-5. Processor Graphics Frame Buffer Accesses

Memory Access GR06(3:2)	A0000h - AFFFFh	B0000h - B7FFFh MDA	B8000h - BFFFFh
00	Processor Graphics	Processor Graphics	Processor Graphics
01	Processor Graphics	PCI Express* bridge or DMI interface	PCI Express* bridge or DMI interface
10	PCI Express* bridge or DMI interface	Processor Graphics	PCI Express* bridge or DMI interface
11	PCI Express* bridge or DMI interface	PCI Express* bridge or DMI interface	Processor Graphics

Note: Additional qualification within Processor Graphics comprehends internal MDA support. The VGA and MDA enabling bits detailed below control segments not mapped to Processor Graphics.

VGA I/O range is defined as addresses where A[15:0] are in the ranges 03B0h to 03BBh, and 03C0h to 03DFh. VGA I/O accesses are directed to Processor Graphics depends on the following configuration:

- Processor Graphics controller in Device 2 is enabled through register DEVEN.D2EN bit 4.
- Processor Graphics VGA in Device 0 Function 0 is enabled through register GGC bit 1.
- Processor Graphics's I/O accesses (PCICMD2 04 – 05h, IOAE bit 0) in Device 2 are enabled.

- VGA I/O decodes for Processor Graphics uses 16 address bits (15:0) there is no aliasing. This is different when compared to a bridge device (Device 1) that used only 10 address bits (A 9:0) for VGA I/O decode.
- VGA I/O input/output address select (VGA Miscellaneous Output register - MSR Register, bit 0) is used to select mapping of I/O access as defined in the following table.

Table 2-6. Processor Graphics VGA I/O Mapping

I/O Access MSRb0	3CX	3DX	3B0h – 3BBh	3BCh – 3BFh
0	Processor Graphics	PCI Express* bridge or DMI interface	Processor Graphics	PCI Express* bridge or DMI interface
1	Processor Graphics	Processor Graphics	PCI Express* bridge or DMI interface	PCI Express* bridge or DMI interface

Note: Additional qualification within Processor Graphics comprehends internal MDA support. The VGA and MDA enabling bits detailed below control ranges not mapped to Processor Graphics.

For regions mapped outside of the Processor Graphics (or if Processor Graphics is disabled), the legacy VGA memory range A0000h – BFFFFh are mapped to the DMI Interface or PCI Express* depending on the programming of the VGA Enable bit in the BCTRL configuration register in the PEG configuration space, and the MDAPxx bits in the Legacy Access Control (LAC) register in Device 0 configuration space. The same register controls mapping VGA I/O address ranges. The VGA I/O range is defined as addresses where A[9:0] are in the ranges 3B0h to 3BBh and 3C0h to 3DFh (inclusive of ISA address aliases – A[15:10] are not decoded). The function and interaction of these two bits is described below:

VGA Enable: Controls the routing of processor initiated transactions targeting VGA compatible I/O and memory address ranges. When this bit is set, the following processor accesses will be forwarded to the PCI Express*:

- Memory accesses in the range 0A0000h to 0BFFFFh
- I/O addresses where A[9:0] are in the ranges 3B0h to 3BBh and 3C0h to 3DFh (including ISA address aliases – A[15:10] are not decoded)

When this bit is set to a “1”:

- Forwarding of these accesses issued by the processor is independent of the I/O address and memory address ranges defined by the previously defined base and limit registers.
- Forwarding of these accesses is also independent of the settings of the ISA Enable settings if this bit is “1”.
- Accesses to I/O address range x3BCh – x3BFh are forwarded to the DMI Interface.

When this bit is set to a "0":

- Accesses to I/O address range x3BCh – x3BFh are treated like any other I/O accesses; the cycles are forwarded to PCI Express* if the address is within IOBASE and IOLIMIT and ISA enable bit is not set. Otherwise, these accesses are forwarded to the DMI interface.
- VGA compatible memory and I/O range accesses are not forwarded to PCI Express* but rather they are mapped to the DMI Interface, unless they are mapped

to PCI Express* using I/O and memory range registers defined above (IOBASE, IOLIMIT)

The following table shows the behavior for all combinations of MDA and VGA.

Table 2-7. VGA and MDA IO Transaction Mapping

VGA_en	MDAP	Range	Destination	Exceptions / Notes
0	0	VGA, MDA	DMI interface	
0	1	Illegal		Undefined behavior results
1	0	VGA	PCI Express*	
1	1	VGA	PCI Express*	
1	1	MDA	DMI interface	x3BCh – x3BEh will also go to DMI interface

The same registers control mapping of VGA I/O address ranges. The VGA I/O range is defined as addresses where A[9:0] are in the ranges 3B0h to 3BBh and 3C0h to 3DFh (inclusive of ISA address aliases – A[15:10] are not decoded). The function and interaction of these two bits is described below.

MDA Present (MDAP): This bit works with the VGA Enable bit in the BCTRL register of Device 1 to control the routing of processor-initiated transactions targeting MDA compatible I/O and memory address ranges. This bit should not be set when the VGA Enable bit is not set. If the VGA enable bit is set, accesses to I/O address range x3BCh – x3BFh are forwarded to the DMI Interface. If the VGA enable bit is not set, accesses to I/O address range x3BCh – x3BFh are treated just like any other I/O accesses; that is, the cycles are forwarded to PCI Express* if the address is within IOBASE and IOLIMIT and the ISA enable bit is not set; otherwise, the accesses are forwarded to the DMI Interface. MDA resources are defined as the following:

Table 2-8. MDA Resources

Range Type	Address
Memory	0B0000h – 0B7FFFh
I/O	3B4h, 3B5h, 3B8h, 3B9h, 3BAh, 3BFh (Including ISA address aliases, A[15:10] are not used in decode)

Any I/O reference that includes the I/O locations listed above, or their aliases, will be forwarded to the DMI interface even if the reference includes I/O locations not listed above.

For I/O reads that are split into multiple DWord accesses, this decode applies to each DWord independently. For example, a read to x3B3h and x3B4h (quadword read to x3B0h with BE#=E7h) will result in a DWord read from PEG at 3B0h (BE#=Eh), and a DWord read from DMI at 3B4h (BE=7h). Since the processor will not issue I/O writes crossing the DWord boundary, this case does not exist for writes.

Summary of decode priority:

- Processor Graphics VGA, if enabled, gets:
  - 03C0h – 03CFh: always
  - 03B0h – 03BBh: if MSR[0]=0 (MSR is I/O register 03C2h)
  - 03D0h – 03DFh: if MSR[0]=1

Note: 03BCh – 03BFh never decodes to Processor Graphics; 3BCh – 3BEh are parallel port I/Os, and 3BFh is

only used by true MDA devices.

- Else, if MDA Present (if VGA on PEG is enabled), DMI gets:
  - x3B4,5,8,9,A,F (any access with any of these bytes enabled, regardless of the other BEs)
- Else, if VGA on PEG is enabled, PEG gets:
  - x3B0h – x3BBh
  - x3C0h – x3CFh
  - x3D0h – x3DFh
- Else, if ISA Enable=1, DMI gets:
  - upper 768 bytes of each 1K block
- Else, IOBASE/IOLIMIT apply.

2.17 I/O Mapped Registers

The processor contains two registers that reside in the processor I/O address space - the Configuration Address (CONFIG_ADDRESS, port 0xCF8) Register and the Configuration Data (CONFIG_DATA, port 0xCFC) Register. The Configuration Address Register enables/disables the configuration space and determines what portion of configuration space is visible through the Configuration Data window.

§ §

3 Host Bridge and DRAM Controller (D0:F0)

This chapter documents the Host Bridge and DRAM Controller.

Table 3-1. Summary of Host Bridge and DRAM Controller (D0:F0)

Host Bridge/DRAM Registers (D0:F0)
Memory Controller (MCHBAR) Registers
Power Management (MCHBAR) Registers
Host Controller (MCHBAR) Registers
Direct Media Interface BAR (DMIBAR) Registers
REGBAR Registers
PCI Express Egress Port BAR (PXPEPBAR) Registers
VTDPVC0BAR Registers

3.1 Host Bridge/DRAM Registers (D0:F0)

This chapter documents the registers in Bus: 0, Device 0, Function 0.

Note: These registers apply to all processors.

3.1.1 Summary of Registers

Table 3-2. Summary of Bus: 0, Device: 0, Function: 0 Registers

Offset	Size (Bytes)	Register Name (Register Symbol)	Default Value
0h	2	Vendor ID (VID_0_0_0_PCI)	8086h
2h	2	Device ID (DID_0_0_0_PCI)	5A00h
4h	2	PCI Command (PCICMD_0_0_0_PCI)	0006h
6h	2	PCI Status (PCISTS_0_0_0_PCI)	0090h
8h	1	Revision Identification (RID_0_0_0_PCI)	00h
9h	1	Class Code Programming Interface (CC_PI_0_0_0_PCI)	00h
Ah	2	Basic Class Code (CC_BCC_0_0_0_PCI)	0600h
Eh	1	Header Type (HDR_0_0_0_PCI)	00h
2Ch	2	Subsystem Vendor Identification (SVID_0_0_0_PCI)	0000h
2Eh	2	Subsystem Identification (SID_0_0_0_PCI)	0000h
34h	1	Capabilities Pointer (CAPPTR_0_0_0_PCI)	E0h
40h	8	PCI Express Egress Port Base Address (PXPEPBAR_0_0_0_PCI)	0000000000000000h
48h	8	MCHBAR Base Address Register (MCHBAR_0_0_0_PCI)	0000000000000000h
50h	2	Graphics Control (GGC_0_0_0_PCI)	0500h

Offset	Size (Bytes)	Register Name (Register Symbol)	Default Value
54h	4	Device Enable (DEVEN_0_0_0_PCI)	0000F49Fh
58h	4	Protected Audio Video Path Control (PAVPC_0_0_0_PCI)	00000001h
5Ch	4	DMA Protected Range (DPR_0_0_0_PCI)	00000000h
60h	8	PCIEXBAR Base Address Register (PCIEXBAR_0_0_0_PCI)	0000000000000000h
68h	8	DMIBAR Base Address Register (DMIBAR_0_0_0_PCI)	0000000000000000h
80h	1	Programmable Attribute Map 0 (PAM0_0_0_0_PCI)	00h
81h	1	Programmable Attribute Map 1 (PAM1_0_0_0_PCI)	00h
82h	1	Programmable Attribute Map 2 (PAM2_0_0_0_PCI)	00h
83h	1	Programmable Attribute Map 3 (PAM3_0_0_0_PCI)	00h
84h	1	Programmable Attribute Map 4 (PAM4_0_0_0_PCI)	00h
85h	1	Programmable Attribute Map 5 (PAM5_0_0_0_PCI)	00h
86h	1	Programmable Attribute Map 6 (PAM6_0_0_0_PCI)	00h
87h	1	Legacy Access Control (LAC_0_0_0_PCI)	10h
A0h	8	Top of Memory (TOM_0_0_0_PCI)	0000007FFFF00000h
A8h	8	Top of Upper Usable DRAM (TOUUD_0_0_0_PCI)	0000000000000000h
B0h	4	Base Data of Stolen Memory (BDSM_0_0_0_PCI)	00000000h
B4h	4	Base of GTT Stolen Memory (BGSM_0_0_0_PCI)	00100000h
B8h	4	TSEG Memory Base (TSEGMB_0_0_0_PCI)	00000000h
BCh	4	Top of Low Usable DRAM (TOLUD_0_0_0_PCI)	00100000h
C8h	2	Error Status (ERRSTS_0_0_0_PCI)	0000h
CAh	2	Error Command (ERRCMD_0_0_0_PCI)	0000h
CCh	2	SMI DMI Special Cycle (SMICMD_0_0_0_PCI)	0000h
CEh	2	SMI DMI Special Cycle (SCICMD_0_0_0_PCI)	0000h
DCh	4	Scratchpad Data (SKPD_0_0_0_PCI)	00000000h
E4h	4	Capabilities A (CAPID0_A_0_0_0_PCI)	00000000h
E8h	4	Capabilities B (CAPID0_B_0_0_0_PCI)	00000000h
ECh	4	Capabilities C (CAPID0_C_0_0_0_PCI)	00000000h

3.1.2 Vendor ID (VID_0_0_0_PCI) — Offset 0h

This register combined with the Device Identification register uniquely identifies any PCI device.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:0, F:0] + 0h	8086h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
15:0	8086h RO	**Vendor ID (VID):** PCI standard identification for Intel.

3.1.3 Device ID (DID_0_0_0_PCI) — Offset 2h

This register combined with the Vendor Identification register uniquely identifies any PCI device.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:0, F:0] + 2h	5A00h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
15:8	5Ah RO	**Device ID MSB (DID_MSB):** Upper byte of the Device ID.
7:0	00h RO	**Device ID LSB (DID_LSB):** Lower byte of the Device ID.

3.1.4 PCI Command (PCICMD_0_0_0_PCI) — Offset 4h

Since Device #0 does not physically reside on PCI_A many of the bits are not implemented.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:0, F:0] + 4h	0006h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:10	0h RO	**Reserved**
9	0h RO	**Fast Back-To-Back (FB2B):** Fast Back-to-Back Enable: This bit controls whether or not the master can do fast back-to-back write. Since device 0 is strictly a target this bit is not implemented and is hardwired to 0. Writes to this bit position have no effect.
8	0h RW	**SERR Enable (SERRE):** SERR Enable: This bit is a global enable bit for Device 0 SERR messaging. The CPU communicates the SERR condition by sending an SERR message over DMI to the PCH. 1: The CPU is enabled to generate SERR messages over DMI for specific Device 0 error conditions that are individually enabled in the ERRCMD and DMIUEMSK registers. The error status is reported in the ERRSTS, PCISTS, and DMIUEST registers. 0: The SERR message is not generated by the Host for Device 0. This bit only controls SERR messaging for Device 0. Other integrated devices have their own SERRE bits to control error reporting for error conditions occurring in each device. The control bits are used in a logical OR manner to enable the SERR DMI message mechanism. OPI N/A
7	0h RO	**Parity Error Enable (ADSTEP):** Address/Data Stepping Enable: Address/data stepping is not implemented in the CPU, and this bit is hardwired to 0. Writes to this bit position have no effect.
6	0h RW	**Parity Error Enable (PERRE):** OPI - N/A Parity Error Enable: Controls whether or not the Master Data Parity Error bit in the PCI Status register can bet set. 0: Master Data Parity Error bit in PCI Status register can NOT be set. 1: Master Data Parity Error bit in PCI Status register CAN be set.
5	0h RO	**Video Palette Snooping (VGASNOOP):** VGA Palette Snoop Enable: The CPU does not implement this bit and it is hardwired to a 0. Writes to this bit position have no effect.
4	0h RO	**Memory Write and Invalidate Enable (MWIE):** Memory Write and Invalidate Enable: The CPU will never issue memory write and invalidate commands. This bit is therefore hardwired to 0. Writes to this bit position will have no effect.
3	0h RO	**Special Cycle Enable (SCE):** Special Cycle Enable: The CPU does not implement this bit and it is hardwired to a 0. Writes to this bit position have no effect.
2	1h RO	**Bus Master Enable (BME):** Bus Master Enable: The CPU is always enabled as a master on the backbone. This bit is hardwired to a 1. Writes to this bit position have no effect.
1	1h RO	**Memory Access Enable (MAE):** Memory Access Enable: The CPU always allows access to main memory, except when such access would violate security principles. Such exceptions are outside the scope of PCI control. This bit is not implemented and is hardwired to 1. Writes to this bit position have no effect.

Bit Range	Default & Access	Field Name (ID): Description
0	0h RO	**I/O Access Enable (IOAE):** I/O Access Enable: This bit is not implemented in the CPU and is hardwired to a 0. Writes to this bit position have no effect.

3.1.5 PCI Status (PCISTS_0_0_0_PCI) — Offset 6h

This status register reports the occurrence of error events on Device 0s PCI interface. Since Device 0 does not physically reside on PCI_A many of the bits are not implemented.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:0, F:0] + 6h	0090h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15	0h RW/1C/V	**DPE:** Detected Parity Error: This bit is set when this Device receives a Poisoned TLP.
14	0h RW/1C/V	**SSE:** Signaled System Error: This bit is set to 1 when Device 0 generates an SERR message over DMI for any enabled Device 0 error condition. Device 0 error conditions are enabled in the PCICMD, ERRCMD, and DMIUEMSK registers. Device 0 error flags are read/reset from the PCISTS, ERRSTS, or DMIUEST registers. Software clears this bit by writing a 1 to it.
13	0h RW/1C/V	**RMAS:** Received Master Abort Status: This bit is set when the CPU generates a DMI request that receives an Unsupported Request completion packet. Software clears this bit by writing a 1 to it.
12	0h RW/1C/V	**RTAS:** Received Target Abort Status: This bit is set when the CPU generates a DMI request that receives a Completer Abort completion packet. Software clears this bit by writing a 1 to it.
11	0h RO	**STAS:** Signaled Target Abort Status: The CPU will not generate a Target Abort DMI completion packet or Special Cycle. This bit is not implemented and is hardwired to a 0. Writes to this bit position have no effect.
10:9	0h RO	**DEVT:** DEVSEL Timing: These bits are hardwired to 00. Writes to these bit positions have no affect. Device 0 does not physically connect to PCI_A. These bits are set to 00 (fast decode) so that optimum DEVSEL timing for PCI_A is not limited by the Host.
8	0h RW/1C/V	**Master Data Parity Error Detected (DPD):** Master Data Parity Error Detected: This bit is set when DMI received a Poisoned completion from PCH. This bit can only be set when the Parity Error Enable bit in the PCI Command register is set.
7	1h RO	**Fast Back-To-Back (FB2B):** This bit is hardwired to 1. Writes to these bit positions have no effect. Device 0 does not physically connect to PCI_A. This bit is set to 1 (indicating fast back-to-back capability) so that the optimum setting for PCI_A is not limited by the Host.

Bit Range	Default & Access	Field Name (ID): Description
6	0h RO	**Reserved**
5	0h RO	**66MHz PCI Capable (MC66):** Hardwired to 0.
4	1h RO	**Capability List (CLIST):** Capability List: This bit is hardwired to 1 to indicate to the configuration software that this device/function implements a list of new capabilities. A list of new capabilities is accessed via register CAPPTR at configuration address offset 34h. Register CAPPTR contains an offset pointing to the start address within configuration space of this device where the Capability Identification register resides.
3:0	0h RO	**Reserved**

3.1.6 Revision Identification (RID_0_0_0_PCI) — Offset 8h

This register contains the revision number of Device #0.

These bits are read only and writes to this register have no effect.

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:0, F:0] + 8h	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:4	0h RO	**Revision ID MSB (RID_MSB):** Four upper bits of the Revision ID
3:0	0h RO	**Revision ID (RID):** Four lower bits of the Revision ID

3.1.7 Class Code Programming Interface (CC_PI_0_0_0_PCI) — Offset 9h

This register (split from original CC) identifies a register-specific programming interface.

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:0, F:0] + 9h	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:0	00h RO	**PI:** Programming Interface: This is an 8-bit value that indicates the programming interface of this device. This value does not specify a particular register set layout and provides no practical use for this device.

3.1.8 Basic Class Code (CC_BCC_0_0_0_PCI) — Offset Ah

This register (split from original CC) identifies the basic function of the device and a more specific sub-class.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:0, F:0] + Ah	0600h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
15:8	06h RO	**BCC:** Base Class Code: This is an 8-bit value that indicates the base class code for the Host Bridge device. This code has the value 06h, indicating a Bridge device.
7:0	00h RO	**SUBCC:** Sub-Class Code: This is an 8-bit value that indicates the category of Bridge into which the Host Bridge device falls. The code is 00h indicating a Host Bridge.

3.1.9 Header Type (HDR_0_0_0_PCI) — Offset Eh

This register identifies the header layout of the configuration space. No physical register exists at this location.

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:0, F:0] + Eh	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:0	00h RO	**HDR:** PCI Header: This field always returns 0 to indicate that the Host Bridge is a single function device with standard header layout. Reads and writes to this location have no effect.

3.1.10 Subsystem Vendor Identification (SVID_0_0_0_PCI) — Offset 2Ch

This value is used to identify the vendor of the subsystem.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:0, F:0] + 2Ch	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:0	0000h RW/L	**SUBVID:** Subsystem Vendor ID: This field should be programmed during boot-up to indicate the vendor of the system board. After it has been written once, it becomes read only. **Locked by:** TLDMIREGS.WO_STATUS0_0_0_0_DMIBAR.SUBVIDWOS

3.1.11 Subsystem Identification (SID_0_0_0_PCI) — Offset 2Eh

This value is used to identify a particular subsystem.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:0, F:0] + 2Eh	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:0	0000h RW/L	**SUBID:** Subsystem ID: This field should be programmed during BIOS initialization. After it has been written once, it becomes read only. **Locked by:** TLDMIREGS.WO_STATUS0_0_0_0_DMIBAR.SUBIDWOS

3.1.12 Capabilities Pointer (CAPPTR_0_0_0_PCI) — Offset 34h

The CAPPTR provides the offset that is the pointer to the location of the first device capability in the capability list.

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:0, F:0] + 34h	E0h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:0	E0h RO	**CAPPTR:** Capabilities Pointer: Pointer to the offset of the first capability ID register block. In this case the first capability is the product-specific Capability Identifier (CAPID0).

3.1.13 PCI Express Egress Port Base Address (PXPEPBAR_0_0_0_PCI) — Offset 40h

This is the base address for the PCI Express Egress Port MMIO Configuration space. There is no physical memory within this 4KB window that can be addressed. The 4KB reserved by this register does not alias to any PCI 2.3 compliant memory mapped space. On reset, the EGRESS port MMIO configuration space is disabled and must be enabled by writing a 1 to PXPEPBAREN [Dev 0, offset 40h, bit 0].

All the bits in this register are locked in Intel TXT mode.

Type	Size	Offset	Default
PCI	64 bit	[B:0, D:0, F:0] + 40h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:12	0000000h RW	**PXPEPBAR:** This field corresponds to bits 38 to 12 of the base address PCI Express Egress Port MMIO configuration space. BIOS will program this register resulting in a base address for a 4KB block of contiguous memory address space. This register ensures that a naturally aligned 4KB space is allocated within the first 512GB of addressable memory space. System Software uses this base address to program the PCI Express Egress Port MMIO register set. All the bits in this register are locked in Intel TXT mode.
11:1	0h RO	**Reserved**
0	0h RW	**PXPEPBAR Enable (PXPEPBAREN):** 0: PXPEPBAR is disabled and does not claim any memory 1: PXPEPBAR memory mapped accesses are claimed and decoded appropriately This register is locked by Intel TXT.

3.1.14 MCHBAR Base Address Register (MCHBAR_0_0_0_PCI) — Offset 48h

This is the base address for the Host Memory Mapped Configuration space.

There is no physical memory within this 32KB window that can be addressed.

The 32KB reserved by this register does not alias to any PCI 2.3 compliant memory mapped space.

On reset, the Host MMIO Memory Mapped Configuration space is disabled and must be enabled by writing a 1 to MCHBAREN [Dev 0, offset48h, bit 0].

All the bits in this register are locked in Intel TXT mode.

The register space contains memory control, initialization, timing, buffer strength registers, clocking registers and power and thermal management registers.

Type	Size	Offset	Default
PCI	64 bit	[B:0, D:0, F:0] + 48h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:16	000000h RW	**MCHBAR:** This field corresponds to bits 38 to 16 of the base address Host Memory Mapped configuration space. BIOS will program this register resulting in a base address for a 64KB block of contiguous memory address space. This register ensures that a naturally aligned 64KB space is allocated within the first 512GB of addressable memory space. System Software uses this base address to program the Host Memory Mapped register set. All the bits in this register are locked in Intel TXT mode.
15:1	0h RO	**Reserved**
0	0h RW	**MCHBAREN:** 0: MCHBAR is disabled and does not claim any memory 1: MCHBAR memory mapped accesses are claimed and decoded appropriately This register is locked in Intel TXT mode.

3.1.15 Graphics Control (GGC_0_0_0_PCI) — Offset 50h

All the bits in this register are Intel TXT lockable.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:0, F:0] + 50h	0500h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
15:8	05h RW/L	**GMS:** This field is used to select the amount of Main Memory that is pre-allocated to support the Internal Graphics device in VGA (non-linear) and Native (linear) modes. The BIOS ensures that memory is pre-allocated only when Internal graphics is enabled. This register is also Intel TXT lockable. Hardware does not clear or set any of these bits automatically based on IGD being disabled/enabled. BIOS Requirement: BIOS must not set this field to 0h if IVD (bit 1 of this register) is 0. **Locked by:** GGC_0_0_0_PCI.GGCLCK

Bit Range	Default & Access	Field Name (ID): Description
7:6	0h RW/L	**GGMS:** This field is used to select the amount of Main Memory that is pre-allocated to support the Internal Graphics Translation Table. The BIOS ensures that memory is pre-allocated only when Internal graphics is enabled. GSM is assumed to be a contiguous physical DRAM space with DSM, and BIOS needs to allocate a contiguous memory chunk. Hardware will derive the base of GSM from DSM only using the GSM size programmed in the register. Hardware functionality in case of programming this value to Reserved is not guaranteed. **Locked by:** GGC_0_0_0_PCI.GGCLCK
5:3	0h RO	**Reserved**
2	0h RW/L	**VAMEN:** Enables the use of the iGFX engines for Versatile Acceleration. 1 - iGFX engines are in Versatile Acceleration Mode. Device 2 Class Code is 048000h. 0 - iGFX engines are in iGFX Mode. Device 2 Class Code is 030000h. **Locked by:** GGC_0_0_0_PCI.GGCLCK
1	0h RW/L	**IVD:** 0: Enable. Device 2 (IGD) claims VGA memory and IO cycles, the Sub-Class Code within Device 2 Class Code register is 00. 1: Disable. Device 2 (IGD) does not claim VGA cycles (Memory and IO), and the Sub-Class Code field within Device 2 function 0 Class Code register is 80. BIOS Requirement: BIOS must not set this bit to 0 if the GMS field (bits 7:3 of this register) pre-allocates no memory. **Locked by:** GGC_0_0_0_PCI.GGCLCK
0	0h RW/L	**GGCLCK:** When set to 1b, this bit will lock all bits in this register. **Locked by:** GGC_0_0_0_PCI.GGCLCK

3.1.16 Device Enable (DEVEN_0_0_0_PCI) — Offset 54h

Allows for enabling/disabling of PCI devices and functions that are within the CPU package. The table below the bit definitions describes the behavior of all combinations of transactions to devices controlled by this register. All the bits in this register are Intel TXT Lockable.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:0, F:0] + 54h	0000F49Fh

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:16	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
15	1h RW/L	**D8EN:** 0: Bus 0 Device 8 is disabled and not visible. 1: Bus 0 Device 8 is enabled and visible. This bit will be set to 0b and remain 0b if Device 8 capability is disabled. **Locked by:** CAPID0_B_0_0_0_PCI.GMM_DIS
14	1h RW/L	**D14F0EN:** VMD Enable - 0: Bus 0 Device 14 Function 0 is disabled and hidden. 1: Bus 0 Device 14 Function 0 is enabled and visible. **Locked by:** CAPID0_B_0_0_0_PCI.VMD_DIS
13	1h RW/L	**D6EN:** 0: Bus 0 Device 6 Function 0 is disabled and not visible. 1: Bus 0 Device 6 Function 0 is enabled and visible. This bit will be set to 0b and remain 0b if Device 6 Function 0 capability is disabled. **Locked by:** CAPID0_A_0_0_0_PCI.PEG60D
12	1h RW/L	**D9EN:** 0: Bus 0 Device 9 is disabled and not visible. 1: Bus 0 Device 9 is enabled and visible. This bit will be set to 0b and remain 0b if Device 9 capability is disabled. **Locked by:** CAPID0_B_0_0_0_PCI.NPK_DIS
11	0h RO	**Reserved**
10	1h RW/L	**D5EN:** 0: Bus 0 Device 5 is disabled and not visible. 1: Bus 0 Device 5 is enabled and visible. This bit will be set to 0b and remain 0b if Device 5 capability is disabled. **Locked by:** CAPID0_B_0_0_0_PCI.IMGU_DIS
9:8	0h RO	**Reserved**
7	1h RW/L	**D4EN:** 0: Bus 0 Device 4 is disabled and not visible. 1: Bus 0 Device 4 is enabled and visible. This bit will be set to 0b and remain 0b if Device 4 capability is disabled. **Locked by:** CAPID0_A_0_0_0_PCI.CDD
6:5	0h RO	**Reserved**
4	1h RW/L	**D2EN:** 0: Bus 0 Device 2 is disabled and hidden 1: Bus 0 Device 2 is enabled and visible This bit will be set to 0b and remain 0b if Device 2 capability is disabled. **Locked by:** CAPID0_A_0_0_0_PCI.IGD
3	1h RW/L	**D1F0EN:** 0: Bus 0 Device 1 Function 0 is disabled and hidden. 1: Bus 0 Device 1 Function 0 is enabled and visible. This bit will be set to 0b and remain 0b if PEG10 capability is disabled. **Locked by:** CAPID0_A_0_0_0_PCI.PEG10D
2	1h RW/L	**D1F1EN:** 0: Bus 0 Device 1 Function 1 is disabled and hidden. 1: Bus 0 Device 1 Function 1 is enabled and visible. **Locked by:** CAPID0_A_0_0_0_PCI.PEG11D

Bit Range	Default & Access	Field Name (ID): Description
1	1h RW/L	**D1F2EN:** 0: Bus 0 Device 1 Function 2 is disabled and hidden. 1: Bus 0 Device 1 Function 2 is enabled and visible. **Locked by:** CAPID0_A_0_0_0_PCI.PEG12D
0	1h RO	**D0EN:** Bus 0 Device 0 Function 0 may not be disabled and is therefore hardwired to 1.

3.1.17 Protected Audio Video Path Control (PAVPC_0_0_0_PCI) — Offset 58h

All the bits in this register are locked by Intel TXT. When locked the R/W bits are RO.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:0, F:0] + 58h	00000001h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:20	000h RW/L	**PCMBASE:** Sizes supported: 1M, 2M, 4M and 8M. Base value programmed (from Top of Stolen Memory) itself defines the size of the WOPCM. Separate WOPCM size programming is redundant information and not required. Default 1M size programming. 4M recommended. This register is locked (becomes read-only) when PAVPE = 1b. **Locked by:** PAVPC_0_0_0_PCI.PAVPLCK
19:7	0h RO	**Reserved**
6	0h RW/L	**ASMFEN:** ASMF method enabled 0b Disabled (default). 1b Enabled. This register is locked when PAVPLCK is set. **Locked by:** PAVPC_0_0_0_PCI.PAVPLCK
5	0h RO	**Reserved**
4	0h RW/L	**OVTATTACK:** Override of Unsolicited Connection State Attack and Terminate. 0: Disable Override. Attack Terminate allowed. 1: Enable Override. Attack Terminate disallowed. This register bit is locked when PAVPE is set. **Locked by:** PAVPC_0_0_0_PCI.PAVPLCK

Bit Range	Default & Access	Field Name (ID): Description
3	0h RW/L	**HVYMODSEL:** This bit is applicable only for PAVP2 operation mode or for PAVP3 mode only if the per-App memory configuration is disabled. 0: Lite Mode (Non-Serpent mode) 1: Serpent Mode For PAVP3 mode, this one type boot time programming has been replaced by per-App programming (through the Media Crypto Copy command). Note that PAVP2 or PAVP3 mode selection is done by programming bit 8 of the MFX_MODE - Video Mode register. **Locked by:** PAVPC_0_0_0_PCI.PAVPLCK
2	0h RW/L	**PAVP Lock (PAVPLCK):** This bit locks all writable contents in this register when set (including itself). Only a hardware reset can unlock the register again. This lock bit needs to be set only if PAVP is enabled (bit 1 of this register is asserted). **Locked by:** PAVPC_0_0_0_PCI.PAVPLCK
1	0h RW/L	**PAVPE:** 0: PAVP functionality is disabled. 1: PAVP functionality is enabled. This register is locked when PAVPLCK is set. **Locked by:** PAVPC_0_0_0_PCI.PAVPLCK
0	1h RW/L	**PCME:** This field enables Protected Content Memory within Graphics Stolen Memory. This memory is the same as the WOPCM area, whose size is defined by bit 5 of this register. This register is locked when PAVPLOCK is set. A value of 0 in this field indicates that Protected Content Memory is disabled, and cannot be programmed in this manner when PAVP is enabled. A value of 1 in this field indicates that Protected Content Memory is enabled, and is the only programming option available when PAVP is enabled. For non-PAVP3 Mode, even for Lite mode configuration, this bit should be programmed to 1 and HVYMODESEL = 0). This bit should always be programmed to 1 if bits 1 and 2 (PAVPE and PAVP lock bits) are both set. With per-application Memory configuration support, the range check for the WOPCM memory area should always happen when this bit is set, regardless of Lite mode, Serpent mode, PAVP2 or PAVP3 mode programming. **Locked by:** PAVPC_0_0_0_PCI.PAVPLCK

3.1.18 DMA Protected Range (DPR_0_0_0_PCI) — Offset 5Ch

DMA protected range register.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:0, F:0] + 5Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:20	000h RW/V/L	**TOPOFDPR:** Top address + 1 of DPR. This is the base of TSEG. Bits 19:0 of the BASE reported here are 0x0_0000.
19:12	0h RO	**Reserved**
11:4	00h RW/L	**DPRSIZE:** This is the size of memory, in MB, that will be protected from DMA accesses. A value of 0x00 in this field means no additional memory is protected. The maximum amount of memory that will be protected is 255 MB. The amount of memory reported in this field will be protected from all DMA accesses, including translated CPU accesses and graphics. The top of the protected range is the BASE of TSEG -1. Note: If TSEG is not enabled, then the top of this range becomes the base of stolen graphics, or ME stolen space or TOLUD, whichever would have been the location of TSEG, assuming it had been enabled. The DPR range works independently of any other range, including the NoDMA.TABLE protection or the PMRC checks in VTd, and is done post any VTd translation or Intel TXT NoDMA lookup. Therefore incoming cycles are checked against this range after the VTd translation and faulted if they hit this protected range, even if they passed the VTd translation or were clean in the NoDMA lookup. All the memory checks are ORed with respect to NOT being allowed to go to memory. So if either PMRC, DPR, NoDMA table lookup, NoDMA.TABLE.PROTECT OR a VTd translation disallows the cycle, then the cycle is not allowed to go to memory. Or in other words, all the above checks must pass before a cycle is allowed to DRAM. **Locked by:** DPR_0_0_0_PCI.LOCK
3	0h RO	**Reserved**
2	0h RW/L	**EPM:** This field controls DMA accesses to the DMA Protected Range (DPR) region. 0: DPR is disabled 1: DPR is enabled. All DMA requests accessing DPR region are blocked. HW reports the status of DPR enable/disable through the PRS field in this register. When this bit change, one must have to wait till the status (PRS) has updated before changing it again. **Locked by:** DPR_0_0_0_PCI.LOCK
1	0h RW/V/L	**PRS:** This field indicates the status of DPR. 0: DPR protection disabled 1: DPR protection enabled
0	0h RW/L	**LOCK:** All bits which may be updated by SW in this register are locked down when this bit is set. **Locked by:** DPR_0_0_0_PCI.LOCK

3.1.19 PCIEXBAR Base Address Register (PCIEXBAR_0_0_0_PCI) — Offset 60h

Defines the PCIEXBAR base address.

Type	Size	Offset	Default
PCI	64 bit	[B:0, D:0, F:0] + 60h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:31	00h RW	**PCIEXBAR:** This field corresponds to bits 38 to 32 of the base address for PCI Express enhanced configuration space including bus segments. BIOS will program this register resulting in a base address for a contiguous memory address space. The size of the range is defined by bits [3:1] of this register. This Base address shall be assigned on a boundary consistent with the number of buses (defined by the Length field in this register) above TOLUD and still within the 39-bit addressable memory space. The address bits decoded depend on the length of the region defined by this register. The address used to access the PCI Express configuration space for a specific device can be determined as follows: PCI Express Base Address +Segment Number*256MB+ Bus Number * 1MB + Device Number * 32KB + Function Number * 4KB This address is the beginning of the 4KB space that contains both the PCI compatible configuration space and the PCI Express extended configuration space.
30	0h RW/V	**ADMSK1024:** This bit is either part of the PCI Express Base Address (R/W) or part of the Address Mask (RO, read 0b), depending on the value of bits [3:1] in this register.
29	0h RW/V	**ADMSK512:** This bit is either part of the PCI Express Base Address (R/W) or part of the Address Mask (RO, read 0b), depending on the value of bits [3:1] in this register.
28	0h RW/V	**ADMSK256:** This bit is either part of the PCI Express Base Address (R/W) or part of the Address Mask (RO, read 0b), depending on the value of bits [3:1] in this register.
27	0h RW/V	**ADMSK128:** This bit is either part of the PCI Express Base Address (R/W) or part of the Address Mask (RO, read 0b), depending on the value of bits [3:1] in this register.
26	0h RW/V	**ADMSK64:** This bit is either part of the PCI Express Base Address (R/W) or part of the Address Mask (RO, read 0b), depending on the value of bits [3:1] in this register.
25:4	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
3:1	0h RW	**LENGTH:** This field describes the length of this region. 000: 256MB (buses 0-255). Bits 38:28 are decoded in the PCI Express Base Address Field. 001: 128MB (buses 0-127). Bits 38:27 are decoded in the PCI Express Base Address Field. 010: 64MB (buses 0-63). Bits 38:26 are decoded in the PCI Express Base Address Field. 011: 512MB (buses 0-512). Bits 38:29 are decoded in the PCI Express Base Address Field. 100: 1024MB (buses 0-1024). Bits 38:30 are decoded in the PCI Express Base Address Field. 101: 2048MB (buses 0-2048). Bits 38:31 are decoded in the PCI Express Base Address Field. 110: 4096MB (buses 0-4096). Bits 38:32 are decoded in the PCI Express Base Address Field. 111:Rreserved.
0	0h RW	**PCIEXBAREN:** PCIEX BAR Enable

3.1.20 DMIBAR Base Address Register (DMIBAR_0_0_0_PCI) — Offset 68h

This is the base address for the Root Complex configuration space. This window of addresses contains the Root Complex Register set for the PCI Express Hierarchy associated with the Host Bridge. There is no physical memory within this 4KB window that can be addressed. The 4KB reserved by this register does not alias to any PCI 2.3 compliant memory mapped space. On reset, the Root Complex configuration space is disabled and must be enabled by writing a 1 to DMIBAREN [Dev 0, offset 68h, bit 0] All the bits in this register are locked in Intel TXT mode.

Type	Size	Offset	Default
PCI	64 bit	[B:0, D:0, F:0] + 68h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:12	0000000h RW	**DMIBAR:** This field corresponds to bits 38 to 12 of the base address DMI configuration space. BIOS will program this register resulting in a base address for a 4KB block of contiguous memory address space. This register ensures that a naturally aligned 4KB space is allocated within the first 512GB of addressable memory space. System Software uses this base address to program the DMI register set. All the Bits in this register are locked in Intel TXT mode.
11:1	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
0	0h RW	**DMIBAREN:** 0: DMIBAR is disabled and does not claim any memory 1: DMIBAR memory mapped accesses are claimed and decoded appropriately This register is locked by Intel TXT.

3.1.21 Programmable Attribute Map 0 (PAM0_0_0_0_PCI) — Offset 80h

This register controls the read, write and shadowing attributes of the BIOS range from F_0000h to F_FFFFh. The Uncore allows programmable memory attributes on 13 legacy memory segments of various sizes in the 768KB to 1MB address range. Seven Programmable Attribute Map (PAM) registers are used to support these features. Cache-ability of these areas is controlled via the MTRR register in the core.

Two bits are used to specify memory attributes for each memory segment. These bits apply to host accesses to the PAM areas. These attributes are:

RE - Read Enable. When RE=1, the host read accesses to the corresponding memory segment are claimed by the Uncore and directed to main memory. Conversely, when RE=0, the host read accesses are directed to DMI.

WE - Write Enable. When WE=1, the host write accesses to the corresponding memory segment are claimed by the Uncore and directed to main memory. Conversely, when WE=0, the host read accesses are directed to DMI.

The RE and WE attributes permit a memory segment to be Read Only, Write Only, Read/Write or Disabled. For example, if a memory segment has RE=1 and WE=0, the segment is Read Only.

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:0, F:0] + 80h	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	RW

Bit Range	Default & Access	Field Name (ID): Description
7:6	0h RO	**Reserved**
5:4	0h RW/L	**HIENABLE:** This field controls the steering of read and write cycles that address the BIOS area from 0F_0000h to 0F_FFFFh. 00: DRAM Disabled. All accesses are directed to DMI. 01: Read Only. All reads are sent to DRAM, all writes are forwarded to DMI. 10: Write Only. All writes are sent to DRAM, all reads are serviced by DMI. 11: Normal DRAM Operation. All reads and writes are serviced by DRAM. **Locked by:** PAM0_0_0_0_PCI.LOCK
3:1	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
0	0h RW/L	**LOCK:** If this bit is set, all of the PAM* registers are locked (cannot be written) **Locked by:** PAM0_0_0_PCI.LOCK

3.1.22 Programmable Attribute Map 1 (PAM1_0_0_0_PCI) — Offset 81h

This register controls the read, write and shadowing attributes of the BIOS range from C_0000h to C_7FFFh. The Uncore allows programmable memory attributes on 13 legacy memory segments of various sizes in the 768KB to 1MB address range. Seven Programmable Attribute Map (PAM) registers are used to support these features. Cache-ability of these areas is controlled via the MTRR register in the core.

Two bits are used to specify memory attributes for each memory segment. These bits apply to host accesses to the PAM areas. These attributes are:

RE - Read Enable. When RE=1, the host read accesses to the corresponding memory segment are claimed by the Uncore and directed to main memory. Conversely, when RE=0, the host read accesses are directed to DMI.

WE - Write Enable. When WE=1, the host write accesses to the corresponding memory segment are claimed by the Uncore and directed to main memory. Conversely, when WE=0, the host read accesses are directed to DMI.

The RE and WE attributes permit a memory segment to be Read Only, Write Only, Read/Write or Disabled. For example, if a memory segment has RE=1 and WE=0, the segment is Read Only.

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:0, F:0] + 81h	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	RW

Bit Range	Default & Access	Field Name (ID): Description
7:6	0h RO	**Reserved**
5:4	0h RW/L	**HIENABLE:** This field controls the steering of read and write cycles that address the BIOS area from 0C_4000h to 0C_7FFFh. 00: DRAM Disabled. All accesses are directed to DMI. 01: Read Only. All reads are sent to DRAM, all writes are forwarded to DMI. 10: Write Only. All writes are sent to DRAM, all reads are serviced by DMI. 11: Normal DRAM Operation. All reads and writes are serviced by DRAM. **Locked by:** PAM0_0_0_PCI.LOCK
3:2	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
1:0	0h RW/L	**LOENABLE:** This field controls the steering of read and write cycles that address the BIOS area from 0C0000h to 0C3FFFh. 00: DRAM Disabled. All reads are sent to DRAM. All writes are forwarded to DMI. 01: Read Only. All reads are sent to DRAM. All writes are forwarded to DMI. 10: Write Only. All writes are sent to DRAM. All reads are serviced by DMI. 11: Normal DRAM Operation. All reads and writes are serviced by DRAM. **Locked by:** PAM0_0_0_0_PCI.LOCK

3.1.23 Programmable Attribute Map 2 (PAM2_0_0_0_PCI) — Offset 82h

This register controls the read, write and shadowing attributes of the BIOS range from C_8000h to C_FFFFh. The Uncore allows programmable memory attributes on 13 legacy memory segments of various sizes in the 768KB to 1MB address range. Seven Programmable Attribute Map (PAM) registers are used to support these features. Cache-ability of these areas is controlled via the MTRR register in the core.

Two bits are used to specify memory attributes for each memory segment. These bits apply to host accesses to the PAM areas. These attributes are:

RE - Read Enable. When RE=1, the host read accesses to the corresponding memory segment are claimed by the Uncore and directed to main memory. Conversely, when RE=0, the host read accesses are directed to DMI.

WE - Write Enable. When WE=1, the host write accesses to the corresponding memory segment are claimed by the Uncore and directed to main memory. Conversely, when WE=0, the host read accesses are directed to DMI.

The RE and WE attributes permit a memory segment to be Read Only, Write Only, Read/Write or Disabled. For example, if a memory segment has RE=1 and WE=0, the segment is Read Only.

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:0, F:0] + 82h	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	RW

Bit Range	Default & Access	Field Name (ID): Description
7:6	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
5:4	0h RW/L	**HIENABLE:** This field controls the steering of read and write cycles that address the BIOS area from 0CC000h to 0CFFFFh. 00: DRAM Disabled. All accesses are directed to DMI. 01: Read Only. All reads are sent to DRAM, all writes are forwarded to DMI. 10: Write Only. All writes are sent to DRAM, all reads are serviced by DMI. 11: Normal DRAM Operation. All reads and writes are serviced by DRAM. **Locked by:** PAM0_0_0_0_PCI.LOCK
3:2	0h RO	**Reserved**
1:0	0h RW/L	**LOENABLE:** This field controls the steering of read and write cycles that address the BIOS area from 0C8000h to 0CBFFFh. 00: DRAM Disabled. All reads are sent to DRAM. All writes are forwarded to DMI. 01: Read Only. All reads are sent to DRAM. All writes are forwarded to DMI. 10: Write Only. All writes are sent to DRAM. All reads are serviced by DMI. 11: Normal DRAM Operation. All reads and writes are serviced by DRAM. **Locked by:** PAM0_0_0_0_PCI.LOCK

3.1.24 Programmable Attribute Map 3 (PAM3_0_0_0_PCI) — Offset 83h

This register controls the read, write and shadowing attributes of the BIOS range from D0000h to D7FFFh. The Uncore allows programmable memory attributes on 13 legacy memory segments of various sizes in the 768KB to 1MB address range. Seven Programmable Attribute Map (PAM) registers are used to support these features. Cache-ability of these areas is controlled via the MTRR register in the core.

Two bits are used to specify memory attributes for each memory segment. These bits apply to host accesses to the PAM areas. These attributes are:

RE - Read Enable. When RE=1, the host read accesses to the corresponding memory segment are claimed by the Uncore and directed to main memory. Conversely, when RE=0, the host read accesses are directed to DMI.

WE - Write Enable. When WE=1, the host write accesses to the corresponding memory segment are claimed by the Uncore and directed to main memory. Conversely, when WE=0, the host read accesses are directed to DMI.

The RE and WE attributes permit a memory segment to be Read Only, Write Only, Read/Write or Disabled. For example, if a memory segment has RE=1 and WE=0, the segment is Read Only.

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:0, F:0] + 83h	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	RW

Bit Range	Default & Access	Field Name (ID): Description
7:6	0h RO	**Reserved**
5:4	0h RW/L	**HIENABLE:** This field controls the steering of read and write cycles that address the BIOS area from 0D4000h to 0D7FFFh. 00: DRAM Disabled. All accesses are directed to DMI. 01: Read Only. All reads are sent to DRAM, all writes are forwarded to DMI. 10: Write Only. All writes are sent to DRAM, all reads are serviced by DMI. 11: Normal DRAM Operation. All reads and writes are serviced by DRAM. **Locked by:** PAM0_0_0_0_PCI.LOCK
3:2	0h RO	**Reserved**
1:0	0h RW/L	**LOENABLE:** This field controls the steering of read and write cycles that address the BIOS area from 0D0000h to 0D3FFFh. 00: DRAM Disabled. All reads are sent to DRAM. All writes are forwarded to DMI. 01: Read Only. All reads are sent to DRAM. All writes are forwarded to DMI. 10: Write Only. All writes are sent to DRAM. All reads are serviced by DMI. 11: Normal DRAM Operation. All reads and writes are serviced by DRAM. **Locked by:** PAM0_0_0_0_PCI.LOCK

3.1.25 Programmable Attribute Map 4 (PAM4_0_0_0_PCI) — Offset 84h

This register controls the read, write and shadowing attributes of the BIOS range from D8000h to DFFFFh. The Uncore allows programmable memory attributes on 13 legacy memory segments of various sizes in the 768KB to 1MB address range. Seven Programmable Attribute Map (PAM) registers are used to support these features. Cache-ability of these areas is controlled via the MTRR register in the core.

Two bits are used to specify memory attributes for each memory segment. These bits apply to host accesses to the PAM areas. These attributes are:

RE - Read Enable. When RE=1, the host read accesses to the corresponding memory segment are claimed by the Uncore and directed to main memory. Conversely, when RE=0, the host read accesses are directed to DMI.

WE - Write Enable. When WE=1, the host write accesses to the corresponding memory segment are claimed by the Uncore and directed to main memory. Conversely, when WE=0, the host read accesses are directed to DMI.

The RE and WE attributes permit a memory segment to be Read Only, Write Only, Read/Write or Disabled. For example, if a memory segment has RE=1 and WE=0, the segment is Read Only.

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:0, F:0] + 84h	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	RW

Bit Range	Default & Access	Field Name (ID): Description
7:6	0h RO	**Reserved**
5:4	0h RW/L	**HIENABLE:** This field controls the steering of read and write cycles that address the BIOS area from 0DC000h to 0DFFFFh. 00: DRAM Disabled. All accesses are directed to DMI. 01: Read Only. All reads are sent to DRAM, all writes are forwarded to DMI. 10: Write Only. All writes are sent to DRAM, all reads are serviced by DMI. 11: Normal DRAM Operation. All reads and writes are serviced by DRAM. **Locked by:** PAM0_0_0_0_PCI.LOCK
3:2	0h RO	**Reserved**
1:0	0h RW/L	**LOENABLE:** This field controls the steering of read and write cycles that address the BIOS area from 0D8000h to 0DBFFFh. 00: DRAM Disabled. All reads are sent to DRAM. All writes are forwarded to DMI. 01: Read Only. All reads are sent to DRAM. All writes are forwarded to DMI. 10: Write Only. All writes are sent to DRAM. All reads are serviced by DMI. 11: Normal DRAM Operation. All reads and writes are serviced by DRAM. **Locked by:** PAM0_0_0_0_PCI.LOCK

3.1.26 Programmable Attribute Map 5 (PAM5_0_0_0_PCI) — Offset 85h

This register controls the read, write and shadowing attributes of the BIOS range from E_0000h to E_7FFFh. The Uncore allows programmable memory attributes on 13 legacy memory segments of various sizes in the 768KB to 1MB address range. Seven Programmable Attribute Map (PAM) registers are used to support these features. Cache-ability of these areas is controlled via the MTRR register in the core.

Two bits are used to specify memory attributes for each memory segment. These bits apply to host accesses to the PAM areas. These attributes are:

RE - Read Enable. When RE=1, the host read accesses to the corresponding memory segment are claimed by the Uncore and directed to main memory. Conversely, when RE=0, the host read accesses are directed to DMI.

WE - Write Enable. When WE=1, the host write accesses to the corresponding memory segment are claimed by the Uncore and directed to main memory. Conversely, when WE=0, the host read accesses are directed to DMI.

The RE and WE attributes permit a memory segment to be Read Only, Write Only, Read/Write or Disabled. For example, if a memory segment has RE=1 and WE=0, the segment is Read Only.

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:0, F:0] + 85h	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	RW

Bit Range	Default & Access	Field Name (ID): Description
7:6	0h RO	**Reserved**
5:4	0h RW/L	**HIENABLE:** This field controls the steering of read and write cycles that address the BIOS area from 0E4000h to 0E7FFFh. 00: DRAM Disabled. All accesses are directed to DMI. 01: Read Only. All reads are sent to DRAM, all writes are forwarded to DMI. 10: Write Only. All writes are sent to DRAM, all reads are serviced by DMI. 11: Normal DRAM Operation. All reads and writes are serviced by DRAM. **Locked by:** PAM0_0_0_0_PCI.LOCK
3:2	0h RO	**Reserved**
1:0	0h RW/L	**LOENABLE:** This field controls the steering of read and write cycles that address the BIOS area from 0E0000h to 0E3FFFh. 00: DRAM Disabled. All reads are sent to DRAM. All writes are forwarded to DMI. 01: Read Only. All reads are sent to DRAM. All writes are forwarded to DMI. 10: Write Only. All writes are sent to DRAM. All reads are serviced by DMI. 11: Normal DRAM Operation. All reads and writes are serviced by DRAM. **Locked by:** PAM0_0_0_0_PCI.LOCK

3.1.27 Programmable Attribute Map 6 (PAM6_0_0_0_PCI) — Offset 86h

This register controls the read, write and shadowing attributes of the BIOS range from E_8000h to E_FFFFh. The Uncore allows programmable memory attributes on 13 legacy memory segments of various sizes in the 768KB to 1MB address range. Seven Programmable Attribute Map (PAM) registers are used to support these features. Cache-ability of these areas is controlled via the MTRR register in the core.

Two bits are used to specify memory attributes for each memory segment. These bits apply to host accesses to the PAM areas. These attributes are:

RE - Read Enable. When RE=1, the host read accesses to the corresponding memory segment are claimed by the Uncore and directed to main memory. Conversely, when RE=0, the host read accesses are directed to DMI.

WE - Write Enable. When WE=1, the host write accesses to the corresponding memory segment are claimed by the Uncore and directed to main memory. Conversely, when WE=0, the host read accesses are directed to DMI.

The RE and WE attributes permit a memory segment to be Read Only, Write Only, Read/Write or Disabled. For example, if a memory segment has RE=1 and WE=0, the segment is Read Only.

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:0, F:0] + 86h	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	RW

Bit Range	Default & Access	Field Name (ID): Description
7:6	0h RO	**Reserved**
5:4	0h RW/L	**HIENABLE:** This field controls the steering of read and write cycles that address the BIOS area from 0EC000h to 0EFFFFh. 00: DRAM Disabled. All accesses are directed to DMI. 01: Read Only. All reads are sent to DRAM, all writes are forwarded to DMI. 10: Write Only. All writes are sent to DRAM, all reads are serviced by DMI. 11: Normal DRAM Operation. All reads and writes are serviced by DRAM. **Locked by:** PAM0_0_0_0_PCI.LOCK
3:2	0h RO	**Reserved**
1:0	0h RW/L	**LOENABLE:** This field controls the steering of read and write cycles that address the BIOS area from 0E8000h to 0EBFFFh. 00: DRAM Disabled. All reads are sent to DRAM. All writes are forwarded to DMI. 01: Read Only. All reads are sent to DRAM. All writes are forwarded to DMI. 10: Write Only. All writes are sent to DRAM. All reads are serviced by DMI. 11: Normal DRAM Operation. All reads and writes are serviced by DRAM. **Locked by:** PAM0_0_0_0_PCI.LOCK

3.1.28 Legacy Access Control (LAC_0_0_0_PCI) — Offset 87h

This 8-bit register controls steering of MDA cycles and a fixed DRAM hole from 15-16MB.

There can only be at most one MDA device in the system.

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:0, F:0] + 87h	10h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
7	0h RW	**HEN:** This field enables a memory hole in DRAM space. The DRAM that lies behind this space is not remapped. 0: No memory hole. 1: Memory hole from 15MB to 16MB. This bit is Intel TXT lockable.
6:5	0h RO	**Reserved**
4	1h RW	**MDAPCIE:** This bit works with the VGA Enable bits in the BCTRL register of Non PEG devices to control the routing of CPU initiated transactions targeting MDA compatible I/O and memory address ranges. This bit should be set to 1 by default. It is assumed that these devices will not need to support legacy MDA graphics. However this single bit is added just to support this rare case of using MDA over these devices. The behavior of this bit field is identical to bits [3:0]
3	0h RW	**MDAP60:** This bit works with the VGA Enable bits in the BCTRL register of Device 1 Function 2 to control the routing of CPU initiated transactions targeting MDA compatible I/O and memory address ranges. This bit should not be set if device 1 function 2 VGA Enable bit is not set. If device 1 function 2 VGA enable bit is not set, then accesses to IO address range x3BCh-x3BFh remain on the backbone. If the VGA enable bit is set and MDA is not present, then accesses to IO address range x3BCh-x3BFh are forwarded to PCI Express through device 1 function 2 if the address is within the corresponding IOBASE and IOLIMIT, otherwise they remain on the backbone. MDA resources are defined as the following: Memory: 0B0000h - 0B7FFFh I/O: 3B4h, 3B5h, 3B8h, 3B9h, 3BAh, 3BFh, (including ISA address aliases, A[15:10] are not used in decode) Any I/O reference that includes the I/O locations listed above, or their aliases, will remain on the backbone even if the reference also includes I/O locations not listed above. The following table shows the behavior for all combinations of MDA and VGA: VGAEN MDAP Description 0 0 All References to MDA and VGA space are not claimed by Device 1 Function 2. 0 1 Illegal combination 1 0 All VGA and MDA references are routed to PCI Express Graphics Attach device 1 function 2. 1 1 All VGA references are routed to PCI Express Graphics Attach device 1 function 2. MDA references are not claimed by device 1 function 2. VGA and MDA memory cycles can only be routed across PEG12 when MAE (PCICMD12[1]) is set. VGA and MDA I/O cycles can only be routed across PEG12 if IOAE (PCICMD12[0]) is set.

Bit Range	Default & Access	Field Name (ID): Description
2	0h RW	**MDAP12:** This bit works with the VGA Enable bits in the BCTRL register of Device 1 Function 2 to control the routing of CPU initiated transactions targeting MDA compatible I/O and memory address ranges. This bit should not be set if device 1 function 2 VGA Enable bit is not set. If device 1 function 2 VGA enable bit is not set, then accesses to IO address range x3BCh-x3BFh remain on the backbone. If the VGA enable bit is set and MDA is not present, then accesses to IO address range x3BCh-x3BFh are forwarded to PCI Express through device 1 function 2 if the address is within the corresponding IOBASE and IOLIMIT, otherwise they remain on the backbone. MDA resources are defined as the following: Memory: 0B0000h - 0B7FFFh I/O: 3B4h, 3B5h, 3B8h, 3B9h, 3BAh, 3BFh, (including ISA address aliases, A[15:10] are not used in decode) Any I/O reference that includes the I/O locations listed above, or their aliases, will remain on the backbone even if the reference also includes I/O locations not listed above. The following table shows the behavior for all combinations of MDA and VGA: VGAEN MDAP Description 0 0 All References to MDA and VGA space are not claimed by Device 1 Function 2. 0 1 Illegal combination 1 0 All VGA and MDA references are routed to PCI Express Graphics Attach device 1 function 2. 1 1 All VGA references are routed to PCI Express Graphics Attach device 1 function 2. MDA references are not claimed by device 1 function 2. VGA and MDA memory cycles can only be routed across PEG12 when MAE (PCICMD12[1]) is set. VGA and MDA I/O cycles can only be routed across PEG12 if IOAE (PCICMD12[0]) is set.
1	0h RW	**MDAP11:** This bit works with the VGA Enable bits in the BCTRL register of Device 1 Function 1 to control the routing of CPU initiated transactions targeting MDA compatible I/O and memory address ranges. This bit should not be set if device 1 function 1 VGA Enable bit is not set. If device 1 function 1 VGA enable bit is not set, then accesses to IO address range x3BCh-x3BFh remain on the backbone. If the VGA enable bit is set and MDA is not present, then accesses to IO address range x3BCh-x3BFh are forwarded to PCI Express through device 1 function 1 if the address is within the corresponding IOBASE and IOLIMIT, otherwise they remain on the backbone. MDA resources are defined as the following: Memory: 0B0000h - 0B7FFFh I/O: 3B4h, 3B5h, 3B8h, 3B9h, 3BAh, 3BFh, (including ISA address aliases, A[15:10] are not used in decode) Any I/O reference that includes the I/O locations listed above, or their aliases, will remain on the backbone even if the reference also includes I/O locations not listed above. The following table shows the behavior for all combinations of MDA and VGA: VGAEN MDAP Description 0 0 All References to MDA and VGA space are not claimed by Device 1 Function 1. 0 1 Illegal combination 1 0 All VGA and MDA references are routed to PCI Express Graphics Attach device 1 function 1. 1 1 All VGA references are routed to PCI Express Graphics Attach device 1 function 1. MDA references are not claimed by device 1 function 1. VGA and MDA memory cycles can only be routed across PEG11 when MAE (PCICMD11[1]) is set. VGA and MDA I/O cycles can only be routed across PEG11 if IOAE (PCICMD11[0]) is set.

Bit Range	Default & Access	Field Name (ID): Description
0	0h RW	**MDAP10:** This bit works with the VGA Enable bits in the BCTRL register of Device 1 Function 0 to control the routing of CPU initiated transactions targeting MDA compatible I/O and memory address ranges. This bit should not be set if device 1 function 0 VGA Enable bit is not set. If device 1 function 0 VGA enable bit is not set, then accesses to IO address range x3BCh-x3BFh remain on the backbone. If the VGA enable bit is set and MDA is not present, then accesses to IO address range x3BCh-x3BFh are forwarded to PCI Express through device 1 function 0 if the address is within the corresponding IOBASE and IOLIMIT, otherwise they remain on the backbone. MDA resources are defined as the following: Memory: 0B0000h - 0B7FFFh I/O: 3B4h, 3B5h, 3B8h, 3B9h, 3BAh, 3BFh, (including ISA address aliases, A[15:10] are not used in decode) Any I/O reference that includes the I/O locations listed above, or their aliases, will remain on the backbone even if the reference also includes I/O locations not listed above. The following table shows the behavior for all combinations of MDA and VGA: VGAEN MDAP Description 0 0 All References to MDA and VGA space are not claimed by Device 1 Function 0. 0 1 Illegal combination 1 0 All VGA and MDA references are routed to PCI Express Graphics Attach device 1 function 0. 1 1 All VGA references are routed to PCI Express Graphics Attach device 1 function 0. MDA references are not claimed by device 1 function 0. VGA and MDA memory cycles can only be routed across PEG10 when MAE (PCICMD10[1]) is set. VGA and MDA I/O cycles can only be routed across PEG10 if IOAE (PCICMD10[0]) is set.

3.1.29 Top of Memory (TOM_0_0_0_PCI) — Offset A0h

This Register contains the size of physical memory.

BIOS determines the memory size reported to the OS using this Register.

Type	Size	Offset	Default
PCI	64 bit	[B:0, D:0, F:0] + A0h	0000007FFFF00000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:20	7FFFFh RW/L	**TOM:** This register reflects the total amount of populated physical memory. This is NOT necessarily the highest main memory address (holes may exist in main memory address map due to addresses allocated for memory mapped IO). These bits correspond to address bits 38:20 (1MB granularity). Bits 19:0 are assumed to be 0. All the bits in this register are locked in Intel TXT mode. **Locked by:** TOM_0_0_0_PCI.LOCK

Bit Range	Default & Access	Field Name (ID): Description
19:1	0h RO	**Reserved**
0	0h RW/L	**LOCK:** This bit will lock all writable settings in this register, including itself. **Locked by:** TOM_0_0_0_PCI.LOCK

3.1.30 Top of Upper Usable DRAM (TOUUD_0_0_0_PCI) — Offset A8h

This 64 bit register defines the Top of Upper Usable DRAM.

Configuration software must set this value to TOM minus all ME stolen memory if reclaim is disabled. If reclaim is enabled, this value must be set to reclaim limit + 1byte, 1MB aligned, since reclaim limit is 1MB aligned. Address bits 19:0 are assumed to be 000_0000h for the purposes of address comparison. The Host interface positively decodes an address towards DRAM if the incoming address is less than the value programmed in this register and greater than or equal to 4GB.

BIOS Restriction: Minimum value for TOUUD is 4GB.

These bits are Intel TXT lockable.

Type	Size	Offset	Default
PCI	64 bit	[B:0, D:0, F:0] + A8h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:20	00000h RW/L	**TOUUD:** This register contains bits 38 to 20 of an address one byte above the maximum DRAM memory above 4G that is usable by the operating system. Configuration software must set this value to TOM minus all ME stolen memory if reclaim is disabled. If reclaim is enabled, this value must be set to reclaim limit 1MB aligned since reclaim limit + 1byte is 1MB aligned. Address bits 19:0 are assumed to be 000_0000h for the purposes of address comparison. The Host interface positively decodes an address towards DRAM if the incoming address is less than the value programmed in this register and greater than 4GB. All the bits in this register are locked in Intel TXT mode. **Locked by:** TOUUD_0_0_0_PCI.LOCK
19:1	0h RO	**Reserved**
0	0h RW/L	**LOCK:** This bit will lock all writable settings in this register, including itself. **Locked by:** TOUUD_0_0_0_PCI.LOCK

3.1.31 Base Data of Stolen Memory (BDSM_0_0_0_PCI) — Offset B0h

This register contains the base address of graphics data stolen DRAM memory. BIOS determines the base of graphics data stolen memory by subtracting the graphics data stolen memory size (PCI Device 0 offset 52 bits 7:4) from TOLUD (PCI Device 0 offset BC bits 31:20).

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:0, F:0] + B0h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:20	000h RW/L	**BDSM:** This register contains bits 31 to 20 of the base address of stolen DRAM memory. BIOS determines the base of graphics stolen memory by subtracting the graphics stolen memory size (PCI Device 0 offset 50 bits 15:8) from TOLUD (PCI Device 0 offset BC bits 31:20). **Locked by:** BDSM_0_0_0_PCI.LOCK
19:1	0h RO	**Reserved**
0	0h RW/L	**LOCK:** This bit will lock all writable settings in this register, including itself. **Locked by:** BDSM_0_0_0_PCI.LOCK

3.1.32 Base of GTT Stolen Memory (BGSM_0_0_0_PCI) — Offset B4h

This register contains the base address of stolen DRAM memory for the GTT. BIOS determines the base of GTT stolen memory by subtracting the GTT graphics stolen memory size (PCI Device 0 offset 52 bits 9:8) from the Graphics Base of Data Stolen Memory (PCI Device 0 offset B0 bits 31:20).

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:0, F:0] + B4h	00100000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:20	001h RW/L	**BGSM:** This register contains the base address of stolen DRAM memory for the GTT. BIOS determines the base of GTT stolen memory by subtracting the GTT graphics stolen memory size (PCI Device 0 offset 50 bits 7:6) from the Graphics Base of Data Stolen Memory (PCI Device 0 offset B0 bits 31:20). **Locked by:** BGSM_0_0_0_PCI.LOCK
19:1	0h RO	**Reserved**
0	0h RW/L	**LOCK:** This bit will lock all writable settings in this register, including itself. **Locked by:** BGSM_0_0_0_PCI.LOCK

3.1.33 TSEG Memory Base (TSEGMB_0_0_0_PCI) — Offset B8h

This register contains the base address of TSEG DRAM memory. BIOS determines the base of TSEG memory which must be at or below Graphics Base of GTT Stolen Memory (PCI Device 0 Offset B4 bits 31:20).

NOTE: BIOS must program TSEGMB to a 8MB naturally aligned boundary.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:0, F:0] + B8h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:20	000h RW/L	**TSEGMB:** This register contains the base address of TSEG DRAM memory. BIOS determines the base of TSEG memory which must be at or below Graphics Base of GTT Stolen Memory (PCI Device 0 Offset B4 bits 31:20). BIOS must program the value of TSEGMB to be the same as BGSM when TSEG is disabled. **Locked by:** TSEGMB_0_0_0_PCI.LOCK
19:1	0h RO	**Reserved**
0	0h RW/L	**LOCK:** This bit will lock all writable settings in this register, including itself. **Locked by:** TSEGMB_0_0_0_PCI.LOCK

3.1.34 Top of Low Usable DRAM (TOLUD_0_0_0_PCI) — Offset BCh

This 32 bit register defines the Top of Low Usable DRAM. TSEG, GTT Graphics memory and Graphics Stolen Memory are within the DRAM space defined. From the top, the Host optionally claims 1 to 64MBs of DRAM for internal graphics if enabled, 1or 2MB of DRAM for GTT Graphics Stolen Memory (if enabled) and 1, 2, or 8 MB of DRAM for TSEG if enabled.

Programming Example:

C1DRB3 is set to 4GB

TSEG is enabled and TSEG size is set to 1MB

Internal Graphics is enabled, and Graphics Mode Select is set to 32MB

GTT Graphics Stolen Memory Size set to 2MB

BIOS knows the OS requires 1G of PCI space.

BIOS also knows the range from 0_FEC0_0000h to 0_FFFF_FFFFh is not usable by the system. This 20MB range at the very top of addressable memory space is lost to APIC and Intel TXT.

According to the above equation, TOLUD is originally calculated to: 4GB = 1_0000_0000h

The system memory requirements are: 4GB (max addressable space) - 1GB PCI space) - 35MB (lost memory) = 3GB - 35MB (minimum granularity) = 0_ECB0_0000h

Since 0_ECB0_0000h (PCI and other system requirements) is less than 1_0000_0000h, TOLUD should be programmed to ECBh.

These bits are Intel TXT lockable.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:0, F:0] + BCh	00100000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:20	001h RW/L	**TOLUD:** This register contains bits 31 to 20 of an address one byte above the maximum DRAM memory below 4G that is usable by the operating system. Address bits 31 down to 20 programmed to 01h implies a minimum memory size of 1MB. Configuration software must set this value to the smaller of the following 2 choices: maximum amount memory in the system minus ME stolen memory plus one byte or the minimum address allocated for PCI memory. Address bits 19:0 are assumed to be 0_0000h for the purposes of address comparison. The Host interface positively decodes an address towards DRAM if the incoming address is less than the value programmed in this register. The Top of Low Usable DRAM is the lowest address above both Graphics Stolen memory and TSEG. BIOS determines the base of Graphics Stolen Memory by subtracting the Graphics Stolen Memory Size from TOLUD and further decrements by TSEG size to determine base of TSEG. All the Bits in this register are locked in Intel TXT mode. This register must be 1MB aligned when reclaim is enabled. **Locked by:** TOLUD_0_0_0_PCI.LOCK
19:1	0h RO	**Reserved**
0	0h RW/L	**LOCK:** This bit will lock all writable settings in this register, including itself. **Locked by:** TOLUD_0_0_0_PCI.LOCK

3.1.35 Error Status (ERRSTS_0_0_0_PCI) — Offset C8h

This register is used to report various error conditions via the SERR DMI messaging mechanism. An SERR DMI message is generated on a zero to one transition of any of these flags (if enabled by the ERRCMD and PCICMD registers).

These bits are set regardless of whether or not the SERR is enabled and generated. After the error processing is complete, the error logging mechanism can be unlocked by clearing the appropriate status bit by software writing a 1 to it.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:0, F:0] + C8h	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:2	0h RO	**Reserved**
1	0h RW/1C/V/P	**Data Uncorrectable Error (DMERR):** If this bit is set to 1, a memory read data transfer had an uncorrectable multiple-bit error. When this bit is set, the column, row, bank, and rank that caused the error and the error syndrome, are logged in the ECC Error Log register in the channel where the error occurred. Once this bit is set, the ECCERRLOGx fields are locked until the CPU clears this bit by writing a 1. Software uses bits [1:0] to detect whether the logged error address is for a Single-bit or a Multiple-bit error.
0	0h RW/1C/V/P	**Data Single Bit Correctable Error (DSERR):** If this bit is set to 1, a memory read data transfer had a single-bit correctable error and the corrected data was returned to the requesting agent. When this bit is set the column, row, bank, and rank where the error occurred and the syndrome of the error are logged in the ECC Error Log register in the channel where the error occurred. Once this bit is set the ECCERRLOGx fields are locked to further single-bit error updates until the CPU clears this bit by writing a 1. A multiple bit error that occurs after this bit is set will overwrite the ECCERRLOGx fields with the multiple-bit error signature and the DMERR bit will also be set. A single bit error that occurs after a multibit error will set this bit but will not overwrite the other fields.

3.1.36 Error Command (ERRCMD_0_0_0_PCI) — Offset CAh

This register controls the Host Bridge responses to various system errors. Since the Host Bridge does not have an SERRB signal, SERR messages are passed from the CPU to the PCH over DMI.

When a bit in this register is set, a SERR message will be generated on DMI whenever the corresponding flag is set in the ERRSTS register. The actual generation of the SERR message is globally enabled for Device #0 via the PCI Command register.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:0, F:0] + CAh	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:2	0h RO	**Reserved**
1	0h RW	**Data Uncorrectable Error (DMERR):** 1: The Host Bridge generates an SERR message over DMI when it detects a multiple-bit error reported by the DRAM controller. 0: Reporting of this condition via SERR messaging is disabled. For systems not supporting ECC this bit must be disabled.
0	0h RW	**Data Single Bit Correctable Error (DSERR):** 1: The Host Bridge generates an SERR special cycle over DMI when the DRAM controller detects a single bit error. 0: Reporting of this condition via SERR messaging is disabled. For systems that do not support ECC this bit must be disabled.

3.1.37 SMI DMI Special Cycle (SMICMD_0_0_0_PCI) — Offset CCh

This register enables various errors to generate an SMI DMI special cycle. When an error flag is set in the ERRSTS register, it can generate an SERR, SMI, or SCI DMI special cycle when enabled in the ERRCMD, SMICMD, or SCICMD registers, respectively. Note that one and only one message type can be enabled.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:0, F:0] + CCh	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:2	0h RO	**Reserved**
1	0h RW	**SMI on Multiple Bit Error (DMESMI):** 1: The Host generates an SMI DMI message when it detects a multiple-bit error reported by the DRAM controller. 0: Reporting of this condition via SMI messaging is disabled. For systems not supporting ECC this bit must be disabled.

Bit Range	Default & Access	Field Name (ID): Description
0	0h RW	**Single Bit Error (DSESMI):** 1: The Host generates an SMI DMI special cycle when the DRAM controller detects a single bit error. 0: Reporting of this condition via SMI messaging is disabled. For systems that do not support ECC this bit must be disabled.

3.1.38 SMI DMI Special Cycle (SCICMD_0_0_0_PCI) — Offset CEh

This register enables various errors to generate an SCI DMI special cycle. When an error flag is set in the ERRSTS register, it can generate an SERR, SMI, or SCI DMI special cycle when enabled in the ERRCMD, SMICMD, or SCICMD registers, respectively. Note that one and only one message type can be enabled.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:0, F:0] + CEh	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:2	0h RO	**Reserved**
1	0h RW	**SCI on Multiple Bit Error (DMESCI):** 1: The Host generates an SCI DMI message when it detects a multiple-bit error reported by the DRAM controller. 0: Reporting of this condition via SCI messaging is disabled. For systems not supporting ECC this bit must be disabled.
0	0h RW	**SCI on Single Bit Error (DSESCI):** 1: The Host generates an SCI DMI special cycle when the DRAM controller detects a single bit error. 0: Reporting of this condition via SCI messaging is disabled. For systems that do not support ECC this bit must be disabled.

3.1.39 Scratchpad Data (SKPD_0_0_0_PCI) — Offset DCh

This register holds 32 writable bits with no functionality behind them. It is for the convenience of BIOS and graphics drivers.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:0, F:0] + DCh	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RW	**SKPD:** 1 DWORD of data storage.

3.1.40 Capabilities A (CAPID0_A_0_0_0_PCI) — Offset E4h

Processor capability enumeration

.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:0, F:0] + E4h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RW/L	**NVME Device 3 Function 0 Disable (NVME_DIS):** 0: Device 3 Function 0 and associated memory spaces are accessible. 1: Device 3 Function 0 (NVMe F0) and associated memory space are disabled by hardwiring the D3F0EN field, bit 5 of the SoC Device Enable register
30	0h RW/L	**PCIe Device 1 Function 2 Disable (PEG12D):** 0: Device 1 Function 2 and associated memory spaces are accessible. 1: Device 1 Function 2 and associated memory and IO spaces are disabled by hardwiring the D1F2EN field, bit 1 of the Device Enable register, (DEVEN Dev 0 Offset 54h) to 0.
29	0h RW/L	**PCIe Device 1 Function 1 Disable (PEG11D):** 0: Device 1 Function 1 and associated memory spaces are accessible. 1: Device 1 Function 1 and associated memory and IO spaces are disabled by hardwiring the D1F1EN field, bit 2 of the Device Enable register, (DEVEN Dev 0 Offset 54h) to 0.
28	0h RW/L	**PCIe Device 1 Function 0 Disable (PEG10D):** 0: Device 1 Function 0 and associated memory spaces are accessible. 1: Device 1 Function 0 and associated memory and IO spaces are disabled by hardwiring the D1F0EN field, bit 3 of the Device Enable register, (DEVEN Dev 0 Offset 54h) to 0.

Bit Range	Default & Access	Field Name (ID): Description
27	0h RW/L	**PCIe Link Width Up-config Disable (PELWUD):** 0: Link width upconfig is supported. The Processor advertises upconfig capability using the data rate symbol in its TS2 training ordered sets during Configuration.Complete. The CPU responds to link width upconfigs initiated by the downstream device. 1: Link width upconfig is NOT supported. The Processor does not advertise upconfig capability using the data rate field in TS2 training ordered sets during Configuration.Complete. The CPU does not respond to link width upconfigs initiated by the downstream device.
26	0h RW/L	**DMI Width (DW):** 0: DMI x4 1: DMI x2
25	0h RW/L	**DRAM ECC Disable (ECCDIS):** 0: ECC is supported 1: ECC is not supported
24	0h RW/L	**Force DRAM ECC Enable (FDEE):** 0: DRAM ECC optional via software. 1: DRAM ECC enabled. MCHBAR C0MISCCTL bit [0] and C1MISCCTL bit [0] are forced to 1 and Read-Only. Note that FDEE and ECCDIS must not both be set to 1.
23	0h RW/L	**VT-d Disable (VTDD):** 0: VT-d is supported 1: VT-d is not supported
22	0h RW/L	**DMI GEN2 Disable (DMIG2DIS):** 0: Capable of running DMI in Gen 2 mode 1: Not capable of running DMI in Gen 2 mode
21	0h RW/L	**PCIe Controller Gen 2 Disable (PEGG2DIS):** 0: Capable of running any of the PEG controllers in Gen 2 mode 1: Not capable of running any of the PEG controllers in Gen 2 mode
20:19	0h RW/L	**DRAM Maximum Size per Channel (DDRSZ):** This field defines the maximum allowed memory size per channel. • 0: Unlimited (64GB per channel) • 1: Maximum 8GB per channel • 2: Maximum 4GB per channel • 3: Maximum 2GB per channel
18	0h RW/L	**PCIe Controller Device 6 Function 0 Disabled (PEG60D):** PCIe Controller Device 6 Function 0 is disabled 0: Device 6 Function 0 is supported 1: Device 6 Function 0 is not supported
17	0h RW/L	**DRAM 1N Timing Disable (D1NM):** 0: Part is capable of supporting 1n mode timings on the DDR interface. 1: Part is not capable of supporting 1n mode. Only supported timings are 2n or greater.
16	0h RO	**Reserved**
15	0h RW/L	**DPPM Device Disable (CDD):** 0: DPPM Device enabled. 1: DPPM Device disabled.

Bit Range	Default & Access	Field Name (ID): Description
14	0h RW/L	**2 DIMMs Per Channel Enable (DDPCD):** Allows Dual Channel operation but only supports 1 DIMM per channel. 0: 2 DIMMs per channel enabled 1: 2 DIMMs per channel disabled. This setting hardwires bits 2 and 3 of the rank population field for each channel to zero. (MCHBAR offset 260h, bits 22-23 for channel 0 and MCHBAR offset 660h, bits 22-23 for channel 1)
13	0h RW/L	**X2APIC Enable (X2APIC_EN):** Extended Interrupt Mode. 0b: Hardware does not support Extended APIC mode. 1b: Hardware supports Extended APIC mode.
12	0h RW/L	**Dual Memory Channel Support (PDCD):** 0: Capable of Dual Channel 1: Not Capable of Dual Channel - only single channel capable.
11	0h RW/L	**Internal Graphics Disable (IGD):** 0: There is a graphics engine within this CPU. Internal Graphics Device (Device 2) is enabled and all of its memory and I/O spaces are accessible. Configuration cycles to Device 2 will be completed within the CPU. All non-SMM memory and IO accesses to VGA will be handled based on Memory and IO enables of Device 2 and IO registers within Device 2 and VGA Enable of the PCI to PCI bridge control register in Devices 1 and 6 (If PCI Express GFX attach is supported). A selected amount of Graphics Memory space is pre-allocated from the main memory based on Graphics Mode Select (GMS in the GGC Register). Graphics Memory is pre-allocated above TSEG Memory. 1: There is no graphics engine within this CPU. Internal Graphics Device (Device 2) and all of its memory and I/O functions are disabled. Configuration cycle targeted to Device 2 will be passed on to DMI. In addition, all clocks to internal graphics logic are turned off. All non-SMM memory and IO accesses to VGA will be handled based on VGA Enable of the PCI to PCI bridge control register in Devices 1 and 6. DEVEN [4:3] (Device 0, offset 54h) have no meaning. Device 2 Functions 0 and 1 are disabled and hidden.
10	0h RW/L	**DID0 Override Enable (DID0OE):** 0: Disable ability to override DID0 - For production 1: Enable ability to override DID - For debug and samples only
9:8	0h RO	**Reserved**
7:4	0h RW/L	**Compatibility Revision ID (CRID):** Compatibility Revision ID
3	0h RW/L	**Memory Overclocking (DDR_OVERCLOCK):** Memory Overclocking is enabled. When supported, memory can be trained at higher than default maximum frequencies. 0: Memory Overclocking is not supported 1: Memory Overclocking is supported
2:0	0h RO	**Reserved**

3.1.41 Capabilities B (CAPID0_B_0_0_0_PCI) — Offset E8h

Processor capability enumeration

.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:0, F:0] + E8h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RW/L	**Image Processing Unit (IPU) Disable (IPU_DIS):** 0: Device 5 associated memory spaces are accessible. 1: Device 5 associated memory and IO spaces are disabled by hardwiring the D1F2EN field, bit 1 of the Device Enable register, (DEVEN Dev 0 Offset 54h) to 0.
30	0h RW/L	**Processor Trace Disable (PT_DIS):** 0: Processor Trace associated memory spaces are accessible. 1: Processor Trace associated memory and IO spaces are disabled by hardwiring the D1F2EN field, bit 1 of the Device Enable register, (DEVEN Dev 0 Offset 54h) to 0.
29	0h RW/L	**Overclocking Enabled (OC_ENABLED):** 0: Overclocking is Disabled 1: Overclocking is Enabled If overclocking is enabled, MSR FLEX_RATIO.OC_BINS contains how many bits of over-clocking are supported. The encoding is as follows: 0: Overclocking is Disabled 1-6: Turbo ratio limits can be incremented by this amount 7: Unlimited If overclocking is disabled, FLEX_RATIO.OC_BINS is meaningless.
28	0h RW/L	**SMT Capability (SMT):** This setting indicates whether the processor is SMT (HyperThreading) capable.
27:25	0h RW/L	**Cache Size (CACHESZ):** This setting indicates the supporting cache sizes.
24	0h RW/L	**SVM Disable (SVM_DISABLE):** 0: SVM enabled 1: SVM disabled
23:21	0h RW/L	**Memory 100MHz Reference Clock (PLL_REF100_CFG):** DDR Maximum Frequency Capability with 100MHz memory reference clock (ref_clk). 0: 100 MHz memory reference clock is not supported 1-6: Reserved 7: Unlimited
20	0h RW/L	**PCIe Gen 3 Disable (PEGG3_DIS):** 0: Capable of running any of the Gen 3-compliant PCIe controllers in Gen 3 mode (Devices 0/1/0, 0/1/1, 0/1/2, 0/6/0) 1: Not capable of running any of the PCIe controllers in Gen 3 mode
19	0h RW/L	**Processor Package Type (PKGTYP):** This setting indicates the CPU Package Type.
18	0h RW/L	**Additive Graphics Enabled (ADDGFXEN):** 0: Additive Graphics is disabled 1: Additive Graphics is enabled
17	0h RW/L	**Additive Graphics Capability Disable (ADDGFXCAP):** 0: Capable of Additive Graphics 1: Not capable of Additive Graphics

Bit Range	Default & Access	Field Name (ID): Description
16	0h RW/L	**PCIe x16 Disable (PEGX16D):** 0: Capable of x16 PCIe Port 1: Not Capable of x16 PCIe port, instead PCIe limited to x8 and below. Causes PCIe port to enable and train logical lanes 7:0 only. Logical lanes 15:8 are powered down (unless in use by the other PEG port or the embedded Display Port), and the Max Link Width field of the Link Capability register reports x8 instead of x16. (In the case of lane reversal, lanes 15:8 are active and lanes 7:0 are powered down.)
15	0h RW/L	**DMI Gen 3 Disable (DMIG3DIS):** DMI Gen 3 Disable
14:12	0h RW/L	**2 Level Memory Technology Support (LTECH):** 0: 1LM 1: EDRAM0 3: EDRAM0+1 Other values are reserved.
11	0h RW/L	**HDCP Disable (HDCPD):** 0: Capable of HDCP 1: HDCP Disabled
10:9	0h RO	**Reserved**
8	0h RW/L	**GNA (GMM) Disable (GNA_DIS):** 0: Device 8 associated memory spaces are accessible. 1: Device 8 associated memory and IO spaces are disabled by hardwiring the D8EN field, bit 1 of the Device Enable register, (DEVEN Dev 0 Offset 54h) to 0.
7	0h RW/L	**DDD:** 0: Debug mode 1: Production mode
6:4	0h RO	**Reserved**
3	0h RW/L	**S/H OPI Enable (SH_OPI_EN):** Specifies if OPI or DMI are enabled for S/H models. 0: DMI is enabled 1: OPI is enabled
2	0h RW/L	**VMD Disable (VMD_DIS):** Indicates if VMD is disabled.
1	0h RW/L	**Global Single PCIe Lane (DPEGFX1):** This bit has no effect on Device 1 unless Device 1 is configured for at least two ports via PEG0CFGSEL strap. 0: All PCIe port widths do not depend on their respective BCTRL[VGAEN]. 1: Each PCIe port width is limited to x1 operation when its respective BCTRL[VGAEN] is set to 1b.
0	0h RW/L	**Single PCIe Lane (SPEGFX1):** This bit has no effect on Device 1 unless Device 1 is configured for a single port via PEG0CFGSEL strap. 0: Device 1 Function 0 width does not depend on its BCTRL[VGAEN]. 1: Device 1 Function 0 width is limited to x1 operation when its respective BCTRL[VGAEN] is set to 1.

3.1.42 Capabilities C (CAPID0_C_0_0_0_PCI) — Offset ECh

Processor capability enumeration

.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:0, F:0] + ECh	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:29	0h RO	**Reserved**
28	0h RW/L	**PCIe Gen 4 Disable (PEGG4_DIS):** PCIe Gen 4 Disabled. This field will be strap selectable/modifiable to enable PCH Pairing capabilities. 0: Capable of running any of the Gen 4-compliant PCIe controllers in Gen 4 mode (Devices 0/1/0, 0/1/1, 0/1/2, 0/6/0) 1: Not capable of running any of the PEG controllers in Gen 4 mode
27:23	00h RW/L	**Maximum DDR4 Frequency (MAX_DATA_RATE_DDR4):** DDR4 Maximum Frequency Capability in 266Mhz units. This value is relevant only when CAPID0_A_0_0_0_PCI.DDR_OVERCLOCK is zero (DDR overclocking is not supported). 0: Unlimited 1-31: multiples of 266MHz
22	0h RW/L	**DDR4 Support (DDR4_EN):** 0: DDR4 is not supported 1: DDR4 is supported
21:17	00h RW/L	**Maximum LPDDR4 Frequency (MAX_DATA_RATE_LPDDR4):** LPDDR4 Maximum Frequency Capability in 266Mhz units. This value is relevant only when CAPID0_A_0_0_0_PCI.DDR_OVERCLOCK is zero (DDR overclocking is not supported). 0: Unlimited 1-31: multiples of 266MHz
16	0h RW/L	**LPDDR4 Support (LPDDR4_EN):** 0: LPDDR4 memory is not supported 1: LPDDR4 memory is supported
15	0h RO	**Reserved**
14	0h RW/L	**Dynamic Memory Frequency Change Disable (QCLK_GV_DIS):** 0: Dynamic Memory Frequency Change is enabled 1: Dynamic Memory Frequency Change is disabled
13:10	0h RO	**Reserved**
9	0h RW/L	**SGX Disabled (SGX_DIS):** Software Guard Extension (Intel® SGX) Disabled: Indicates that Intel® SGX is not available on this processor
8:7	0h RW/L	**BCLKOCRANGE:** BCLK (Base clock) Overclocking maximum frequency. • 0: BCLK overclocking is disabled • 1: BCLK maximum frequency is 115MHz • 2: BCLK maximum frequency is 130MHz • 3: Unlimited BCLK maximum frequency

Bit Range	Default & Access	Field Name (ID): Description
6	0h RW/L	**Internal Display Disabled (IDD):** Specifies whether the Internal Display is Disabled. 0: Internal Display is enabled. 1: Internal Display is disabled.
5	0h RW/L	**DISPLAY PIPE3 (DISPLAY_PIPE3):** 0: 3rd Display is disabled 1: 3rd Display is enabled
4:0	00h RW/L	**Max Data Rate At GEAR1 (MAX_DATA_RATE_AT_GEAR1):** This field reports the maximum Data Rate of the memory controller in GEAR 1 in 266Mhz units. This value is relevant only when CAPID0_A_0_0_0_PCI.DDR_OVERCLOCK is zero (DDR overclocking is not supported). 0: Unlimited 1-31: Multiples of 266MHz

3.2 Memory Controller (MCHBAR) Registers

This chapter documents the Memory Controller MCHBAR registers.

Base address of these registers are defined in the MCHBAR_0_0_0_PCI register in Bus: 0, Device: 0, Function: 0.

The MCHBAR exposes 3 sets of memory controller registers channel 0, channel 1 as well broadcast.

- Channel 0 offset range: 4000h-43FFh
- Channel 1 offset range: 4400h-47FFh
- Broadcast offset range: 4C00h-4FFFh

Memory Controller Broadcast register behavior is to write to all channels and read from channel 0.

Note: For brevity, only channel 0 is documented. For channel 1 registers add 0x0400, for broadcast add 0x0C00 to the channel 0 register offset

Note: These registers apply to all processors.

3.2.1 Summary of Registers

Table 3-3. Summary of MCHBAR Registers

Offset	Size (Bytes)	Register Name (Register Symbol)	Default Value
4000h	4	PRE Command Timing (TC_PRE_0_0_0_MCHBAR)	18863808h
4004h	4	ACT Command Timing (TC_ACT_0_0_0_MCHBAR)	01088410h
400Ch	4	RD to RD Timings (TC_RDRD_0_0_0_MCHBAR)	04040404h
4010h	4	RD to WR Timings (TC_RDWR_0_0_0_MCHBAR)	04040404h
4014h	4	WR to RD Timings (TC_WRRD_0_0_0_MCHBAR)	04040404h
4018h	4	WR to WR Timings (TC_WRWR_0_0_0_MCHBAR)	04040404h
4020h	8	Roundtrip Latency (SC_ROUNDTRIP_LATENCY_0_0_0_MCHBAR)	1919191919191919h
4034h	4	ECC Debug Control (ECC_DEBUG_0_0_0_MCHBAR)	00000000h
4048h	4	ECC Error Log 0 (ECCERRLOG0_0_0_0_MCHBAR)	00000000h
404Ch	4	ECC Error Log 0 (ECCERRLOG1_0_0_0_MCHBAR)	00000000h
4050h	8	Power Down Timing (TC_PWRDN_0_0_0_MCHBAR)	0000000404440404h
4070h	8	ODT Command Timing (TC_ODT_0_0_0_MCHBAR)	0000000001850000h
4080h	4	ODT Matrix (SC_ODT_MATRIX_0_0_0_MCHBAR)	00000000h
4088h	8	Scheduler Configuration (SC_GS_CFG_0_0_0_MCHBAR)	0000000000001020h
4224h	4	MR4 Rank Temperature (LPDDR_MR4_RANK_TEMPERATURE_0_0_0_MCHBAR)	03030303h
4228h	4	DDR4 Temperature (DDR4_MPR_RANK_TEMPERATURE_0_0_0_MCHBAR)	01010101h
4238h	4	Refresh Parameters (TC_RFP_0_0_0_MCHBAR)	4600980Fh
423Ch	4	Refresh Timing Parameters (TC_RFTP_0_0_0_MCHBAR)	00B41004h

Offset	Size (Bytes)	Register Name (Register Symbol)	Default Value
4240h	4	Self-Refresh Timing Parameters (TC_SRFTP_0_0_0_MCHBAR)	00000200h
4244h	4	Refresh Stagger Control (MC_REFRESH_STAGGER_0_0_0_MCHBAR)	00000000h
4248h	4	ZQCAL Control (TC_ZQCAL_0_0_0_MCHBAR)	32010000h
4254h	4	Memory Controller Initial State (MC_INIT_STATE_0_0_0_MCHBAR)	0000000Fh
4260h	4	DIMM Idle Energy (PM_DIMM_IDLE_ENERGY_0_0_0_MCHBAR)	00000000h
4264h	4	DIMM Power-Down Energy (PM_DIMM_PD_ENERGY_0_0_0_MCHBAR)	00000000h
4268h	4	DIMM ACT Energy (PM_DIMM_ACT_ENERGY_0_0_0_MCHBAR)	00000000h
426Ch	4	DIMM RD Energy (PM_DIMM_RD_ENERGY_0_0_0_MCHBAR)	00000000h
4270h	4	DIMM WR Energy (PM_DIMM_WR_ENERGY_0_0_0_MCHBAR)	00000000h
4274h	4	ECC Inject Count (ECC_INJECT_COUNT_0_0_0_MCHBAR)	FFFFFFFFh
4278h	4	WR Delay (SC_WR_DELAY_0_0_0_MCHBAR)	00000003h
4288h	4	Per Bank Refresh (SC_PBR_0_0_0_MCHBAR)	0000F011h
4294h	4	Miscellaneous Timing Constrains (TC_LPDDR4_MISC_0_0_0_MCHBAR)	00000056h
42C4h	4	Self-Refresh Exit Timing Parameters (TC_SREXITTP_0_0_0_MCHBAR)	00000000h
43FCh	4	Miscellaneous Control Register (MCMNTS_SPARE_0_0_0_MCHBAR)	00000000h
5000h	4	Inter-Channel Decode Parameters (MAD_INTER_CHANNEL_0_0_0_MCHBAR)	00000000h
5004h	4	Intra-Channel 0 Decode Parameters (MAD_INTRA_CH0_0_0_0_MCHBAR)	00000000h
5008h	4	Intra-Channel 1 Decode Parameters (MAD_INTRA_CH1_0_0_0_MCHBAR)	00000000h
500Ch	4	Channel 0 DIMM Characteristics (MAD_DIMM_CH0_0_0_0_MCHBAR)	00000000h
5010h	4	Channel 1 DIMM Characteristics (MAD_DIMM_CH1_0_0_0_MCHBAR)	00000000h
5024h	4	Channel Hash (CHANNEL_HASH_0_0_0_MCHBAR)	00000000h
5028h	4	Channel Enhanced Hash (CHANNEL_EHASH_0_0_0_MCHBAR)	00000000h
5040h	4	GT Request Counter (PWM_GT_REQCOUNT_0_0_0_MCHBAR)	00000000h
5044h	4	IA Request Counter (PWM_IA_REQCOUNT_0_0_0_MCHBAR)	00000000h
5048h	4	I/O Request Counter (PWM_IO_REQCOUNT_0_0_0_MCHBAR)	00000000h
5050h	4	Memory Read Request Counter (PWM_RDDATA_COUNT_0_0_0_MCHBAR)	00000000h
5054h	4	Memory Write Request Counter (PWM_WRDATA_COUNT_0_0_0_MCHBAR)	00000000h
5058h	4	Memory Command Request Counter (PWM_COMMAND_COUNT_0_0_0_MCHBAR)	00000000h
5060h	4	Self Refresh Mode Control (PM_SREF_CONFIG_0_0_0_MCHBAR)	00000200h
5088h	8	Address Compare for ECC Error Inject (ECC_INJ_ADDR_COMPARE_0_0_0_MCHBAR)	0000000000000000h
5090h	8	Remap Base (REMAPBASE_0_0_0_MCHBAR)	0000007FFFF00000h
5098h	8	Remap Limit (REMAPLIMIT_0_0_0_MCHBAR)	0000000000000000h
5158h	8	Address Mask for ECC Error Inject (ECC_INJ_ADDR_MASK_0_0_0_MCHBAR)	00000001FFFFFFFFh

Offset	Size (Bytes)	Register Name (Register Symbol)	Default Value
5400h	8	GFX-VT Base Address Register (GFXVTBAR_0_0_0_MCHBAR_NCU)	0000000000000000h
5408h	8	EDRAMBAR Base Address Register (EDRAMBAR_0_0_0_MCHBAR_NCU)	0000000000000000h
5410h	8	VT-d VC0 Base Address Register (VTDPVC0BAR_0_0_0_MCHBAR_NCU)	0000000000000000h
5418h	4	Interrupt Redirection Control (INTRDIRCTL_0_0_0_MCHBAR_NCU)	00000000h
6A40h	8	IA Exclusion IMR Base Address (IMRIAEXCBASE_MCHBAR_CBO_INGRESS)	0000000000000000h
6A48h	8	IA Exclusion IMR Limit Address (IMRIAEXCLIMIT_MCHBAR_CBO_INGRESS)	0000000000000000h
6A50h	8	GT Exclusion IMR Base Address (IMRGTEXCBASE_MCHBAR_CBO_INGRESS)	0000000000000000h
6A58h	8	GT Exclusion IMR Limit Address (IMRGTEXCLIMIT_MCHBAR_CBO_INGRESS)	0000000000000000h

3.2.2 PRE Command Timing (TC_PRE_0_0_0_MCHBAR) — Offset 4000h

DDR timing constraints related to PRE commands

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 4000h	18863808h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:24	18h RW/L	**tWRPRE Timing Parameter (TWRPRE):** Holds DDR timing parameter tWRPRE. WR to PRE same bank minimum delay in tCK cycles. Supported range is 18-159. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
23:21	4h RW/L	**tPPD Timing Parameter (TPPD):** Holds DDR timing parameter tPPD (for LPDDR4 only). PRE/PREALL to PRE/PREALL (same rank) minimum delay in tCK cycles. This parameter is ignored for non LPDDR4 DRAM technology. Supported range is 4-7. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
20:16	06h RW/L	**tRDPRE Timing Parameter (TRDPRE):** Holds DDR timing parameter tRDPRE. RD to PRE same bank minimum delay in tCK cycles. Supported range is 6-15 **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG

Bit Range	Default & Access	Field Name (ID): Description
15:9	1Ch RW/L	**tRAS Timing Parameter (TRAS):** Holds DDR timing parameter tRAS. ACT to PRE same bank minimum delay in tCK cycles. For DDR/LPDDR Supported range is 28-90 **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
8:6	0h RW/L	**tRPab_ext Timing Parameter (TRPAB_EXT):** Holds the value of tRPab-tRPpb for LPDDR in tCK cycles. LPDDR technologies requires a longer time from PREALL to ACT vs. PRE to ACT, the offset between the two should be programmed to this field. When using DDR4 this field should be programmed to 0. For LPDDR4 the following restrictions apply: For single/dual rank sub channels tRP-tRPab_ext > 6. For three/four ranks sub channels tRP-tRPab_ext > 8. Supported range is 0-6. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
5:0	08h RW/L	**tRP Timing Parameter (TRP):** Holds DDR timing parameter tRP (and tRCD). PRE to ACT same bank minimum delay in tCK cycles. ACT to CAS (RD or WR) same bank minimum delay in tCK cycles. Supported range is 8-59. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG

3.2.3 ACT Command Timing (TC_ACT_0_0_0_MCHBAR) — Offset 4004h

DDR timing constraints related to ACT commands

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 4004h	01088410h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:27	0h RO	**Reserved**
26:21	08h RW/L	**tRCD_wr Timing Parameter (TRCD_WR):** Holds DDR timing parameter tRCD for writes in tCK cycles. This field should be configured to be the same as TC_PRE_0_0_0_MCHBAR.tRP. Supported range is 8-59 **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
20:18	2h RW/L	**Derating Extensions (DERATING_EXT):** Holds LPDDR timing parameters derating tRAS, tRRD, tRP and tRCD in tCK cycles. When LPDDR is hot, this value is added to the appropriate timing parameters. For non LP devices program the field to 0. Supported range is 0-4. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG

Bit Range	Default & Access	Field Name (ID): Description
17:13	04h RW/L	**tRRD Different Group (TRRD_DG):** Holds DDR timing parameter tRRD. ACT to ACT (different bank group in DDR4) minimum delay in tCK cycles. Supported range is 4-22. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
12:8	04h RW/L	**tRRD Same Group (TRRD_SG):** Holds DDR timing parameter tRRD/tRRD_L. For LPDDR3 program tRRD, for DDR4 program tRRD_L. ACT to ACT (same bank group in DDR4) minimum delay in tCK cycles. Supported range is 4-22. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
7	0h RO	**Reserved**
6:0	10h RW/L	**tFAW Timing Parameter (TFAW):** Holds DDR timing parameter tFAW (four activates window). In tCK cycles. Supported range is 16-88. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG

3.2.4 RD to RD Timings (TC_RDRD_0_0_0_MCHBAR) — Offset 400Ch

DDR timing constraints related to timing between read and read transactions

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 400Ch	04040404h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:30	0h RO	**Reserved**
29:24	04h RW/L	**tRDRD Different DIMM (TRDRD_DD):** Minimum delay from RD to RD to the other DIMM in tCK cycles Supported range is 4-54. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
23:22	0h RO	**Reserved**
21:16	04h RW/L	**tRDRD Different Rank (TRDRD_DR):** Minimum delay from RD to RD to the other rank in the same DIMM in tCK cycles Supported range is 4-54. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
15:14	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
13:8	04h RW/L	**tRDRD Different Group (TRDRD_DG):** DDR4: Minimum delay from RD to RD to the different bank group in tCK cycles Supported range is 4-54. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
7:6	0h RO	**Reserved**
5:0	04h RW/L	**tRDRD Same Group (TRDRD_SG):** DDR4: Minimum delay from RD to RD to the same bank group in tCK cycles Supported range is 4-54. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG

3.2.5 RD to WR Timings (TC_RDWR_0_0_0_MCHBAR) — Offset 4010h

DDR timing constraints related to timing between read and write transactions

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 4010h	04040404h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:30	0h RO	**Reserved**
29:24	04h RW/L	**tRDWR Different DIMM (TRDWR_DD):** Minimum delay from RD to WR to the other DIMM in tCK cycles Supported range is 4-54. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
23:22	0h RO	**Reserved**
21:16	04h RW/L	**tRDWR Different Rank (TRDWR_DR):** Minimum delay from RD to WR to the other rank in the same DIMM in tCK cycles Supported range is 4-54. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
15:14	0h RO	**Reserved**
13:8	04h RW/L	**tRDWR Different Group (TRDWR_DG):** DDR4: Minimum delay from RD to WR to the different bank group in tCK cycles Supported range is 4-54. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
7:6	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
5:0	04h RW/L	**tRDWR Same Group (TRDWR_SG):** DDR4: Minimum delay from RD to WR to the same bank group in tCK cycles Supported range is 4-54. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG

3.2.6 WR to RD Timings (TC_WRRD_0_0_0_MCHBAR) — Offset 4014h

DDR timing constraints related to timing between write and read transactions

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 4014h	04040404h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:30	0h RO	**Reserved**
29:24	04h RW/L	**tWRRD Different DIMM (TWRRD_DD):** Minimum delay from WR to RD to the other DIMM in tCK cycles Supported range is 4-54. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
23:22	0h RO	**Reserved**
21:16	04h RW/L	**tWRRD Different Rank (TWRRD_DR):** Minimum delay from WR to RD to the other rank in the same DIMM in tCK cycles Supported range is 4-54. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
15	0h RO	**Reserved**
14:8	04h RW/L	**tWRRD Different Group (TWRRD_DG):** DDR4: Minimum delay from WR to RD to the different bank group in tCK cycles Supported range is 4-65. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
7:0	04h RW/L	**tWRRD Same Group (TWRRD_SG):** DDR4: Minimum delay from WR to RD to the same bank group in tCK cycles Supported range is 4-145. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG

3.2.7 WR to WR Timings (TC_WRWR_0_0_0_MCHBAR) — Offset 4018h

DDR timing constraints related to timing between write and write transactions

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 4018h	04040404h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:30	0h RO	**Reserved**
29:24	04h RW/L	**tWRWR Different DIMM (TWRWR_DD):** Minimum delay from WR to WR to the other DIMM in tCK cycles Supported range is 4-54. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
23:22	0h RO	**Reserved**
21:16	04h RW/L	**tWRWR Different Rank (TWRWR_DR):** Minimum delay from WR to WR to the other rank in the same DIMM in tCK cycles Supported range is 4-54. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
15:14	0h RO	**Reserved**
13:8	04h RW/L	**tWRWR Different Group (TWRWR_DG):** DDR4: Minimum delay from WR to WR to the different bank group in tCK cycles Supported range is 4-54. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
7:6	0h RO	**Reserved**
5:0	04h RW/L	**tWRWR Same Group (TWRWR_SG):** DDR4: Minimum delay from WR to WR to the same bank group in tCK cycles Supported range is 4-54. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG

3.2.8 Roundtrip Latency (SC_ROUNDTRIP_LATENCY_0_0_0_MCHBAR) — Offset 4020h

Read Round-trip latency per rank

Type	Size	Offset	Default
MMIO	64 bit	MCHBAR + 4020h	1919191919191919h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
63	0h RO	**Reserved**
62:56	19h RW/L	**Rank 7 Latency (RANK_7_LATENCY):** Latency from read command to rank 7 until first data chunk return to MC in QCLK cycles Supported range is 19-120. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
55	0h RO	**Reserved**
54:48	19h RW/L	**Rank 6 Latency (RANK_6_LATENCY):** Latency from read command to rank 6 until first data chunk return to MC in QCLK cycles Supported range is 19-120. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
47	0h RO	**Reserved**
46:40	19h RW/L	**Rank 5 Latency (RANK_5_LATENCY):** Latency from read command to rank 5 until first data chunk return to MC in QCLK cycles Supported range is 19-120. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
39	0h RO	**Reserved**
38:32	19h RW/L	**Rank 5 Latency (RANK_4_LATENCY):** Latency from read command to rank 4 until first data chunk return to MC in QCLK cycles Supported range is 19-120. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
31	0h RO	**Reserved**
30:24	19h RW/L	**Rank 3 Latency (RANK_3_LATENCY):** Latency from read command to rank 3 until first data chunk return to MC in QCLK cycles Supported range is 19-120. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
23	0h RO	**Reserved**
22:16	19h RW/L	**Rank 2 Latency (RANK_2_LATENCY):** Latency from read command to rank 2 until first data chunk return to MC in QCLK cycles Supported range is 19-120. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG

Bit Range	Default & Access	Field Name (ID): Description
15	0h RO	**Reserved**
14:8	19h RW/L	**Rank 1 Latency (RANK_1_LATENCY):** Latency from read command to rank 1 until first data chunk return to MC in QCLK cycles Supported range is 19-120. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
7	0h RO	**Reserved**
6:0	19h RW/L	**Rank 0 Latency (RANK_0_LATENCY):** Latency from read command to rank 0 until first data chunk return to MC in QCLK cycles Supported range is 19-120. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG

3.2.9 ECC Debug Control (ECC_DEBUG_0_0_0_MCHBAR) — Offset 4034h

This register defines ECC Debug features

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 4034h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:5	0h RO	**Reserved**
4	0h RW/L	**ECC Correction Disable (ECC_CORRECTION_DISABLE):** When set, disables ECC correction. In this mode the memory controller reports any error type as uncorrectable. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_DFT
3	0h RO	**Reserved**
2:0	0h RW/L	**Error Injection Mode (ECC_INJECT):** ECC error inject options: • 000b: No ECC error injection. • 001b: Inject correctable ECC error on ECC_INJ_ADDR_COMPARE register match. • 011b: Inject correctable ECC error on ECC error insertion counter. • 101b: Inject non-recoverable ECC error on ECC_INJ_ADDR_COMPARE register match (same as on poison) • 111b: Inject non-recoverable ECC error on ECC error insertion counter (same as on poison) **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_DFT

3.2.10 ECC Error Log 0 (ECCERRLOG0_0_0_0_MCHBAR) — Offset 4048h

This register logs ECC error information.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 4048h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:29	0h RO/V/P	**ERRBANK:** This field holds the Bank Address of the read transaction that had the ECC error.
28:27	0h RO/V/P	**ERRRANK:** This field holds the Rank ID of the read transaction that had the ECC error.
26:24	0h RO/V/P	**ERRCHUNK:** Holds the chunk number of the error stored in the register.
23:16	00h RO/V/P	**ERRSYND:** This field contains the error syndrome. A value of 0xFF indicates that the error is due to poisoning.
15:2	0h RO	**Reserved**
1	0h RO/V/P	**MERRSTS:** This bit is set when an uncorrectable multiple-bit error occurs on a memory read data transfer. When this bit is set, the address that caused the error and the error syndrome are also logged and they are locked until this bit is cleared. This bit is cleared when the corresponding bit in 0.0.0.PCI.ERRSTS is cleared.
0	0h RO/V/P	**Single Bit Error Status (CERRSTS):** This bit is set when a correctable single-bit error occurs on a memory read data transfer. When this bit is set, the address that caused the error and the error syndrome are also logged and they are locked to further single bit errors, until this bit is cleared. A multiple bit error that occurs after this bit is set will override the address/error syndrome information. This bit is cleared when the corresponding bit in 0.0.0.PCI.ERRSTS is cleared.

3.2.11 ECC Error Log 0 (ECCERRLOG1_0_0_0_MCHBAR) — Offset 404Ch

This register logs ECC error information.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 404Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31	0h RO	**Reserved**
30:29	0h RO/V/P	**Error Bank Group (ERRBANKGROUP):** This field holds the DRAM bank group address of the read transaction that had the ECC error.
28:17	000h RO/V/P	**Error Column (ERRCOL):** This field holds the DRAM column address of the read transaction that had the ECC error.
16:0	00000h RO/V/P	**Error Row (ERRROW):** This field holds the DRAM row (page) address of the read transaction that had the ECC error.

3.2.12 Power Down Timing (TC_PWRDN_0_0_0_MCHBAR) — Offset 4050h

DDR timing constraints related to power down

Type	Size	Offset	Default
MMIO	64 bit	MCHBAR + 4050h	0000000404440404h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:40	0h RO	**Reserved**
39:32	04h RW/L	**TWRPDEN:** Holds DDR timing parameter tWRPDEN. WR to power down minimum delay in tCK cycles. Supported range is 4-159. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
31	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
30:24	04h RW/L	**tRDPDEN Timing Parameter (TRDPDEN):** Holds DDR timing parameter for tRDPDEN. RD to power down minimum delay in tCK cycles. Supported range is 4-95. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
23:22	1h RW/L	**tPRPDEN Timing Parameter (TPRPDEN):** Holds DDR timing parameter tPRPDEN. PRE to power down minimum delay in tCK cycles. Supported range is 1-3. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
21:16	04h RW/L	**tXP Timing Parameter (TXPDLL):** Holds DDR timing parameter tXP. Power up to RD/WR minimum delay in tCK cycles Applicable for DDR4 in case of exit from PPD when DRAM is configured to slow-exit mode Supported range is 4-63. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
15:13	0h RO	**Reserved**
12:8	04h RW/L	**tXP Timing Parameter (TXP):** Holds DDR timing parameter tXP. Power up to any command minimum delay in tCK cycles. Supported range is 4-16. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
7:5	0h RO	**Reserved**
4:0	04h RW/L	**tCKE Timing Parameter (TCKE):** Holds DDR timing parameter tCKE. Power down to power up (and vice versa) minimum delay in tCK cycles. Note that for LPDDR4 this value is also used for tCKCKEL and tCKELCMD. For LPDDR4 tSR (minimum self refresh time) is calculated to be tCKE*2. Supported range is 4-16. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG

3.2.13 ODT Command Timing (TC_ODT_0_0_0_MCHBAR) — Offset 4070h

ODT timing related parameters

Type	Size	Offset	Default
MMIO	64 bit	MCHBAR + 4070h	0000000001850000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:28	0h RO	**Reserved**
27:22	06h RW/L	**tCWL Timing Parameter (TCWL):** Holds DDR timing parameter tCWL (sometimes referred to as tWCL). Write command to data delay in tCK cycles. Supported range is 4-34 (maximum is for 1N mode) For LPDDR4 the minimum supported value is 4. For DDR4 the minimum supported value is 5. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
21:16	05h RW/L	**tCL Timing Parameter (TCL):** Holds DDR timing parameter tCL. Read command to data delay in tCK cycles. Supported range is 4-36 (but only up to 31 for DDR3). **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
15:0	0h RO	**Reserved**

3.2.14 ODT Matrix (SC_ODT_MATRIX_0_0_0_MCHBAR) — Offset 4080h

ODT matrix (enabled using SC_GS_CFG_0_0_0_MCHBAR.enable_odt_matrix

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 4080h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:28	0h RW/L	**Write Rank 3 (WRITE_RANK_3):** Indicate which ranks should terminate when writing to rank 3 (bits 3:0 correspond to ODT pins 3:0.) **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
27:24	0h RW/L	**Write Rank 2 (WRITE_RANK_2):** Indicate which ranks should terminate when writing to rank 2 (bits 3:0 correspond to ODT pins 3:0). **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG

Bit Range	Default & Access	Field Name (ID): Description
23:20	0h RW/L	**Write Rank 1 (WRITE_RANK_1):** Indicate which ranks should terminate when writing to rank 1 (bits 3:0 correspond to ODT pins 3:0). **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
19:16	0h RW/L	**Write Rank 0 (WRITE_RANK_0):** Indicate which ranks should terminate when writing to rank 0 (bits 3:0 correspond to ODT pins 3:0), **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
15:12	0h RW/L	**Read Rank 3 (READ_RANK_3):** Indicate which ranks should terminate when reading from rank 3 (bits 3:0 correspond to ODT pins 3:0) Note that according to DRAM spec the target rank should not be terminated. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
11:8	0h RW/L	**Read Rank 2 (READ_RANK_2):** Indicate which ranks should terminate when reading from rank 2 (bits 3:0 correspond to ODT pins 3:0) Note that according to DRAM spec the target rank should not be terminated. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
7:4	0h RW/L	**Read Rank 1 (READ_RANK_1):** Indicate which ranks should terminate when reading from rank 1 (bits 3:0 correspond to ODT pins 3:0) Note that according to DRAM spec the target rank should not be terminated. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
3:0	0h RW/L	**Read Rank 0 (READ_RANK_0):** Indicate which ranks should terminate when reading from rank 0 (bits 3:0 correspond to ODT pins 3:0) Note that according to DRAM spec the target rank should not be terminated. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG

3.2.15 Scheduler Configuration (SC_GS_CFG_0_0_0_MCHBAR) — Offset 4088h

this register is used for Scheduler configuration

Type	Size	Offset	Default
MMIO	64 bit	MCHBAR + 4088h	0000000000001020h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:34	0h RO	**Reserved**
33:32	0h RW/L	**DDR4 1 DIMM Per Channel (DDR4_1DPC):** Performance optimization for 1 DIMM Per Channel (1DPC) with dual rank. To be used only with Intel Memory reference Code as there are several low level configurations to enable it. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG

Bit Range	Default & Access	Field Name (ID): Description
31	0h RW/L	**Gear2 Mode (GEAR2):** Indicate that MC is working in Gear-2 (Qclk is half the data transfer clock of the DRAM) **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
30	0h RW/L	**No Gear2 Param Divide (NO_GEAR2_PARAM_DIVIDE):** Don't do RU[param/2] for DRAM timing parameters when in gear-2, treat the value given in them in DCLKs instead of tCK clocks. For extending the existing ranges (mainly for Overclocking). **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
29:28	0h RW/L	**x8 Device (X8_DEVICE):** DIMM is made out of X8 devices LSB is for DIMM 0, MSB is for DIMM 1. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
27:15	0h RO	**Reserved**
14:12	1h RW/L	**tCPDED Timing Parameter (TCPDED):** Holds DDR timing parameter tCPDED. Power down to command bus tri-state delay in tCK cycles (for DDR4) Supported range is 1-7 in 1N mode. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
11:8	0h RW/L	**Address Mirror (ADDRESS_MIRROR):** DIMM routing causes address mirroring For DDR4: bit 0: DIMM 0 (rank 1 bus is mirrored) bit 1: DIMM 1 (rank 3 bus is mirrored) For LPDDR4 bit 0: Sub channel 0 ranks 0 and 2 CA bus is mirrored. bit 1: Sub channel 1 ranks 0 and 2 CA bus is mirrored. bit 2: Sub channel 0 ranks 1 and 3 CA bus is mirrored. bit 3: Sub channel 1 ranks 1 and 3 CA bus is mirrored. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
7:5	1h RW/L	**N to 1 Ratio (N_TO_1_RATIO):** When using N:1 command stretch mode, every how many B2B valid command cycles a bubble is required Supported range is 1 to 7 **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
4:3	0h RW/L	**CMD Stretch (CMD_STRETCH):** Command stretch mode: 00 - 1N 01 - 2N 10 - 3N 11 - N:1 Notice that in Gear2 MC uses only the low phase of Dclk for commands, effectively doing a 2N by default. setting 2N in Gear2 will result in 4N at DDR interface **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
2:0	0h RO	**Reserved**

3.2.16 MR4 Rank Temperature (LPDDR_MR4_RANK_TEMPERATURE_0_0_0_MCHBAR) — Offset 4224h

This register holds the latest MR4 read per rank and used to determine the required refresh rate and thermal conditions of the DRAMs.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 4224h	03030303h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:27	0h RO	**Reserved**
26:24	3h RW/V/L	**Rank 3 (RANK_3):** Rank 3 refresh rate. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_PWR_MNGMENT
23:19	0h RO	**Reserved**
18:16	3h RW/V/L	**Rank 2 (RANK_2):** Rank 2 refresh rate. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_PWR_MNGMENT
15:11	0h RO	**Reserved**
10:8	3h RW/V/L	**Rank 1 (RANK_1):** Rank 1 refresh rate. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_PWR_MNGMENT
7:3	0h RO	**Reserved**
2:0	3h RW/V/L	**Rank 0 (RANK_0):** Rank 0 refresh rate. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_PWR_MNGMENT

3.2.17 DDR4 Temperature (DDR4_MPR_RANK_TEMPERATURE_0_0_0_MCHBAR) — Offset 4228h

This register holds the latest temperature read per rank and used to determine the required refresh rate and thermal conditions of the DRAMs.

Encodings are:

0: Cold (below 45C), single refresh rate required, DRAM may drop refreshes if allowed

1: Normal operating temperature (45C-85C), single refresh rate, DRAM may drop refreshes if double rate refreshes are given

2: Hot (Above 85C), double refresh rate

3: Reserved

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 4228h	01010101h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:26	0h RO	**Reserved**
25:24	1h RW/V/L	**Rank 3 (RANK_3):** Rank 3 refresh rate **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_PWR_MNGMENT
23:18	0h RO	**Reserved**
17:16	1h RW/V/L	**Rank 2 (RANK_2):** Rank 2 refresh rate **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_PWR_MNGMENT
15:10	0h RO	**Reserved**
9:8	1h RW/V/L	**Rank 1 (RANK_1):** Rank 1 refresh rate **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_PWR_MNGMENT
7:2	0h RO	**Reserved**
1:0	1h RW/V/L	**Rank 0 (RANK_0):** Rank 0 refresh rate **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_PWR_MNGMENT

3.2.18 Refresh Parameters (TC_RFP_0_0_0_MCHBAR) — Offset 4238h

Refresh parameters

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 4238h	4600980Fh

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:25	23h RW/L	**tREFI x9 (TREFIX9):** Maximum time allowed between refreshes to a rank (in intervals of 1024 DCLK cycles). Should be programmed to 8 * tREFI / 1024 (to allow for possible delays from ZQ or ISOC). **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
24:17	0h RO	**Reserved**
16	0h RW/L	**tREFI Counter While MC Refresh (COUNTTREFIWHILEREFENOFF):** Setting this bit will enable tREFI counter while MC refresh enable is not set. Sometimes refresh enable bit is cleared in order to block maintenance operations. MC may want to accumulate refresh debt at that time, setting this bit enable it. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
15:12	9h RW/L	**Refresh Panic Threshold (REFRESH_PANIC_WM):** tREFI count level in which the refresh priority is panic (default is 9). The Maximum value for this field is 9. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
11:8	8h RW/L	**Refresh Priority Threshold (REFRESH_HP_WM):** tREFI count level that turns the refresh priority to high (default is 8) **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
7:0	0Fh RW/L	**Rank Idle (OREF_RI):** Rank idle period that defines an opportunity for refresh, in DCLK cycles **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG

3.2.19 Refresh Timing Parameters (TC_RFTP_0_0_0_MCHBAR) — Offset 423Ch

Refresh timing parameters

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 423Ch	00B41004h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:26	0h RO	**Reserved**
25:16	0B4h RW/L	**tRFC Timing Parameter (TRFC):** Time of refresh: from beginning of refresh until next ACT or refresh is allowed (in tCK cycles, default is 180) **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
15:0	1004h RW/L	**tREFI Timing Parameter (TREFI):** Defines the average period between refreshes and the rate that tREFI counter is incremented (in DCLK cycles). It is suggested to set tREFI to a 2.8% lower value than the JEDEC spec. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG

3.2.20 Self-Refresh Timing Parameters (TC_SRFTP_0_0_0_MCHBAR) — Offset 4240h

Self-refresh timing parameters

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 4240h	00000200h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:12	0h RO	**Reserved**
11:0	200h RW/L	**tXSDLL Timing Parameter (TXSDLL):** Delay between DDR SR exit and the first command that requires data RD/WR from DDR. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG

3.2.21 Refresh Stagger Control (MC_REFRESH_STAGGER_0_0_0_MCHBAR) — Offset 4244h

Refresh stagger control

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 4244h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:13	0h RO	**Reserved**
12	0h RW/L	**Refresh Stagger Mode (REF_STAGGER_MODE):** This bit sets the refresh staggering mode 0b: Per DIMM refresh stagger. 1b: Per channel refresh stagger. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
11	0h RW/L	**Refresh Stagger Enable (REF_STAGGER_EN):** When set, this bit enables refresh staggering **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
10:0	000h RW/L	**Refresh Interval (REF_INTERVAL):** Refresh Interval period in DCLKS **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG

3.2.22 ZQCAL Control (TC_ZQCAL_0_0_0_MCHBAR) — Offset 4248h

ZQCAL control.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 4248h	32010000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:20	320h RW/L	**TZQCAL:** LPDDR4 tZQCAL in tCK cycles. Should typically be set to 1usec **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
19:10	040h RW/L	**TZQCS:** For DDR4 holds tCK value in DCLK cycles. For LPDDR4 holds tZQLAT in DCLK cycles **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
9:0	0h RO	**Reserved**

3.2.23 Memory Controller Initial State (MC_INIT_STATE_0_0_0_MCHBAR) — Offset 4254h

Holds information on available ranks

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 4254h	0000000Fh

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:8	0h RO	**Reserved**
7:0	0Fh RW/L	**Rank Occupancy (RANK_OCCUPANCY):** Indicates which ranks are occupied in the system. Non-enhanced channels (DDR4): • Bit 0: Rank 0 • Bit 1: Rank 1 • Bit 2: Rank 2 • Bit 3: Rank 3 Enhanced channels (LPDDR4): • Bit 0: Rank 0 = Sub channel 0 Rank 0 • Bit 1: Rank 1 = Sub channel 0 Rank 1 • Bit 2: Rank 2 = Sub channel 1 Rank 0 • Bit 3: Rank 3 = Sub channel 1 Rank 1 • Bit 4: Sub channel 0 Rank 2 • Bit 5: Sub channel 0 Rank 3 • Bit 6: Sub channel 1 Rank 2 • Bit 7: Sub channel 1 Rank 3 Note: Default on reset is all ranks enabled due to DDRIO requirements, BIOS MRC will write these bits to the proper values after reset based on the actual rank configuration. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG

3.2.24 DIMM Idle Energy (PM_DIMM_IDLE_ENERGY_0_0_0_MCHBAR) — Offset 4260h

This register defines the energy of an idle DIMM with CKE on.

Each 6-bit field corresponds to an integer multiple of the base DRAM command energy for that DIMM.

There are 2 6-bit fields, one per DIMM.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 4260h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:14	0h RO	**Reserved**
13:8	00h RW/L	**DIMM1 Idle Energy (DIMM1_IDLE_ENERGY):** This register defines the energy consumed by DIMM1 for one clock cycle when the DIMM is idle with CKE on. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_PWR_MNGMENT
7:6	0h RO	**Reserved**
5:0	00h RW/L	**DIMM0 Idle Energy (DIMM0_IDLE_ENERGY):** This register defines the energy consumed by DIMM0 for one clock cycle when the DIMM is idle with CKE on. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_PWR_MNGMENT

3.2.25 DIMM Power-Down Energy (PM_DIMM_PD_ENERGY_0_0_0_MCHBAR) — Offset 4264h

This register defines the energy of an idle DIMM with CKE off.

Each 6-bit field corresponds to an integer multiple of the base DRAM command energy for that DIMM.

There are 2 6-bit fields, one per DIMM.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 4264h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:14	0h RO	**Reserved**
13:8	00h RW/L	**DIMM1 Power-Down Energy (DIMM1_PD_ENERGY):** This register defines the energy consumed by DIMM1 for one clock cycle when the DIMM is idle with CKE off. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_PWR_MNGMENT

Bit Range	Default & Access	Field Name (ID): Description
7:6	0h RO	**Reserved**
5:0	00h RW/L	**DIMM0 Power-Down Energy (DIMM0_PD_ENERGY):** This register defines the energy consumed by DIMM0 for one clock cycle when the DIMM is idle with CKE off. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_PWR_MNGMENT

3.2.26 DIMM ACT Energy (PM_DIMM_ACT_ENERGY_0_0_0_MCHBAR) — Offset 4268h

This register defines the combined energy contribution of activate and precharge commands.

Each 8-bit field corresponds to an integer multiple of the base DRAM command energy for that DIMM.

There are 2 8-bit fields, one per DIMM.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 4268h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:16	0h RO	**Reserved**
15:8	00h RW/L	**DIMM1 ACT Energy (DIMM1_ACT_ENERGY):** This register defines the combined energy contribution of activate and precharge commands. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_PWR_MNGMENT
7:0	00h RW/L	**DIMM0 ACT Energy (DIMM0_ACT_ENERGY):** This register defines the combined energy contribution of activate and precharge commands. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_PWR_MNGMENT

3.2.27 DIMM RD Energy (PM_DIMM_RD_ENERGY_0_0_0_MCHBAR) — Offset 426Ch

This register defines the energy contribution of a read CAS command.

Each 8-bit field corresponds to an integer multiple of the base DRAM command energy for that DIMM.

There are 2 8-bit fields, one per DIMM.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 426Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:16	0h RO	**Reserved**
15:8	00h RW/L	**DIMM1 RD Energy (DIMM1_RD_ENERGY):** This register defines the energy contribution of a read CAS command. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_PWR_MNGMENT
7:0	00h RW/L	**DIMM0 RD Energy (DIMM0_RD_ENERGY):** This register defines the energy contribution of a read CAS command. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_PWR_MNGMENT

3.2.28 DIMM WR Energy (PM_DIMM_WR_ENERGY_0_0_0_MCHBAR) — Offset 4270h

This register defines the energy contribution of a write CAS command.

Each 8-bit field corresponds to an integer multiple of the base DRAM command energy for that DIMM.

There are 2 8-bit fields, one per DIMM.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 4270h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:16	0h RO	**Reserved**
15:8	00h RW/L	**DIMM1 WR Energy (DIMM1_WR_ENERGY):** This register defines the energy contribution of a write CAS command. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_PWR_MNGMENT

Bit Range	Default & Access	Field Name (ID): Description
7:0	00h RW/L	**DIMM0 WR Energy (DIMM0_WR_ENERGY):** This register defines the energy contribution of a write CAS command. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_PWR_MNGMENT

3.2.29 ECC Inject Count (ECC_INJECT_COUNT_0_0_0_MCHBAR) — Offset 4274h

This register defines the count of write chunks (64-bit data packets) until the next ECC error injection in case ECC_inject field in ECC_DEBUG_CONFIG is 110b or 111b. The count is of chunks in order to allow creating ECC errors on different 64-bit chunks

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 4274h	FFFFFFFFh

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:0	FFFFFFFFh RW/L	**Chunk Count (COUNT):** Chunk count for error inject **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_DFT

3.2.30 WR Delay (SC_WR_DELAY_0_0_0_MCHBAR) — Offset 4278h

This register defines the number of cycles decreased/increased from tCWL (TC_ODT_0_0_0_MCHBAR.tCWL) in Dclks.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 4278h	00000003h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:13	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
12	0h RW/L	**Add 1 Qclk delay (ADD_1QCLK_DELAY):** In Gear2, MC QCLK is actually tCK of the DDR, the regular MC register can only set even number of cycles (working in Dclk == 2 * tCK), this bit gives an option to delay the write data by one tCK **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
11:6	00h RW/L	**Increased To tCWL (ADD_TCWL):** The number of cycles (DCLK) increased to tCWL. Make sure tCWL + Add_tCWL doesn't overflow. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
5:0	03h RW/L	**Decreased From tCWL (DEC_TCWL):** The number of cycles (DCLK) decreased from tCWL. Configuring this number to be larger than tCWL is invalid **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG

3.2.31 Per Bank Refresh (SC_PBR_0_0_0_MCHBAR) — Offset 4288h

Per Bank Refresh parameters

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 4288h	0000F011h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:20	0h RO	**Reserved**
19:10	03Ch RW/L	**tRFCpb Timing Parameter (TRFCPB):** Refresh time in tCK for REFpb **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
9:4	01h RW/L	**Per Bank Refresh Exit on Idle Count (PBR_EXIT_ON_IDLE_CNT):** Number of tREFI cycles to count before switching PBR off for better clock gating. A value of 0 means no Idle exit. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
3	0h RW/L	**Per Bank Refresh Disable on Hot (PBR_DISABLE_ON_HOT):** Disable PBR when LP4 is at 0.25xtREFI condition **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
2	0h RO	**Reserved**
1	0h RW/L	**Per Bank Refresh Out-of-Order Disable (PBR_OOO_DIS):** Disable out of order scheduling of banks for LP4 **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG
0	1h RW/L	**Per Bank Refresh Disable (PBR_DISABLE):** Disable PBR (per bank refresh) for LP4 (DDR4 force PBR off) **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG

3.2.32 Miscellaneous Timing Constrains (TC_LPDDR4_MISC_0_0_0_MCHBAR) — Offset 4294h

Miscellaneous timing constrains

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 4294h	00000056h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:7	0h RO	**Reserved**
6:0	56h RW/L	**tOSCO Timing Parameter (TOSCO):** Delay between DQS_OSC counter stop to MR18/19 read **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG

3.2.33 Self-Refresh Exit Timing Parameters (TC_SREXITTP_0_0_0_MCHBAR) — Offset 42C4h

Self-refresh exit (SRX) timing parameters

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 42C4h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:10	0h RO	**Reserved**
9:0	000h RW/L	**tXSR Timing Parameter (TXSR):** Exit self refresh to valid commands delay. in LP4 configure this parameter for tXSR or tXSR abort if used. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG

3.2.34 Miscellaneous Control Register (MCMNTS_SPARE_0_0_0_MCHBAR) — Offset 43FCh

Miscellaneous control register.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 43FCh	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:14	0h RO	**Reserved**
13:12	0h RW/L	**Decoder Extended Bank Hashing (DECODER_EBH):** Enable address decoder Extended bank hashing. Bit 0: Enable XaB Bit 1: Enable XbB **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_DFT
11	0h RO	**Reserved**
10	0h RW/L	**Disable Low Refresh Rate (DISLOWREFRATE):** Don't allow refresh rate lower than 1X **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_DFT
9	0h RW/L	**Force x4 Refreshes (FORCEX4REF):** Force accelerated refreshes, four times the refresh number. Should be mutually exclusive with ForceX2Ref and ForceX8Ref. Constant X4 refreshes may block channel from entering self refresh. In case of staggered refreshes and fully occupied channel it can cause performance degradation. Use with caution. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_DFT
8	0h RW/L	**Force x2 Refreshes (FORCEX2REF):** Force accelerated refreshes, twice the refresh number. Should be mutually exclusive with ForceX4Ref and ForceX8Ref. Constant x2 refreshes may block channel from entering self refresh. In case of staggered refreshes and fully occupied channel it can cause a performance degradation. Use with caution. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_DFT
7:0	0h RO	**Reserved**

3.2.35 Inter-Channel Decode Parameters (MAD_INTER_CHANNEL_0_0_0_MCHBAR) — Offset 5000h

This register holds parameters used by the channel decode stage.

It defines virtual channel L mapping, as well as channel S size.

Also defined is the DDR type installed in the system (what DDR/LPDDR type is used).

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 5000h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:20	0h RO	**Reserved**
19:12	00h RW/L	**Channel S Size (CH_S_SIZE):** Channel S size in multiplies of 0.5GB. Supported range is 0GB - 64GB. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_ADDR_MAP
11:5	0h RO	**Reserved**
4	0h RW/L	**Channel L Mapping (CH_L_MAP):** Channel L mapping to physical channel. 0b: Channel 0 1b: Channel 1 **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_ADDR_MAP
3	0h RW/L	**Enhanced Channel Mode (ECHM):** Enhanced channel mode for LPDDR4 indicate that the channel operates as two 32bit channels instead of one 64bit channel. In this mode DIMM 0 is mapped to DQ bits 31:0 and DIMM 1 is mapped to DQ bits 63:32. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_ADDR_MAP
2:0	0h RW/L	**DDR Type (DDR_TYPE):** Defines the DDR type: 0: DDR4 3: LPDDR4 Other values are reserved **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_ADDR_MAP

3.2.36 Intra-Channel 0 Decode Parameters (MAD_INTRA_CH0_0_0_0_MCHBAR) — Offset 5004h

This register holds parameters used by the DRAM decode stage.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 5004h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:14	0h RO	**Reserved**
13:12	0h RW/L	**ECC Channel Configuration (ECC):** 0: No ECC active in the channel. 1: ECC is active in IO, ECC logic is not active. 2: ECC is disabled in IO, but ECC logic is enabled. 3: ECC active in both IO and ECC logic. Notes: • This field must be programmed identically for all populated channels. • In a system with ECC this field must be programmed to 1 during training and then 3 before transitioning from training mode to Normal mode. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_ADDR_MAP
11:9	0h RO	**Reserved**
8	0h RW/L	**Enhanced Interleaving Mode (EIM):** 0b: Disabled 1b: Enabled **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_ADDR_MAP
7:5	0h RO	**Reserved**
4	0h RW/L	**Rank Interleaving (RI):** Rank interleaving enable bit 0: Disabled 1: Enabled **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_ADDR_MAP
3:1	0h RO	**Reserved**
0	0h RW/L	**DIMM L Mapping (DIMM_L_MAP):** Virtual DIMM L mapping to physical DIMM 0b: DIMM0 1b: DIMM1 **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_ADDR_MAP

3.2.37 Intra-Channel 1 Decode Parameters (MAD_INTRA_CH1_0_0_0_MCHBAR) — Offset 5008h

This register holds parameters used by the DRAM decode stage.

Note: Bit definitions are the same as MAD_INTRA_CH0_0_0_0_MCHBAR, offset 5004h.

3.2.38 Channel 0 DIMM Characteristics (MAD_DIMM_CH0_0_0_0_MCHBAR) — Offset 500Ch

This register defines the channel DIMM characteristics - number of DIMMs, number of ranks, size and type.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 500Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:30	0h RO	**Reserved**
29	0h RW/L	**DLS BG0 on Bit 11 (DLS_BG0_ON_BIT_11):** when set, BG[0] will be placed on bit 11 of the channel address instead of bit 6. CAS[7] will take zone address 6. 0b: CAS[7] = zoneaddr[11], BG[0] = zoneaddr[6]. 1b: CAS[7] = zoneaddr[6], BG[0] = zoneaddr[11]. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_ADDR_MAP
28	0h RO	**Reserved**
27:26	0h RW/L	**DIMM S Number of Ranks (DSNOR):** DIMM S number of ranks 0b: 1 Rank 1b: 2 Ranks **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_ADDR_MAP
25:24	0h RW/L	**DIMM S Width (DSW):** Width of DDR chips 0: X8 chips 1: X16 chips 2: X32 chips 3: Reserved **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_ADDR_MAP
23	0h RO	**Reserved**
22:16	00h RW/L	**DIMM S Size (DIMM_S_SIZE):** Size of DIMM S in 0.5GB multiples. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_ADDR_MAP
15:11	0h RO	**Reserved**
10:9	0h RW/L	**DIMM L Number of Ranks (DLNOR):** 0: 1 Rank 1: 2 Ranks In ERM (enhanced rank mode): 2: 3 ranks 3: 4 ranks **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_ADDR_MAP

Bit Range	Default & Access	Field Name (ID): Description
8:7	0h RW/L	**DIMM L Width (DLW):** DIMM L width of DDR chips 0: X8 chips 1: X16 chips 2: X32 chips 3: Reserved **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_ADDR_MAP
6:0	00h RW/L	**DIMM L Size (DIMM_L_SIZE):** Size of DIMM L in 0.5GB multiples **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_ADDR_MAP

3.2.39 Channel 1 DIMM Characteristics (MAD_DIMM_CH1_0_0_0_MCHBAR) — Offset 5010h

This register defines the channel DIMM characteristics - number of DIMMs, number of ranks, size and type.

Note: Bit definitions are the same as MAD_DIMM_CH0_0_0_0_MCHBAR, offset 500Ch.

3.2.40 Channel Hash (CHANNEL_HASH_0_0_0_MCHBAR) — Offset 5024h

This register defines the MC channel selection function.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 5024h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:29	0h RO	**Reserved**
28	0h RW/L	**Hash Mode (HASH_MODE):** Encoding: 0: Use address bit-6 for channel selection. 1: Use the channel hash function as defined in the other fields of this register. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_ADDR_MAP
27	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
26:24	0h RW/L	**Hash LSB Mask Bit (HASH_LSB_MASK_BIT):** This field specifies the MC Channel interleave bit. The following encoding is used: 0: Addr[6] 1: Addr[7] 2: Addr[8] 3: Addr[9] 4: Addr[10] 5: Addr[11] 6: Addr[12] 7: Addr[13] For example, setting this field to 2 will interleave the channels at a 4 cacheline granularity. BIOS should set this field same as the lowest selected bit in the Mask field of this register. Note that if the Mask field does not include the corresponding interleave bit, it will still be included in the XOR function by the MC decoding logic. **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_ADDR_MAP
23:20	0h RO	**Reserved**
19:6	0000h RW/L	**Hash Mask (HASH_MASK):** The 14-bit mask corresponds to memory request Addr[19:6]. Setting a mask bit to 1 will include that particular address bit in the channel XOR function. For example, if the mask is set to 0C04h, then Channel = Addr[17] Addr[16] Addr[8] **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_ADDR_MAP
5:0	0h RO	**Reserved**

3.2.41 Channel Enhanced Hash (CHANNEL_EHASH_0_0_0_MCHBAR) — Offset 5028h

This register defines the MC Enhanced channel selection function.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 5028h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:29	0h RO	**Reserved**
28	0h RW/L	**Enhanced Hash Mode (EHASH_MODE):** Encoding: 0: Use address bit-6 for channel selection. 1: Use the channel Ehash function as defined in the other fields of this register **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_ADDR_MAP

Bit Range	Default & Access	Field Name (ID): Description
27	0h RO	**Reserved**
26:24	0h RW/L	**Enhanced Hash LSB Mask Bit (EHASH_LSB_MASK_BIT):** This specifies the MC Enhanced Channel interleave bit. The following encoding is used: • 000b: Addr[6] • 001b: Addr[7] • 010b: Addr[8] • 011b: Addr[9] • 100b: Addr[10] • 101b: Addr[11] • 110b: Addr[12] • 111b: Addr[13] For example, setting this field to 10b will interleave the sub channels at a 4 cache line granularity. BIOS should set this field same as the lowest selected bit in the Mask field of this register. Note that if the Mask field does not include the corresponding interleave bit, it will still be included in the XOR function by the MC decoding logic. The addresses above refer to channel addresses. When both channels are populated with sub-channels, addresses in this field that are higher than the HASH_LSB_MASK_BIT (defined in CHANNEL_HASH register) are one bit higher in physical address. Examples: • HASH_LSB_MASK_BIT = 0x2: physical Addr[8] • EHASH_LSB_MASK_BIT = 0x2: channel address[8], physical address [9] **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_ADDR_MAP
23:20	0h RO	**Reserved**
19:6	0000h RW/L	**Enhanced Hash Mask (EHASH_MASK):** The 14 bit mask corresponds to memory request Addr[19:6]. Setting a mask bit to 1 will include that particular address bit in the channel XOR function. For example, if the mask is set to 0C04h, then Channel = Addr[17] Addr[16] Addr[8]. The addresses above refer to channel addresses. When both channels are populated with sub-channels, addresses in this field that are higher than the HASH_LSB_MASK_BIT (defined in CHANNEL_HASH register) are one bit higher in physical address. Examples: • HASH_LSB_MASK_BIT = 0x2: physical Addr[8] • EHASH_LSB_MASK_BIT=0x2: channel address[8], physical address [9] **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_ADDR_MAP
5:0	0h RO	**Reserved**

3.2.42 GT Request Counter (PWM_GT_REQCOUNT_0_0_0_MCHBAR) — Offset 5040h

Counts every read/write request entering the Memory Controller to DRAM (sum of all channels) from the GT engine. Each partial write request counts as a request incrementing this counter. However same-cache-line partial write requests are combined to a single 64-byte data transfers from DRAM. Therefore multiplying the number of requests by 64-bytes will lead to inaccurate GT memory bandwidth. The inaccuracy is proportional to the number of same-cache-line partial writes combined.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 5040h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RW/V/L	**Request Count (COUNT):** Number of accesses **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_PWR_MNGMENT

3.2.43 IA Request Counter (PWM_IA_REQCOUNT_0_0_0_MCHBAR) — Offset 5044h

Counts every read/write request (demand and HW prefetch) entering the Memory Controller to DRAM (sum of all channels) from IA. Each partial write request counts as a request incrementing this counter. However same-cache-line partial write requests are combined to a single 64-byte data transfers from DRAM. Therefore multiplying the number of requests by 64-bytes will lead to inaccurate IA memory bandwidth. The inaccuracy is proportional to the number of same-cache-line partial writes combined.

Note: Bit definitions are the same as PWM_GT_REQCOUNT_0_0_0_MCHBAR, offset 5040h.

3.2.44 I/O Request Counter (PWM_IO_REQCOUNT_0_0_0_MCHBAR) — Offset 5048h

Counts every read/write request entering the Memory Controller to DRAM (sum of all channels) from all IO sources (e.g. PCIe, Display Engine, USB audio, etc.). Each partial write request counts as a request incrementing this counter. However same-cache-line partial write requests are combined to a single 64-byte data transfers from DRAM. Therefore multiplying the number of requests by 64-bytes will lead to inaccurate IO memory bandwidth. The inaccuracy is proportional to the number of same-cache-line partial writes combined.

Note: Bit definitions are the same as PWM_GT_REQCOUNT_0_0_0_MCHBAR, offset 5040h.

3.2.45 Memory Read Request Counter (PWM_RDDATA_COUNT_0_0_0_MCHBAR) — Offset 5050h

Counts every read (RdCAS) issued by the Memory Controller to DRAM (sum of all channels). All requests result in 64-byte data transfers from DRAM. Use for accurate memory bandwidth calculations.

Note: Bit definitions are the same as PWM_GT_REQCOUNT_0_0_0_MCHBAR, offset 5040h.

3.2.46 Memory Write Request Counter (PWM_WRDATA_COUNT_0_0_0_MCHBAR) — Offset 5054h

Counts every write (WrCAS) issued by the Memory Controller to DRAM (sum of all channels). All requests result in 64-byte data transfers from DRAM. Use for accurate memory bandwidth calculations.

Note: Bit definitions are the same as PWM_GT_REQCOUNT_0_0_0_MCHBAR, offset 5040h.

3.2.47 Memory Command Request Counter (PWM_COMMAND_COUNT_0_0_0_MCHBAR) — Offset 5058h

Counts every command issued by the Memory Controller to DRAM (sum of all channels).

Use for accurate memory bandwidth calculations.

Note: Bit definitions are the same as PWM_GT_REQCOUNT_0_0_0_MCHBAR, offset 5040h.

3.2.48 Self Refresh Mode Control (PM_SREF_CONFIG_0_0_0_MCHBAR) — Offset 5060h

Defines if and when DDR can go into Self Refresh

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 5060h	00000200h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:16	0h RO	**Reserved**
15:0	0200h RW/V/L	**Idle Timer (IDLE_TIMER):** This value is used when the SREF_enable field is set. It defines the number of cycles that there should not be any transaction in order to enter self-refresh. Supported range is 512 to 64K-1 **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_PWR_MNGMENT

3.2.49 Address Compare for ECC Error Inject (ECC_INJ_ADDR_COMPARE_0_0_0_MCHBAR) — Offset 5088h

Address compare for ECC error inject.

Error injection is issued when ECC_Inj_Addr_Compare[32:0] = ADDR[38:6] AND ECC_Inj_Addr_Mask[32:0]

Type	Size	Offset	Default
MMIO	64 bit	MCHBAR + 5088h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:33	0h RO	**Reserved**
32:0	000000000h RW/L	**ADDRESS:** Inject error when ECC_Inj_Addr_Compare[32:0] == ADDR[38:6] and ECC_Inj_Addr_Mask[31:0] **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_DFT

3.2.50 Remap Base (REMAPBASE_0_0_0_MCHBAR) — Offset 5090h

The value in this register defines the lower boundary of the Remap window.

The Remap window is inclusive of this address.

In the decoder A[19:0] of the Remap Base Address are assumed to be 0's.

Thus the bottom of the defined memory range will be aligned to a 1MB boundary.

When the value in this register is greater than the value programmed into the Remap Limit register, the Remap window is disabled.

These bits are Intel TXT lockable.

Type	Size	Offset	Default
MMIO	64 bit	MCHBAR + 5090h	0000007FFFF00000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
38:20	7FFFFh RW	**Remap Base Address (REMAPBASE):** The value in this register defines the lower boundary of the Remap window. The Remap window is inclusive of this address. In the decoder Address[19:0] of the Remap Base Address are assumed to be 0's. Thus the bottom of the defined memory range will be aligned to a 1MB boundary. When the value in this register is greater than the value programmed into the Remap Limit register, the Remap window is disabled. These bits are Intel TXT lockable.
19:0	0h RO	**Reserved**

3.2.51 Remap Limit (REMAPLIMIT_0_0_0_MCHBAR) — Offset 5098h

The value in this register defines the upper boundary of the Remap window.

The Remap window is inclusive of this address.

In the decoder Address[19:0] of the Remap Limit Address are assumed to be F's.

Thus the top of the defined range will be one byte less than a 1MB boundary.

When the value in this register is less than the value programmed into the Remap Base register, the Remap window is disabled.

These Bits are Intel TXT lockable.

Type	Size	Offset	Default
MMIO	64 bit	MCHBAR + 5098h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:20	00000h RW	**Remap Limit (REMAPLMT):** The value in this register defines the upper boundary of the Remap window. The Remap window is inclusive of this address. In the decoder Address[19:0] of the Remap Limit Address are assumed to be F's. Thus the top of the defined range will be one byte less than a 1MB boundary. When the value in this register is less than the value programmed into the Remap Base register, the Remap window is disabled. These Bits are Intel TXT lockable.
19:0	0h RO	**Reserved**

3.2.52 Address Mask for ECC Error Inject (ECC_INJ_ADDR_MASK_0_0_0_MCHBAR) — Offset 5158h

Address compare for ECC error inject. Error injection is issued when

ECC_Inj_Addr_Compare[32:0] = ADDR[38:6] AND ECC_Inj_Addr_Mask[32:0]

Type	Size	Offset	Default
MMIO	64 bit	MCHBAR + 5158h	00000001FFFFFFFFh

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:33	0h RO	**Reserved**
32:0	1FFFFFFFFh RW/L	**ADDRESS:** Inject error when ECC_INJ_ADDR_COMPARE_0_0_0_MCHBAR[32:0] = ADDR[38:6] AND ECC_INJ_ADDR_MASK_0_0_0_MCHBAR[32:0] **Locked by:** MC_LOCK_0_0_0_MCHBAR.LOCK_MC_DFT

3.2.53 GFX-VT Base Address Register (GFXVTBAR_0_0_0_MCHBAR_NCU) — Offset 5400h

This is the base address for the Graphics VT configuration space.

There is no physical memory within this 4KB window that can be addressed.

The 4KB reserved by this register does not alias to any PCI 2.3 compliant memory mapped space.

On reset, the GFX-VT configuration space is disabled and must be enabled by writing a 1 to GFX-VTBAREN.

All the bits in this register are locked in TXT mode.

BIOS programs this register after which the register cannot be altered.

Type	Size	Offset	Default
MMIO	64 bit	MCHBAR + 5400h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:12	0000000h RW/V	**GFX-VT BAR Base Address (GFXVTBAR):** This field corresponds to bits 38 to 12 of the base address GFX-VT configuration space. BIOS will program this register resulting in a base address for a 4KB block of contiguous memory address space. This register ensures that a naturally aligned 4KB space is allocated within the first 512GB of addressable memory space. System Software uses this base address to program the GFX-VT register set. All the Bits in this register are locked in TXT mode.
11:1	0h RO	**Reserved**
0	0h RW/V/L	**GFX-VT BAR Enable (GFXVTBAREN):** 0: GFX-VTBAR is disabled and does not claim any memory 1: GFX-VTBAR memory mapped accesses are claimed and decoded appropriately This bit will remain 0 if VTd capability is disabled. **Locked by:** CAPID0_A_0_0_0_PCI.VTDD

3.2.54 EDRAMBAR Base Address Register (EDRAMBAR_0_0_0_MCHBAR_NCU) — Offset 5408h

This is the base address for the EDRAM configuration space.

There is no physical memory within this 16KB window that can be addressed.

The 16KB reserved by this register does not alias to any PCI 2.3 compliant memory mapped space.

On reset, the EDRAM configuration space is disabled and must be enabled by writing a 1 to EDRAMBAREN.

EDRAMBAREN must be cleared and this register locked before normal operation is enabled.

BIOS programs this register after which the register cannot be altered.

All the bits in this register are locked in TXT mode.

Type	Size	Offset	Default
MMIO	64 bit	MCHBAR + 5408h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:14	0000000h RW/V	**EDRAM BAR Base Address (EDRAMBAR):** This field corresponds to bits 38 to 14 of the base address EDRAM configuration space. BIOS will program this register resulting in a base address for a 16KB block of contiguous memory address space. This register ensures that a naturally aligned 16KB space is allocated within the first 512GB of addressable memory space. System Software uses this base address to program the EDRAM register set. All the Bits in this register are locked in TXT mode.
13:1	0h RO	**Reserved**
0	0h RW/V	**EDRAM BAR Enable (EDRAMBAREN):** 0: EDRAMBAR is disabled and does not claim any memory 1: EDRAMBAR memory mapped accesses are claimed and decoded appropriately

3.2.55 VT-d VC0 Base Address Register (VTDPVC0BAR_0_0_0_MCHBAR_NCU) — Offset 5410h

This is the base address for the DMI/PCIe VC0 configuration space.

There is no physical memory within this 4KB window that can be addressed.

The 4KB reserved by this register does not alias to any PCI 2.3 compliant memory mapped space.

On reset, the DMI/PCIe VC0 configuration space is disabled and must be enabled by writing a 1 to VC0BAREN.

All the bits in this register are locked in TXT mode.

BIOS programs this register after which the register cannot be altered.

Type	Size	Offset	Default
MMIO	64 bit	MCHBAR + 5410h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:12	0000000h RW/V	**VT-d VC0 Base Address (VTVC0BAR):** This field corresponds to bits 38 to 12 of the base address DMI/PCIe VC0 configuration space. BIOS will program this register resulting in a base address for a 4KB block of contiguous memory address space. This register ensures that a naturally aligned 4KB space is allocated within the first 512GB of addressable memory space. System Software uses this base address to program the DMI/PCIe VC0 register set. All the Bits in this register are locked in TXT mode.
11:1	0h RO	**Reserved**
0	0h RW/V/L	**VT-d VC0 BAR Enable (VTVC0BAREN):** 0: VC0BAR is disabled and does not claim any memory 1: VC0BAR memory mapped accesses are claimed and decoded appropriately This bit will remain 0 if VTd capability is disabled. **Locked by:** CAPID0_A_0_0_0_PCI.VTDD

3.2.56 Interrupt Redirection Control (INTRDIRCTL_0_0_0_MCHBAR_NCU) — Offset 5418h

Interrupt Redirection Logic Control register is responsible for setting up schemes and controling the operation of the MSI redirection logic.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 5418h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:9	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
8:6	0h RW/V	**Hash Mode Control (HASHMODCTR):** Select the hash function for the Vector based Hash Mode interrupt redirection control: 000b: select bits 7:4/5:4 for vector cluster/flat algorithm 001b: select bits 6:3/4:3 010b: select bits 4:1/2:1 011b: select bits 3:0/1:0 Other values are reserved.
5	0h RW/V	**Logical Flat or Cluster Mode Override (LOGFLATCLUSTOVREN):** 0: IA32 Logical Flat or Cluster Mode bit is locked as Read only bit. 1: IA32 Logical Flat or Cluster Mode bit may be written by SW, values written by xTPR update are ignored. For one time override of the IA32 Logical Flat or Cluster Mode value, return this bit to its default state after the bit is changed. Leaving this bit as 1 will prevent automatic update of the filter.
4	0h RW/V/L	**Logical Flat or Logical Cluster Mode (LOGFLTCLUSTMOD):** Set by bios to indicate if the OS is running logical flat or logical cluster mode. This bit can also be updated by IntPrioUpd messages. This bit reflects the setup of the filter at any given time. 0: logical flat mode 1: logical cluster mode **Locked by:** INTRDIRCTL_0_0_0_MCHBAR_NCU.LOGFLATCLUSTOVREN
3	0h RW/V	**Cluster Check Sampling Mode (CLASTCHKSMPMOD):** 0: Disable checking for Logical_APICID[31:0] being non-zero when sampling flat/ cluster mode bit in the IntPrioUpd message as part of setting bit 1 in this register 1: Enable the above checking
2:0	0h RW/V	**Redirection Mode Select (RDRMODSEL):** Selects the redirection mode used for MSI interrupts with lowest-priority delivery mode. The following schemes are used: 000: Fixed Priority - select the first enabled APIC in the cluster. 001: Round robin - select the first enabled APIC in round robin manner from last selected APIC. 010: Hash Vector - select the first enabled APIC in rund robin manner starting form the hash of the vector number. 100: PAIR w/ Fixed-priority (deprecated, not supported) 101: PAIR w/ Round-robin (deprecated, not supported) 110: PAIR w/ Hash Vector (deprecated, not supported) Other values are Reserved

3.2.57 IA Exclusion IMR Base Address (IMRIAEXCBASE_MCHBAR_CBO_INGRESS) — Offset 6A40h

This register contains the base address of IA exclusion IMR.

Type	Size	Offset	Default
MMIO	64 bit	MCHBAR + 6A40h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:10	00000000h RW/L	**IA Exclusion IMR Base Address (IMRIAEXCBASE):** This register contains the base address of IA exclusion IMR. **Locked by:** IMRIAEXCBASE_MCHBAR_CBO_INGRESS.LOCK
9:1	0h RO	**Reserved**
0	0h RW/L	**LOCK:** This bit will lock all writable settings in this register, including itself. **Locked by:** IMRIAEXCBASE_MCHBAR_CBO_INGRESS.LOCK

3.2.58 IA Exclusion IMR Limit Address (IMRIAEXCLIMIT_MCHBAR_CBO_INGRESS) — Offset 6A48h

This register contains the limit address of IA exclusion IMR.

Type	Size	Offset	Default
MMIO	64 bit	MCHBAR + 6A48h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:10	00000000h RW/L	**IA Exclusion IMR Limit Address (IMRIAEXCLIMIT):** This register contains the limit address of IA exclusion IMR. **Locked by:** IMRIAEXCLIMIT_MCHBAR_CBO_INGRESS.LOCK
9:1	0h RO	**Reserved**
0	0h RW/L	**LOCK:** This bit will lock all writable settings in this register, including itself. **Locked by:** IMRIAEXCLIMIT_MCHBAR_CBO_INGRESS.LOCK

3.2.59 GT Exclusion IMR Base Address (IMRGTEXCBASE_MCHBAR_CBO_INGRESS) — Offset 6A50h

This register contains the base address of GT exclusion IMR.

Type	Size	Offset	Default
MMIO	64 bit	MCHBAR + 6A50h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:10	00000000h RW/L	**GT Exclusion IMR Base Address (IMRGTEXCBASE):** This register contains the base address of GT exclusion IMR. **Locked by:** IMRGTEXCBASE_MCHBAR_CBO_INGRESS.LOCK
9:1	0h RO	**Reserved**
0	0h RW/L	**LOCK:** This bit will lock all writable settings in this register, including itself. **Locked by:** IMRGTEXCBASE_MCHBAR_CBO_INGRESS.LOCK

3.2.60 GT Exclusion IMR Limit Address (IMRGTEXCLIMIT_MCHBAR_CBO_INGRESS) — Offset 6A58h

This register contains the limit address of GT exclusion IMR.

Type	Size	Offset	Default
MMIO	64 bit	MCHBAR + 6A58h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:10	00000000h RW/L	**GT Exclusion IMR Limit Address (IMRGTEXCLIMIT):** This register contains the limit address of GT exclusion IMR. **Locked by:** IMRGTEXCLIMIT_MCHBAR_CBO_INGRESS.LOCK

Bit Range	Default & Access	Field Name (ID): Description
9:1	0h RO	**Reserved**
0	0h RW/L	**LOCK:** This bit will lock all writable settings in this register, including itself. **Locked by:** IMRGTEXCLIMIT_MCHBAR_CBO_INGRESS.LOCK

3.3 Power Management (MCHBAR) Registers

This chapter documents the power management MCHBAR registers.

Base address of these registers are defined in the MCHBAR_0_0_0_PCI register in Bus: 0, Device: 0, Function: 0.

Note: These registers apply to all processors.

3.3.1 Summary of Registers

Table 3-4. Summary of MCHBAR Registers

Offset	Size (Bytes)	Register Name (Register Symbol)	Default Value
5824h	4	BIOS POST Code (BIOS_POST_CODE_0_0_0_MCHBAR_PCU)	00000000h
5828h	8	Cycle Sum of All Active Cores (PKG_IA_C0_ANY_SUM_0_0_0_MCHBAR_PCU)	0000000000000000h
5830h	8	Cycle Sum of Any Active Core (PKG_IA_C0_ANY_0_0_0_MCHBAR_PCU)	0000000000000000h
5838h	8	Cycle Sum of Active Graphics (PKG_GT_C0_ANY_0_0_0_MCHBAR_PCU)	0000000000000000h
5840h	8	Cycle Sum of Overlapping Active GT and Core (PKG_GT_AND_IA_OVERLAP_0_0_0_MCHBAR_PCU)	0000000000000000h
5848h	8	Cycle Sum of Any Active GT Slice (PKG_GT_C0_ANY_SLICE_0_0_0_MCHBAR_PCU)	0000000000000000h
5850h	8	Cycle Sum of All Active GT Slice (PKG_GT_C0_SLICES_SUM_0_0_0_MCHBAR_PCU)	0000000000000000h
5858h	8	Cycle Sum of Any GT Media Engine (PKG_GT_C0_ANY_MEDIA_0_0_0_MCHBAR_PCU)	0000000000000000h
5860h	8	Ratio Sum of Any Active Core (PKG_IA_C0_ANY_RATIO_0_0_0_MCHBAR_PCU)	0000000000000000h
5868h	8	Ratio Sum of Active GT (PKG_GT_C0_ANY_RATIO_0_0_0_MCHBAR_PCU)	0000000000000000h
5870h	8	Ratio Sum of Active GT Slice (PKG_GT_C0_ANY_SLICE_RATIO_0_0_0_MCHBAR_PCU)	0000000000000000h
58E0h	8	DDR Power Limit (DDR_RAPL_LIMIT_0_0_0_MCHBAR_PCU)	0000000000000000h
58F0h	4	Package RAPL Performance Status (PACKAGE_RAPL_PERF_STATUS_0_0_0_MCHBAR_PCU)	00000000h
58FCh	4	IA Performance Limit Reasons (IA_PERF_LIMIT_REASONS_0_0_0_MCHBAR_PCU)	00000000h
5900h	4	GT Performance Limit Reasons (GT_PERF_LIMIT_REASONS_0_0_0_MCHBAR_PCU)	00000000h
5918h	8	System Agent Performance Status (SA_PERF_STATUS_0_0_0_MCHBAR_PCU)	0000002000000000h
5920h	4	Primary Plane Turbo Policy (PRIP_TURBO_PLCY_0_0_0_MCHBAR_PCU)	00000000h
5924h	4	Secondary Plane Turbo Policy (SECP_TURBO_PLCY_0_0_0_MCHBAR_PCU)	00000010h
5928h	4	Primary Plane Energy Status (PRIP_NRG_STTS_0_0_0_MCHBAR_PCU)	00000000h
592Ch	4	Secondary Plane Energy Status (SECP_NRG_STTS_0_0_0_MCHBAR_PCU)	00000000h

Offset	Size (Bytes)	Register Name (Register Symbol)	Default Value
5938h	4	Package Power SKU Unit (PACKAGE_POWER_SKU_UNIT_0_0_0_MCHBAR_PCU)	000A0E03h
593Ch	4	Package Energy Status (PACKAGE_ENERGY_STATUS_0_0_0_MCHBAR_PCU)	00000000h
5948h	4	GT Performance Status (GT_PERF_STATUS_0_0_0_MCHBAR_PCU)	00000000h
5968h	4	Power Plane 0 Efficient Cycles (PP0_EFFICIENT_CYCLES_0_0_0_MCHBAR_PCU)	00000000h
596Ch	4	Power Plane 0 Thread Activity (PP0_THREAD_ACTIVITY_0_0_0_MCHBAR_PCU)	00000000h
597Ch	4	Primary Plane 0 Temperature (PP0_TEMPERATURE_0_0_0_MCHBAR_PCU)	00000000h
5994h	4	RP-State Limits (RP_STATE_LIMITS_0_0_0_MCHBAR_PCU)	000000FFh
5998h	4	RP-State Capability (RP_STATE_CAP_0_0_0_MCHBAR_PCU)	00000000h
599Ch	4	Temperature Target (TEMPERATURE_TARGET_0_0_0_MCHBAR_PCU)	00000000h
59A0h	8	Package Power Limit (PACKAGE_RAPL_LIMIT_0_0_0_MCHBAR_PCU)	0000000000000000h
59C0h	4	Thermal Status GT (THERM_STATUS_GT_0_0_0_MCHBAR_PCU)	08000000h
59C4h	4	Thermal Interrupt GT (THERM_INTERRUPT_GT_0_0_0_MCHBAR_PCU)	00000000h
59C8h	4	Device Idle Duration Override (DEVICE_IDLE_DURATION_OVERRIDE_0_0_0_MCHBAR_PCU)	00000000h
59F0h	8	Package GT C0 EUs SUM (PKG_GT_C0_EUS_SUM)	0000000000000000h
59F8h	8	Package GT C0 Media Sum (PKG_GT_C0_MEDIA_SUM)	0000000000000000h
5A08h	4	FIVR FFFC EMI Control (FFFC_EMI_CONTROL_0_0_0_MCHBAR_PCU)	00000000h
5A0Ch	4	FIVR FFFC RFI Control (FFFC_RFI_CONTROL_0_0_0_MCHBAR_PCU)	00000000h
5A18h	4	FIVR FFFC RFI Control 2 (FFFC_RFI_CONTROL2_0_0_0_MCHBAR_PCU)	00000000h
5D10h	8	Scratchpad Register (SSKPD_0_0_0_MCHBAR_PCU)	0000000000000000h
5DA0h	4	BIOS Mailbox Data (BIOS_MAILBOX_DATA_0_0_0_MCHBAR_PCU)	00000000h
5DA4h	4	BIOS Mailbox Interface (BIOS_MAILBOX_INTERFACE_0_0_0_MCHBAR_PCU)	00000000h
5DA8h	4	BIOS Reset Complete (BIOS_RESET_CPL_0_0_0_MCHBAR_PCU)	00000000h
5E00h	4	Memory Controller BIOS Request (MC_BIOS_REQ_0_0_0_MCHBAR_PCU)	00000000h
5E04h	4	Memory Controller BIOS Data (MC_BIOS_DATA_0_0_0_MCHBAR_PCU)	00000000h
5F00h	4	System Agent Power Management Control (SAPMCTL_0_0_0_MCHBAR_PCU)	00002106h
5F3Ch	4	Configurable TDP Nominal (CONFIG_TDP_NOMINAL_0_0_0_MCHBAR_PCU)	00000000h
5F40h	8	Configurable TDP Level 1 (CONFIG_TDP_LEVEL1_0_0_0_MCHBAR_PCU)	0000000000000000h
5F48h	8	Configurable TDP Level 1 (CONFIG_TDP_LEVEL2_0_0_0_MCHBAR_PCU)	0000000000000000h
5F50h	4	Configurable TDP Control (CONFIG_TDP_CONTROL_0_0_0_MCHBAR_PCU)	00000000h

Offset	Size (Bytes)	Register Name (Register Symbol)	Default Value
5F54h	4	Turbo Activation Ratio (TURBO_ACTIVATION_RATIO_0_0_0_MCHBAR_PCU)	00000000h
5F58h	4	Overclocking Status (OC_STATUS_0_0_0_MCHBAR_PCU)	00000000h
5F60h	8	Base Clock (BCLK) Frequency (BCLK_FREQ_0_0_0_MCHBAR)	0000000000000000h

3.3.2 BIOS POST Code (BIOS_POST_CODE_0_0_0_MCHBAR_PCU) — Offset 5824h

This register holds 32 writable bits with no functionality behind them.

BIOS writes the current POST code here (port 80).

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 5824h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RW	**POST Code (POSTCODE):** BIOS will write the current POST code in this field

3.3.3 Cycle Sum of All Active Cores (PKG_IA_C0_ANY_SUM_0_0_0_MCHBAR_PCU) — Offset 5828h

Sum the cycles per number of active cores

Type	Size	Offset	Default
MMIO	64 bit	MCHBAR + 5828h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:0	00000000 00000000h RO/V	**DATA:** The counter value is incremented as a function of the number of cores that reside in C0 and are active. If N cores are simultaneously in C0, then the number of clock ticks that are incremented is N. Counter rate is the Max Non-Turbo frequency (same as TSC).

3.3.4 Cycle Sum of Any Active Core (PKG_IA_C0_ANY_0_0_0_MCHBAR_PCU) — Offset 5830h

Sum the cycles of any active cores.

Type	Size	Offset	Default
MMIO	64 bit	MCHBAR + 5830h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:0	00000000 00000000h RO/V	**DATA:** This counter increments whenever one (or more) IA cores are active and in C0 state. Counter rate is the Max Non-Turbo frequency (same as TSC).

3.3.5 Cycle Sum of Active Graphics (PKG_GT_C0_ANY_0_0_0_MCHBAR_PCU) — Offset 5838h

Sum the cycles of activity of the GT.

Type	Size	Offset	Default
MMIO	64 bit	MCHBAR + 5838h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:0	00000000 00000000h RO/V	**DATA:** This counter increments whenever GT slices or un-slices are active and in C0 state. Counter rate is the Max Non-Turbo frequency (same as TSC).

3.3.6 Cycle Sum of Overlapping Active GT and Core (PKG_GT_AND_IA_OVERLAP_0_0_0_MCHBAR_PCU) — Offset 5840h

Sum the cycles of overlap time between any IA cores and GT.

Type	Size	Offset	Default
MMIO	64 bit	MCHBAR + 5840h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:0	00000000 00000000h RO/V	**DATA:** This counter increments whenever GT slices or un-slices are active and in C0 state and in overlap with one of the IA cores that is active and in C0 state. Counter rate is the Max Non-Turbo frequency (same as TSC).

3.3.7 Cycle Sum of Any Active GT Slice (PKG_GT_C0_ANY_SLICE_0_0_0_MCHBAR_PCU) — Offset 5848h

Sum the cycles of any active GT slice.

Type	Size	Offset	Default
MMIO	64 bit	MCHBAR + 5848h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:0	00000000 00000000h RO/V	**DATA:** This counter increments whenever a GT slice (one of more) is active. Counter rate is the Crystal clock.

3.3.8 Cycle Sum of All Active GT Slice (PKG_GT_C0_SLICES_SUM_0_0_0_MCHBAR_PCU) — Offset 5850h

Sum the cycles of the sum of all active GT slices.

Type	Size	Offset	Default
MMIO	64 bit	MCHBAR + 5850h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
63:0	00000000 00000000h RW/V/L	**DATA:** This counter increments by the sum of all active GT slices. Counter rate is the Crystal clock.

3.3.9 Cycle Sum of Any GT Media Engine (PKG_GT_C0_ANY_MEDIA_0_0_0_MCHBAR_PCU) — Offset 5858h

Sum the cycles of any media GT engine.

Type	Size	Offset	Default
MMIO	64 bit	MCHBAR + 5858h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
63:0	00000000 00000000h RW/V/L	**DATA:** This counter increments whenever any GT media engine is active. Counter rate is the Crystal clock.

3.3.10 Ratio Sum of Any Active Core (PKG_IA_C0_ANY_RATIO_0_0_0_MCHBAR_PCU) — Offset 5860h

Similar to PKG_IA_C0_ANY_0_0_0_MCHBAR_PCU, but increments in the P-State ratio of the cores.

Type	Size	Offset	Default
MMIO	64 bit	MCHBAR + 5860h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:0	00000000 00000000h RO/V	**DATA:** This counter increments whenever one or more IA cores are active and in C0 state. Counter rate is the Max Non-Turbo frequency (same as TSC)

3.3.11 Ratio Sum of Active GT (PKG_GT_C0_ANY_RATIO_0_0_0_MCHBAR_PCU) — Offset 5868h

Similar to PKG_GT_C0_ANY_0_0_0_MCHBAR_PCU, but increments in the RP-State ratio of the GT slice or un-slice.

Type	Size	Offset	Default
MMIO	64 bit	MCHBAR + 5868h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:0	00000000 00000000h RO/V	**DATA:** This counter increments whenever GT slices or un-slices are active and in C0 state. Counter rate is the Max Non-Turbo frequency (same as TSC)

3.3.12 Ratio Sum of Active GT Slice (PKG_GT_C0_ANY_SLICE_RATIO_0_0_0_MCHBAR_PCU) — Offset 5870h

Similar to PKG_GT_C0_ANY_SLICE_0_0_0_MCHBAR_PCU, but increments in the RP-State ratio of the GT slice.

Type	Size	Offset	Default
MMIO	64 bit	MCHBAR + 5870h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:0	00000000 00000000h RO/V	**DATA:** This counter increments whenever any GT slice is active. Counter rate is the Crystal clock.

3.3.13 DDR Power Limit (DDR_RAPL_LIMIT_0_0_0_MCHBAR_PCU) — Offset 58E0h

Allows software to set power limits for the DRAM domain and measurement attributes associated with each limit.

Type	Size	Offset	Default
MMIO	64 bit	MCHBAR + 58E0h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
63	0h RW/L	**LOCKED:** When set, this entire register becomes read-only. This bit will typically be set by BIOS during boot. **Locked by:** DDR_RAPL_LIMIT_0_0_0_MCHBAR_PCU.LOCKED
62:48	0h RO	**Reserved**
47	0h RW/L	**Power Limitation #2 Enable (LIMIT2_ENABLE):** Power Limit 2 (PL2) enable bit for DDR domain. **Locked by:** DDR_RAPL_LIMIT_0_0_0_MCHBAR_PCU.LOCKED
46:32	0000h RW/L	**Power Limitation #2 (LIMIT2_POWER):** Power Limit 2 (PL2) for DDR domain in Watts. Format is U11.3: Resolution 0.125W, Range 0-2047.875W. **Locked by:** DDR_RAPL_LIMIT_0_0_0_MCHBAR_PCU.LOCKED
31:24	0h RO	**Reserved**
23:22	0h RW/L	**Limitation #1 Time Window X (LIMIT1_TIME_WINDOW_X):** Power Limit 1 (PL1) time window X value, for DDR domain. Actual time window for RAPL is: (1/1024 seconds) * (1+(X/4)) * (2Y) **Locked by:** DDR_RAPL_LIMIT_0_0_0_MCHBAR_PCU.LOCKED
21:17	00h RW/L	**Limitation #1 Time Window Y (LIMIT1_TIME_WINDOW_Y):** Power Limit 1 (PL1) time window Y value, for DDR domain. Actual time window for RAPL is: (1/1024 seconds) * (1+(X/4)) * (2Y) **Locked by:** DDR_RAPL_LIMIT_0_0_0_MCHBAR_PCU.LOCKED
16	0h RO	**Reserved**
15	0h RW/L	**Power Limit 1 Enable (LIMIT1_ENABLE):** Power Limit 1 (PL1) enable bit for DDR domain. **Locked by:** DDR_RAPL_LIMIT_0_0_0_MCHBAR_PCU.LOCKED
14:0	0000h RW/L	**Power Limit 1 (LIMIT1_POWER):** Power Limit 1 (PL1) for DDR domain in Watts. Format is U11.3: Resolution 0.125W, Range 0-2047.875W. **Locked by:** DDR_RAPL_LIMIT_0_0_0_MCHBAR_PCU.LOCKED

3.3.14 Package RAPL Performance Status (PACKAGE_RAPL_PERF_STATUS_0_0_0_MCHBAR_PCU) — Offset 58F0h

Package RAPL Performance Status Register. This register provides information on the performance impact of the RAPL power limit and indicates the duration for processor went below the requested P-state due to package power constraint.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 58F0h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RO/V/P	**COUNTS:** Counter of the time units within which RAPL was limiting P-states. If limitation occurred anywhere within the time window of 1/1024 seconds, the count will be incremented (limitation on accuracy). This data can serve as a proxy for the potential performance impacts of RAPL on cores performance.

3.3.15 IA Performance Limit Reasons (IA_PERF_LIMIT_REASONS_0_0_0_MCHBAR_PCU) — Offset 58FCh

This register specifies the reasons for Core frequency throttling.

The first 16 bits are status bits. They change depending whether the specific throttling reason is active.

The remaining 16 bits are log bits. Once a status bit asserts, the matching log bit asserts as well but the latter stays high until cleared by software.

Software can write 0h to this register to clear the log bits.

Note: Throttling is reported only when the P-State request is higher than the current P-State.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 58FCh	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:30	0h RO	**Reserved**
29	0h RW/0C/V	**Turbo Attenuation Status (TURBO_ATTEN_LOG):** Indicates that the frequency has throttled due to rapid frequency changes that lead to a performance loss.
28	0h RW/0C/V	**Maximum Turbo Log (MAX_TURBO_LIMIT_LOG):** Indicates that the frequency has throttled due to exceeding turbo limits.

Bit Range	Default & Access	Field Name (ID): Description
27	0h RW/0C/V	**PL2/PL3 Status (PBM_PL2_LOG):** Indicates that the frequency has throttled due to exceeding PL2, PSysPL2, PL3 or PSysPL3 power limits.
26	0h RW/0C/V	**PL1 Log (PBM_PL1_LOG):** Indicates that the frequency has throttled due to exceeding PL1 or PSysPL1 power limits.
25	0h RW/0C/V	**FIVR Thermal Design Current Log (FIVR_TDC_LOG):** Indicates that the frequency has throttled due to exceeding the FIVR Thermal Design Current limit.
24	0h RW/0C/V	**Electrical Design Protection Log (EDP_LOG):** Indicates that the frequency has throttled due to exceeding the EDP limits. EDP limits are IccMax, PL4 and Voltage Limits.
23	0h RW/0C/V	**VR Thermal Design Current Log (VR_TDC_LOG):** Indicates that the frequency has throttled due to exceeding the VR Thermal Design Current limit.
22	0h RW/0C/V	**VR is Hot Log (VR_THERMALERT_LOG):** Indicates that the frequency has throttled due to a VR HOT event (any processor VR).
21	0h RW/0C/V	**Running Average Thermal Limit Log (RATL_LOG):** Indicates that the frequency has throttled due to RATL thermal throttling.
20	0h RO	**Reserved**
19	0h RW/0C/V	**PCS Log (PCS_LIMIT_LOG):** Indicates that the frequency has throttled due to exceeding PECI power limits.
18	0h RW/0C/V	**DDR Power Log (PBM_DDR_LOG):** Indicates that the frequency has throttled due to exceeding DDR power limits.
17	0h RW/0C/V	**Thermal Log (THERMAL_LOG):** Indicates that the frequency has throttled due to thermals reaching TjMax.
16	0h RW/0C/V	**PROCHOT# Log (PROCHOT_LOG):** Indicates that the frequency has throttled due to PROCHOT# assertion.
15:14	0h RO	**Reserved**
13	0h RO/V	**Turbo Attenuation Status (TURBO_ATTEN):** Indicates that the frequency is throttled due to rapid frequency changes that lead to a performance loss.
12	0h RO/V	**Maximum Turbo Status (MAX_TURBO_LIMIT):** Indicates that the frequency is throttled due to exceeding turbo limits.
11	0h RO/V	**PL2/3 Status (PBM_PL2):** Indicates that the frequency is throttled due to exceeding PL2, PSysPL2, PL3 or PSysPL3 power limits.
10	0h RO/V	**PL1 Status (PBM_PL1):** Indicates that the frequency is throttled due to exceeding PL1 or PSysPL1 power limits.
9	0h RO/V	**FIVR Thermal Design Current Status (FIVR_TDC):** Indicates that the frequency is throttled due to exceeding the FIVR Thermal Design Current limit.
8	0h RO/V	**Electrical Design Protection Status (EDP):** Indicates that the frequency is throttled due to exceeding the EDP limits. EDP limits are IccMax, PL4 and Voltage Limits.
7	0h RO/V	**VR Thermal Design Current Status (VR_TDC):** Indicates that the frequency is throttled due to exceeding the VR Thermal Design Current limit.

Bit Range	Default & Access	Field Name (ID): Description
6	0h RO/V	**VR is Hot Status (VR_THERMALERT):** Indicates that the frequency is throttled due to a VR HOT event (any processor VR).
5	0h RO/V	**Running Average Thermal Limit Status (RATL):** Indicates that the frequency is throttled due to RATL thermal throttling.
4	0h RO	**Reserved**
3	0h RO/V	**PCS Status (PCS_LIMIT):** Indicates that the frequency is throttled due to exceeding PECI power limits.
2	0h RO/V	**DDR Power Status (PBM_DDR):** Indicates that the frequency is throttled due to exceeding DDR power limits.
1	0h RO/V	**Thermal Status (THERMAL):** Indicates that the frequency is throttled due to thermals reaching TjMax.
0	0h RO/V	**PROCHOT# Status (PROCHOT):** Indicates that the frequency is throttled due to PROCHOT# assertion.

3.3.16 GT Performance Limit Reasons (GT_PERF_LIMIT_REASONS_0_0_0_MCHBAR_PCU) — Offset 5900h

This register specifies the reasons for GT frequency throttling.

The first 16 bits are status bits. They change depending whether the specific throttling reason is active.

The remaining 16 bits are log bits. Once a status bit asserts, the matching log bit asserts as well but the latter stays high until cleared by software.

Software can write 0h to this register to clear the log bits.

Note: Throttling is reported only when the RP-State request is higher than the current RP-State.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 5900h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RO	**Reserved**
30	0h RW/0C/V	**Minimum Supported Power Log (MSPE_LOG):** Indicates that the frequency has throttled due to the processor was running below the minimum supported power.

Bit Range	Default & Access	Field Name (ID): Description
29	0h RW/0C/V	**Maximum Turbo Log (MAX_TURBO_LIMIT_LOG):** Indicates that the frequency has throttled due to exceeding turbo limits. When GT has more than 1 slice, the additional slices may cause GT to operate at a lower frequency.
28	0h RW/0C/V	**Inefficient Operation Log (INEFFICIENT_OPERATION_LOG):** Indicates that the frequency has throttled due to efficiency concerns.
27	0h RW/0C/V	**PL2/PL3 Status (PBM_PL2_LOG):** Indicates that the frequency has throttled due to exceeding PL2, PSysPL2, PL3 or PSysPL3 power limits.
26	0h RW/0C/V	**PL1 Log (PBM_PL1_LOG):** Indicates that the frequency has throttled due to exceeding PL1 or PSysPL1 power limits.
25	0h RO	**Reserved**
24	0h RW/0C/V	**Electrical Design Protection Log (EDP_LOG):** Indicates that the frequency has throttled due to exceeding the EDP limits. EDP limits are IccMax, PL4 and Voltage Limits.
23	0h RW/0C/V	**VR Thermal Design Current Log (VR_TDC_LOG):** Indicates that the frequency has throttled due to exceeding the VR Thermal Design Current limit.
22	0h RW/0C/V	**VR is Hot Log (VR_THERMALERT_LOG):** Indicates that the frequency has throttled due to a VR HOT event (any processor VR).
21	0h RW/0C/V	**Running Average Thermal Limit Log (RATL_LOG):** Indicates that the frequency has throttled due to RATL thermal throttling.
20	0h RO	**Reserved**
19	0h RW/0C/V	**PCS Log (PCS_LIMIT_LOG):** Indicates that the frequency has throttled due to exceeding PECI power limits.
18	0h RW/0C/V	**DDR Power Log (PBM_LIMIT_LOG):** Indicates that the frequency has throttled due to exceeding DDR power limits.
17	0h RW/0C/V	**Thermal Log (THERMAL_LOG):** Indicates that the frequency has throttled due to thermals reaching TjMax.
16	0h RW/0C/V	**PROCHOT# Log (PROCHOT_LOG):** Indicates that the frequency has throttled due to PROCHOT# assertion.
15	0h RO	**Reserved**
14	0h RO/V	**Minimum Supported Power Status (MSPE):** Indicates that the frequency is throttled due to the processor is running below the minimum supported power.
13	0h RO/V	**Maximum Turbo Status (MAX_TURBO_LIMIT):** Indicates that the frequency is throttled due to exceeding turbo limits. When GT has more than 1 slice, the additional slices may cause GT to operate at a lower frequency.
12	0h RO/V	**Inefficient Operation Status (INEFFICIENT_OPERATION):** Indicates that the frequency is throttled due to efficiency concerns.
11	0h RO/V	**PL2/3 Status (PBM_PL2):** Indicates that the frequency is throttled due to exceeding PL2, PSysPL2, PL3 or PSysPL3 power limits.
10	0h RO/V	**PL1 Status (PBM_PL1):** Indicates that the frequency is throttled due to exceeding PL1 or PSysPL1 power limits.

Bit Range	Default & Access	Field Name (ID): Description
9	0h RO	**Reserved**
8	0h RO/V	**Electrical Design Protection Status (EDP):** Indicates that the frequency is throttled due to exceeding the EDP limits. EDP limits are IccMax, PL4 and Voltage Limits.
7	0h RO/V	**VR Thermal Design Current Status (VR_TDC):** Indicates that the frequency is throttled due to exceeding the VR Thermal Design Current limit.
6	0h RO/V	**VR is Hot Status (VR_THERMALERT):** Indicates that the frequency is throttled due to a VR HOT event (any processor VR).
5	0h RO/V	**Running Average Thermal Limit Status (RATL):** Indicates that the frequency is throttled due to RATL thermal throttling.
4	0h RO	**Reserved**
3	0h RO/V	**PCS Status (PCS_LIMIT):** Indicates that the frequency is throttled due to exceeding PECI power limits.
2	0h RO/V	**DDR Power Status (PBM_DDR):** Indicates that the frequency is throttled due to exceeding DDR power limits.
1	0h RO/V	**Thermal Status (THERMAL):** Indicates that the frequency is throttled due to thermals reaching TjMax.
0	0h RO/V	**PROCHOT# Status (PROCHOT):** Indicates that the frequency is throttled due to PROCHOT# assertion.

3.3.17 System Agent Performance Status (SA_PERF_STATUS_0_0_0_MCHBAR_PCU) — Offset 5918h

Indicates current various System Agent PLL ratios.

Operating frequency needs to be calculated according to reference clock (BCLK).

Type	Size	Offset	Default
MMIO	64 bit	MCHBAR + 5918h	0000002000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:56	0h RO	**Reserved**
55:40	0000h RO/V	**System Agent Voltage (SA_VOLTAGE):** Reports the System Agent voltage in u3.13 format. Conversion to Volts: V = SA_VOLTAGE / 8192.0

Bit Range	Default & Access	Field Name (ID): Description
39:32	20h RO/V	**PSF0 PLL Ratio (PSF0_RATIO):** Reports the PSF0 PLL ratio. The PSF0 frequency is: Ratio * 16.67MHz. The supported ratios are {32, 48, 64} = {533MHz, 800MHz, 1067MHz}.
31:24	00h RO/V	**RING UCLK PLL Ratio (UCLK_RATIO):** Used to calculate the ring's frequency. Ring Frequency = UCLK_RATIO * BCLK Notes: • BCLK is read from BCLK_FREQ_0_0_0_MCHBAR.BCLK_FREQ. Value is in KHz. • In the above formula, BCLK is in MHz.
23:18	00h RO/V	**IPU PS Ratio (IPU_PS_RATIO):** IPU PS RATIO. The frequency is 25MHz * Ratio.
17:12	00h RO/V	**IPU IS Divisor (IPU_IS_DIVISOR):** The frequency is 1600MHz/Divisor.
11	0h RO/V	**On Package Interface (OPI) Link Speed (OPI_LINK_SPEED):** 0: 2Gb/s 1: 4Gb/s
10	0h RO/V	**DDR QCLK Reference (QCLK_REFERENCE):** 0: 133.34Mhz. In frequency calculations use 400.0MHz/3.0. 1: 100.00Mhz
9:2	00h RO/V	**DDR QCLK Ratio (QCLK_RATIO):** Reference clock is determined by the QCLK_REFERENCE field. QCLK frequency calculation when QCLK_REFERENCE = 0 (133.34MHz): QCLK frequency = QCLK_RATIO * BCLK * 4.0 / 3.0 QCLK frequency calculation when QCLK_REFERENCE = 1 (100MHz): QCLK frequency = QCLK_RATIO * BCLK Notes: • BCLK is read from BCLK_FREQ_0_0_0_MCHBAR.BCLK_FREQ. Value is in KHz. • In the above formulas, BCLK is in MHz.
1:0	0h RO/V	**Last Display Engine Workpoint Request Served (LAST_DE_WP_REQ_SERVED):** Last display engine workpoint request served by the PCU

3.3.18 Primary Plane Turbo Policy (PRIP_TURBO_PLCY_0_0_0_MCHBAR_PCU) — Offset 5920h

The PRIMARY_PLANE_TURBO_POWER_POLICY and SECONDARY_PLANE_TURBO_POWER_POLICY are used together to balance the power budget between the two power planes.

The power plane with the higher policy will get a higher priority.

The default value will aim to maintain same ratio for IA and GT.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 5920h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:5	0h RO	**Reserved**
4:0	00h RW	**Priority Level (PRIPTP):** A higher number implies a higher priority.

3.3.19 Secondary Plane Turbo Policy (SECP_TURBO_PLCY_0_0_0_MCHBAR_PCU) — Offset 5924h

The PRIMARY_PLANE_TURBO_POWER_POLICY and SECONDARY_PLANE_TURBO_POWER_POLICY are used together to balance the power budget between the two power planes.

The power plane with the higher policy will get a higher priority. The default value will aim to maintain same ratio for IA and GT.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 5924h	00000010h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:5	0h RO	**Reserved**
4:0	10h RW	**Priority Level (SECPTP):** A higher number implies a higher priority.

3.3.20 Primary Plane Energy Status (PRIP_NRG_STTS_0_0_0_MCHBAR_PCU) — Offset 5928h

Reports total energy consumed.

The counter will wrap around and continue counting when it reaches its limit.

The energy status is reported in units which are defined in PACKAGE_POWER_SKU_UNIT_MSR[ENERGY_UNIT].

Software will read this value and subtract the difference from last value read.

The value of this register is updated every 1mSec.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 5928h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RO/V	**DATA:** Energy Value

3.3.21 Secondary Plane Energy Status (SECP_NRG_STTS_0_0_0_MCHBAR_PCU) — Offset 592Ch

Reports total energy consumed. The counter will wrap around and continue counting when it reaches its limit.

The energy status is reported in units which are defined in PACKAGE_POWER_SKU_UNIT_MSR[ENERGY_UNIT].

Software will read this value and subtract the difference from last value read. The value of this register is updated every 1mSec.

Note: Bit definitions are the same as PRIP_NRG_STTS_0_0_0_MCHBAR_PCU, offset 5928h.

3.3.22 Package Power SKU Unit (PACKAGE_POWER_SKU_UNIT_0_0_0_MCHBAR_PCU) — Offset 5938h

Defines units for calculating SKU power and timing parameters.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 5938h	000A0E03h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:20	0h RO	**Reserved**
19:16	Ah RO/V	**Time Unit (TIME_UNIT):** Time Units used for power control registers. The actual unit value is calculated by 1 s / Power(2, TIME_UNIT). The default value of Ah corresponds to 976 usec.
15:13	0h RO	**Reserved**
12:8	0Eh RO/V	**Energy Unit (ENERGY_UNIT):** Energy Units used for power control registers. The actual unit value is calculated by 1 J / Power(2, ENERGY_UNIT). The default value of 14 corresponds to Ux.14 number.
7:4	0h RO	**Reserved**
3:0	3h RO/V	**Power Unit (PWR_UNIT):** Power Units used for power control registers. The actual unit value is calculated by 1 W / Power(2, PWR_UNIT). The default value of 0011b corresponds to 1/8 W.

3.3.23 Package Energy Status (PACKAGE_ENERGY_STATUS_0_0_0_MCHBAR_PCU) — Offset 593Ch

Package energy consumed by the entire CPU (including IA, GT and uncore). The counter will wrap around and continue counting when it reaches its limit.

The energy status is reported in units which are defined in PACKAGE_POWER_SKU_UNIT_MSR[ENERGY_UNIT].

Note: Bit definitions are the same as PRIP_NRG_STTS_0_0_0_MCHBAR_PCU, offset 5928h.

3.3.24 GT Performance Status (GT_PERF_STATUS_0_0_0_MCHBAR_PCU) — Offset 5948h

This register reports GT's current P-States (for both slice and un-slice) and voltage.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 5948h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:29	0h RO	**Reserved**
28:20	000h RO/V	**Slices Ratio (SLICES_RATIO):** GT slices frequency: SLICES_RATIO * 16.666Mhz. When GT is in RC6 this frequency is zero.
19:11	000h RO/V	**Un-slice Ratio (UNSLICE_RATIO):** GT Un-slice frequency: UNSLICE_RATIO * 16.666Mhz. When GT is in RC6 this frequency is zero.
10:0	000h RO/V/P	**Slices Voltage (SLICES_VOLTAGE):** Slices and un-slice voltage in 2.5mV granularity.

3.3.25 Power Plane 0 Efficient Cycles (PP0_EFFICIENT_CYCLES_0_0_0_MCHBAR_PCU) — Offset 5968h

This register stores a value equal to the product of the number of BCLK cycles in which at least one of the IA cores was active and the efficiency score calculated by the PCU.

The efficiency score is a number between 0 and 1 that indicates the IAs efficiency.

Values exceeding 32b will wrap around.

This value is used in conjunction with PP0_ANY_THREAD_ACTIVITY to generate statistics for software.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 5968h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RO/V	**DATA:** Number of Cycles

3.3.26 Power Plane 0 Thread Activity (PP0_THREAD_ACTIVITY_0_0_0_MCHBAR_PCU) — Offset 596Ch

This register stores a value equal to the product of the number of BCLK cycles and the number of IA threads that are running.

Values exceeding 32b will wrap around.

This value is used in conjunction with PP0_ANY_THREAD_ACTIVITY to generate statistics for software.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 596Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RO/V	**DATA:** Number of Cycles.

3.3.27 Primary Plane 0 Temperature (PP0_TEMPERATURE_0_0_0_MCHBAR_PCU) — Offset 597Ch

PP0 (IA Cores) temperature in degrees (C).

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 597Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:8	0h RO	**Reserved**
7:0	00h RO/V	**DATA:** Temperature in degrees (C).

3.3.28 RP-State Limits (RP_STATE_LIMITS_0_0_0_MCHBAR_PCU) — Offset 5994h

This register allows software to limit the maximum frequency of the Integrated Graphics Engine (GT) allowed during run-time.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 5994h	000000FFh

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:8	0h RO	**Reserved**
7:0	FFh RW	**RP0 State Limit (RPSTT_LIM):** This field indicates the maximum frequency limit for the Integrated Graphics Engine (GT) allowed during run-time.

3.3.29 RP-State Capability (RP_STATE_CAP_0_0_0_MCHBAR_PCU) — Offset 5998h

This register contains the maximum base frequency capability for the Integrated Graphics Engine (GT).

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 5998h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:24	0h RO	**Reserved**
23:16	00h RW/P/L	**RPn Capability (RPN_CAP):** RPn is the lowest requestable RP state. This field indicates the RPn PLL ratio for the Integrated Graphics Engine (GT). Values are in units of 50 MHz (assuming BCLK = 100MHz).
15:8	00h RW/P/L	**RP1 Capability (RP1_CAP):** RP1 is the sustained RP state. This field indicates the RP1 PLL ratio for the Integrated Graphics Engine (GT). Values are in units of 50 MHz (assuming BCLK = 100MHz).

Bit Range	Default & Access	Field Name (ID): Description
7:0	00h RW/P/L	**RP0 Capability (RP0_CAP):** RP0 is the highest RP state. This field indicates the maximum RP0 PLL ratio for the Integrated Graphics Engine (GT). Values are in units of 50 MHz (assuming BCLK = 100MHz).

3.3.30 Temperature Target (TEMPERATURE_TARGET_0_0_0_MCHBAR_PCU) — Offset 599Ch

This register is a read-only copy of the TEMPERATURE_TARGET MSR (MSR 1A2h).

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 599Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RW/L	**LOCKED:** When set, this entire register becomes read-only. **Locked by:** TEMPERATURE_TARGET.LOCKED
30	0h RO	**Reserved**
29:24	00h RO/V	**TjMax Tcc Offset (TJ_MAX_TCC_OFFSET):** Temperature offset in degrees (C) from the TjMax. Used for throttling temperature. Will not impact temperature reading. If offset is allowed and set, the throttle will occur and reported at lower then TjMax. **Locked by:** TEMPERATURE_TARGET.LOCKED
23:16	00h RO/V	**Thermal Junction Maximum Temperature (TJMAX):** This field indicates the maximum junction temperature (TjMax), also referred to as the Throttle Temperature, TCC Activation Temperature or Prochot Temperature. This is the temperature at which the Adaptive Thermal Monitor is activated.
15:8	00h RO/V	**Fan Temperature Offset (FAN_TEMP_TARGET_OFST):** Fan Temperature Target Offset (a.k.a. T-Control) indicates the relative offset from the Thermal Monitor Trip Temperature at which fans should be engaged.
7	0h RO	**Reserved**
6:0	00h RO/V	**Tcc Offset Time Window (TCC_OFFSET_TIME_WINDOW):** Describes the RATL averaging time window **Locked by:** TEMPERATURE_TARGET.LOCKED

3.3.31 Package Power Limit (PACKAGE_RAPL_LIMIT_0_0_0_MCHBAR_PCU) — Offset 59A0h

Allows setting PL1 and PL2.

This register has an MSR version as well.

Power limits from this MMIO register and the MSR are evaluated separately.

Type	Size	Offset	Default
MMIO	64 bit	MCHBAR + 59A0h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
63	0h RW/L	**Package Limitation #2 Lock (PKG_PWR_LIM_LOCK):** When set, all settings in this register are locked and are treated as Read Only. This bit will typically set by BIOS during boot time or resume from Sx. **Locked by:** PACKAGE_RAPL_LIMIT_0_0_0_MCHBAR_PCU.PKG_PWR_LIM_LOCK
62:48	0h RO	**Reserved**
47	0h RW/L	**Package Limitation #2 Enable (PKG_PWR_LIM_2_EN):** This bit enables/disables Package Limitation #2 (PL2). 0b: Package Power Limit 2 is Disabled 1b: Package Power Limit 2 is Enabled **Locked by:** PACKAGE_RAPL_LIMIT_0_0_0_MCHBAR_PCU.PKG_PWR_LIM_LOCK
46:32	0000h RW/L	**Package Power Limitation #2 (PKG_PWR_LIM_2):** This field indicates the power limitation #2. The unit of measurement is defined in MSR PACKAGE_POWER_SKU_UNIT[PWR_UNIT]. **Locked by:** PACKAGE_RAPL_LIMIT_0_0_0_MCHBAR_PCU.PKG_PWR_LIM_LOCK
31:24	0h RO	**Reserved**
23:17	00h RW/L	**Package Limitation #1 Time Window (PKG_PWR_LIM_1_TIME):** Specifies the time window used to calculate average power for PL1 and PL2. The timing interval window is Floating Point number given by 1.x * power(2,y). x = PKG_PWR_LIM_1_TIME[23:22] y = PKG_PWR_LIM_1_TIME[21:17] The unit of measurement is defined in MSR PACKAGE_POWER_SKU_UNIT[TIME_UNIT]. The maximal time window is bounded by MSR PACKAGE_POWER_SKU[PKG_MAX_WIN]. The minimum time window is 1 unit of measurement (as defined above). **Locked by:** PACKAGE_RAPL_LIMIT_0_0_0_MCHBAR_PCU.PKG_PWR_LIM_LOCK
16	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
15	0h RW/L	**Package Power Limit 1 Enable (PKG_PWR_LIM_1_EN):** This bit enables/disables Package Power Limit 1. 0b: Package Power Limit 1 is Disabled 1b: Package Power Limit 1 is Enabled **Locked by:** PACKAGE_RAPL_LIMIT_0_0_0_MCHBAR_PCU.PKG_PWR_LIM_LOCK
14:0	0000h RW/L	**Package Power Limit 1 (PKG_PWR_LIM_1):** This field indicates the power limitation #1 (PL1). The unit of measurement is defined in PACKAGE_POWER_SKU_UNIT_MSR[PWR_UNIT]. **Locked by:** PACKAGE_RAPL_LIMIT_0_0_0_MCHBAR_PCU.PKG_PWR_LIM_LOCK

3.3.32 Thermal Status GT (THERM_STATUS_GT_0_0_0_MCHBAR_PCU) — Offset 59C0h

Contains status information about the processors thermal sensor and automatic thermal monitoring facilities.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 59C0h	08000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RO/V	**VALID:** This bit indicates that the TEMPERATURE field is valid. It is set by PCU if the temperature is within valid thermal sensor range.
30:27	1h RO	**RESOLUTION:** Supported resolution in degrees C.
26:23	0h RO	**Reserved**
22:16	00h RO/V	**TEMPERATURE:** This is a temperature offset in degrees C below the TjMax temperature. This number is meaningful only if VALID bit in this register is set.
15	0h RW/0C/V	**Cross Domain Limit Log (CROSS_DOMAIN_LIMIT_LOG):** If set (1), indicates another hardware domain (e.g. processor graphics) has limited energy efficiency optimizations in the processor core domain since the last clearing of this bit or a reset. This bit is sticky, software may clear this bit by writing a zero (0).
14	0h RO/V	**Cross Domain Limit Status (CROSS_DOMAIN_LIMIT_STATUS):** If set (1), indicates another hardware domain (e.g. processor graphics) is currently limiting energy efficiency optimizations in the processor core domain.
13	0h RW/0C/V	**Current Limit Log (CURRENT_LIMIT_LOG):** R/WC0 - If set (1), an electrical current limit has been exceeded that has adversely impacted energy efficiency optimizations since the last clearing of this bit or a reset. This bit is sticky, software may clear this bit by writing a zero (0).

Bit Range	Default & Access	Field Name (ID): Description
12	0h RO/V	**Current Limit Status (CURRENT_LIMIT_STATUS):** If set (1), indicates an electrical current limit (e.g. Electrical Design Point/IccMax) is being exceeded and is adversely impacting energy efficiency optimizations.
11	0h RW/0C/V	**Power Limitation Log (POWER_LIMITATION_LOG):** Sticky bit which indicates whether the current P-State is limited by power limitation since the last clearing of this bit or a reset. Software may clear this bit by writing a zero.
10	0h RO/V	**Power Limitation Status (POWER_LIMITATION_STATUS):** Indicates whether the current P-State is limited by power limitation. For legacy P-State method (not Intel SpeedShift), this bit will be set only if the P-state is limit below the base frequency.
9	0h RW/0C/V	**Threshold2 Log (THRESHOLD2_LOG):** Sticky log bit that asserts on a 0 to 1 or a 1 to 0 transition of the THRESHOLD2_STATUS bit. This bit is set by hardware and cleared by software.
8	0h RO/V	**Threshold2 Status (THRESHOLD2_STATUS):** Indicates that the current temperature is higher than or equal to Threshold 2 temperature.
7	0h RW/0C/V	**Threshold1 Log (THRESHOLD1_LOG):** Sticky log bit that asserts on a 0 to 1 or a 1 to 0 transition of the THRESHOLD1_STATUS bit. This bit is set by hardware and cleared by software.
6	0h RO/V	**Threshold1 Status (THRESHOLD1_STATUS):** Indicates that the current temperature is higher than or equal to Threshold 1 temperature.
5	0h RW/0C/V	**Out Of Specification Log (OUT_OF_SPEC_LOG):** Sticky log bit indicating that the processor operating out of its thermal specification since the last time this bit was cleared. This bit is set by hardware on a 0 to 1 transition of OUT_OF_SPEC_STATUS.
4	0h RO/V	**Out Of Specification Status (OUT_OF_SPEC_STATUS):** Status bit indicating that the processor is operating out of its thermal specification. Once set, this bit only clears on a reset.
3	0h RW/0C/V	**PROCHOT# Log (PROCHOT_LOG):** Sticky log bit indicating that PROCHOT# has been asserted since the last time this bit was cleared by software. This bit is set by hardware on a 0 to 1 transition of PROCHOT_STATUS.
2	0h RO/V	**PROCHOT# Status (PROCHOT_STATUS):** Status bit indicating that PROCHOT# is currently being asserted.
1	0h RW/0C/V	**Thermal Monitor Log (THERMAL_MONITOR_LOG):** Sticky log bit indicating that GT has seen a thermal monitor event since the last time software cleared this bit. This bit is set by hardware on a 0 to 1 transition of THERMAL_MONITOR_STATUS.
0	0h RO/V	**Thermal Monitor Status (THERMAL_MONITOR_STATUS):** Status bit indicating that the Thermal Monitor has tripped and is currently thermally throttling.

3.3.33 Thermal Interrupt GT (THERM_INTERRUPT_GT_0_0_0_MCHBAR_PCU) — Offset 59C4h

Enables and disables the generation of an interrupt on temperature transitions detected with the processors thermal sensors and thermal monitor.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 59C4h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:25	0h RO	**Reserved**
24	0h RW	**Power Interrupt Enable (POWER_INT_ENABLE):** When this bit is set, a thermal interrupt will be sent upon throttling due to power limitations.
23	0h RW	**Threshold2 Interrupt Enable (THRESHOLD_2_INT_ENABLE):** Controls the generation of a thermal interrupt whenever the Thermal Threshold 2 Temperature is crossed.
22:16	00h RW	**Threshold2 Relative Temperature (THRESHOLD_2_REL_TEMP):** This value indicates the offset in degrees below TjMax Temperature that should trigger a Thermal Threshold 2 trip.
15	0h RW	**Threshold1 Interrupt Enable (THRESHOLD_1_INT_ENABLE):** Controls the generation of a thermal interrupt whenever the Thermal Threshold 1 Temperature is crossed.
14:8	00h RW	**Threshold1 Relative Temperature (THRESHOLD_1_REL_TEMP):** This value indicates the offset in degrees below TjMax Temperature that should trigger a Thermal Threshold 1 trip.
7:5	0h RO	**Reserved**
4	0h RW	**Out Of Spec Interrupt Enable (OUT_OF_SPEC_INT_ENABLE):** Thermal interrupt enable for the critical temperature condition which is stored in the Critical Temperature Status bit in IA32_THERM_STATUS.
3	0h RO	**Reserved**
2	0h RW	**Bidirectional PROCHOT# Interrupt Enable (PROCHOT_INT_ENABLE):** If set, a thermal interrupt is delivered on the rising edge of PROCHOT#.
1	0h RW	**Low Temperature Interrupt Enable (LOW_TEMP_INT_ENABLE):** Enables a thermal interrupt to be generated on the transition from a high-temperature to a low-temperature when set, where high temperature is dictated by the thermal monitor trip temperature.
0	0h RW	**High Temperature Interrupt Enable (HIGH_TEMP_INT_ENABLE):** Enables a thermal interrupt to be generated on the transition from a low-temperature to a high-temperature when set, where high temperature is dictated by the thermal monitor trip temperature.

3.3.34 Device Idle Duration Override (DEVICE_IDLE_DURATION_OVERRIDE_0_0_0_MCHBAR_PCU) — Offset 59C8h

MDID override register to be used by OS or software for debug purposes.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 59C8h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RO	**Reserved**
30	0h RW	**Force MDID Override (FORCE_MDID_OVERRIDE):** When this bit is set, and bit 1 (the valid bit) is set, the value specified in this field will be used for MDID purposes. If this bit is clear, and bit 1 (the valid bit) is set, this value should be consumed along with the other MDID registers to determine which value is expiring next and reporting that value.
29	0h RW	**Disable MDID Evaluation (DISABLE_MDID_EVALUATION):** Send a value of disabled to the PCH for the MDID field.
28:8	000000h RW	**Next Device Activity (NEXT_DEVICE_ACTIVITY):** These are in 1us increments and can report a maximum value of approximately 2 seconds
7	0h RW	**Interrupt or Memory (IM):** 0: Interrupt. This is a hint for the idle duration time to the next interrupt. 1: Memory. This is a hint for the idle duration time to the next snoop cycle.
6	0h RW	**Opportunistic or Deterministic (OD):** 0: Opportunistic. This is an opportunistic hint as suggested by the sub-system. 1: Deterministic. This is a deterministic hint as suggested by the sub-system.
5:2	0h RO	**Reserved**
1	0h RW	**VALID:** 0: This Idle Duration Override CSR is not valid 1: This Idle Duration Override CSR is valid
0	0h RO	**Reserved**

3.3.35 Package GT C0 EUs SUM (PKG_GT_C0_EUS_SUM) — Offset 59F0h

The counter value is incremented when PKG_GT_C0_ANY_SLICE increments.

Counts in 24Mhz units.

Type	Size	Offset	Default
MMIO	64 bit	MCHBAR + 59F0h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:0	00000000 00000000h RO/V	**DATA:** Counter value

3.3.36 Package GT C0 Media Sum (PKG_GT_C0_MEDIA_SUM) — Offset 59F8h

The counter value is incremented when PKG_GT_C0_ANY_SLICE increments.

Counts in 24Mhz units.

Type	Size	Offset	Default
MMIO	64 bit	MCHBAR + 59F8h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:0	00000000 00000000h RO/V	**DATA:** Counter value.

3.3.37 FIVR FFFC EMI Control (FFFC_EMI_CONTROL_0_0_0_MCHBAR_PCU) — Offset 5A08h

FIVR FFFC Control Register

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 5A08h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RW	**DATA:** Data field.

3.3.38 FIVR FFFC RFI Control (FFFC_RFI_CONTROL_0_0_0_MCHBAR_PCU) — Offset 5A0Ch

Fivr FFFC Control Register

Note: Bit definitions are the same as FFFC_EMI_CONTROL_0_0_0_MCHBAR_PCU, offset 5A08h.

3.3.39 FIVR FFFC RFI Control 2 (FFFC_RFI_CONTROL2_0_0_0_MCHBAR_PCU) — Offset 5A18h

Fivr FFFC Control Register

Note: Bit definitions are the same as FFFC_EMI_CONTROL_0_0_0_MCHBAR_PCU, offset 5A08h.

3.3.40 Scratchpad Register (SSKPD_0_0_0_MCHBAR_PCU) — Offset 5D10h

This register holds 64 writable bits with no functionality behind them.

It is for the convenience of BIOS and graphics drivers.

Type	Size	Offset	Default
MMIO	64 bit	MCHBAR + 5D10h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
63:0	00000000 00000000h RW/P	**SKPD:** 64bit of data storage.

3.3.41 BIOS Mailbox Data (BIOS_MAILBOX_DATA_0_0_0_MCHBAR_PCU) — Offset 5DA0h

Data register for the BIOS Mailbox.

This register is used in conjunction with BIOS_MAILBOX_INTERFACE.

The BIOS Mailbox is documented in the BIOS Writers Guide.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 5DA0h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RW/V	**DATA:** This field contains the data associated with specific commands.

3.3.42 BIOS Mailbox Interface (BIOS_MAILBOX_INTERFACE_0_0_0_MCHBAR_PCU) — Offset 5DA4h

Control and Status register for the BIOS Mailbox.

This register is used in conjunction with BIOS_MAILBOX_DATA.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 5DA4h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RW/1S/V	**Run/Busy Bit (RUN_BUSY):** Software may write to the two mailbox registers only when RUN_BUSY is cleared (0b). After setting this bit, software will poll this bit until it is cleared. Firmware clears RUN_BUSY after updating the mailbox registers with the result and error code.
30:29	0h RO	**Reserved**
28:16	0000h RW/V	**PARAM2:** This field contains additional parameters associated with specific commands.
15:8	00h RW/V	**PARAM1:** This field contains additional parameters associated with specific commands.
7:0	00h RW/V	**COMMAND:** Software programs the mailbox command ID in this field. On RUN_BUSY assertion this field should contain the command ID. On RUN_BUSY deassrtion this field will contain the error code.

3.3.43 BIOS Reset Complete (BIOS_RESET_CPL_0_0_0_MCHBAR_PCU) — Offset 5DA8h

This register is used by BIOS to inform the PCU that all power management settings have been written and power management can be enabled.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 5DA8h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:2	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
1	0h RW	**PCIe Enumeration Done (PCIE_ENUMERATION_DONE):** This will be set after PCIe enumeration is done. If it is set, the PCU will look at the following bits in DEVEN_0_0_0_PCI: 1: D1F2EN 2: D1F1EN 3: D1F0EN If all of these bits are set to a 0x0, this means that there is nothing connected to the PEG devices and the PCIe PLL can be shut off. Note: Implicit assumption - this bit is asserted prior to (or with) asserting RST_CPL.
0	0h RW/1S	**Reset Complete (RST_CPL):** This bit is set by BIOS to indicate to the CPU Power management function that it has completed to set up all PM relevant configuration and allow CPU Power management function to digest the configuration data and start active PM operation. It is expected that this bit will be set just before BIOS transfer of control to the OS. 0b: Not ready 1b: BIOS PM configuration complete

3.3.44 Memory Controller BIOS Request (MC_BIOS_REQ_0_0_0_MCHBAR_PCU) — Offset 5E00h

This register allows BIOS to request Memory Controller clock frequency.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 5E00h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RW	**RUN/BUSY Bit (RUN_BUSY):** This bit indicates that the BIOS request is pending. BIOS sets this bit together with a command in the lower bits of this register. The PCU may only clear this bit after the BIOS request has completed.
30:17	0h RO	**Reserved**
16	0h RW	**Gear Type (GEAR_TYPE):** 0h: Gear1 (Default) - DDR bus clock is the same as QCLK 1h: Gear2 - DDR PHY bus clock is double of QCLK
15:12	0h RO	**Reserved**
11:8	0h RW	**Reference Clock Type (REQ_TYPE):** Request Type: • 0h: MC frequency request for 133MHz Qclk granularity. • 1h: MC frequency request for 100MHz Qclk granularity. All other values are reserved.

Bit Range	Default & Access	Field Name (ID): Description
7:0	00h RW	**Request Data (REQ_DATA):** This field holds the memory controller frequency request (QCLK). Each bin is 133/ 100MHz and not 266/200MHz. This interface replaces the usage of DCLK ratios and Odd Ratio. QCLK frequency is determined by the MC reference clock (MC_FREQ_TYPE) as well as BCLK. 0h: MC PLL shutdown 1h-2h: Reserved 3h-FFh: QCLK ratio in 133.33MHz or 100MHz increments

3.3.45 Memory Controller BIOS Data (MC_BIOS_DATA_0_0_0_MCHBAR_PCU) — Offset 5E04h

Memory Controller Frequency information for BIOS, during MRC flow.

Reflects the last frequency requested in MC_BIOS_REQ_0_0_0_MCHBAR_PCU.

In case of Dual MRC for System Agent SpeedStep, the value will change according to the MRC requests.

Post MRC will hold the last MRC request and not the current memory frequency.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 5E04h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:17	0h RO	**Reserved**
16	0h RW/L	**Gear Type (GEAR_TYPE):** • 0 - Gear1 (Default) - DDR bus clock is the same as QCLK • 1 - Gear2 - DDR PHY bus clock is double of QCLK
15:12	0h RO	**Reserved**
11:8	0h RW/L	**Reference Clock Type (MC_FREQ_TYPE):** This field holds the memory controller frequency Type. • 0h: MC frequency request for 133MHz Qclk granularity. • 1h: MC frequency request for 100MHz Qclk granularity. All other values are reserved.

Bit Range	Default & Access	Field Name (ID): Description
7:0	00h RW/L	**Memory Controller Frequency (MC_FREQ):** This field holds the memory controller frequency (QCLK). Each bin is 133/100MHz and not 266/200MHz. This interface replaces the usage of DCLK ratios and Odd Ratio. QCLK frequency is determined by the MC reference clock (MC_FREQ_TYPE) as well as BCLK. 0: Memory Controller PLL shutdown 1h-2h: Reserved 3h-FFh: QCLK ratio in 133.33MHz or 100MHz increments

3.3.46 System Agent Power Management Control (SAPMCTL_0_0_0_MCHBAR_PCU) — Offset 5F00h

System Agent Power Management Control.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 5F00h	00002106h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:16	0h RO	**Reserved**
15	0h RW	**Force Memory Master DLL When Display Engine is Active (MDLL_ON_DE):** Force memory master DLL on when the Display Engine is active. This includes cases where memory is not accessed. This bit has to be set only if there are issues with the memory DLL wakeup based on the Self Refresh exit indication from Display Engine. 0b: Display Engine wakes up memory DLL using the Self Refresh exit indication only 1b: Force Memory DLL on when the Display Engine is active
14	0h RW	**Force Memory Controller PLL When Display Engine is Active (MPLL_ON_DE):** Force Memory PLLs (MCPLL and GDPLL) on when the Display Engine is active. This includes cases where memory is not accessed. This bit has to be set only if there are issues with the Memory PLL wakeup based on the Self Refresh exit indication from the Display Engine. 0b: Display Engine wakes up Memory PLLs using the Self Refresh exit indication only 1b: Force Memory PLLs on when the Display Engine is active
13	1h RW	**System Agent Clock Gating Memory Controller PLL (SACG_MPLL):** When this bit is set to 1b, FCLK will never be gated when the memory controller PLL is ON. Otherwise, FCLK gating policies are not affected by the locking of the memory controller PLLs.
12	0h RW	**Non-Snoop Wake Self Refresh Exit (NSWAKE_SREXIT):** When this bit is set to 1b, a Non-Snoop wakeup signal from the PCH will cause the PCU to force the memory controller to exit from Self-Refresh. Otherwise, the Non-Snoop indication will not affect the Self Refresh exit policy.

Bit Range	Default & Access	Field Name (ID): Description
11	0h RW	**System Agent Clock Gating Self Refresh Exit (SACG_SREXIT):** The Display Engine can indicate to the PCU that it wants the Memory Controller to exit self-refresh. When this bit is set to 1b, this request from the Display Engine will cause FCLK to be ungated. Otherwise, this request from the Display Engine has no effect on FCLK gating.
10	0h RW	**Master DLL Shutdown Power State Enable (MDLL_OFF_SEN):** This bit indicates when the Memory Master DLL may be shutdown based on link active power states. 0b: Memory DLL may be shut down in L1 and deeper sleep states. 1b: Memory DLL may be shut down in L0s and deeper sleep states.
9	0h RW	**Memory Controller PLL Shutdown Power State Enable (MPLL_OFF_SEN):** This bit indicates when the Memory PLLs (MCPLL and GDPLL) may be shutdown based on link active power states. 0b: Memory PLLs may be shut down in L1 and deeper sleep states. 1b: Memory PLLs may be shut down in L0s and deeper sleep states.
8	1h RW	**System Agent Clock Gating Power State Enable (SACG_SEN):** This bit indicates when the System Agent clock gating is possible based on link active power states. 0b: System Agent clock gating is allowed in L1 and deeper sleep states. 1b: System Agent clock gating is allowed in L0s and deeper sleep states.
7:3	0h RO	**Reserved**
2	1h RW	**PCIe PLL Shutdown Enable (PPLL_OFF_ENA):** This bit is used to enable shutting down the PCIe/DMI PLL. 0b: PLL shutdown is not allowed 1b: PLL shutdown is allowed
1	1h RW	**Memory Controller PLL Shutdown Enable (MPLL_OFF_ENA):** This bit is used to enable shutting down the Memory Controller PLLs (MCPLL and GDPLL). 0b: PLL shutdown is not allowed 1b: PLL shutdown is allowed
0	0h RW	**System Agent Clock Gating Enable (SACG_ENA):** This bit is used to enable or disable the System Agent Clock Gating (FCLK). 0b: System Agent Clock Gating is Not Allowed 1b: System Agent Clock Gating is Allowed

3.3.47 Configurable TDP Nominal (CONFIG_TDP_NOMINAL_0_0_0_MCHBAR_PCU) — Offset 5F3Ch

This register is used to indicate the Nominal Configurable TDP ratio available for this specific SKU.

System BIOS must use this value while building the _PSS table if the feature is enabled.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 5F3Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:8	0h RO	**Reserved**
7:0	00h RO/V	**TDP Ratio (TDP_RATIO):** Nominal TDP level ratio to be used for this specific processor (in units of 100MHz). Note: A value of 0 in this field indicates invalid/undefined TDP point.

3.3.48 Configurable TDP Level 1 (CONFIG_TDP_LEVEL1_0_0_0_MCHBAR_PCU) — Offset 5F40h

Level 1 Configurable TDP settings.

On SKUs that do not support Configurable TDP, these registers will report 0.

Type	Size	Offset	Default
MMIO	64 bit	MCHBAR + 5F40h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63	0h RO	**Reserved**
62:48	0000h RO/V	**Minimum Package Power (PKG_MIN_PWR):** Minimum package power setting allowed for this Configurable TDP level. Lower values will be clamped up to this value. Units defined in MSR PACKAGE_POWER_SKU[PWR_UNIT]. Similar to PACKAGE_POWER_SKU[PKG_MIN_PWR].
47	0h RO	**Reserved**
46:32	0000h RO/V	**Maximum Package Power (PKG_MAX_PWR):** Maximum package power setting allowed for this Configurable TDP level. Higher values will be clamped down to this value. Units defined in MSR PACKAGE_POWER_SKU[PWR_UNIT]. Similar to PACKAGE_POWER_SKU[PKG_MAX_PWR].

Bit Range	Default & Access	Field Name (ID): Description
31:24	0h RO	**Reserved**
23:16	00h RO/V	**TDP Ratio (TDP_RATIO):** TDP ratio for this Configurable TDP Level.
15	0h RO	**Reserved**
14:0	0000h RO/V	**Package TDP (PKG_TDP):** Power Limit (PL1) for this Configurable TDP level. Units defined in MSR PACKAGE_POWER_SKU[PWR_UNIT] Similar to PACKAGE_POWER_SKU[PKG_TDP]

3.3.49 Configurable TDP Level 1 (CONFIG_TDP_LEVEL2_0_0_0_MCHBAR_PCU) — Offset 5F48h

Level 2 Configurable TDP settings.

On SKUs that do not support Configurable TDP, these registers will report 0.

Note: Bit definitions are the same as CONFIG_TDP_LEVEL1_0_0_0_MCHBAR_PCU, offset 5F40h.

3.3.50 Configurable TDP Control (CONFIG_TDP_CONTROL_0_0_0_MCHBAR_PCU) — Offset 5F50h

Allows platform software to select the TDP level.

Can be done via all three interfaces (MSR, MMIO and PECI/PCS).

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 5F50h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RW/L	**Configurable TDP Lock (CONFIG_TDP_LOCK):** Configurable TDP level select lock. 0b: Unlocked. 1b: Locked till next reset. **Locked by:** CONFIG_TDP_CONTROL.CONFIG_TDP_LOCK
30:2	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
1:0	0h RW/L	**TDP Level (TDP_LEVEL):** Select Configurable TDP level: 0h: Nominal TDP level (default) 1h: Level from CONFIG_TDP_LEVEL_1 2h: Level from CONFIG_TDP_LEVEL_2 3h: Reserved **Locked by:** CONFIG_TDP_CONTROL.CONFIG_TDP_LOCK

3.3.51 Turbo Activation Ratio (TURBO_ACTIVATION_RATIO_0_0_0_MCHBAR_PCU) — Offset 5F54h

This is the MMIO interface for MSR TURBO_ACTIVATION_RATIO (64Ch).

Allows setting a ratio that acts as a threshold for maximum P-State.

When the OS request a P-state equal or higher to this ratio threshold, this request is treated as a maximum P-State request.

This has no affect when using Intel Speed Shift interface, only legacy P-States.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 5F54h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RW/L	**Turbo Activation Ratio Lock (TURBO_ACTIVATION_RATIO_LOCK):** Locks this register until the next reset. 0b: Unlocked 1b: Locked **Locked by:** TURBO_ACTIVATION_RATIO.TURBO_ACTIVATION_RATIO_LOCK
30:8	0h RO	**Reserved**
7:0	00h RW/L	**Maximum Non-Turbo Ratio (MAX_NON_TURBO_RATIO):** CPU will treat any P-state request above this ratio as a request for max turbo 0 is special encoding which disables the feature. **Locked by:** TURBO_ACTIVATION_RATIO.TURBO_ACTIVATION_RATIO_LOCK

3.3.52 Overclocking Status (OC_STATUS_0_0_0_MCHBAR_PCU) — Offset 5F58h

This register exposes the usage of various overclocking features.

Security oriented software can examine which overclocking features have been used and act accordingly.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 5F58h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:1	0h RO	**Reserved**
0	0h RW/L	**Memory Runtime Timing Overclocking Enabled (MC_TIMING_RUNTIME_OC_ENABLED):** Adjusting memory timing values for overclocking is enabled.

3.3.53 Base Clock (BCLK) Frequency (BCLK_FREQ_0_0_0_MCHBAR) — Offset 5F60h

This register reports the BCLK frequency.

It is used by software to calculate various clock frequencies that are derived from BCLK such as Core, Ring, Memory Controller and GT.

Type	Size	Offset	Default
MMIO	64 bit	MCHBAR + 5F60h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
63:32	0h RO	**Reserved**
31:0	00000000h RW/L	**BCLK Frequency (BCLK_FREQ):** Reported BCLK Frequency in KHz

3.4 Host Controller (MCHBAR) Registers

This chapter documents the Host Controller MCHBAR registers.

Base address of these registers are defined in the MCHBAR_0_0_0_PCI register in Bus: 0, Device: 0, Function: 0.

Note: These registers apply to all processors.

3.4.1 Summary of Registers

Table 3-5. Summary of MCHBAR Registers

Offset	Size (Bytes)	Register Name (Register Symbol)	Default Value
7008h	4	HD Audio Engine Bus & Device ID (HDAUDRID_0_0_0_MCHBAR_IMPH)	800000D8h
7020h	4	VLW Control (VLWCTL_0_0_0_MCHBAR)	00000001h
7090h	4	Type-C Sub-system Device Enable (TCSS_DEVEN_0_0_0_MCHBAR_IMPH)	00001FFFh
7094h	4	Capabilities D (CAPID0_D_0_0_0_MCHBAR)	00000000h
7110h	8	REGBAR Base Address (REGBAR_0_0_0_MCHBAR_IMPH)	0000000000000000h

3.4.2 HD Audio Engine Bus & Device ID (HDAUDRID_0_0_0_MCHBAR_IMPH) — Offset 7008h

Indicates the Azalia Bus/Device Identification. The contents of this register contain default value indicating Bus 0 Device 27, and may be only updated once by BIOS, after which the register is locked.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 7008h	800000D8h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	1h RW/L	**HD Audio Engine Enabled (HDAUD_EN):** When this bit is set, the BUSNUM and DEVNUM fields correspond to the ID of the HD Audio Engine. Otherwise, these fields have no meaning. **Locked by:** WRITE_ONCE_LOCK.HDAUD_EN_WOL
30:16	0h RO	**Reserved**
15:8	00h RW/L	**Bus Number (BUSNUM):** Indicates Bus Number for the Azalia Controller. **Locked by:** WRITE_ONCE_LOCK.BUSNUM_WOL

Bit Range	Default & Access	Field Name (ID): Description
7:3	1Bh RW/L	**Device Number (DEVNUM):** Device Number for the Azalia controller. Default value is Device 27. **Locked by:** WRITE_ONCE_LOCK.DEVNUM_WOL
2:0	0h RO	**Reserved**

3.4.3 VLW Control (VLWCTL_0_0_0_MCHBAR) — Offset 7020h

Control and status information associated with VLWs.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 7020h	00000001h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31	0h RW/V/L	**VLW Drop Status (DROP_VLW_STS):** This bit is set by HW if any VLWs are dropped while DROP_VLW_CTL is set.
30:1	0h RO	**Reserved**
0	1h RW	**VLW Drop Control (DROP_VLW_CTL):** When this bit is set VLWs will be silently dropped. Note that the bit is set by reset, meaning VLWs are dropped by default..

3.4.4 Type-C Sub-system Device Enable (TCSS_DEVEN_0_0_0_MCHBAR_IMPH) — Offset 7090h

Allows for enabling/disabling of Type-C PCI devices and functions that are within the CPU package. The table below the bit definitions describes the behavior of all combinations of transactions to devices controlled by this register. All the bits in this register are Intel TXT Lockable.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 7090h	00001FFFh

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:13	0h RO	**Reserved**
12	1h RW/L	**Thunderbolt DMA2 Enable (TBT_DMA2_EN):** 0: DMA2 is disabled and hidden. 1: DMA2 is enabled and visible. **Locked by:** CAPID0_D_0_0_0_MCHBAR.TC_TBT_DMA2_DIS
11	1h RW/L	**Thunderbolt DMA1 Enable (TBT_DMA1_EN):** 0: DMA1 is disabled and hidden. 1: DMA1 is enabled and visible. **Locked by:** CAPID0_D_0_0_0_MCHBAR.TC_TBT_DMA1_DIS
10	1h RW/L	**Thunderbolt DMA0 Enable (TBT_DMA0_EN):** 0: DMA0 is disabled and hidden. 1: DMA0 is enabled and visible. **Locked by:** CAPID0_D_0_0_0_MCHBAR.TC_TBT_DMA0_DIS
9	1h RW/L	**xDCI Enable (XDCI_EN):** 0: xDCI is disabled and hidden. 1: xDCI is enabled and visible. **Locked by:** CAPID0_D_0_0_0_MCHBAR.TC_XDCI_DIS
8	1h RW/L	**xHCI Enable (XHCI_EN):** 0: xHCI is disabled and hidden. 1: xHCI is enabled and visible. **Locked by:** CAPID0_D_0_0_0_MCHBAR.TC_XHCI_DIS
7	1h RW/L	**PCIe7 Enable (PCIE7_EN):** 0: TypeC PCIe Root Port 7 is disabled 1: TypeC PCIe Root Port 7 is enabled **Locked by:** CAPID0_D_0_0_0_MCHBAR.TC_PCIE7_DIS
6	1h RW/L	**PCIe6 Enable (PCIE6_EN):** 0: TypeC PCIe Root Port 6 is disabled 1: TypeC PCIe Root Port 6 is enabled **Locked by:** CAPID0_D_0_0_0_MCHBAR.TC_PCIE6_DIS
5	1h RW/L	**PCIe5 Enable (PCIE5_EN):** 0: TypeC PCIe Root Port 5 is disabled 1: TypeC PCIe Root Port 5 is enabled **Locked by:** CAPID0_D_0_0_0_MCHBAR.TC_PCIE5_DIS
4	1h RW/L	**PCIe4 Enable (PCIE4_EN):** 0: TypeC PCIe Root Port 4 is disabled 1: TypeC PCIe Root Port 4 is enabled **Locked by:** CAPID0_D_0_0_0_MCHBAR.TC_PCIE4_DIS
3	1h RW/L	**PCIe3 Enable (PCIE3_EN):** 0: TypeC PCIe Root Port 3 is disabled 1: TypeC PCIe Root Port 3 is enabled **Locked by:** CAPID0_D_0_0_0_MCHBAR.TC_PCIE3_DIS

Bit Range	Default & Access	Field Name (ID): Description
2	1h RW/L	**PCIe2 Enable (PCIE2_EN):** 0: TypeC PCIe Root Port 2 is disabled 1: TypeC PCIe Root Port 2 is enabled **Locked by:** CAPID0_D_0_0_0_MCHBAR.TC_PCIE2_DIS
1	1h RW/L	**PCIe1 Enable (PCIE1_EN):** 0: TypeC PCIe Root Port 1 is disabled 1: TypeC PCIe Root Port 1 is enabled **Locked by:** CAPID0_D_0_0_0_MCHBAR.TC_PCIE1_DIS
0	1h RW/L	**PCIe0 Enable (PCIE0_EN):** 0: TypeC PCIe Root Port 0 is disabled 1: TypeC PCIe Root Port 0 is enabled **Locked by:** CAPID0_D_0_0_0_MCHBAR.TC_PCIE0_DIS

3.4.5 Capabilities D (CAPID0_D_0_0_0_MCHBAR) — Offset 7094h

Processor capability enumeration

.

Type	Size	Offset	Default
MMIO	32 bit	MCHBAR + 7094h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:17	0h RO	**Reserved**
16	0h RW/L	**TypeC Sub-system IOM Microcontroller Disable (IOM_DIS):** 0: Type C IOM is Enabled 1: Type C IOM is Disabled
15:12	0h RO	**Reserved**
11	0h RW/L	**TypeC Sub-system Thunderbolt DMA1 Disable (TC_TBT_DMA1_DIS):** Indicates if Type-C DMA1 device is disabled.
10	0h RW/L	**TypeC Sub-system Thunderbolt DMA0 Disable (TC_TBT_DMA0_DIS):** Indicates if Type-C DMA0 device is disabled.
9	0h RW/L	**TypeC Sub-system USB xDCI Disable (TC_XDCI_DIS):** Indicates if Type-C XDCI device is disabled.
8	0h RW/L	**TypeC Sub-system USB xHCI Disable (TC_XHCI_DIS):** Indicates if Type-C XHCI device is disabled.
7:4	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
3	0h RW/L	**TypeC Sub-system PCIe3 Disable (TC_PCIE3_DIS):** PCIe3 disable.
2	0h RW/L	**TypeC Sub-system PCIe2 Disable (TC_PCIE2_DIS):** PCIe2 disable.
1	0h RW/L	**TypeC Sub-system PCIe1 Disable (TC_PCIE1_DIS):** PCIe1 disable.
0	0h RW/L	**TypeC Sub-system PCIe0 Disable (TC_PCIE0_DIS):** PCIe0 root port is disabled.

3.4.6 REGBAR Base Address (REGBAR_0_0_0_MCHBAR_IMPH) — Offset 7110h

Defines the base address for REGBAR.

Type	Size	Offset	Default
MMIO	64 bit	MCHBAR + 7110h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:24	0000h RW	**REGBAR Base Address (REGFBAR):** This field corresponds to bits 38 to 24 of the base address MMIO space. BIOS will program this register resulting in a base address for a 16MB block of contiguous memory address space.
23:1	0h RO	**Reserved**
0	0h RW	**REGBAR Enable (REGBAREN):** 0: REGBAR is disabled and does not claim any memory 1: REGBAR memory mapped accesses are claimed and decoded appropriately. **Locked by:** CAPID0_A_0_0_0_PCI.VTDD

3.5 Direct Media Interface BAR (DMIBAR) Registers

This chapter documents the DMIBAR registers. Base address of these registers are defined in the DMIBAR_0_0_0_PCI register in Bus: 0, Device: 0, Function: 0.

Note: These registers apply to all processors.

3.5.1 Summary of Registers

Table 3-6. Summary of DMIBAR Registers

Offset	Size (Bytes)	Register Name (Register Symbol)	Default Value
0h	4	DMI Virtual Channel Enhanced Capability (DMIVCECH_0_0_0_DMIBAR)	04010002h
4h	4	DMI Port VC Capability Register 1 (DMIPVCCAP1_0_0_0_DMIBAR)	00000000h
8h	4	DMI Port VC Capability Register 2 (DMIPVCCAP2_0_0_0_DMIBAR)	00000000h
Ch	2	DMI Port VC Control (DMIPVCCTL_0_0_0_DMIBAR)	0000h
10h	4	DMI VC0 Resource Capability (DMIVC0RCAP_0_0_0_DMIBAR)	00000001h
1Ah	2	DMI VC0 Resource Status (DMIVC0RSTS_0_0_0_DMIBAR)	0002h
1Ch	4	DMI VC1 Resource Capability (DMIVC1RCAP_0_0_0_DMIBAR)	00008001h
26h	2	DMI VC0 Resource Status (DMIVC1RSTS_0_0_0_DMIBAR)	0002h
34h	4	DMI VCm Resource Capability (DMIVCMRCAP_0_0_0_DMIBAR)	00008000h
38h	4	DMI VCm Resource Control (DMIVCMRCTL_0_0_0_DMIBAR)	07000180h
3Eh	2	DMI VCm Resource Status (DMIVCMRSTS_0_0_0_DMIBAR)	0002h
40h	4	DMI Root Complex Link Declaration (DMIRCLDECH_0_0_0_DMIBAR)	08010005h
44h	4	DMI Element Self Description (DMIESD_0_0_0_DMIBAR)	01000202h
50h	4	DMI Link Entry 1 Description (DMILE1D_0_0_0_DMIBAR)	00000000h
58h	4	DMI Link Entry 1 Address (DMILE1A_0_0_0_DMIBAR)	00000000h
5Ch	4	DMI Link Upper Entry 1 Address (DMILUE1A_0_0_0_DMIBAR)	00000000h
60h	4	DMI Link Entry 2 Description (DMILE2D_0_0_0_DMIBAR)	00000000h
68h	4	DMI Link Entry 2 Address (DMILE2A_0_0_0_DMIBAR)	00000000h
88h	2	Link Control (LCTL_0_0_0_DMIBAR)	0000h
1C4h	4	DMI Uncorrectable Error Status (DMIUESTS_0_0_0_DMIBAR)	00000000h
1C8h	4	DMI Uncorrectable Error Mask (DMIUEMSK_0_0_0_DMIBAR)	00000000h
1CCh	4	DMI Uncorrectable Error Severity (DMIUESEV_0_0_0_DMIBAR)	00060010h
1D0h	4	DMI Correctable Error Status (DMICESTS_0_0_0_DMIBAR)	00000000h
1D4h	4	DMI Correctable Error Mask (DMICEMSK_0_0_0_DMIBAR)	00002000h

3.5.2 DMI Virtual Channel Enhanced Capability (DMIVCECH_0_0_0_DMIBAR) — Offset 0h

Indicates DMI Virtual Channel capabilities.

Type	Size	Offset	Default
MMIO	32 bit	DMIBAR + 0h	04010002h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:20	040h RO	**Pointer to Next Capability (PNC):** This field contains the offset to the next PCI Express capability structure in the linked list of capabilities (Link Declaration Capability).
19:16	1h RO	**PCI Express Virtual Channel Capability Version (PCIEVCCV):** Hardwired to 1 to indicate compliances with the 1.1 version of the PCI Express specification. Note: This version does not change for 2.0 compliance.
15:0	0002h RO	**Extended Capability ID (ECID):** Value of 0002h identifies this linked list item (capability structure) as being for PCI Express Virtual Channel registers.

3.5.3 DMI Port VC Capability Register 1 (DMIPVCCAP1_0_0_0_DMIBAR) — Offset 4h

Describes the configuration of PCI Express Virtual Channels associated with this port.

Type	Size	Offset	Default
MMIO	32 bit	DMIBAR + 4h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:7	0h RO	**Reserved**
6:4	0h RO	**Low Priority Extended VC Count (LPEVCC):** Indicates the number of (extended) Virtual Channels in addition to the default VC belonging to the low-priority VC (LPVC) group that has the lowest priority with respect to other VC resources in a strict-priority VC Arbitration. The value of 0 in this field implies strict VC arbitration.
3	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
2:0	0h RW/L	**Extended VC Count (EVCC):** Indicates the number of (extended) Virtual Channels in addition to the default VC supported by the device. The Private Virtual Channel, VC1 and the Manageability Virtual Channel are not included in this count. **Locked by:** TLDMIREGS.WO_STATUS0_0_0_0_DMIBAR.EVCCDWOS

3.5.4 DMI Port VC Capability Register 2 (DMIPVCCAP2_0_0_0_DMIBAR) — Offset 8h

Describes the configuration of PCI Express Virtual Channels associated with this port.

Type	Size	Offset	Default
MMIO	32 bit	DMIBAR + 8h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:24	00h RO	**VC Arbitration Table Offset (VCATO):** This field is reserved for VC Arbitration Table Offset
23:8	0h RO	**Reserved**
7:0	00h RO	**VC Arbitration Capability (VCAC):** This field is reserved for VC Arbitration Capability

3.5.5 DMI Port VC Control (DMIPVCCTL_0_0_0_DMIBAR) — Offset Ch

DMI Port VC Control

Type	Size	Offset	Default
MMIO	16 bit	DMIBAR + Ch	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:4	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
3:1	0h RW	**VC Arbitration Select (VCAS):** This field will be programmed by software to the only possible value as indicated in the VC Arbitration Capability field. The value 000b when written to this field will indicate the VC arbitration scheme is hardware fixed (in the root complex). This field cannot be modified when more than one VC in the LPVC group is enabled. 000: Hardware fixed arbitration scheme. E.G. Round Robin Others: Reserved See the PCI express specification for more details.
0	0h RO	**Load VC Arbitration Table (LVCAT):** This field is reserved for Load VC Arbitration Table

3.5.6 DMI VC0 Resource Capability (DMIVC0RCAP_0_0_0_DMIBAR) — Offset 10h

DMI VC0 Resource Capability

Type	Size	Offset	Default
MMIO	32 bit	DMIBAR + 10h	00000001h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:24	00h RO	**Port Arbitration Table Offset (PATO):** This field is reserved for Port Arbitration Table Offset
23	0h RO	**Reserved**
22:16	00h RO	**Maximum Time Slots (MTS):** This field is reserved for Maximum Time Slots
15	0h RO	**Reject Snoop Transactions (REJSNPT):** 0: Transactions with or without the No Snoop bit set within the TLP header are allowed on this VC. 1: Any transaction for which the No Snoop attribute is applicable but is not set within the TLP Header will be rejected as an Unsupported Request.
14:8	0h RO	**Reserved**
7:0	01h RO	**Port Arbitration Capability (PAC):** Having only bit 0 set indicates that the only supported arbitration scheme for this VC is non-configurable hardware-fixed.

3.5.7 DMI VC0 Resource Status (DMIVC0RSTS_0_0_0_DMIBAR) — Offset 1Ah

Reports the Virtual Channel specific status.

Type	Size	Offset	Default
MMIO	16 bit	DMIBAR + 1Ah	0002h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
15:2	0h RO	**Reserved**
1	1h RO/V	**Virtual Channel 0 Negotiation Pending (VC0NP):** 0: The VC negotiation is complete. 1: The VC resource is still in the process of negotiation (initialization or disabling). This bit indicates the status of the process of Flow Control initialization. It is set by default on Reset, as well as whenever the corresponding Virtual Channel is Disabled or the Link is in the DL_Down state. It is cleared when the link successfully exits the FC_INIT2 state. **BIOS Requirement**: Before using a Virtual Channel, software must check whether the VC Negotiation Pending fields for that Virtual Channel are cleared in both Components on a Link.
0	0h RO	**Reserved**

3.5.8 DMI VC1 Resource Capability (DMIVC1RCAP_0_0_0_DMIBAR) — Offset 1Ch

DMI VC1 Resource Capability

Note: Bit definitions are the same as DMIVC0RCAP_0_0_0_DMIBAR, offset 10h.

3.5.9 DMI VC0 Resource Status (DMIVC1RSTS_0_0_0_DMIBAR) — Offset 26h

Reports the Virtual Channel specific status.

Type	Size	Offset	Default
MMIO	16 bit	DMIBAR + 26h	0002h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
15:2	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
1	1h RO/V	**Virtual Channel 1 Negotiation Pending (VC1NP):** 0: The VC negotiation is complete. 1: The VC resource is still in the process of negotiation (initialization or disabling). Software may use this bit when enabling or disabling the VC. This bit indicates the status of the process of Flow Control initialization. It is set by default on Reset, as well as whenever the corresponding Virtual Channel is Disabled or the Link is in the DL_Down state. It is cleared when the link successfully exits the FC_INIT2 state. Before using a Virtual Channel, software must check whether the VC Negotiation Pending fields for that Virtual Channel are cleared in both Components on a Link.
0	0h RO	**Reserved**

3.5.10 DMI VCm Resource Capability (DMIVCMRCAP_0_0_0_DMIBAR) — Offset 34h

DMI VCm Resource Capability

Type	Size	Offset	Default
MMIO	32 bit	DMIBAR + 34h	00008000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:16	0h RO	**Reserved**
15	1h RO	**Reject Snoop Transactions (REJSNPT):** 0: Transactions with or without the No Snoop bit set within the TLP header are allowed on the VC. 1: When Set, any transaction for which the No Snoop attribute is applicable but is not Set within the TLP Header will be rejected as an Unsupported Request
14:0	0h RO	**Reserved**

3.5.11 DMI VCm Resource Control (DMIVCMRCTL_0_0_0_DMIBAR) — Offset 38h

DMI VCm Resource Settings

Type	Size	Offset	Default
MMIO	32 bit	DMIBAR + 38h	07000180h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RW	**Virtual Channel Enable (VCMEN):** 0: Virtual Channel is disabled. 1: Virtual Channel is enabled. See exceptions below. Software must use the VC Negotiation Pending bit to check whether the VC negotiation is complete. When VC Negotiation Pending bit is cleared, a 1 read from this VC Enable bit indicates that the VC is enabled (Flow Control Initialization is completed for the PCI Express port). A 0b read from this bit indicates that the Virtual Channel is currently disabled. **BIOS Requirement:** 1. To enable a Virtual Channel, the VC Enable bits for that Virtual Channel must be set in both Components on a Link. 2. To disable a Virtual Channel, the VC Enable bits for that Virtual Channel must be cleared in both Components on a Link. 3. Software must ensure that no traffic is using a Virtual Channel at the time it is disabled. 4. Software must fully disable a Virtual Channel in both Components on a Link before re-enabling the Virtual Channel.
30:27	0h RO	**Reserved**
26:24	7h RW	**Virtual Channel ID (VCID):** Assigns a VC ID to the VC resource. Assigned value must be non-zero. This field can not be modified when the VC is already enabled.
23:13	0h RO	**Reserved**
12:8	01h RW/V/L	**Save Restore (FC_FSM_STATE):** This register is for Save Restore to restore the FC FSM
7:0	80h RO	**Traffic Class/Virtual Channel Map (TCVCMMAP):** Indicates the TCs (Traffic Classes) that are mapped to the VC resource. Bit locations within this field correspond to TC values. For example, when bit 7 is set in this field, TC7 is mapped to this VC resource. When more than one bit in this field is set, it indicates that multiple TCs are mapped to the VC resource. In order to remove one or more TCs from the TC/VC Map of an enabled VC, software must ensure that no new or outstanding transactions with the TC labels are targeted at the given Link.

3.5.12 DMI VCm Resource Status (DMIVCMRSTS_0_0_0_DMIBAR) — Offset 3Eh

DMI VCm Resource Status

Type	Size	Offset	Default
MMIO	16 bit	DMIBAR + 3Eh	0002h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
15:2	0h RO	**Reserved**
1	1h RO/V	**Virtual Channel Negotiation Pending (VCNEGPND):** 0: The VC negotiation is complete. 1: The VC resource is still in the process of negotiation (initialization or disabling). Software may use this bit when enabling or disabling the VC. This bit indicates the status of the process of Flow Control initialization. It is set by default on Reset, as well as whenever the corresponding Virtual Channel is Disabled or the Link is in the DL_Down state. It is cleared when the link successfully exits the FC_INIT2 state. Before using a Virtual Channel, software must check whether the VC Negotiation Pending fields for that Virtual Channel are cleared in both Components on a Link.
0	0h RO	**Reserved**

3.5.13 DMI Root Complex Link Declaration (DMIRCLDECH_0_0_0_DMIBAR) — Offset 40h

This capability declares links from the respective element to other elements of the root complex component to which it belongs and to an element in another root complex component. See PCI Express specification for link/topology declaration requirements.

Type	Size	Offset	Default
MMIO	32 bit	DMIBAR + 40h	08010005h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:20	080h RO	**Pointer to Next Capability (PNC):** This field contains the offset to the next PCI Express capability structure in the linked list of capabilities (Internal Link Control Capability).
19:16	1h RO	**Link Declaration Capability Version (LDCV):** Hardwired to 1 to indicate compliances with the 1.1 version of the PCI Express specification. Note: This version does not change for 2.0 compliance.
15:0	0005h RO	**Extended Capability ID (ECID):** Value of 0005h identifies this linked list item (capability structure) as being for PCI Express Link Declaration Capability.

3.5.14 DMI Element Self Description (DMIESD_0_0_0_DMIBAR) — Offset 44h

Provides information about the root complex element containing this Link Declaration Capability.

Type	Size	Offset	Default
MMIO	32 bit	DMIBAR + 44h	01000202h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:24	01h RO	**Port Number (PORTNUM):** Specifies the port number associated with this element with respect to the component that contains this element. This port number value is utilized by the egress port of the component to provide arbitration to this Root Complex Element.
23:16	00h RW/L	**Component ID (CID):** Identifies the physical component that contains this Root Complex Element. **BIOS Requirement:** Must be initialized according to guidelines in the PCI Express* Isochronous/Virtual Channel Support Hardware Programming Specification (HPS). **Locked by:** TLDMIREGS.WO_STATUS0_0_0_0_DMIBAR.CIDDWOS
15:8	02h RO	**Number of Link Entries (NLE):** Indicates the number of link entries following the Element Self Description. This field reports 2 (one for MCH egress port to main memory and one to egress port belonging to ICH on other side of internal link).
7:4	0h RO	**Reserved**
3:0	2h RO	**Element Type (ETYP):** Indicates the type of the Root Complex Element. A value of 2h represents an Internal Root Complex Link (DMI).

3.5.15 DMI Link Entry 1 Description (DMILE1D_0_0_0_DMIBAR) — Offset 50h

First part of a Link Entry which declares an internal link to another Root Complex Element.

Type	Size	Offset	Default
MMIO	32 bit	DMIBAR + 50h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:24	00h RW/L	**Target Port Number (TPN):** Specifies the port number associated with the element targeted by this link entry (egress port of PCH). The target port number is with respect to the component that contains this element as specified by the target component ID. This can be programmed by BIOS, but the default value will likely be correct because the DMI RCRB in the PCH will likely be associated with the default egress port for the PCH meaning it will be assigned port number 0. **Locked by:** TLDMIREGS.WO_STATUS0_0_0_0_DMIBAR.TPNWOS
23:16	00h RW/L	**Target Component ID (TCID):** Identifies the physical component that is targeted by this link entry. BIOS Requirement: Must be initialized according to guidelines in the PCI Express* Isochronous/Virtual Channel Support Hardware Programming Specification (HPS). **Locked by:** TLDMIREGS.WO_STATUS0_0_0_0_DMIBAR.TCIDE1DWOS
15:2	0h RO	**Reserved**
1	0h RO	**Link Type (LTYP):** Indicates that the link points to memory-mapped space (for RCRB). The link address specifies the 64-bit base address of the target RCRB.
0	0h RW/L	**Link Valid (LV):** 0: Link Entry is not valid and will be ignored. 1: Link Entry specifies a valid link. **Locked by:** TLDMIREGS.WO_STATUS0_0_0_0_DMIBAR.LVE1DWOS

3.5.16 DMI Link Entry 1 Address (DMILE1A_0_0_0_DMIBAR) — Offset 58h

Second part of a Link Entry which declares an internal link to another Root Complex Element.

Type	Size	Offset	Default
MMIO	32 bit	DMIBAR + 58h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:12	00000h RW/L	**Link Address (LA):** Memory mapped base address of the RCRB that is the target element (egress port of PCH) for this link entry. **Locked by:** TLDMIREGS.WO_STATUS0_0_0_0_DMIBAR.LAE1DWOS
11:0	0h RO	**Reserved**

3.5.17 DMI Link Upper Entry 1 Address (DMILUE1A_0_0_0_DMIBAR) — Offset 5Ch

Second part of a Link Entry which declares an internal link to another Root Complex Element.

Type	Size	Offset	Default
MMIO	32 bit	DMIBAR + 5Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:8	0h RO	**Reserved**
7:0	00h RW/L	**Upper Link Address (ULA):** Memory mapped base address of the RCRB that is the target element (egress port of PCH) for this link entry. **Locked by:** TLDMIREGS.WO_STATUS0_0_0_0_DMIBAR.ULAE1DWOS

3.5.18 DMI Link Entry 2 Description (DMILE2D_0_0_0_DMIBAR) — Offset 60h

First part of a Link Entry which declares an internal link to another Root Complex Element.

Type	Size	Offset	Default
MMIO	32 bit	DMIBAR + 60h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:24	00h RO	**Target Port Number (TPN):** Specifies the port number associated with the element targeted by this link entry (Egress Port). The target port number is with respect to the component that contains this element as specified by the target component ID.
23:16	00h RW/L	**Target Component ID (TCID):** Identifies the physical or logical component that is targeted by this link entry. **BIOS Requirement**: Must be initialized according to guidelines in the PCI Express* Isochronous/Virtual Channel Support Hardware Programming Specification (HPS). **Locked by:** TLDMIREGS.WO_STATUS0_0_0_0_DMIBAR.TCIDE2DWOS
15:2	0h RO	**Reserved**
1	0h RO	**Link Type (LTYP):** Indicates that the link points to memory-mapped space (for RCRB). The link address specifies the 64-bit base address of the target RCRB.
0	0h RW/L	**Link Valid (LV):** 0: Link Entry is not valid and will be ignored. 1: Link Entry specifies a valid link. **Locked by:** TLDMIREGS.WO_STATUS0_0_0_0_DMIBAR.LVE2DWOS

3.5.19 DMI Link Entry 2 Address (DMILE2A_0_0_0_DMIBAR) — Offset 68h

Second part of a Link Entry which declares an internal link to another Root Complex Element.

Type	Size	Offset	Default
MMIO	32 bit	DMIBAR + 68h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:12	00000h RW/L	**Link Address (LA):** Memory mapped base address of the RCRB that is the target element (Egress Port) for this link entry. **Locked by:** TLDMIREGS.WO_STATUS0_0_0_0_DMIBAR.LAE2DWOS

Bit Range	Default & Access	Field Name (ID): Description
11:0	0h RO	**Reserved**

3.5.20 Link Control (LCTL_0_0_0_DMIBAR) — Offset 88h

Allows control of PCI Express link.

Type	Size	Offset	Default
MMIO	16 bit	DMIBAR + 88h	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:10	0h RO	**Reserved**
9	0h RO	**Hardware Autonomous Width Disable (HAWD):** OPI: Not available When Set, this bit disables hardware from changing the Link width for reasons other than attempting to correct unreliable Link operation by reducing Link width. Devices that do not implement the ability autonomously to change Link width are permitted to hardwire this bit to 0b.
8	0h RO	**Reserved**
7	0h RW	**Extended Sync (ES):** OPI: Not available 0: Standard Fast Training Sequence (FTS). 1: Forces the transmission of additional ordered sets when exiting the L0s state and when in the Recovery state. This mode provides external devices (e.g., logic analyzers) monitoring the Link time to achieve bit and symbol lock before the link enters L0 and resumes communication. This is a test mode only and may cause other undesired side effects such as buffer overflows or underruns.
6	0h RO	**Reserved**
5	0h RO	**Retrain Link (RL):** 0: Normal operation. 1: Full Link retraining is initiated by directing the Physical Layer LTSSM from L0, L0s, or L1 states to the Recovery state. This bit always returns 0 when read. This bit is cleared automatically (no need to write a 0).
4:2	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
1:0	0h RO	**Active State PM (ASPM):** Controls the level of active state power management supported on the given link. 00b: Disabled 01b: L0s Entry Supported 10b: L1 Entry Supported 11b: L0s and L1 Entry Supported

3.5.21 DMI Uncorrectable Error Status (DMIUESTS_0_0_0_DMIBAR) — Offset 1C4h

This register is for test and debug purposes only.

Type	Size	Offset	Default
MMIO	32 bit	DMIBAR + 1C4h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:21	0h RO	**Reserved**
20	0h RW/1C/V/P	**Unsupported Request Error Status (URES):** Unsupported Request Error Status
19	0h RO	**Reserved**
18	0h RW/1C/V/P	**Malformed TLP Status (MTLPS):** Malformed TLP Status
17	0h RW/1C/V/P	**Receiver Overflow Status (ROS):** Receiver Overflow Status
16	0h RW/1C/V/P	**Unexpected Completion Status (UCS):** Unexpected Completion Status
15	0h RO	**Reserved**
14	0h RW/1C/V/P	**Completion Timeout Status (CTS):** Completion Timeout Status
13	0h RO	**Reserved**
12	0h RW/1C/V/P	**Poisoned TLP Status (PTLPS):** Poisoned TLP Status

Bit Range	Default & Access	Field Name (ID): Description
11:5	0h RO	**Reserved**
4	0h RW/1C/V/P	**Data Link Protocol Error Status (DLPES):** Data Link Protocol Error Status
3:0	0h RO	**Reserved**

3.5.22 DMI Uncorrectable Error Mask (DMIUEMSK_0_0_0_DMIBAR) — Offset 1C8h

This register is for test and debug purposes only.

Type	Size	Offset	Default
MMIO	32 bit	DMIBAR + 1C8h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:23	0h RO	**Reserved**
22	0h RW/P	**2 Bit Error Mask (ECCERRM):** 2 Bit Error Mask
21	0h RO	**Reserved**
20	0h RW/P	**Unsupported Request Error Mask (UREM):** Unsupported Request Error Mask
19	0h RO	**Reserved**
18	0h RW/P	**Malformed TLP Mask (MTLPM):** Malformed TLP Mask
17	0h RW/P	**Receiver Overflow Mask (ROM):** Receiver Overflow Mask
16	0h RW/P	**Unexpected Completion Mask (UCM):** Unexpected Completion Mask
15	0h RO	**Reserved**
14	0h RW/P	**Completion Timeout Mask (CPLTM):** Completion Timeout Mask
13	0h RO	**Reserved**
12	0h RW/P	**Poisoned TLP Mask (PTLPM):** Poisoned TLP Mask

Bit Range	Default & Access	Field Name (ID): Description
11:5	0h RO	**Reserved**
4	0h RW/P	**Data Link Protocol Error Mask (DLPEM):** Data Link Protocol Error Mask
3:0	0h RO	**Reserved**

3.5.23 DMI Uncorrectable Error Severity (DMIUESEV_0_0_0_DMIBAR) — Offset 1CCh

This register controls whether an individual error is reported as a non-fatal or fatal error. An error is reported as fatal when the corresponding error bit in the severity register is set. If the bit is cleared, the corresponding error is considered nonfatal. It is for test and debug purposes only.

Type	Size	Offset	Default
MMIO	32 bit	DMIBAR + 1CCh	00060010h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:23	0h RO	**Reserved**
22	0h RW/P	**2 Bit Error Mask (ECCERRS):** 2 Bit Error Mask
21	0h RO	**Reserved**
20	0h RW/P	**Unsupported Request Error Severity (URES):** Unsupported Request Error Severity
19	0h RO	**ECRC Error Severity (ECRCES):** ECRC Error Severity
18	1h RW/P	**Malformed TLP Error Severity (MTLPES):** Malformed TLP Error Severity
17	1h RW/P	**Receiver Overflow Error Severity (ROEV):** Receiver Overflow Error Severity
16	0h RW/P	**Unexpected Completion Error Severity (UCES):** Unexpected Completion Error Severity
15	0h RO	**Completer Abort Error Severity (CAES):** Completer Abort Error Severity
14	0h RW/P	**Completion Timeout Error Severity (CTES):** Completion Timeout Error Severity
13	0h RO	**Flow Control Protocol Error Severity (FCPES):** Flow Control Protocol Error Severity

Bit Range	Default & Access	Field Name (ID): Description
12	0h RW/P	**Poisoned TLP Error Severity (PTLPES):** Poisoned TLP Error Severity
11:5	0h RO	**Reserved**
4	1h RW/P	**Data Link Protocol Error Severity (DLPES):** Data Link Protocol Error Severity
3:0	0h RO	**Reserved**

3.5.24 DMI Correctable Error Status (DMICESTS_0_0_0_DMIBAR) — Offset 1D0h

This register is for test and debug purposes only.

Type	Size	Offset	Default
MMIO	32 bit	DMIBAR + 1D0h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:14	0h RO	**Reserved**
13	0h RW/1C/V/P	**Advisory Non-Fatal Error Status (ANFES):** When set, indicates that an Advisory Non-Fatal Error occurred.
12	0h RW/1C/V/P	**Replay Timer Timeout Status (RTTS):** Replay Timer Timeout Status
11:9	0h RO	**Reserved**
8	0h RW/1C/V/P	**REPLAY_NUM Rollover Status (RNRS):** REPLAY_NUM Rollover Status
7	0h RW/1C/V/P	**Bad DLLP Status (BDLLPS):** Bad DLLP Status
6	0h RW/1C/V/P	**Bad TLP Status (BTLPS):** Bad TLP Status
5:1	0h RO	**Reserved**
0	0h RW/1C/V/P	**Receiver Error Status (RES):** Physical layer receiver Error occurred. These errors include: elastic Buffer Collision, 8b/10b error, De-skew Timeout Error.

3.5.25 DMI Correctable Error Mask (DMICEMSK_0_0_0_DMIBAR) — Offset 1D4h

This register is for test and debug purposes only.

Type	Size	Offset	Default
MMIO	32 bit	DMIBAR + 1D4h	00002000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:14	0h RO	**Reserved**
13	1h RW/P	**Advisory Non-Fatal Error Mask (ANFEM):** When set, masks Advisory Non-Fatal errors from: • Signaling ERR_COR to the device control register • Updating the Uncorrectable Error Status register. This register is set by default to enable compatibility with software that does not comprehend Role-Based Error Reporting.
12:0	0h RO	**Reserved**

3.6 REGBAR Registers

This chapter documents the REGBAR registers. Base address of these registers are defined in the REGBAR_0_0_0_MCHBAR_IMPH register which resides in the MCHBAR register collection.

Note: These registers apply to all processors.

3.6.1 Summary of Registers

Table 3-7. Summary of REGBAR Registers

Offset	Size (Bytes)	Register Name (Register Symbol)	Default Value
0h	4	IOM PCH Request FIFO Last Entry (IOM_PCH_REQ_FIFO_LAST_ENTRY)	00000000h
4h	4	IOM PCH Task FIFO Last Entry (IOM_PCH_REQ_FIFO_EXT_ENTRY)	00000000h
Ch	4	IOM Firmware IMR Status (IOM_CSME_IMR_IOM_STATUS)	00000000h
10h	4	PHY Image Status in IMR (IOM_CSME_IMR_PHY_STATUS)	00000000h
14h	4	Thunderbolt Firmware Status in IMR (IOM_CSME_IMR_TBT_STATUS)	00000000h
3Ch	4	IOM TypeC Configuration Strap 1 (IOM_TYPEC_CONFIGURATION_1)	00000000h
40h	4	TypeC Configuration 1 (IOM_TYPEC_SW_CONFIGURATION_1)	00040200h
48h	4	TypeC Configuration 3 (IOM_TYPEC_SW_CONFIGURATION_3)	00000000h
50h	4	TypeC Subsystem Status 1 (IOM_TYPEC_STATUS_1)	00000000h
58h	4	IOM TCSS Device Enable (IOM_TCSS_DEVEN)	00000000h
5Ch	4	IOM TCSS Port Map (IOM_TCSS_PORT_MAP)	00000400h
98h	4	TypeC Configuration 4 (IOM_TYPEC_SW_CONFIGURATION_4)	00000000h
14Ch	4	IOM PM Status (IOM_PM_STATUS)	0000001Fh
16Ch	4	Port Status 0 (IOM_PORT_STATUS[0])	00000000h
170h	4	Port Status 1 (IOM_PORT_STATUS[1])	00000000h
174h	4	Port Status 2 (IOM_PORT_STATUS[2])	00000000h
178h	4	Port Status 3 (IOM_PORT_STATUS[3])	00000000h
102Ch	4	IOM DisplayPort Resource Management 0 (IOM_DP_RESOURCE_MNG[0])	00000000h
1030h	4	IOM DisplayPort Resource Management 1 (IOM_DP_RESOURCE_MNG[1])	00000000h
1038h	4	IOM DisplayPort HW Resource Semaphore 0 (IOM_DP_RESOURCE_SEMAPHORE[0])	00000000h
103Ch	4	IOM DisplayPort HW Resource Semaphore 1 (IOM_DP_RESOURCE_SEMAPHORE[1])	00000000h
1044h	4	DisplayPort Input Graphics Source Policy Management (DPIN_GFX_SRC_POLICY_MGMT)	00000000h
118Ch	4	IOM Firmware Current Task (IOM_FW_CURRENT_TASK)	00000000h
12C8h	4	IOM Firmware Info (IOM_FW_INFO)	00000000h

3.6.2 IOM PCH Request FIFO Last Entry (IOM_PCH_REQ_FIFO_LAST_ENTRY) — Offset 0h

This is the entry pointed to by the rd_ptr of the fifo, every read from this register will update the rd_ptr, thus loading the next entry to this register.

Type	Size	Offset	Default
MMIO	32 bit	REGBAR + 0h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:30	0h RO	**Reserved**
29:27	0h RO	**STAGE:** stage of the execution. Always starts with 0. Progress according to the progress of the thread
26:24	0h RO	**Reserved**
23:16	00h RO	**DATA:** With Command 3, equals ModeData
15:12	0h RO	**PARAMS:** Command 1: x, x, ORI, UFP Command 3: ModeType Command 4: x, x, IRQ, LVL
11:8	0h RO	**USB2 Port Number (USB2_PORT_NUM):** USB2 Port Number: 1's based number (first port = port 1). Up to 16 ports can be encoded. A value of '0h' means port 16
7:4	0h RO	**USB3 Port Number (USB3_PORT_NUM):** USB3 Port Number: 1's based number (first port = port 1). Up to 16 ports can be encoded. A value of '0h' means port 16
3:0	0h RO	**Request Opcode (OPCODE):** Request Opcode.

3.6.3 IOM PCH Task FIFO Last Entry (IOM_PCH_REQ_FIFO_EXT_ENTRY) — Offset 4h

This is the entry pointed to by the rd_ptr of the FIFO, every read from this register will update the rd_ptr, thus loading the next entry to this register.

Type	Size	Offset	Default
MMIO	32 bit	REGBAR + 4h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RO	**Last Entry (DATA):** Last Entry.

3.6.4 IOM Firmware IMR Status (IOM_CSME_IMR_IOM_STATUS) — Offset Ch

IOM FW Status in IMR

Type	Size	Offset	Default
MMIO	32 bit	REGBAR + Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31	0h RO	**FW Download Done (DONE):** FW download to IMR is done
30	0h RO	**Valid Authentication (VALID):** Valid: although the FW is in the IMR, it failed authentication and therefore shouldn't be trusted. 0: Untrusted FW, 1: Successful authentication, FW is trusted and can be used.
29:22	00h RO	**Error Code (ERROR_CODE):** Error code Logged by CSME while populating IOM FW portion of the IOM image.
21:0	0h RO	**Reserved**

3.6.5 PHY Image Status in IMR (IOM_CSME_IMR_PHY_STATUS) — Offset 10h

PHY Image Status in IMR

Type	Size	Offset	Default
MMIO	32 bit	REGBAR + 10h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31	0h RO	**FW Download Done (DONE):** FW download to IMR is done
30	0h RO	**Valid Authentication (VALID):** Valid: although the FW is in the IMR, it failed authentication and therefore shouldn't be trusted. 0: Untrusted FW, 1: Successful authentication, FW is trusted and can be used.
29:22	00h RO	**Error Code (ERROR_CODE):** ERROR CODE Logged by CSME while populating PHY IMR.
21:16	0h RO	**Reserved**
15:0	0000h RO	**Firmware Version (FW_VERSION):** The version of firmware that the PHY is using.

3.6.6 Thunderbolt Firmware Status in IMR (IOM_CSME_IMR_TBT_STATUS) — Offset 14h

Thunderbolt Firmware Status in IMR.

Type	Size	Offset	Default
MMIO	32 bit	REGBAR + 14h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31	0h RO	**FW Download Done (DONE):** FW download to IMR is done
30	0h RO	**Valid Authentication (VALID):** Valid: although the FW is in the IMR, it failed authentication and therefore shouldn't be trusted. 0: Untrusted FW, 1: Successful authentication, FW is trusted and can be used.
29:22	00h RO	**Error Code (ERROR_CODE):** ERROR CODE Logged by CSME while populating Thunderbolt IMR.

Bit Range	Default & Access	Field Name (ID): Description
21:16	0h RO	**Reserved**
15:0	0000h RO	**Firmware Version (FW_VERSION):** The version of firmware that Thunderbolt is using.

3.6.7 IOM TypeC Configuration Strap 1 (IOM_TYPEC_CONFIGURATION_1) — Offset 3Ch

This register hold the TypeC configuration.

Type	Size	Offset	Default
MMIO	32 bit	REGBAR + 3Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:16	0h RO	**Reserved**
15:12	0h RO	**Fixed Connection Port 4 (FIXED_CONNECTION_PORT4):** • 0001b: DisplayPort or HDMI • 0010b: DisplayPort Input • Other values are reserved
11:8	0h RO	**Fixed Connection Port 3 (FIXED_CONNECTION_PORT3):** • 0001b: DisplayPort or HDMI • 0010b: DisplayPort Input • Other values are reserved
7:4	0h RO	**Fixed Connection Port 2 (FIXED_CONNECTION_PORT2):** • 0001b: DisplayPort or HDMI • 0010b: DisplayPort Input • Other values are reserved
3:0	0h RO	**Fixed Connection Port 1 (FIXED_CONNECTION_PORT1):** • 0001b: DisplayPort or HDMI • 0010b: DisplayPort Input • Other values are reserved

3.6.8 TypeC Configuration 1 (IOM_TYPEC_SW_CONFIGURATION_1) — Offset 40h

Various configuration options for the TypeC subsystem

Type	Size	Offset	Default
MMIO	32 bit	REGBAR + 40h	00040200h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RW/L	**LOCK:** Locks this register from further changes. **Locked by:** IOM_TYPEC_SW_CONFIGURATION_1.LOCK
30:19	0h RO	**Reserved**
18	1h RW/L	**Compatibility Revision ID Enable (CRID_EN):** Enable for Compatibility Revision ID(CRID) **Locked by:** IOM_TYPEC_SW_CONFIGURATION_1.LOCK
17	0h RW	**All Monitors Off (ALL_MONITORS_OFF):** ALL Monitors are off BIOS indication that all monitors are off and it is allowed to enable deeper PM states.
16	0h RW/V	**D3 Cold Acknowledge (D3_COLD_ACK):** IOM acknowledge for D3 cold request. 0: TCSS out of D3Cold 1: TCSS is in D3Cold
15	0h RW	**D3 Cold Request (D3_COLD_REQ):** BIOS sets this bit when all devices are in D3 Hot. It indicates that the IOM can try putting the TCSS in TCCOLD state.
14	0h RW	**EC REPLAY on S45 (BIOS_EC_REPLAY_CONNECTION_S4S5):** S3 - if a device is attached must have support from EC to replay connection map to shut the rail down **Locked by:** MEM_IOM_TYPEC_SW_CONFIGURATION_1.LOCK
13	0h RW	**EC REPLAY on S3 (BIOS_EC_REPLAY_CONNECTION_S3):** S3 - if a device is attached must have support from EC to replay connection map to shut the rail down **Locked by:** MEM_IOM_TYPEC_SW_CONFIGURATION_1.LOCK
12:10	0h RO	**Reserved**
9	1h RW/L	**D3 Cold Enable (D3_COLD_EN):** Enable D3 cold for TCSS. **Locked by:** IOM_TYPEC_SW_CONFIGURATION_1.LOCK
8	0h RW/L	**D3 Hot Enable (D3_HOT_EN):** Enable D3 hot for TCSS. **Locked by:** IOM_TYPEC_SW_CONFIGURATION_1.LOCK
7:0	00h RW/L	**DisplayPort Input (DPin) Map (DPIN_MAP):** Active DPin port. BIOS read DPin present from PCH's GPIO and updates this field accordingly. **Locked by:** IOM_TYPEC_SW_CONFIGURATION_1.LOCK

3.6.9 TypeC Configuration 3 (IOM_TYPEC_SW_CONFIGURATION_3) — Offset 48h

Define AUX orientation.

If Aux Orientation override is enabled and set, the AUX orientation is flipped

Type	Size	Offset	Default
MMIO	32 bit	REGBAR + 48h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RW/L	**LOCK:** Locks this register from further changes. **Locked by:** IOM_TYPEC_SW_CONFIGURATION_3.LOCK
30:8	0h RO	**Reserved**
7	0h RW/L	**Port 4 Aux Orientation (PORT4_AUX_ORIENTATION):** This bit's value is used only if Aux Orientation Override enable bit is set. This bit indicates if USB lanes are swapped on the motherboard for routing ease ONLY. This bit is set to 0, when Aux lines are correctly routed to the USB-C connector. This bit is set to 1, when Aux lines are swapped on the motherboard to the USB-C connector. **Locked by:** IOM_TYPEC_SW_CONFIGURATION_3.LOCK
6	0h RW/L	**Port 4 Retimer Enable (PORT4_RETIMER_ENABLE):** Port Retimer Enable **Locked by:** IOM_TYPEC_SW_CONFIGURATION_3.LOCK
5	0h RW/L	**Port 3 Aux Orientation (PORT3_AUX_ORIENTATION):** This bit's value is used only if Aux Orientation Override enable bit is set. This bit indicates if USB lanes are swapped on the motherboard for routing ease ONLY. This bit is set to 0, when Aux lines are correctly routed to the USB-C connector. This bit is set to 1, when Aux lines are swapped on the motherboard to the USB-C connector. **Locked by:** IOM_TYPEC_SW_CONFIGURATION_3.LOCK
4	0h RW/L	**Port 3 Retimer Enable (PORT3_RETIMER_ENABLE):** Port Retimer Enable **Locked by:** IOM_TYPEC_SW_CONFIGURATION_3.LOCK
3	0h RW/L	**Port 2 Aux Orientation (PORT2_AUX_ORIENTATION):** This bit's value is used only if Aux Orientation Override enable bit is set. This bit indicates if USB lanes are swapped on the motherboard for routing ease ONLY. This bit is set to 0, when Aux lines are correctly routed to the USB-C connector. This bit is set to 1, when Aux lines are swapped on the motherboard to the USB-C connector. **Locked by:** IOM_TYPEC_SW_CONFIGURATION_3.LOCK

Bit Range	Default & Access	Field Name (ID): Description
2	0h RW/L	**Port 2 Retimer Enable (PORT2_RETIMER_ENABLE):** Port Retimer Enable **Locked by:** IOM_TYPEC_SW_CONFIGURATION_3.LOCK
1	0h RW/L	**Port 1 Aux Orientation (PORT1_AUX_ORIENTATION):** This bit's value is used only if Aux Orientation Override enable bit is set. This bit indicates if USB lanes are swapped on the motherboard for routing ease ONLY. This bit is set to 0, when Aux lines are correctly routed to the USB-C connector. This bit is set to 1, when Aux lines are swapped on the motherboard to the USB-C connector. **Locked by:** IOM_TYPEC_SW_CONFIGURATION_3.LOCK
0	0h RW/L	**Port 1 Retimer Enable (PORT1_RETIMER_ENABLE):** Port Retimer Enable **Locked by:** IOM_TYPEC_SW_CONFIGURATION_3.LOCK

3.6.10 TypeC Subsystem Status 1 (IOM_TYPEC_STATUS_1) — Offset 50h

Indicate TCSS status.

Type	Size	Offset	Default
MMIO	32 bit	REGBAR + 50h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31	0h RO	**TypeC Subsystem Ready (TYPEC_SS_READY):** TypeC Subsystem is ready
30	0h RO	**IOM Ready (IOM_READY):** This indication means IOM FW got out of reset and ready.
29:8	0h RO	**Reserved**
7:0	00h RO	**Fixed Connection Configured (FIXED_CONNECTION_CONFIGURED):** DP fixed connection are configured.

3.6.11 IOM TCSS Device Enable (IOM_TCSS_DEVEN) — Offset 58h

IOM TCSS Device enable Register

Type	Size	Offset	Default
MMIO	32 bit	REGBAR + 58h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:12	0h RO	**Reserved**
11	0h RO	**Thunderbolt DMA1 Enable (TBT_DMA1_EN):** 0: DMA1 is disabled and hidden. 1: DMA1 is enabled and visible.
10	0h RO	**Thunderbolt DMA0 Enable (TBT_DMA0_EN):** 0: DMA0 is disabled and hidden. 1: DMA0 is enabled and visible.
9	0h RO	**XDCI Enable (XDCI_EN):** 0: Bus 0 Device 13 Function 1 is disabled and hidden. 1: Bus 0 Device 13 Function 1 is enabled and visible.
8	0h RO	**XHCI Enable (XHCI_EN):** 0: Bus 0 Device 13 Function 1 is disabled and hidden. 1: Bus 0 Device 13 Function 1 is enabled and visible.
7:4	0h RO	**Reserved**
3	0h RO	**PCIE3 Enable (PCIE3_EN):** 0: TypeC PCIe root port 3 is disabled 1: TypeC PCIe root port 3 is enabled.
2	0h RO	**PCIE2 Enable (PCIE2_EN):** 0: TypeC PCIe root port2 is disabled 1: TypeC PCIe root port 2 is enabled.
1	0h RO	**PCIE1 Enable (PCIE1_EN):** 0: TypeC PCIe root port 1 is disabled 1: TypeC PCIe root port 1 is enabled.
0	0h RO	**PCIE0 Enable (PCIE0_EN):** 0: TypeC PCIe root port 0 is disabled 1: TypeC PCIe root port 0 is enabled.

3.6.12 IOM TCSS Port Map (IOM_TCSS_PORT_MAP) — Offset 5Ch

IOM TCSS Port Map register

Type	Size	Offset	Default
MMIO	32 bit	REGBAR + 5Ch	00000400h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:11	0h RO	**Reserved**
10	1h RO	**HTI DIS (HTI_DIS):** High Speed Tracing Interface Disable.
9:8	0h RO	**Max number of DPIN (MAX_NUM_OF_DPIN):** Max number of DPIN
7:4	0h RO	**Reserved**
3	0h RO	**Port 4 Enable (PORT_4_EN):** PORT 4 Enable
2	0h RO	**Port 3 Enable (PORT_3_EN):** PORT 3 Enable
1	0h RO	**Port 2 Enable (PORT_2_EN):** PORT 2 Enable
0	0h RO	**Port 1 Enable (PORT_1_EN):** PORT 1 Enable

3.6.13 TypeC Configuration 4 (IOM_TYPEC_SW_CONFIGURATION_4) — Offset 98h

Defines High Speed Lane (HSL) orientation.

If High Speed Lane Orientation override is enabled and set, the High Speed Lane Orientation is flipped.

Type	Size	Offset	Default
MMIO	32 bit	REGBAR + 98h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RW/L	**LOCK:** Locks this register from further changes. **Locked by:** IOM_TYPEC_SW_CONFIGURATION_4.LOCK

Bit Range	Default & Access	Field Name (ID): Description
30:8	0h RO	**Reserved**
7	0h RW/L	**Port 4 High Speed Lane Orientation (PORT4_HSL_ORIENTATION):** This bit's value is used only if High Speed Lane Orientation Override enable bit is set. This bit indicates if HSL lanes are swapped on the motherboard for routing ease ONLY. This bit is set to 0, when HSL lines are correctly routed to the USB-C connector. This bit is set to 1, when HSL lines are swapped on the motherboard to the USB-C connector. **Locked by:** IOM_TYPEC_SW_CONFIGURATION_4.LOCK
6	0h RW/L	**Port 4 High Speed Lane Orientation Override (PORT4_HSL_ORIENTATION_OVRRD_EN):** This bit controls if High Speed Lane Orientation is done by the processor or externally by platform component (retimer/PD/Port controller). This bit is set to 0, when retimer is present on the system. i.e. High Speed Lane Orientation is done by retimer. This bit is set to 1, when retimer is NOT present on the system i.e. High Speed Lane Orientation is done by the processor. This bit is set to 0, when retimer is NOT present on the system & PD or Port controller has High Speed Lane Orientation mux i.e. USB orientation is done by PD or Port controller & the processor does NOT do High Speed Lane Orientation. **Locked by:** IOM_TYPEC_SW_CONFIGURATION_4.LOCK
5	0h RW/L	**Port 3 High Speed Lane Orientation (PORT3_HSL_ORIENTATION):** This bit's value is used only if High Speed Lane Orientation Override enable bit is set. This bit indicates if HSL lanes are swapped on the motherboard for routing ease ONLY. This bit is set to 0, when HSL lines are correctly routed to the USB-C connector. This bit is set to 1, when HSL lines are swapped on the motherboard to the USB-C connector. **Locked by:** IOM_TYPEC_SW_CONFIGURATION_4.LOCK
4	0h RW/L	**Port 3 High Speed Lane Orientation Override (PORT3_HSL_ORIENTATION_OVRRD_EN):** This bit controls if High Speed Lane Orientation is done by the processor or externally by platform component (retimer/PD/Port controller). This bit is set to 0, when retimer is present on the system. i.e. High Speed Lane Orientation is done by retimer. This bit is set to 1, when retimer is NOT present on the system i.e. High Speed Lane Orientation is done by the processor. This bit is set to 0, when retimer is NOT present on the system & PD or Port controller has High Speed Lane Orientation mux i.e. USB orientation is done by PD or Port controller & the processor does NOT do High Speed Lane Orientation. **Locked by:** IOM_TYPEC_SW_CONFIGURATION_4.LOCK
3	0h RW/L	**Port 2 High Speed Lane Orientation (PORT2_HSL_ORIENTATION):** This bit's value is used only if High Speed Lane Orientation Override enable bit is set. This bit indicates if HSL lanes are swapped on the motherboard for routing ease ONLY. This bit is set to 0, when HSL lines are correctly routed to the USB-C connector. This bit is set to 1, when HSL lines are swapped on the motherboard to the USB-C connector. **Locked by:** IOM_TYPEC_SW_CONFIGURATION_4.LOCK

Bit Range	Default & Access	Field Name (ID): Description
2	0h RW/L	**Port 2 High Speed Lane Orientation Override (PORT2_HSL_ORIENTATION_OVRRD_EN):** This bit controls if High Speed Lane Orientation is done by the processor or externally by platform component (retimer/PD/Port controller). This bit is set to 0, when retimer is present on the system. i.e. High Speed Lane Orientation is done by retimer. This bit is set to 1, when retimer is NOT present on the system i.e. High Speed Lane Orientation is done by the processor. This bit is set to 0, when retimer is NOT present on the system & PD or Port controller has High Speed Lane Orientation mux i.e. USB orientation is done by PD or Port controller & the processor does NOT do High Speed Lane Orientation. **Locked by:** IOM_TYPEC_SW_CONFIGURATION_4.LOCK
1	0h RW/L	**Port 1 High Speed Lane Orientation (PORT1_HSL_ORIENTATION):** This bit's value is used only if High Speed Lane Orientation Override enable bit is set. This bit indicates if HSL lanes are swapped on the motherboard for routing ease ONLY. This bit is set to 0, when HSL lines are correctly routed to the USB-C connector. This bit is set to 1, when HSL lines are swapped on the motherboard to the USB-C connector. **Locked by:** IOM_TYPEC_SW_CONFIGURATION_4.LOCK
0	0h RW/L	**Port 1 High Speed Lane Orientation Override (PORT1_HSL_ORIENTATION_OVRRD_EN):** This bit controls if High Speed Lane Orientation is done by the processor or externally by platform component (retimer/PD/Port controller). This bit is set to 0, when retimer is present on the system. i.e. High Speed Lane Orientation is done by retimer. This bit is set to 1, when retimer is NOT present on the system i.e. High Speed Lane Orientation is done by the processor. This bit is set to 0, when retimer is NOT present on the system & PD or Port controller has High Speed Lane Orientation mux i.e. USB orientation is done by PD or Port controller & the processor does NOT do High Speed Lane Orientation. **Locked by:** IOM_TYPEC_SW_CONFIGURATION_4.LOCK

3.6.14 IOM PM Status (IOM_PM_STATUS) — Offset 14Ch

Holds the current power management status of the TCSS.

Type	Size	Offset	Default
MMIO	32 bit	REGBAR + 14Ch	0000001Fh

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:6	0h RO	**Reserved**
5	0h RO	**GoSS Message Received (GOSS_RECVD):** HW Sets upon receiving it and Clears on a PM Response.
4	1h RO	**Global IOM Blocked (GLOBAL_IOM_BLOCKED):** IOM Global Blocked Status. Set by Firmware on a Block Ack to the PCU and Cleared by HW on Unblock.

Bit Range	Default & Access	Field Name (ID): Description
3:0	Fh RO	**TCSS PM State (TCSS_PM_STATE):** Current TCSS PM state TC0-TC7 [0000b-0111b]. 1111b is TCReset state

3.6.15 Port Status 0 (IOM_PORT_STATUS[0]) — Offset 16Ch

TypeC port (PHY) status and control.

Note that 'Port' and 'PHY' are used interchangeably

Type	Size	Offset	Default
MMIO	32 bit	REGBAR + 16Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31	0h RO	**Port Is Connected (PORT_IS_CONNECTED):** Status indication that the port is connected. 0x0: Port is not connected. 0x1: Port is connected (IOM FW is done configuring the port).
30:29	0h RO	**Reserved**
28	0h RO	**Aux Orientation (AUX_ORI):** Aux orientation status Status. 0: Orientation is not flipped. 1: Orientation is flipped.
27:20	00h RO	**Mode Type (MODE_TYPE):** Various usage models. Example is to specify the NiDnT overlay mode or Intel debug overlay mode.
19:12	00h RO	**HPD Status (DHPD):** HPD status. DHPD[1:0] - HPD current state. 0x0: No HPD. 0x1: HPD asserted. 0x2: HPD deasserted. 0x3 Invalid. DHPD[2:2] - HPD current state source. 0x0: PCH. 0x1: Thunderbolt DHPD[3:3] - HPD current state destination. 0x0: DP. 0x1: DPin. DHPD[5:4] - Deferred HPD current state. 0x0: No HPD. 0x1: HPD asserted. 0x2: HPD deasserted. 0x3 Invalid. DHPD[6:6] - Deferred HPD current state source. 0x0: PCH. 0x1: Thunderbolt DHPD[7:7] - Reserved.
11	0h RO	**High Speed Link Orientation Status (HSL_ORI):** High-Speed Link Orientation Status. 0: Orientation is not flipped. 1: Orientation is flipped.
10	0h RO	**Upstream Facing Port Status (UFP):** 0: Downstream facing port. TCSS USB is configured to be the Host. 1: Upstream facing port. TCSS USB is configured to be the Device.

Bit Range	Default & Access	Field Name (ID): Description
9:6	0h RO	**Port activity type (ACTIVITY_TYPE):** Port activity type. The TypeC PHY is flexible thus it can be configured for various possible connections. • 0x0: Undefined • 0x1: Fixed connection • 0x2: DisplayPort Input • 0x3: USB3 • 0x4: Safe mode • 0x5: Alt mode DisplayPort • 0x6: Alt mode DisplayPort MFD (Multi Function Device) • 0x7: Alt mode Thunderbolt • 0x8: HTI (High-speed Trace Interface - used for debug) • 0x9: Alt mode NiDnT (Debug mode) • 0xA: DBGACC (Debug accessory) • 0xB: HTI direct (Debug) • 0xC: Alt mode USB3 • 0xD: Alt mode Thunderbolt USB3 • 0xE: No Thunderbolt allowed
5	0h RO	**Configuration Done (CFG_DONE):** Control / Status bit to indicate that the port configuration is complete. This bit is also tied to the PHY common lane reset. 1: Port configuration is complete. Deassert TypeC PHY (port) common lane reset. 0: Port configuration is not complete. Assert TypeC PHY (port) common lane reset.
4	0h RO	**Port in Transition (PORT_IN_TRANSITION):** Indicator that the port bring-up is in progress.
3	0h RO	**Port Enabled (PORT_EN):** Status indicator if the PHY is enabled by BIOS.
2:0	0h RO	**PHY Command (CMD):** PHY Command: 0x0: NO-OP, 0x1: Wake PHY, 0x2: VNN OFF prep, 0x3: VNNAON OFF prep

3.6.16 Port Status 1 (IOM_PORT_STATUS[1]) — Offset 170h

TypeC port (PHY) status and control.

Note that 'Port' and 'PHY' are used interchangeably

Type	Size	Offset	Default
MMIO	32 bit	REGBAR + 170h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31	0h RO	**Port Is Connected (PORT_IS_CONNECTED):** Status indication that the port is connected. 0x0: Port is not connected. 0x1: Port is connected (IOM FW is done configuring the port).

Bit Range	Default & Access	Field Name (ID): Description
30:29	0h RO	**Reserved**
28	0h RO	**Aux Orientation (AUX_ORI):** Aux orientation status Status. 0: Orientation is not flipped. 1: Orientation is flipped.
27:20	00h RO	**Mode Type (MODE_TYPE):** Various usage models. Example is to specify the NiDnT overlay mode or Intel debug overlay mode.
19:12	00h RO	**HPD Status (DHPD):** HPD status. DHPD[1:0] - HPD current state. 0x0: No HPD. 0x1: HPD asserted. 0x2: HPD deasserted. 0x3 Invalid. DHPD[2:2] - HPD current state source. 0x0: PCH. 0x1: Thunderbolt DHPD[3:3] - HPD current state destination. 0x0: DP. 0x1: DPin. DHPD[5:4] - Deferred HPD current state. 0x0: No HPD. 0x1: HPD asserted. 0x2: HPD deasserted. 0x3 Invalid. DHPD[6:6] - Deferred HPD current state source. 0x0: PCH. 0x1: Thunderbolt DHPD[7:7] - Reserved.
11	0h RO	**High Speed Link Orientation Status (HSL_ORI):** 0: Orientation is not flipped. 1: Orientation is flipped.
10	0h RO	**Upstream Facing Port Status (UFP):** 0: Downstream facing port. TCSS USB is configured to be the Host. 1: Upstream facing port. TCSS USB is configured to be the Device.
9:6	0h RO	**Port Activity Type (ACTIVITY_TYPE):** port activity type: 0000b: USB3 0001b: Safe mode 0010b: Fixed connection 0100b: HTI (High-speed Trace Interface - used for debug) 0101b: NiDnT 1000b: DisplayPort-Inout 1100b: USB3 Alt mode 1101b: DisplayPort alt mode 1110b: DisplayPort alt mode MFD (Multi Function Device) 1111b: Thunderbolt alt mode
5	0h RO	**Configuration Done (CFG_DONE):** Control / Status bit to indicate that the port configuration is complete. This bit is also tied to the PHY common lane reset. 1: Port configuration is complete. Deassert TypeC PHY (port) common lane reset. 0: Port configuration is not complete. Assert TypeC PHY (port) common lane reset.
4	0h RO	**Port in Transition (PORT_IN_TRANSITION):** Indicator that the port bring-up is in progress.
3	0h RO	**Port Enabled (PORT_EN):** Status indicator if the PHY is enabled by BIOS.
2:0	0h RO	**PHY Command (CMD):** PHY Command: 0x0: NO-OP, 0x1: Wake PHY, 0x2: VNN OFF prep, 0x3: VNNAON OFF prep

3.6.17 Port Status 2 (IOM_PORT_STATUS[2]) — Offset 174h

TypeC port (PHY) status and control.

Note that 'Port' and 'PHY' are used interchangeably

Type	Size	Offset	Default
MMIO	32 bit	REGBAR + 174h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31	0h RO	**Port Is Connected (PORT_IS_CONNECTED):** Status indication that the port is connected. 0: Port is not connected. 1: Port is connected (IOM FW is done configuring the port).
30:29	0h RO	**Reserved**
28	0h RO	**Aux Orientation (AUX_ORI):** 0: Orientation is not flipped. 1: Orientation is flipped.
27:20	00h RO	**Mode Type (MODE_TYPE):** Various usage models. Example is to specify the NiDnT overlay mode or Intel debug overlay mode.
19:12	00h RO	**HPD Status (DHPD):** HPD status. DHPD[1:0] - HPD current state. 0x0: No HPD. 0x1: HPD asserted. 0x2: HPD deasserted. 0x3 Invalid. DHPD[2:2] - HPD current state source. 0x0: PCH. 0x1: Thunderbolt DHPD[3:3] - HPD current state destination. 0x0: DP. 0x1: DPin. DHPD[5:4] - Deferred HPD current state. 0x0: No HPD. 0x1: HPD asserted. 0x2: HPD deasserted. 0x3 Invalid. DHPD[6:6] - Deferred HPD current state source. 0x0: PCH. 0x1: Thunderbolt DHPD[7:7] - Reserved.
11	0h RO	**High Speed Link Orientation Status (HSL_ORI):** 0: Orientation is not flipped. 1: Orientation is flipped.
10	0h RO	**Upstream Facing Port Status (UFP):** 0: Downstream facing port. TCSS USB is configured to be the Host. 1: Upstream facing port. TCSS USB is configured to be the Device.
9:6	0h RO	**Port Activity Type (ACTIVITY_TYPE):** port activity type: 0000b: USB3 0001b: Safe mode 0010b: Fixed connection 0100b: HTI (High-speed Trace Interface - used for debug) 0101b: NiDnT 1000b: DisplayPort-Inout 1100b: USB3 Alt mode 1101b: DisplayPort alt mode 1110b: DisplayPort alt mode MFD (Multi Function Device) 1111b: Thunderbolt alt mode

Bit Range	Default & Access	Field Name (ID): Description
5	0h RO	**Configuration Done (CFG_DONE):** Control / Status bit to indicate that the port configuration is complete. This bit is also tied to the PHY common lane reset. 1: Port configuration is complete. Deassert TypeC PHY (port) common lane reset. 0: Port configuration is not complete. Assert TypeC PHY (port) common lane reset.
4	0h RO	**Port in Transition (PORT_IN_TRANSITION):** Indicator that the port bring-up is in progress.
3	0h RO	**Port Enabled (PORT_EN):** Status indicator if the PHY is enabled by BIOS.
2:0	0h RO	**PHY Command (CMD):** PHY Command: 0x0: NO-OP, 0x1: Wake PHY, 0x2: VNN OFF prep, 0x3: VNNAON OFF prep

3.6.18 Port Status 3 (IOM_PORT_STATUS[3]) — Offset 178h

TypeC port (PHY) status and control.

Note that 'Port' and 'PHY' are used interchangeably

Type	Size	Offset	Default
MMIO	32 bit	REGBAR + 178h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31	0h RO	**Port Is Connected (PORT_IS_CONNECTED):** Status indication that the port is connected. 0x0: Port is not connected. 0x1: Port is connected (IOM FW is done configuring the port).
30:29	0h RO	**Reserved**
28	0h RO	**Aux Orientation (AUX_ORI):** 0: Orientation is not flipped. 1: Orientation is flipped.
27:20	00h RO	**Mode Type (MODE_TYPE):** Various usage models. Example is to specify the NiDnT overlay mode or Intel debug overlay mode.

Bit Range	Default & Access	Field Name (ID): Description
19:12	00h RO	**HPD Status (DHPD):** HPD status. DHPD[1:0] - HPD current state. 0x0: No HPD. 0x1: HPD asserted. 0x2: HPD deasserted. 0x3 Invalid. DHPD[2:2] - HPD current state source. 0x0: PCH. 0x1: Thunderbolt DHPD[3:3] - HPD current state destination. 0x0: DP. 0x1: DPin. DHPD[5:4] - Deferred HPD current state. 0x0: No HPD. 0x1: HPD asserted. 0x2: HPD deasserted. 0x3 Invalid. DHPD[6:6] - Deferred HPD current state source. 0x0: PCH. 0x1: Thunderbolt DHPD[7:7] - Reserved.
11	0h RO	**High Speed Link Orientation Status (HSL_ORI):** 0: Orientation is not flipped. 1: Orientation is flipped.
10	0h RO	**Upstream Facing Port Status (UFP):** 0: Downstream facing port. TCSS USB is configured to be the Host. 1: Upstream facing port. TCSS USB is configured to be the Device.
9:6	0h RO	**Port Activity Type (ACTIVITY_TYPE):** port activity type: 0000b: USB3 0001b: Safe mode 0010b: Fixed connection 0100b: HTI (High-speed Trace Interface - used for debug) 0101b: NiDnT 1000b: DisplayPort-Inout 1100b: USB3 Alt mode 1101b: DisplayPort alt mode 1110b: DisplayPort alt mode MFD (Multi Function Device) 1111b: Thunderbolt alt mode
5	0h RO	**Configuration Done (CFG_DONE):** Control / Status bit to indicate that the port configuration is complete. This bit is also tied to the PHY common lane reset. 1: Port configuration is complete. Deassert TypeC PHY (port) common lane reset. 0: Port configuration is not complete. Assert TypeC PHY (port) common lane reset.
4	0h RO	**Port in Transition (PORT_IN_TRANSITION):** Indicator that the port bring-up is in progress.
3	0h RO	**Port Enabled (PORT_EN):** Status indicator if the PHY is enabled by BIOS.
2:0	0h RO	**PHY Command (CMD):** PHY Command: 0x0: NO-OP, 0x1: Wake PHY, 0x2: VNN OFF prep, 0x3: VNNAON OFF prep

3.6.19 IOM DisplayPort Resource Management 0 (IOM_DP_RESOURCE_MNG[0]) — Offset 102Ch

IOM DisplayPort Resource Management

Type	Size	Offset	Default
MMIO	32 bit	REGBAR + 102Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:8	0h RO	**Reserved**
7:4	0h RO	**DisplayPort 1 Ownership (DP1_ALLOC):** 0x0: Free 0x1: CM 0x2: IOM 0x3-0xF: Reserved
3:0	0h RO	**DisplayPort 0 Ownership (DP0_ALLOC):** 0x0: Free 0x1: CM 0x2: IOM 0x3-0xF: Reserved

3.6.20 IOM DisplayPort Resource Management 1 (IOM_DP_RESOURCE_MNG[1]) — Offset 1030h

IOM DisplayPort Resource Management

Note: Bit definitions are the same as IOM_DP_RESOURCE_MNG[0], offset 102Ch.

3.6.21 IOM DisplayPort HW Resource Semaphore 0 (IOM_DP_RESOURCE_SEMAPHORE[0]) — Offset 1038h

IOM DisplayPort HW Resource Semaphore

Type	Size	Offset	Default
MMIO	32 bit	REGBAR + 1038h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31	0h RO	**Semaphore Lock (SEMLOCK):** Semaphore lock bit - Master write this bit with its ID. If successfully written Master Owns this resource. Master Should clear the lock as soon as possible.

Bit Range	Default & Access	Field Name (ID): Description
30:4	0h RO	**Reserved**
3:0	0h RO	**Requester ID (REQUESTER_ID):** 0x0: CM 0x1: IOM 0x2-0xF: Reserved

3.6.22 IOM DisplayPort HW Resource Semaphore 1 (IOM_DP_RESOURCE_SEMAPHORE[1]) — Offset 103Ch

IOM DisplayPort HW Resource Semaphore

Note: Bit definitions are the same as IOM_DP_RESOURCE_SEMAPHORE[0], offset 1038h.

3.6.23 DisplayPort Input Graphics Source Policy Management (DPIN_GFX_SRC_POLICY_MGMT) — Offset 1044h

iGfx vs dGfx source policy management for TypeC port display mode

Type	Size	Offset	Default
MMIO	32 bit	REGBAR + 1044h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:28	0h RO	**External DPin Pipes (EXT_DPIN_PORTS):** Configured to # of DPin Pipes available
27:24	0h RO	**Internal Display Pipes (INT_DISP_PIPES):** Configured to # of Display Pipes available in Display Engine
23:16	00h RO	**GFX Source Policy Override Select (GFX_SRC_POLICY_OVERRIDE_SELECT):** 0: iGfx 1: dGfx: each bit represent each ports from 0 to 7
15:8	00h RO	**GFX Source Policy Override Enable (GFX_SRC_POLICY_OVERRIDE_ENABLE):** Bit 0: Port 0 Source override enable Bit 1: Port 1 Source override enable ... Bit 7: Port 7 Source override enable
7:0	00h RO	**GFX Source Policy (GFX_SRC_POLICY):** 0x0: All Internal 0x1: All external 0x2: Start external. When run out move to internal Else Reserved until new policies identified

3.6.24 IOM Firmware Current Task (IOM_FW_CURRENT_TASK) — Offset 118Ch

Updated at the beginning of every task management.

Type	Size	Offset	Default
MMIO	32 bit	REGBAR + 118Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:30	0h RO	**Reserved**
29:27	0h RO	**Execution Stage (STAGE):** Always starts with 0. Progresses according to the progress of the thread.
26:24	0h RO	**Initiating Group (GROUP):** • 000b: PCH initiated • 001b: IOM Firmware initiated • 010b: IOM Hardware initiated • 011b: Power Management initiated • Other values are reserved
23:16	00h RO	**Task Data (DATA):** Task Data
15:12	0h RO	**Command Parameter (PARAMS):** IOM Firmware command parameter.
11:8	0h RO	**USB2 Port Number (USB2_PORT_NUM):** 1s based number (first port = port 1). Up to 16 ports can be encoded. A value of '0h' means port 16
7:4	0h RO	**USB3 Port Number (USB3_PORT_NUM):** 1s based number (first port = port 1). Up to 16 ports can be encoded. A value of 0h means port 16
3:0	0h RO	**OPCODE:** Task Opcode

3.6.25 IOM Firmware Info (IOM_FW_INFO) — Offset 12C8h

IOM Firmware information register. This register is updated by IOM Firmware at boot time with the version info related to the loaded IOM Firmware image.

Type	Size	Offset	Default
MMIO	32 bit	REGBAR + 12C8h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:24	0h RO	**Reserved**
23:16	00h RO	**Family Version (FW_FAMILY):** Type of FW according to SKU.
15:8	00h RO	**CSME Version (FW_IMR_VERSION):** CSME Version.
7:0	00h RO	**Firmware Version (FW_VERSION):** IOM Firmware Version.

3.7 PCI Express Egress Port BAR (PXPEPBAR) Registers

This chapter documents the PXPEPBAR registers. Base address of these registers are defined in the PXPEPBAR_0_0_0_PCI register in Bus: 0, Device: 0, Function: 0.

Note: These registers apply to all processors.

3.7.1 Summary of Registers

Table 3-8. Summary of PXPEPBAR Registers

Offset	Size (Bytes)	Register Name (Register Symbol)	Default Value
0h	4	Egress Port Virtual Channel Capabilities (EPVCECH_0_0_0_PXPEPBAR)	04010002h
4h	4	Egress Port Virtual Channel Capability Register 1 (EPPVCCAP1_0_0_0_PXPEPBAR)	00000001h
8h	4	Egress Port Virtual Channel Capability Register 2 (EPPVCCAP2_0_0_0_PXPEPBAR)	00000000h
Ch	2	Egress Port Virtual Channel Control (EPPVCCTL_0_0_0_PXPEPBAR)	0000h
10h	4	Egress Port Virtual Channel 0 Resource Capability (EPVC0RCAP_0_0_0_PXPEPBAR)	00000001h
14h	4	Egress Port Virtual Channel 0 Resource Control (EPVC0RCTL_0_0_0_PXPEPBAR)	800000FFh
1Ah	2	Egress Port Virtual Channel 0 Resource Status (EPVC0RSTS_0_0_0_PXPEPBAR)	0000h
1Ch	4	Egress Port Virtual Channel 1 Resource Capability (EPVC1RCAP_0_0_0_PXPEPBAR)	00008001h
20h	4	Egress Port Virtual Channel 1 Resource Control (EPVC1RCTL_0_0_0_PXPEPBAR)	01000000h
26h	2	Egress Port Virtual Channel 1 Resource Status (EPVC1RSTS_0_0_0_PXPEPBAR)	0000h
40h	4	Egress Port Capablity Declaration (EPRCLDECH_0_0_0_PXPEPBAR)	00010005h
44h	4	Egress Port Element Declaration Capability (EPESD_0_0_0_PXPEPBAR)	00000501h
50h	4	Egress Port Link Element Declaration 1 (EPLE1D_0_0_0_PXPEPBAR)	01000000h
58h	4	Egress Port Link Another Root Complex Declaration 1 (EPLE1A_0_0_0_PXPEPBAR)	00000000h
5Ch	4	Egress Port Second Link Declaration 1 (EPULE1A_0_0_0_PXPEPBAR)	00000000h
60h	4	Egress Port Link Element Declaration 2 (EPLE2D_0_0_0_PXPEPBAR)	02000002h
68h	4	Egress Port Link Another Root Complex Declaration 2 (EPLE2A_0_0_0_PXPEPBAR)	00000000h
6Ch	4	Egress Port Second Link Declaration 2 (EPULE2A_0_0_0_PXPEPBAR)	00000000h
70h	4	Egress Port Link Element Declaration 3 (EPLE3D_0_0_0_PXPEPBAR)	03000002h
78h	4	Egress Port Link Another Root Complex Declaration 3 (EPLE3A_0_0_0_PXPEPBAR)	00000000h
7Ch	4	Egress Port Second Link Declaration 3 (EPULE3A_0_0_0_PXPEPBAR)	00000000h

Offset	Size (Bytes)	Register Name (Register Symbol)	Default Value
80h	4	Egress Port Link Element Declaration 4 (EPLE4D_0_0_0_PXPEPBAR)	04000002h
88h	4	Egress Port Link Another Root Complex Declaration 4 (EPLE4A_0_0_0_PXPEPBAR)	00000000h
8Ch	4	Egress Port Second Link Declaration 4 (EPULE4A_0_0_0_PXPEPBAR)	00000000h
90h	4	Egress Port Link Element Declaration 5 (EPLE5D_0_0_0_PXPEPBAR)	05000002h
98h	4	Egress Port Link Another Root Complex Declaration 5 (EPLE5A_0_0_0_PXPEPBAR)	00000000h
9Ch	4	Egress Port Second Link Declaration 5 (EPULE5A_0_0_0_PXPEPBAR)	00000000h

3.7.2 Egress Port Virtual Channel Capabilities (EPVCECH_0_0_0_PXPEPBAR) — Offset 0h

Indicates Egress Port Virtual Channel capabilities.

Type	Size	Offset	Default
MMIO	32 bit	PXPEPBAR + 0h	04010002h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:20	040h RO	**Pointer to Next Capability (PNC):** This field contains the offset to the next PCI Express capability structure in the linked list of capabilities (Link Declaration Capability). Bits [21:20] are reserved and software must mask them to allow for future uses of these bits
19:16	1h RO	**PCI Express Virtual Channel Capability Version (PCIEVCCV):** Hardwired to 1 to indicate compliances with the 1.1 version of the PCI Express specification. Note: This version does not change for 2.0 compliance.
15:0	0002h RO	**Extended Capability ID (ECID):** Value of 0002h identifies this linked list item (capability structure) as being for PCI Express Virtual Channel registers.

3.7.3 Egress Port Virtual Channel Capability Register 1 (EPPVCCAP1_0_0_0_PXPEPBAR) — Offset 4h

Egress Port Virtual Channel Capability Register 1

Type	Size	Offset	Default
MMIO	32 bit	PXPEPBAR + 4h	00000001h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:12	0h RO	**Reserved**
11:10	0h RO	**Port Arbitration Table Entry Size (PATES):** Indicates that the size of the Port Arbitration table entry is 1 bit.
9:8	0h RO	**Reference Clock (RC):** Indicates the reference clock for Virtual Channels that support time-based WRR Port Arbitration. 00:100 ns
7	0h RO	**Reserved**
6:4	0h RO	**Low Priority Extended Virtual Channel Count (LPEVCC):** Indicates the number of Virtual Channels (extended). Virtual Channels in addition to the default Virtual Channel belonging to the low-priority Virtual Channel (LPVC) group that has the lowest priority with respect to other Virtual Channel resources in a strict-priority Virtual Channel Arbitration. The value of 0 in this field implies strict Virtual Channel arbitration.
3	0h RO	**Reserved**
2:0	1h RW/L	**Extended Virtual Channel Count (EVCC):** Indicates the number of (extended) Virtual Channels in addition to the default Virtual Channel supported by the device. **Locked by:** TLDMIREGS.WO_STATUS0_0_0_0_DMIBAR.EVCCPWOS

3.7.4 Egress Port Virtual Channel Capability Register 2 (EPPVCCAP2_0_0_0_PXPEPBAR) — Offset 8h

Egress Port Virtual Channel Capability Register 2

Type	Size	Offset	Default
MMIO	32 bit	PXPEPBAR + 8h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:24	00h RO	**VC Arbitration Table Offset (VCATO):** This field is reserved for Virtual Channel Arbitration Table Offset (VCATO)

Bit Range	Default & Access	Field Name (ID): Description
23:0	0h RO	**Reserved**

3.7.5 Egress Port Virtual Channel Control (EPPVCCTL_0_0_0_PXPEPBAR) — Offset Ch

Egress Port Virtual Channel Control

Type	Size	Offset	Default
MMIO	16 bit	PXPEPBAR + Ch	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:4	0h RO	**Reserved**
3:1	0h RW	**VC Arbitration Select (VCAS):** This field will be programmed by software to the only possible value as indicated in the Virtual Channel Arbitration Capability field. The value 000b when written to this field will indicate the Virtual Channel arbitration scheme is hardware fixed (in the root complex). This field cannot be modified when more than one Virtual Channel in the LPVC group is enabled.
0	0h RO	**Load Virtual Channel Arbitration Table (LVCAT):** This field is reserved for Load Virtual Channel Arbitration Table (LVCAT)

3.7.6 Egress Port Virtual Channel 0 Resource Capability (EPVC0RCAP_0_0_0_PXPEPBAR) — Offset 10h

Egress Port Virtual Channel 0 Resource Capability

Type	Size	Offset	Default
MMIO	32 bit	PXPEPBAR + 10h	00000001h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:24	00h RO	**Port Arbitration Table Offset (PATO):** No VC0 port arbitration necessary.

Bit Range	Default & Access	Field Name (ID): Description
23	0h RO	**Reserved**
22:16	00h RO	**Maximum Time Slots (MTS):** No VC0 port arbitration necessary.
15	0h RO	**Reject Snoop Transactions (RSNPT):** 0: Transactions with or without the No Snoop bit set within the TLP header are allowed on this VC. 1: When Set, any transaction for which the No Snoop attribute is applicable but is not Set within the TLP Header will be rejected as an Unsupported Request.
14:8	0h RO	**Reserved**
7:0	01h RO	**Port Arbitration Capability (PAC):** Indicates types of Port Arbitration supported by this VC0 resource. The default value of 01h indicates that the only port arbitration capability for VC0 is non-configurable, hardware-fixed arbitration scheme.

3.7.7 Egress Port Virtual Channel 0 Resource Control (EPVC0RCTL_0_0_0_PXPEPBAR) — Offset 14h

Controls the resources associated with Egress Port Virtual Channel 0.

Type	Size	Offset	Default
MMIO	32 bit	PXPEPBAR + 14h	800000FFh

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	1h RO	**VC0 Enable (VC0E):** For VC0 this is hardwired to 1 and read only as VC0 can never be disabled.
30:27	0h RO	**Reserved**
26:24	0h RO	**VC0 ID (VC0ID):** Assigns a Virtual Channel ID to the Virtual Channel resource. For VC0 this is hardwired to 0 and read only.
23:20	0h RO	**Reserved**
19:17	0h RW	**Port Arbitration Select (PAS):** This field configures the Virtual Channel resource to provide a particular Port Arbitration service. The value of 0h corresponds to the bit position of the only asserted bit in the Port Arbitration Capability field.
16:8	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
7:1	7Fh RW	**TC/VC0 Map (TCVC0M):** Indicates the TCs (Traffic Classes) that are mapped to the Virtual Channel resource. Bit locations within this field correspond to TC values. For example, when bit 7 is set in this field, TC7 is mapped to this Virtual Channel resource. When more than one bit in this field is set, it indicates that multiple TCs are mapped to the Virtual Channel resource. In order to remove one or more TCs from the TC/VC Map of an enabled VC, software must ensure that no new or outstanding transactions with the TC labels are targeted at the given Link.
0	1h RO	**TC0/VC0 Map (TC0VC0M):** Traffic Class 0 is always routed to VC0.

3.7.8 Egress Port Virtual Channel 0 Resource Status (EPVC0RSTS_0_0_0_PXPEPBAR) — Offset 1Ah

Egress Port Virtual Channel 0 Resource Status

Type	Size	Offset	Default
MMIO	16 bit	PXPEPBAR + 1Ah	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
15:2	0h RO	**Reserved**
1	0h RO/V	**VC0 Negotiation Pending (VC0NP):** 0: The Virtual Channel negotiation is complete. 1: The Virtual Channel resource is still in the process of negotiation (initialization or disabling). For this default VC, this bit indicates the status of the process of Flow Control initialization. Before using a Virtual Channel, software must check whether the Virtual Channel Negotiation Pending fields for that Virtual Channel are cleared in both Components on a Link.
0	0h RO	**Reserved**

3.7.9 Egress Port Virtual Channel 1 Resource Capability (EPVC1RCAP_0_0_0_PXPEPBAR) — Offset 1Ch

Egress Port Virtual Channel 1 Resource Capability

Type	Size	Offset	Default
MMIO	32 bit	PXPEPBAR + 1Ch	00008001h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:24	00h RO	**Port Arbitration Table Offset (PATO):** No VC0 port arbitration is necessary.
23	0h RO	**Reserved**
22:16	00h RO	**Maximum Time Slots (MTS):** No VC0 port arbitration is necessary.
15	1h RO	**Reject Snoop Transactions (RSNPT):** 0: Transactions with or without the No Snoop bit set within the TLP header are allowed on this VC. 1: When Set, any transaction for which the No Snoop attribute is applicable but is not Set within the TLP Header will be rejected as an Unsupported Request.
14:8	0h RO	**Reserved**
7:0	01h RO	**Port Arbitration Capability (PAC):** Indicates types of Port Arbitration supported by this VC1 resource. The default value of 01h indicates that the only port arbitration capability for VC1 is a non-configurable, hardware-fixed arbitration scheme.

3.7.10 Egress Port Virtual Channel 1 Resource Control (EPVC1RCTL_0_0_0_PXPEPBAR) — Offset 20h

Egress Port Virtual Channel 1 Resource Control

Type	Size	Offset	Default
MMIO	32 bit	PXPEPBAR + 20h	01000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RW	**VC1 Enable (VC1E):** VC1 Enable: This bit will be ignored by the hardware. The bit is R/W for specification compliance, but writing to it will result in no behavior change in the hardware (other than the bit value reflecting the written value). 0: Virtual Channel is disabled. 1: Virtual Channel is enabled. See exceptions in note below. Software must use the Virtual Channel Negotiation Pending bit to check whether the Virtual Channel negotiation is complete. When Virtual Channel Negotiation Pending bit is cleared, a 1 read from this Virtual Channel Enable bit indicates that the Virtual Channel is enabled (Flow Control Initialization is completed for the PCI Express port). A 0 read from this bit indicates that the Virtual Channel is currently disabled. Notes: 1. To enable a Virtual Channel, the Virtual Channel Enable bits for that Virtual Channel must be set in both Components on a Link. 2. To disable a Virtual Channel, the Virtual Channel Enable bits for that Virtual Channel must be cleared in both Components on a Link. 3. Software must ensure that no traffic is using a Virtual Channel at the time it is disabled. 4. Software must fully disable a Virtual Channel in both Components on a Link before re-enabling the Virtual Channel.
30:27	0h RO	**Reserved**
26:24	1h RW	**VC1 ID (VC1ID):** Assigns a Virtual Channel ID to the Virtual Channel resource. Assigned value must be non-zero. This field can not be modified when the Virtual Channel is already enabled.
23:20	0h RO	**Reserved**
19:17	0h RW	**Port Arbitration Select (PAS):** This field configures the Virtual Channel resource to provide a particular Port Arbitration service. The default value of 0h corresponds to bit position of the only asserted bit in the Port Arbitration Capability field.
16:8	0h RO	**Reserved**
7:1	00h RW	**TC/VC1 Map (TCVC1M):** Indicates the TCs (Traffic Classes) that are mapped to the Virtual Channel resource. Bit locations within this field correspond to TC values. For example, when bit 7 is set in this field, TC7 is mapped to this Virtual Channel resource. When more than one bit in this field is set, it indicates that multiple TCs are mapped to the Virtual Channel resource. In order to remove one or more TCs from the TC/VC Map of an enabled VC, software must ensure that no new or outstanding transactions with the TC labels are targeted at the given Link.
0	0h RO	**TC0/VC1 Map (TC0VC1M):** Traffic Class 0 is always routed to VC0.

3.7.11 Egress Port Virtual Channel 1 Resource Status (EPVC1RSTS_0_0_0_PXPEPBAR) — Offset 26h

Egress Port Virtual Channel 1 Resource Status

Type	Size	Offset	Default
MMIO	16 bit	PXPEPBAR + 26h	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
15:2	0h RO	**Reserved**
1	0h RO/V	**VC1 Negotiation Pending (VC1NP):** 0: The Virtual Channel negotiation is complete. 1: The Virtual Channel resource is still in the process of negotiation (initialization or disabling). For this non-default Virtual Channel, software may use this bit when enabling or disabling the VC. Before using a Virtual Channel, software must check whether the Virtual Channel Negotiation Pending fields for that Virtual Channel are cleared in both Components on a Link.
0	0h RO	**Port Arbitration Table Status (PATS):** This field is reserved for Port Arbitration Table Status (PATS)

3.7.12 Egress Port Capablity Declaration (EPRCLDECH_0_0_0_PXPEPBAR) — Offset 40h

Egress Port Capablity Declaration

Type	Size	Offset	Default
MMIO	32 bit	PXPEPBAR + 40h	00010005h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:20	000h RO	**Pointer to Next Capability (PNC):** This value terminates the PCI Express extended capabilities list associated with this RCRB.
19:16	1h RO	**Link Declaration Capability Version (LDCV):** Hardwired to 1 to indicate compliances with the 1.0 version of the PCI Express specification. Note: This version does not change for 2.0 compliance.

Bit Range	Default & Access	Field Name (ID): Description
15:0	0005h RO	**Extended Capability ID (ECID):** Value of 5h identifies this linked list item (capability structure) as being for PCI Express Link Declaration Capability.

3.7.13 Egress Port Element Declaration Capability (EPESD_0_0_0_PXPEPBAR) — Offset 44h

Provides information about the root complex element containing this Link Declaration Capability.

Type	Size	Offset	Default
MMIO	32 bit	PXPEPBAR + 44h	00000501h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:24	00h RO	**Port Number (PN):** This field specifies the port number associated with this element with respect to the component that contains this element. Value of 00 h indicates to configuration software that this is the default egress port.
23:16	00h RW/L	**Component ID (CID):** Identifies the physical component that contains this Root Complex Element. BIOS Requirement: Must be initialized according to guidelines in the PCI Express* Isochronous/Virtual Channel Support Hardware Programming Specification (HPS). **Locked by:** TLDMIREGS.WO_STATUS0_0_0_0_DMIBAR.CIDPWOS
15:8	05h RO	**Number of Link Entries (NLE):** Indicates the number of link entries following the Element Self Description. This field reports 5 (one each for PEG0, PEG11 PEG12, PEG1 and DMI).
7:4	0h RO	**Reserved**
3:0	1h RO	**Element Type (ET):** Indicates the type of the Root Complex Element. Value of 1 h represents a port to system memory.

3.7.14 Egress Port Link Element Declaration 1 (EPLE1D_0_0_0_PXPEPBAR) — Offset 50h

First part of a Link Entry which declares an internal link to another Root Complex Element.

Type	Size	Offset	Default
MMIO	32 bit	PXPEPBAR + 50h	01000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:24	01h RO	**Target Port Number (TPN):** Specifies the port number associated with the element targeted by this link entry (DMI). The target port number is with respect to the component that contains this element as specified by the target component ID.
23:16	00h RW/L	**Target Component ID (TCID):** Identifies the physical or logical component that is targeted by this link entry. BIOS Requirement: Must be initialized according to guidelines in the PCI Express* Isochronous/Virtual Channel Support Hardware Programming Specification (HPS). **Locked by:** TLDMIREGS.WO_STATUS0_0_0_0_DMIBAR.TCIDE1PWOS
15:2	0h RO	**Reserved**
1	0h RO	**Link Type (LTYP):** Indicates that the link points to memory-mapped space (for RCRB). The link address specifies the 64-bit base address of the target RCRB.
0	0h RW/L	**Link Valid (LV):** 0: Link Entry is not valid and will be ignored. 1: Link Entry specifies a valid link. **Locked by:** TLDMIREGS.WO_STATUS0_0_0_0_DMIBAR.LVE1PWOS

3.7.15 Egress Port Link Another Root Complex Declaration 1 (EPLE1A_0_0_0_PXPEPBAR) — Offset 58h

Second part of a Link Entry which declares an internal link to another Root Complex Element.

Type	Size	Offset	Default
MMIO	32 bit	PXPEPBAR + 58h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:12	00000h RW/L	**Low Link Address (LLA):** Memory mapped base address of the RCRB that is the target element (DMI) for this link entry. **Locked by:** TLDMIREGS.WO_STATUS0_0_0_0_DMIBAR.LLAE1PWOS

Bit Range	Default & Access	Field Name (ID): Description
11:0	0h RO	**Reserved**

3.7.16 Egress Port Second Link Declaration 1 (EPULE1A_0_0_0_PXPEPBAR) — Offset 5Ch

Second part of a Link Entry which declares an internal link to another Root Complex Element.

Type	Size	Offset	Default
MMIO	32 bit	PXPEPBAR + 5Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:8	0h RO	**Reserved**
7:0	00h RW/L	**Upper Link Address (ULA):** Memory mapped base address of the RCRB that is the target element (DMI) for this link entry. **Locked by:** TLDMIREGS.WO_STATUS0_0_0_0_DMIBAR.ULAE1PWOS

3.7.17 Egress Port Link Element Declaration 2 (EPLE2D_0_0_0_PXPEPBAR) — Offset 60h

First part of a Link Entry which declares an internal link to another Root Complex Element.

Type	Size	Offset	Default
MMIO	32 bit	PXPEPBAR + 60h	02000002h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:24	02h RO	**Target Port Number (TPN):** Specifies the port number associated with the element targeted by this link entry (PEG1.0). The target port number is with respect to the component that contains this element as specified by the target component ID.

Bit Range	Default & Access	Field Name (ID): Description
23:16	00h RW/L	**Target Component ID (TCID):** Identifies the physical or logical component that is targeted by this link entry. A value of 0 is reserved. Component IDs start at 1. This value is a mirror of the value in the Component ID field of all elements in this component. BIOS Requirement: Must be initialized according to guidelines in the PCI Express* Isochronous/Virtual Channel Support Hardware Programming Specification (HPS). **Locked by:** TLDMIREGS.WO_STATUS0_0_0_0_DMIBAR.TCIDE2PWOS
15:2	0h RO	**Reserved**
1	1h RO	**Link Type (LTYP):** Indicates that the link points to configuration space of the integrated device which controls the x16 root port for PEG0. The link address specifies the configuration address (segment, bus, device, function) of the target root port.
0	0h RW/L	**Link Valid (LV):** 0: Link Entry is not valid and will be ignored. 1: Link Entry specifies a valid link. **Locked by:** TLDMIREGS.WO_STATUS0_0_0_0_DMIBAR.LVE2PWOS

3.7.18 Egress Port Link Another Root Complex Declaration 2 (EPLE2A_0_0_0_PXPEPBAR) — Offset 68h

Second part of a Link Entry which declares an internal link to another Root Complex Element.

Type	Size	Offset	Default
MMIO	32 bit	PXPEPBAR + 68h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:12	00000h RW/L	**Low Link Address (LLA):** Memory mapped base address of the RCRB that is the target element (DMI) for this link entry. **Locked by:** TLDMIREGS.WO_STATUS0_0_0_0_DMIBAR.LLAE2PWOS
11:0	0h RO	**Reserved**

3.7.19 Egress Port Second Link Declaration 2 (EPULE2A_0_0_0_PXPEPBAR) — Offset 6Ch

Second part of a Link Entry which declares an internal link to another Root Complex Element.

Type	Size	Offset	Default
MMIO	32 bit	PXPEPBAR + 6Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:8	0h RO	**Reserved**
7:0	00h RW/L	**Upper Link Address (ULA):** Memory mapped base address of the RCRB that is the target element (DMI) for this link entry. **Locked by:** TLDMIREGS.WO_STATUS0_0_0_0_DMIBAR.ULAE2PWOS

3.7.20 Egress Port Link Element Declaration 3 (EPLE3D_0_0_0_PXPEPBAR) — Offset 70h

First part of a Link Entry which declares an internal link to another Root Complex Element.

Type	Size	Offset	Default
MMIO	32 bit	PXPEPBAR + 70h	03000002h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:24	03h RO	**Target Port Number (TPN):** Specifies the port number associated with the element targeted by this link entry (PEG1.1). The target port number is with respect to the component that contains this element as specified by the target component ID.
23:16	00h RW/L	**Target Component ID (TCID):** Identifies the physical or logical component that is targeted by this link entry. A value of 0 is reserved. Component IDs start at 1. This value is a mirror of the value in the Component ID field of all elements in this component. BIOS Requirement: Must be initialized according to guidelines in the PCI Express* Isochronous/Virtual Channel Support Hardware Programming Specification (HPS). **Locked by:** TLDMIREGS.WO_STATUS0_0_0_0_DMIBAR.TCIDE3PWOS
15:2	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
1	1h RO	**Link Type (LTYP):** Indicates that the link points to configuration space of the integrated device which controls the x16 root port for PEG1. The link address specifies the configuration address (segment, bus, device, function) of the target root port.
0	0h RW/L	**Link Valid (LV):** 0: Link Entry is not valid and will be ignored. 1: Link Entry specifies a valid link. **Locked by:** TLDMIREGS.WO_STATUS0_0_0_0_DMIBAR.LVE3PWOS

3.7.21 Egress Port Link Another Root Complex Declaration 3 (EPLE3A_0_0_0_PXPEPBAR) — Offset 78h

Second part of a Link Entry which declares an internal link to another Root Complex Element.

Type	Size	Offset	Default
MMIO	32 bit	PXPEPBAR + 78h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:12	00000h RW/L	**Low Link Address (LLA):** Memory mapped base address of the RCRB that is the target element (DMI) for this link entry. **Locked by:** TLDMIREGS.WO_STATUS0_0_0_0_DMIBAR.LLAE3PWOS
11:0	0h RO	**Reserved**

3.7.22 Egress Port Second Link Declaration 3 (EPULE3A_0_0_0_PXPEPBAR) — Offset 7Ch

Second part of a Link Entry which declares an internal link to another Root Complex Element.

Type	Size	Offset	Default
MMIO	32 bit	PXPEPBAR + 7Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:8	0h RO	**Reserved**
7:0	00h RW/L	**Upper Link Address (ULA):** Memory mapped base address of the RCRB that is the target element (DMI) for this link entry **Locked by:** TLDMIREGS.WO_STATUS0_0_0_0_DMIBAR.ULAE3PWOS

3.7.23 Egress Port Link Element Declaration 4 (EPLE4D_0_0_0_PXPEPBAR) — Offset 80h

First part of a Link Entry which declares an internal link to another Root Complex Element.

Type	Size	Offset	Default
MMIO	32 bit	PXPEPBAR + 80h	04000002h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:24	04h RO	**Target Port Number (TPN):** Specifies the port number associated with the element targeted by this link entry (PEG1.2). The target port number is with respect to the component that contains this element as specified by the target component ID.
23:16	00h RW/L	**Target Component ID (TCID):** Identifies the physical or logical component that is targeted by this link entry. A value of 0 is reserved. Component IDs start at 1. This value is a mirror of the value in the Component ID field of all elements in this component. BIOS Requirement: Must be initialized according to guidelines in the PCI Express* Isochronous/Virtual Channel Support Hardware Programming Specification (HPS). **Locked by:** TLDMIREGS.WO_STATUS0_0_0_0_DMIBAR.TCIDE4PWOS
15:2	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
1	1h RO	**Link Type (LTYP):** Indicates that the link points to configuration space of the integrated device which controls the x16 root port for PEG1. The link address specifies the configuration address (segment, bus, device, function) of the target root port.
0	0h RW/L	**Link Valid (LV):** 0: Link Entry is not valid and will be ignored. 1: Link Entry specifies a valid link. **Locked by:** TLDMIREGS.WO_STATUS0_0_0_0_DMIBAR.LVE4PWOS

3.7.24 Egress Port Link Another Root Complex Declaration 4 (EPLE4A_0_0_0_PXPEPBAR) — Offset 88h

Second part of a Link Entry which declares an internal link to another Root Complex Element.

Type	Size	Offset	Default
MMIO	32 bit	PXPEPBAR + 88h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:12	00000h RW/L	**Low Link Address (LLA):** Memory mapped base address of the RCRB that is the target element (DMI) for this link entry. **Locked by:** TLDMIREGS.WO_STATUS0_0_0_0_DMIBAR.LLAE4PWOS
11:0	0h RO	**Reserved**

3.7.25 Egress Port Second Link Declaration 4 (EPULE4A_0_0_0_PXPEPBAR) — Offset 8Ch

Second part of a Link Entry which declares an internal link to another Root Complex Element.

Type	Size	Offset	Default
MMIO	32 bit	PXPEPBAR + 8Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:8	0h RO	**Reserved**
7:0	00h RW/L	**Upper Link Address (ULA):** Memory mapped base address of the RCRB that is the target element (DMI) for this link entry. **Locked by:** TLDMIREGS.WO_STATUS1_0_0_0_DMIBAR.ULAE4PWOS

3.7.26 Egress Port Link Element Declaration 5 (EPLE5D_0_0_0_PXPEPBAR) — Offset 90h

First part of a Link Entry which declares an internal link to another Root Complex Element.

Type	Size	Offset	Default
MMIO	32 bit	PXPEPBAR + 90h	05000002h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:24	05h RO	**Target Port Number (TPN):** Specifies the port number associated with the element targeted by this link entry (PEG6.0). The target port number is with respect to the component that contains this element as specified by the target component ID.
23:16	00h RW/L	**Target Component ID (TCID):** Identifies the physical or logical component that is targeted by this link entry. A value of 0 is reserved. Component IDs start at 1. This value is a mirror of the value in the Component ID field of all elements in this component. BIOS Requirement: Must be initialized according to guidelines in the PCI Express* Isochronous/Virtual Channel Support Hardware Programming Specification (HPS). **Locked by:** TLDMIREGS.WO_STATUS1_0_0_0_DMIBAR.TCIDE5PWOS
15:2	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
1	1h RO	**Link Type (LTYP):** Indicates that the link points to configuration space of the integrated device which controls the x16 root port for PEG1. The link address specifies the configuration address (segment, bus, device, function) of the target root port.
0	0h RW/L	**Link Valid (LV):** 0: Link Entry is not valid and will be ignored. 1: Link Entry specifies a valid link. **Locked by:** TLDMIREGS.WO_STATUS1_0_0_0_DMIBAR.LVE5PWOS

3.7.27 Egress Port Link Another Root Complex Declaration 5 (EPLE5A_0_0_0_PXPEPBAR) — Offset 98h

Second part of a Link Entry which declares an internal link to another Root Complex Element.

Type	Size	Offset	Default
MMIO	32 bit	PXPEPBAR + 98h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:12	00000h RW/L	**Low Link Address (LLA):** Memory mapped base address of the RCRB that is the target element (DMI) for this link entry. **Locked by:** TLDMIREGS.WO_STATUS1_0_0_0_DMIBAR.LLAE5PWOS
11:0	0h RO	**Reserved**

3.7.28 Egress Port Second Link Declaration 5 (EPULE5A_0_0_0_PXPEPBAR) — Offset 9Ch

Second part of a Link Entry which declares an internal link to another Root Complex Element.

Type	Size	Offset	Default
MMIO	32 bit	PXPEPBAR + 9Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:8	0h RO	**Reserved**
7:0	00h RW/L	**Upper Link Address (ULA):** Upper Link Address: Memory mapped base address of the RCRB that is the target element (DMI) for this link entry. **Locked by:** TLDMIREGS.WO_STATUS1_0_0_0_DMIBAR.ULAE5PWOS

3.8 VTDPVC0BAR Registers

This chapter documents the VC0PREMAP BAR registers. Base address of these registers are defined in the VTDPVC0BAR_0_0_0_MCHBAR_NCU register which resides in the MCHBAR register collection.

Note: These registers apply to all processors.

3.8.1 Summary of Registers

Table 3-9. Summary of VTDPVC0BAR Registers

Offset	Size (Bytes)	Register Name (Register Symbol)	Default Value
0h	4	Version Register (VER_REG_0_0_0_VTDBAR)	00000010h
8h	8	Capability Register (CAP_REG_0_0_0_VTDBAR)	00D2008C40660462h
10h	8	Extended Capability Register (ECAP_REG_0_0_0_VTDBAR)	0000000000F050DAh
18h	4	Global Command Register (GCMD_REG_0_0_0_VTDBAR)	00000000h
1Ch	4	Global Status Register (GSTS_REG_0_0_0_VTDBAR)	00000000h
20h	8	Root Table Address Register (RTADDR_REG_0_0_0_VTDBAR)	0000000000000000h
28h	8	Context Command Register (CCMD_REG_0_0_0_VTDBAR)	0800000000000000h
34h	4	Fault Status Register (FSTS_REG_0_0_0_VTDBAR)	00000000h
38h	4	Fault Event Control Register (FECTL_REG_0_0_0_VTDBAR)	80000000h
3Ch	4	Fault Event Data Register (FEDATA_REG_0_0_0_VTDBAR)	00000000h
40h	4	Fault Event Address Register (FEADDR_REG_0_0_0_VTDBAR)	00000000h
44h	4	Fault Event Upper Address Register (FEUADDR_REG_0_0_0_VTDBAR)	00000000h
58h	8	Advanced Fault Log Register (AFLOG_REG_0_0_0_VTDBAR)	0000000000000000h
64h	4	Protected Memory Enable Register (PMEN_REG_0_0_0_VTDBAR)	00000000h
68h	4	Protected Low Memory Base Register (PLMBASE_REG_0_0_0_VTDBAR)	00000000h
6Ch	4	Protected Low-Memory Limit Register (PLMLIMIT_REG_0_0_0_VTDBAR)	00000000h
70h	8	Protected High-Memory Base Register (PHMBASE_REG_0_0_0_VTDBAR)	0000000000000000h
78h	8	Protected High-Memory Limit Register (PHMLIMIT_REG_0_0_0_VTDBAR)	0000000000000000h
80h	8	Invalidation Queue Head Register (IQH_REG_0_0_0_VTDBAR)	0000000000000000h
88h	8	Invalidation Queue Tail Register (IQT_REG_0_0_0_VTDBAR)	0000000000000000h
90h	8	Invalidation Queue Address Register (IQA_REG_0_0_0_VTDBAR)	0000000000000000h
9Ch	4	Invalidation Completion Status Register (ICS_REG_0_0_0_VTDBAR)	00000000h
A0h	4	Invalidation Event Control Register (IECTL_REG_0_0_0_VTDBAR)	80000000h
A4h	4	Invalidation Event Data Register (IEDATA_REG_0_0_0_VTDBAR)	00000000h

Offset	Size (Bytes)	Register Name (Register Symbol)	Default Value
A8h	4	Invalidation Event Address Register (IEADDR_REG_0_0_0_VTDBAR)	00000000h
ACh	4	Invalidation Event Upper Address Register (IEUADDR_REG_0_0_0_VTDBAR)	00000000h
B8h	8	Interrupt Remapping Table Address Register (IRTA_REG_0_0_0_VTDBAR)	0000000000000000h
DCh	4	Page Request Status Register (PRESTS_REG_0_0_0_VTDBAR)	00000000h
E0h	4	Page Request Event Control Register (PRECTL_REG_0_0_0_VTDBAR)	80000000h
E4h	4	Page Request Event Data Register (PREDATA_REG_0_0_0_VTDBAR)	00000000h
E8h	4	Page Request Event Address Register (PREADDR_REG_0_0_0_VTDBAR)	00000000h
ECh	4	Page Request Event Upper Address Register (PREUADDR_REG_0_0_0_VTDBAR)	00000000h
400h	8	Fault Recording Register Low [0] (FRCDL_REG_0_0_0_VTDBAR)	0000000000000000h
408h	8	Fault Recording Register High [0] (FRCDH_REG_0_0_0_VTDBAR)	0000000000000000h
500h	8	Invalidate Address Register (IVA_REG_0_0_0_VTDBAR)	0000000000000000h
508h	8	IOTLB Invalidate Register (IOTLB_REG_0_0_0_VTDBAR)	0200000000000000h

3.8.2 Version Register (VER_REG_0_0_0_VTDBAR) — Offset 0h

Register to report the architecture version supported. Backward compatibility for the architecture is maintained with new revision numbers, allowing software to load remapping hardware drivers written for prior architecture versions.

Type	Size	Offset	Default
MMIO	32 bit	VTDPVC0BAR + 0h	00000010h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:8	0h RO	**Reserved**
7:4	1h RO	**Major Version Number (MAJOR):** Indicates supported architecture version.
3:0	0h RO	**Minor Version Number (MINOR):** Indicates supported architecture minor version.

3.8.3 Capability Register (CAP_REG_0_0_0_VTDBAR) — Offset 8h

Register to report general remapping hardware capabilities.

Type	Size	Offset	Default
MMIO	64 bit	VTDPVC0BAR + 8h	00D2008C40660462h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:57	0h RO	**Reserved**
56	0h RO	**First Level 64-KByte Page SupportP (FL1GP):** A value of 1 in this field indicates 1-GByte page size is supported for first-level translation.
55	1h RO	**Read Draining (DRD):** • 0 = Hardware does not support draining of DMA read requests. • 1 = Hardware supports draining of DMA read requests.
54	1h RO	**Write Draining (DWD):** • 0 = Hardware does not support draining of DMA write requests. • 1 = Hardware supports draining of DMA write requests.
53:48	12h RO	**Maximum Address Mask Value (MAMV):** The value in this field indicates the maximum supported value for the Address Mask (AM) field in the Invalidation Address register (IVA_REG) and IOTLB Invalidation Descriptor (iotlb_inv_dsc) used for invalidations of second-level translation. This field is valid only when the PSI field in Capability register is reported as Set.
47:40	00h RO	**Number of Fault-Recording Registers (NFR):** Number of fault recording registers is computed as N+1, where N is the value reported in this field. Implementations must support at least one fault recording register (NFR = 0) for each remapping hardware unit in the platform. The maximum number of fault recording registers per remapping hardware unit is 256.
39	1h RO	**Page Selective Invalidation (PSI):** • 0 = Hardware supports only domain and global invalidates for IOTLB.{*}1 = Hardware supports page selective, domain and global invalidates for IOTLB. Hardware implementations reporting this field as set are recommended to support a Maximum Address Mask Value (MAMV) value of at least 9 (or 18 if supporting 1GB pages with second level translation).
38	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
37:34	3h RO	**Second Level Large Page Support (SLLPS):** This field indicates the super page sizes supported by hardware. A value of 1 in any of these bits indicates the corresponding super-page size is supported. The super-page sizes corresponding to various bit positions within this field are: • 0 = 21-bit offset to page frame (2MB) • 1 = 30-bit offset to page frame (1GB) • 2 = 39-bit offset to page frame (512GB) • 3 = 48-bit offset to page frame (1TB) Hardware implementations supporting a specific super-page size must support all smaller super-page sizes, i.e. only valid values for this field are 0000b, 0001b, 0011b, 0111b, 1111b.
33:24	040h RO	**Fault-Recording Register Offset (FRO):** This field specifies the location to the first fault recording register relative to the register base address of this remapping hardware unit. If the register base address is X, and the value reported in this field is Y, the address for the first fault recording register is calculated as X+(16*Y).
23	0h RO	**Reserved**
22	1h RO	**Zero Length Read (ZLR):** • 0 = Indicates the remapping hardware unit blocks (and treats as fault) zero length DMA read requests to write-only pages. • 1 = Indicates the remapping hardware unit supports zero length DMA read requests to write-only pages. DMA remapping hardware implementations are recommended to report ZLR field as Set.
21:16	26h RO	**Maximum Guest Address Width (MGAW):** This field indicates the maximum DMA virtual addressability supported by remapping hardware. The Maximum Guest Address Width (MGAW) is computed as (N+1), where N is the value reported in this field. For example, a hardware implementation supporting 48-bit MGAW reports a value of 47 (101111b) in this field. If the value in this field is X, untranslated and translated DMA requests to addresses above 2(x+1)-1 are always blocked by hardware. Translations requests to address above 2(x+1)-1 from allowed devices return a null Translation Completion Data Entry with R=W=0. Guest addressability for a given DMA request is limited to the minimum of the value reported through this field and the adjusted guest address width of the corresponding page-table structure. (Adjusted guest address widths supported by hardware are reported through the SAGAW field). Implementations are recommended to support MGAW at least equal to the physical addressability (host address width) of the platform.
15:13	0h RO	**Reserved**
12:8	04h RO	**Supported Adjusted Guest Address Widths (SAGAW):** This 5-bit field indicates the supported adjusted guest address widths (which in turn represents the levels of page-table walks for the 4KB base page size) supported by the hardware implementation. A value of 1 in any of these bits indicates the corresponding adjusted guest address width is supported. The adjusted guest address widths corresponding to various bit positions within this field are: • 0 = 30-bit AGAW (2-level page table) • 1 = 39-bit AGAW (3-level page table) • 2 = 48-bit AGAW (4-level page table) • 3 = 57-bit AGAW (5-level page table) • 4 = 64-bit AGAW (6-level page table) Software must ensure that the adjusted guest address width used to setup the page tables is one of the supported guest address widths reported in this field.

Bit Range	Default & Access	Field Name (ID): Description
7	0h RO	**Caching Mode (CM):** • 0 = Not-present and erroneous entries are not cached in any of the renmapping caches. Invalidations are not required for modifications to individual not present or invalid entries. However, any modifications that result in decreasing the effective permissions or partial permission increases require invalidations for them to be effective. • 1 = Not-present and erroneous mappings may be cached in the remapping caches. Any software updates to the remapping structures (including updates to not-present or erroneous entries) require explicit invalidation. Hardware implementations of this architecture must support a value of 0 in this field.
6	1h RO	**Protected High-Memory Region (PHMR):** • 0 = Indicates protected high-memory region is not supported. • 1 = Indicates protected high-memory region is supported.
5	1h RO	**Protected Low-Memory Region (PLMR):** • 0 = Indicates protected low-memory region is not supported. • 1 = Indicates protected low-memory region is supported.
4	0h RO	**Required Write-Buffer Flushing (RWBF):** • 0 = Indicates no write-buffer flushing is needed to ensure changes to memory-resident structures are visible to hardware. • 1 = Indicates software must explicitly flush the write buffers to ensure updates made to memory-resident remapping structures are visible to hardware.
3	0h RO	**Advanced Fault Logging (AFL):** • 0 = Indicates advanced fault logging is not supported. Only primary fault logging is supported. • 1 = Indicates advanced fault logging is supported.
2:0	2h RO	**Number of Domains Supported (ND):** • 000b = Hardware supports 4-bit domain-ids with support for up to 16 domains. • 001b = Hardware supports 6-bit domain-ids with support for up to 64 domains. • 010b = Hardware supports 8-bit domain-ids with support for up to 256 domains. • 011b = Hardware supports 10-bit domain-ids with support for up to 1024 domains. • 100b = Hardware supports 12-bit domain-ids with support for up to 4K domains. • 100b = Hardware supports 14-bit domain-ids with support for up to 16K domains. • 110b = Hardware supports 16-bit domain-ids with support for up to 64K domains. • 111b = Reserved.

3.8.4 Extended Capability Register (ECAP_REG_0_0_0_VTDBAR) — Offset 10h

Register to report remapping hardware extended capabilities.

Type	Size	Offset	Default
MMIO	64 bit	VTDPVC0BAR + 10h	0000000000F050DAh

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:41	0h RO	**Reserved**
40	0h RO	**Process Address Space ID Support (PASID):** • 0 = Hardware does not support requests tagged with Process Address Space IDs. • 1 = Hardware supports requests tagged with Process Address Space IDs.
39:35	00h RO	**PASID Size Supported (PSS):** This field reports the PASID size supported by the remapping hardware for requests-with-PASID. A value of N in this field indicates hardware supports PASID field of N+1 bits (For example, value of 7 in this field, indicates 8-bit PASIDs are supported). Requests-with-PASID with PASID value beyond the limit specified by this field are treated as error by the remapping hardware. This field is valid only when PASID field is reported as Set.
34	0h RO	**Extended Accessed Flag Support (EAFS):** • 0 = Hardware does not support the extended-accessed (EA) bit in first-level paging-structure entries. • 1 = Hardware supports the extended accessed (EA) bit in first-level paging-structure entries. This field is valid only when PASID field is reported as Set.
33	0h RO	**No Write Flag Support (NWFS):** • 0 = Hardware ignores the No Write (NW) flag in Device-TLB translationrequests, and behaves as if NW is always 0. • 1 = Hardware supports the No Write (NW) flag in Device-TLB translationrequests. This field is valid only when Device-TLB support (DT) field is reported as Set.
32	0h RO	**PASID-Only Translations (POT):** • 0 = Hardware does not support PASID-only Translation Type in extended-context-entries. • 1 = Hardware supports PASID-only Translation Type in extended-context-entries. This field is valid only when PASID field is reported as Set.
31	0h RO	**Supervisor Request Support (SRS):** • 0 = H/W does not support requests-with-PASID seeking supervisor privilege. • 1 = H/W supports requests-with-PASID seeking supervisor privilege. The field is valid only when PASID field is reported as Set.
30	0h RO	**Execute Request Support (ERS):** • 0 = H/W does not support requests-with-PASID seeking execute permission. • 1 = H/W supports requests-with-PASID seeking execute permission. This field is valid only when PASID field is reported as Set.
29	0h RO	**Page Request Support (PRS):** • 0 = Hardware does not support Page Requests. • 1 = Hardware supports Page Requests This field is valid only when Device-TLB (DT) field is reported as Set.
28	0h RO	**IGN:** Ignore this field

Bit Range	Default & Access	Field Name (ID): Description
27	0h RO	**Deferred Invalidate Support (DIS):** • 0 = Hardware does not support deferred invalidations of IOTLB and Device-TLB. • 1 = Hardware supports deferred invalidations of IOTLB and Device-TLB. This field is valid only when PASID field is reported as Set.
26	0h RO	**Nested Translation Support (NEST):** • 0 = Hardware does not support nested translations. • 1 = Hardware supports nested translations. This field is valid only when PASID field is reported as Set.
25	0h RO	**Memory Type Support (MTS):** • 0 = Hardware does not support Memory Type in first-level translation and Extended Memory type in second-level translation. • 1 = Hardware supports Memory Type in first-level translation and Extended Memory type in second-level translation. This field is valid only when PASID and ECS fields are reported as Set. Remapping hardware units with, one or more devices that operate in processor coherency domain, under its scope must report this field as Set.
24	0h RO	**Extended Context Support (ECS):** • 0 = Hardware does not support extended-root-entries and extended-context-entries. • 1 = Hardware supports extended-root-entries and extended-context-entries. Implementations reporting PASID or PRS fields as Set, must report this field as Set.
23:20	Fh RO	**Maximum Handle Mask Value (MHMV):** The value in this field indicates the maximum supported value for the Handle Mask (HM) field in the interrupt entry cache invalidation descriptor (iec_inv_dsc). This field is valid only when the IR field in Extended Capability register is reported as Set.
19:18	0h RO	**Reserved**
17:8	050h RO	**IOTLB Register Offset (IRO):** This field specifies the offset to the IOTLB registers relative to the register base address of this remapping hardware unit. If the register base address is X, and the value reported in this field is Y, the address for the first IOTLB invalidation register is calculated as X+(16*Y).
7	1h RO	**Snoop Control (SC):** • 0 = Hardware does not support 1-setting of the SNP field in the page-table entries. • 1 = Hardware supports the 1-setting of the SNP field in the page-table entries.
6	1h RO	**Pass Through (PT):** • 0 = Hardware does not support pass-through translation type in context entries and extended-context-entries. • 1 = Hardware supports pass-through translation type in context entries and extended-context-entries. Pass-through translation is specified through Translation-Type (T) field value of 10b in context-entries, or T field value of 010b in extended-context-entries. Hardware implementations supporting PASID must report a value of 1b in this field.
5	0h RO	**Reserved**
4	1h RO	**Extended Interrupt Mode (EIM):** • 0 = On Intel64 platforms, hardware supports only 8-bit APIC-IDs (xAPIC mode). • 1 = On Intel64 platforms, hardware supports 32-bit APIC-IDs (x2APIC mode). This field is valid only on Intel64 platforms reporting Interrupt Remapping support (IR field Set).

Bit Range	Default & Access	Field Name (ID): Description
3	1h RO	**Interrupt Remapping support (IR):** • 0 = Hardware does not support interrupt remapping. • 1 = Hardware supports interrupt remapping. Implementations reporting this field as Set must also support Queued Invalidation (QI).
2	0h RO	**Device-TLB Support (DT):** • 0 = Hardware does not support device-IOTLBs. • 1 = Hardware supports Device-IOTLBs. Implementations reporting this field as Set must also support Queued Invalidation (QI). Hardware implementations supporting I/O Page Requests (PRS field Set in Extended Capability register) must report a value of 1b in this field.
1	1h RO	**Queued Invalidation Support (QI):** • 0 = Hardware does not support queued invalidations. • 1 = Hardware supports queued invalidations.
0	0h RO	**Page-Walk Coherency (C):** This field indicates if hardware access to the root, context, extended-context and interrupt-remap tables, and second-level paging structures for requests-without-PASID, are coherent (snooped) or not. • 0 = Indicates hardware accesses to remapping structures are non-coherent. • 1 = Indicates hardware accesses to remapping structures are coherent. Hardware access to advanced fault log, invalidation queue, invalidation semaphore, page-request queue, PASID-table, PASID-state table, and first-level page-tables are always coherent.

3.8.5 Global Command Register (GCMD_REG_0_0_0_VTDBAR) — Offset 18h

Register to control remapping hardware. If multiple control fields in this register need to be modified, software must serialize the modifications through multiple writes to this register.

Type	Size	Offset	Default
MMIO	32 bit	VTDPVC0BAR + 18h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RW	**Translation Enable (TE):** Software writes to this field to request hardware to enable/disable DMA-remapping: • 0 = Disable DMA remapping. • 1 = Enable DMA remapping. Hardware reports the status of the translation enable operation through the TES field in the Global Status register. There may be active DMA requests in the platform when software updates this field. Hardware must enable or disable remapping logic only at deterministic transaction boundaries, so that any in-flight transaction is either subject to remapping or not at all. Hardware implementations supporting DMA draining must drain any in-flight DMA read/write requests queued within the Root-Complex before completing the translation enable command and reflecting the status of the command through the TES field in the Global Status register. The value returned on a read of this field is undefined.
30	0h WO	**Set Root Table Pointer (SRTP):** Software sets this field to set/update the root-entry table pointer used by hardware. The root-entry table pointer is specified through the Root-entry Table Address (RTA_REG) register. Hardware reports the status of the Set Root Table Pointer operation through the RTPS field in the Global Status register. The Set Root Table Pointer operation must be performed before enabling or re-enabling (after disabling) DMA remapping through the TE field. .After a Set Root Table Pointer operation, software must globally invalidate the context cache and then globally invalidate of IOTLB. This is required to ensure hardware uses only the remapping structures referenced by the new root table pointer, and not stale cached entries. While DMA remapping hardware is active, software may update the root table pointer through this field. However, to ensure valid in-flight DMA requests are deterministically remapped, software must ensure that the structures referenced by the new root table pointer are programmed to provide the same remapping results as the structures referenced by the previous root-table pointer. Clearing this bit has no effect. The value returned on read of this field is undefined.
29	0h RO	**Set Fault Log (SFL):** This field is valid only for implementations supporting advanced fault logging. Software sets this field to request hardware to set/update the fault-log pointer used by hardware. The fault-log pointer is specified through Advanced Fault Log register. Hardware reports the status of the Set Fault Log operation through the FLS field in the Global Status register. The fault log pointer must be set before enabling advanced fault logging (through EAFL field). Once advanced fault logging is enabled, the fault log pointer may be updated through this field while DMA remapping is active. Clearing this bit has no effect. The value returned on read of this field is undefined.

Bit Range	Default & Access	Field Name (ID): Description
28	0h RO	**Enable Advanced Fault Logging (EAFL):** This field is valid only for implementations supporting advanced fault logging. Software writes to this field to request hardware to enable or disable advanced fault logging: • 0 = Disable advanced fault logging. In this case, translation faults are reported through the Fault Recording registers. • 1 = Enable use of memory-resident fault log. When enabled, translation faults are recorded in the memory-resident log. The fault log pointer must be set in hardware (through the SFL field) before enabling advanced fault logging. Hardware reports the status of the advanced fault logging enable operation through the AFLS field in the Global Status register. The value returned on read of this field is undefined.
27	0h RO	**Write Buffer Flush (WBF):** This bit is valid only for implementations requiring write buffer flushing. Software sets this field to request that hardware flush the Root-Complex internal write buffers. This is done to ensure any updates to the memory-resident remapping structures are not held in any internal write posting buffers. Hardware reports the status of the write buffer flushing operation through the WBFS field in the Global Status register. Clearing this bit has no effect. The value returned on a read of this field is undefined.
26	0h RW	**Queued Invalidation Enable (QIE):** This field is valid only for implementations supporting queued invalidations. Software writes to this field to enable or disable queued invalidations. • 0 = Disable queued invalidations. • 1 = Enable use of queued invalidations. Hardware reports the status of queued invalidation enable operation through QIES field in the Global Status register. The value returned on a read of this field is undefined.
25	0h RW	**Interrupt Remapping Enable (IRE):** This field is valid only for implementations supporting interrupt remapping. • 0 = Disable interrupt-remapping hardware. • 1 = Enable interrupt-remapping hardware. Hardware reports the status of the interrupt remapping enable operation through the IRES field in the Global Status register. There may be active interrupt requests in the platform when software updates this field. Hardware must enable or disable interrupt-remapping logic only at deterministic transaction boundaries, so that any in-flight interrupts are either subject to remapping or not at all. Hardware implementations must drain any in-flight interrupts requests queued in the Root-Complex before completing the interrupt-remapping enable command and reflecting the status of the command through the IRES field in the Global Status register. The value returned on a read of this field is undefined.

Bit Range	Default & Access	Field Name (ID): Description
24	0h WO	**Set Interrupt Remap Table Pointer (SIRTP):** This field is valid only for implementations supporting interrupt-remapping. Software sets this field to set/update the interrupt remapping table pointer used by hardware. The interrupt remapping table pointer is specified through the Interrupt Remapping Table Address (IRTA_REG) register. Hardware reports the status of the Set Interrupt Remap Table Pointer operation through the IRTPS field in the Global Status register. The Set Interrupt Remap Table Pointer operation must be performed before enabling or re-enabling (after disabling) interrupt-remapping hardware through the IRE field. After a Set Interrupt Remap Table Pointer operation, software must globally invalidate the interrupt entry cache. This is required to ensure hardware uses only the interrupt-remapping entries referenced by the new interrupt remap table pointer, and not any stale cached entries. While interrupt remapping is active, software may update the interrupt remapping table pointer through this field. However, to ensure valid in-flight interrupt requests are deterministically remapped, software must ensure that the structures referenced by the new interrupt remap table pointer are programmed to provide the same remapping results as the structures referenced by the previous interrupt remap table pointer. Clearing this bit has no effect. The value returned on a read of this field is undefined.
23	0h RW	**Compatibility Format Interrupt (CFI):** This field is valid only for Intel64 implementations supporting interrupt-remapping. Software writes to this field to enable or disable Compatibility Format interrupts on Intel64 platforms. The value in this field is effective only when interrupt-remapping is enabled and Extended Interrupt Mode (x2APIC mode) is not enabled. • 0 = Block Compatibility format interrupts. • 1 = Process Compatibility format interrupts as pass-through (bypass interrupt remapping). Hardware reports the status of updating this field through the CFIS field in the Global Status register. The value returned on a read of this field is undefined.
22:0	0h RO	**Reserved**

3.8.6 Global Status Register (GSTS_REG_0_0_0_VTDBAR) — Offset 1Ch

Register to report general remapping hardware status.

Type	Size	Offset	Default
MMIO	32 bit	VTDPVC0BAR + 1Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31	0h RO/V	**Translation Enable Status (TES):** This field indicates the status of DMA-remapping hardware. • 0 = DMA-remapping hardware is not enabled. • 1 = DMA-remapping hardware is enabled

Bit Range	Default & Access	Field Name (ID): Description
30	0h RO/V	**Root Table Pointer Status (RTPS):** This field indicates the status of the root- table pointer in hardware. This field is cleared by hardware when software sets the SRTP field in the Global Command register. This field is set by hardware when hardware completes the Set Root Table Pointer operation using the value provided in the Root-Entry Table Address register.
29	0h RO	**Fault Log Status (FLS):** This field: • Is cleared by hardware when software Sets the SFL field in the Global Command register. • Is Set by hardware when hardware completes the Set Fault Log Pointer operation using the value provided in the Advanced Fault Log register.
28	0h RO	**Advanced Fault Logging Status (AFLS):** This field is valid only for implementations supporting advanced fault logging. It indicates the advanced fault logging status: • 0 = Advanced Fault Logging is not enabled. • 1 = Advanced Fault Logging is enabled.
27	0h RO	**Write Buffer Flush Status (WBFS):** This field is valid only for implementations requiring write buffer flushing. This field indicates the status of the write buffer flush command. It is: • Set by hardware when software sets the WBF field in the Global Command register. • Cleared by hardware when hardware completes the write buffer flushing operation.
26	0h RO/V	**Queued Invalidation Enable Status (QIES):** This field indicates queued invalidation enable status. • 0 = queued invalidation is not enabled. • 1 = queued invalidation is enabled
25	0h RO/V	**Interrupt Remapping Enable Status (IRES):** This field indicates the status of Interrupt-remapping hardware. • 0 = Interrupt-remapping hardware is not enabled. • 1 = Interrupt-remapping hardware is enabled
24	0h RO/V	**Interrupt Remapping Pointer Status (IRTPS):** This field indicates the status of the interrupt remapping table pointer in hardware. This field is cleared by hardware when software sets the SIRTP field in the Global Command register. This field is Set by hardware when hardware completes the set interrupt remap table pointer operation using the value provided in the Interrupt Remapping Table Address register.
23	0h RO/V	**Compatibility Format Interrupt Status (CFIS):** This field indicates the status of Compatibility format interrupts on Intel64 implementations supporting interrupt-remapping. The value reported in this field is applicable only when interrupt-remapping is enabled and Extended Interrupt Mode (x2APIC mode) is not enabled. • 0 = Compatibility format interrupts are blocked. • 1 = Compatibility format interrupts are processed as pass-through (bypassing interrupt remapping).
22:0	0h RO	**Reserved**

3.8.7 Root Table Address Register (RTADDR_REG_0_0_0_VTDBAR) — Offset 20h

Register providing the base address of root-entry table.

Type	Size	Offset	Default
MMIO	64 bit	VTDPVC0BAR + 20h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
63:12	00000000 00000h RW	**Root Table Address (RTA):** This register points to base of page aligned, 4KB-sized root-entry table in system memory. Hardware ignores and not implements bits 63:HAW, where HAW is the host address width. Software specifies the base address of the root-entry table through this register, and programs it in hardware through the SRTP field in the Global Command register. Reads of this register returns value that was last programmed to it.
11	0h RW	**Root Table Type (RTT):** This field specifies the type of root-table referenced by the Root Table Address (RTA) field: • 0 = Root Table. • 1 = Extended Root Table
10:0	0h RO	**Reserved**

3.8.8 Context Command Register (CCMD_REG_0_0_0_VTDBAR) — Offset 28h

Register to manage context cache. The act of writing the uppermost byte of the CCMD_REG with the ICC field Set causes the hardware to perform the context-cache invalidation.

Type	Size	Offset	Default
MMIO	64 bit	VTDPVC0BAR + 28h	0800000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
63	0h RW/V	**Invalidate Context Cache (ICC):** Software requests invalidation of context-cache by setting this field. Software must also set the requested invalidation granularity by programming the CIRG field. Software must read back and check the ICC field is Clear to confirm the invalidation is complete. Software must not update this register when this field is set. Hardware clears the ICC field to indicate the invalidation request is complete. Hardware also indicates the granularity at which the invalidation operation was performed through the CAIG field. Software must submit a context-cache invalidation request through this field only when there are no invalidation requests pending at this remapping hardware unit. Since information from the context-cache may be used by hardware to tag IOTLB entries, software must perform domain-selective (or global) invalidation of IOTLB after the context cache invalidation has completed. Hardware implementations reporting write-buffer flushing requirement (RWBF=1 in Capability register) must implicitly perform a write buffer flush before invalidating the context cache.
62:61	0h RW	**Context Invalidation Request Granularity (CIRG):** Software provides the requested invalidation granularity through this field when setting the ICC field: • 00: Reserved. • 01: Global Invalidation request. • 10: Domain-selective invalidation request. The target domain-id must be specified in the DID field. • 11: Device-selective invalidation request. The target source-id(s) must be specified through the SID and FM fields, and the domain-id (that was programmed in the context-entry for these device(s)) must be provided in the DID field. Hardware implementations may process an invalidation request by performing invalidation at a coarser granularity than requested. Hardware indicates completion of the invalidation request by clearing the ICC field. At this time, hardware also indicates the granularity at which the actual invalidation was performed through the CAIG field.
60:59	1h RO/V	**Context Actual Invalidation Granularity (CAIG):** Hardware reports the granularity at which an invalidation request was processed through the CAIG field at the time of reporting invalidation completion (by clearing the ICC field). The following are the encodings for this field: • 00: Reserved. • 01: Global Invalidation performed. This could be in response to a global, domain-selective or device-selective invalidation request. • 10: Domain-selective invalidation performed using the domain-id specified by software in the DID field. This could be in response to a domain-selective or device-selective invalidation request. • 11: Device-selective invalidation performed using the source-id and domain-id specified by software in the SID and FM fields. This can only be in response to a device-selective invalidation request.
58:34	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
33:32	0h RW	**Function Mask (FM):** Software may use the Function Mask to perform device-selective invalidations on behalf of devices supporting PCI Express Phantom Functions...This field specifies which bits of the function number portion (least significant three bits) of the SID field to mask when performing device-selective invalidations. The following encodings are defined for this field: • 00: No bits in the SID field masked. • 01: Mask most significant bit of function number in the SID field. • 10: Mask two most significant bit of function number in the SID field. • 11: Mask all three bits of function number in the SID field. The context-entries corresponding to all the source-ids specified through the FM and SID fields must have to the domain-id specified in the DID field.
31:16	0000h RW	**SID:** Indicates the source-id of the device whose corresponding context-entry needs to be selectively invalidated. This field along with the FM field must be programmed by software for device-selective invalidation requests.
15:0	0000h RW	**DID:** Indicates the id of the domain whose context-entries need to be selectively invalidated. This field must be programmed by software for both domain-selective and device-selective invalidation requests. The Capability register reports the domain-id width supported by hardware. Software must ensure that the value written to this field is within this limit. Hardware may ignore and not implement bits15:N, where N is the supported domain-id width reported in the Capability register.

3.8.9 Fault Status Register (FSTS_REG_0_0_0_VTDBAR) — Offset 34h

Register indicating the various error status.

Type	Size	Offset	Default
MMIO	32 bit	VTDPVC0BAR + 34h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:16	0h RO	**Reserved**
15:8	00h RO	**Fault Record Index (FRI):** This field is valid only when the PPF field is Set. The FRI field indicates the index (from base) of the fault recording register to which the first pending fault was recorded when the PPF field was Set by hardware. The value read from this field is undefined when the PPF field is clear.
7	0h RW/1C	**Page Request Overflow (PRO):** Hardware detected a Page Request Overflow error. Hardware implementations not supporting the Page Request Queue implement this bit as RsvdZ.

Bit Range	Default & Access	Field Name (ID): Description
6	0h RO	**Invalidation Time-out Error (ITE):** Hardware detected a Device-IOTLB invalidation completion time-out. At this time, a fault event may be generated based on the programming of the Fault Event Control register. Hardware implementations not supporting device Device-IOTLBs implement this bit as RsvdZ.
5	0h RO	**Invalidation Completion Error (ICE):** Hardware received an unexpected or invalid Device-IOTLB invalidation completion. This could be due to either an invalid ITag or invalid source-id in an invalidation completion response. At this time, a fault event may be generated based on the programming of hte Fault Event Control register. Hardware implementations not supporting Device-IOTLBs implement this bit as RsvdZ.
4	0h RW/1C	**Invalidation Queue Error (IQE):** Hardware detected an error associated with the invalidation queue. This could be due to either a hardware error while fetching a descriptor from the invalidation queue, or hardware detecting an erroneous or invalid descriptor in the invalidation queue. At this time, a fault event may be generated based on the programming of the Fault Event Control register. Hardware implementations not supporting queued invalidations implement this bit as RsvdZ.
3	0h RO	**Advanced Pending Fault (APF):** When this field is Clear, hardware sets this field when the first fault record (at index 0) is written to a fault log. At this time, a fault event is generated based on the programming of the Fault Event Control register. Software writing 1 to this field clears it. Hardware implementations not supporting advanced fault logging implement this bit as RsvdZ.
2	0h RO	**Advanced Fault Overflow (AFO):** Hardware sets this field to indicate advanced fault log overflow condition. At this time, a fault event is generated based on the programming of the Fault Event Control register. Software writing 1 to this field clears it. Hardware implementations not supporting advanced fault logging implement this bit as RsvdZ.
1	0h RO/V	**Primary Pending Fault (PPF):** This field indicates if there are one or more pending faults logged in the fault recording registers. Hardware computes this field as the logical OR of Fault (F) fields across all the fault recording registers of this remapping hardware unit. • 0 = No pending faults in any of the fault recording registers. • 1 = One or more fault recording registers has pending faults. The FRI field is updated by hardware whenever the PPF field is set by hardware. Also, depending on the programming of Fault Event Control register, a fault event is generated when hardware sets this field.
0	0h RW/1C	**Primary Fault Overflow (PFO):** Hardware sets this field to indicate overflow of fault recording registers. Software writing 1 clears this field. When this field is Set, hardware does not record any new faults until software clears this field.

3.8.10 Fault Event Control Register (FECTL_REG_0_0_0_VTDBAR) — Offset 38h

Register specifying the fault event interrupt message control bits.

Type	Size	Offset	Default
MMIO	32 bit	VTDPVC0BAR + 38h	80000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	1h RW	**Interrupt Mask (IM):** • 0 = No masking of interrupt. When an interrupt condition is detected, hardware issues an interrupt message (using the Fault Event Data and Fault Event Address register values). • 1 = This is the value on reset. Software may mask interrupt message generation by setting this field. Hardware is prohibited from sending the interrupt message when this field is set.
30	0h RO/V	**Interrupt Pending (IP):** Hardware sets the IP field whenever it detects an interrupt condition, which is defined as: • When primary fault logging is active, an interrupt condition occurs when hardware records a fault through one of the Fault Recording registers and sets the PPF field in Fault Status register. • When advanced fault logging is active, an interrupt condition occurs when hardware records a fault in the first fault record (at index 0) of the current fault log and sets the APF field in the Fault Status register. • Hardware detected error associated with the Invalidation Queue, setting the IQE field in the Fault Status register. • Hardware detected invalid Device-IOTLB invalidation completion, setting the ICE field in the Fault Status register. • Hardware detected Device-IOTLB invalidation completion time-out, setting the ITE field in the Fault Status register. If any of the status fields in the Fault Status register was already Set at the time of setting any of these fields, it is not treated as a new interrupt condition. The IP field is kept set by hardware while the interrupt message is held pending. The interrupt message could be held pending due to interrupt mask (IM field) being Set or other transient hardware conditions. The IP field is cleared by hardware as soon as the interrupt message pending condition is serviced. This could be due to either: • Hardware issuing the interrupt message due to either change in the transient hardware condition that caused interrupt message to be held pending, or due to software clearing the IM field. • Software servicing all the pending interrupt status fields in the Fault Status register as follows: - When primary fault logging is active, software clearing the Fault (F) field in all the Fault Recording registers with faults, causing the PPF field in Fault Status register to be evaluated as clear. - Software clearing other status fields in the Fault Status register by writing back the value read from the respective fields.
29:0	0h RO	**Reserved**

3.8.11 Fault Event Data Register (FEDATA_REG_0_0_0_VTDBAR) — Offset 3Ch

Register specifying the interrupt message data

Type	Size	Offset	Default
MMIO	32 bit	VTDPVC0BAR + 3Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:16	0000h RW	**Extended Interrupt Message Data (EIMD):** This field is valid only for implementations supporting 32-bit interrupt data fields. Hardware implementations supporting only 16-bit interrupt data may treat this field as RsvdZ.
15:0	0000h RW	**Interrupt Message Data (IMD):** Data value in the interrupt request.

3.8.12 Fault Event Address Register (FEADDR_REG_0_0_0_VTDBAR) — Offset 40h

Register specifying the interrupt message address.

Type	Size	Offset	Default
MMIO	32 bit	VTDPVC0BAR + 40h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:2	00000000h RW	**Message Address (MA):** When fault events are enabled, the contents of this register specify the DWORD-aligned address (bits 31:2) for the interrupt request.
1:0	0h RO	**Reserved**

3.8.13 Fault Event Upper Address Register (FEUADDR_REG_0_0_0_VTDBAR) — Offset 44h

Register specifying the interrupt message upper address.

Type	Size	Offset	Default
MMIO	32 bit	VTDPVC0BAR + 44h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RW	**Message Upper Address (MUA):** Hardware implementations supporting Extended Interrupt Mode are required to implement this register. Hardware implementations not supporting Extended Interrupt Mode may treat this field as RsvdZ.

3.8.14 Advanced Fault Log Register (AFLOG_REG_0_0_0_VTDBAR) — Offset 58h

Register to specify the base address of the memory-resident fault-log region. This register is treated as RsvdZ for implementations not supporting advanced translation fault logging (AFL field reported as 0 in the Capability register).

Type	Size	Offset	Default
MMIO	64 bit	VTDPVC0BAR + 58h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:12	0000000000000h RO	**Fault Log Address (FLA):** This field specifies the base of 4KB aligned fault-log region in system memory. Hardware ignores and does not implement bits 63:HAW, where HAW is the host address width. Software specifies the base address and size of the fault log region through this register, and programs it in hardware through the SFL field in the Global Command register. When implemented, reads of this field return the value that was last programmed to it.
11:9	0h RO	**Fault Log Size (FLS):** This field specifies the size of the fault log region pointed by the FLA field. The size of the fault log region is 2X * 4KB, where X is the value programmed in this register. When implemented, reads of this field return the value that was last programmed to it.
8:0	0h RO	**Reserved**

3.8.15 Protected Memory Enable Register (PMEN_REG_0_0_0_VTDBAR) — Offset 64h

Register to enable the DMA-protected memory regions setup through the PLMBASE,..PLMLIMT, PHMBASE, PHMLIMIT registers. This register is always treated as RO for implementations not supporting protected memory regions (PLMR and PHMR fields reported as Clear in the Capability register).

Protected memory regions may be used by software to securely initialize remapping structures in memory. To avoid impact to legacy BIOS usage of memory, software is recommended to not overlap protected memory regions with any reserved memory regions of the platform reported through the Reserved Memory Region Reporting (RMRR) structures.

Type	Size	Offset	Default
MMIO	32 bit	VTDPVC0BAR + 64h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RW	**Enable Protected Memory (EPM):** This field controls DMA accesses to the protected low-memory and protected high-memory regions. • 0 = Protected memory regions are disabled. • 1 = Protected memory regions are enabled.DMA requests accessing protected memory regions are handled as follows: - When DMA remapping is not enabled, all DMA requests accessing protected memory regions are blocked. - When DMA remapping is enabled: • DMA requests processed as pass-through (Translation Type value of 10b in Context-Entry) and accessing the protected memory regions are blocked. • DMA requests with translated address (AT=10b) and accessing the protected memory regions are blocked. • DMA requests that are subject to address remapping, and accessing the protected memory regions may or may not be blocked by hardware. For such requests, software must not depend on hardware protection of the protected memory regions, and instead program the DMA-remapping page-tables to not allow DMA to protected memory regions. Remapping hardware access to the remapping structures are not subject to protected memory region checks. DMA requests blocked due to protected memory region violation are not recorded or reported as remapping faults. Hardware reports the status of the protected memory enable/disable operation through the PRS field in this register.Hardware implementations supporting DMA draining must drain any in-flight translated DMA requests queued within the Root-Complex before indicating the protected memory region as enabled through the PRS field.
30:1	0h RO	**Reserved**
0	0h RO/V	**Protected Region Status (PRS):** This field indicates the status of protected memory region(s): • 0 = Protected memory region(s) disabled. • 1 = Protected memory region(s) enabled.

3.8.16 Protected Low Memory Base Register (PLMBASE_REG_0_0_0_VTDBAR) — Offset 68h

Register to set up the base address of DMA-protected low-memory region below 4GB. This register must be set up before enabling protected memory through PMEN_REG, and must not be updated when protected memory regions are enabled.

This register is always treated as RO for implementations not supporting protected low memory region (PLMR field reported as Clear in the Capability register).

The alignment of the protected low memory region base depends on the number of reserved bits (N:0) of this register. Software may determine N by writing all 1s to this register, and finding the most significant zero bit position with 0 in the value read back from the register. Bits N:0 of this register is decoded by hardware as all 0s...Software must setup the protected low memory region below 4GB.

Software must not modify this register when protected memory regions are enabled (PRS field Set in PMEN_REG).

Type	Size	Offset	Default
MMIO	32 bit	VTDPVC0BAR + 68h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:20	000h RW	**Protected Low-Memory Base (PLMB):** This register specifies the base of protected low-memory region in system memory.
19:0	0h RO	**Reserved**

3.8.17 Protected Low-Memory Limit Register (PLMLIMIT_REG_0_0_0_VTDBAR) — Offset 6Ch

Register to set up the limit address of DMA-protected low-memory region below 4GB. This register must be set up before enabling protected memory through PMEN_REG, and must not be updated when protected memory regions are enabled

This register is always treated as RO for implementations not supporting protected low memory region (PLMR field reported as Clear in the Capability register)

The alignment of the protected low memory region limit depends on the number of reserved bits (N:0) of this register. Software may determine N by writing all 1s to this register, and finding most significant zero bit position with 0 in the value read back from the register. Bits N:0 of the limit register is decoded by hardware as all 1s

The Protected low-memory base and limit registers functions as follows:

- Programming the protected low-memory base and limit registers with the same value in bits 31: (N+1) specifies a protected low-memory region of size 2(N+1) bytes

- Programming the protected low-memory limit register with a value less than the protected low-memory base register disables the protected low-memory region

Software must not modify this register when protected memory regions are enabled (PRS field Set in PMEN_REG).

Type	Size	Offset	Default
MMIO	32 bit	VTDPVC0BAR + 6Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:20	000h RW	**Protected Low-Memory Limit (PLML):** This register specifies the last host physical address of the DMA-protected low-memory region in system memory.
19:0	0h RO	**Reserved**

3.8.18 Protected High-Memory Base Register (PHMBASE_REG_0_0_0_VTDBAR) — Offset 70h

Register to set up the base address of DMA-protected high-memory region. This register must be set up before enabling protected memory through PMEN_REG, and must not be updated when protected memory regions are enabled

This register is always treated as RO for implementations not supporting protected high memory region (PHMR field reported as Clear in the Capability register)

The alignment of the protected high memory region base depends on the number of reserved bits (N:0) of this register. Software may determine N by writing all 1s to this register, and finding most significant zero bit position below host address width (HAW) in the value read back from the register. Bits N:0 of this register are decoded by hardware as all 0s

Software may setup the protected high memory region either above or below 4GB

Software must not modify this register when protected memory regions are enabled (PRS field Set in PMEN_REG).

Type	Size	Offset	Default
MMIO	64 bit	VTDPVC0BAR + 70h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:20	00000h RW	**Protected High-Memory Base (PHMB):** This register specifies the base of protected (high) memory region in system memory Hardware ignores, and does not implement, bits 63:HAW, where HAW is the host address width.
19:0	0h RO	**Reserved**

3.8.19 Protected High-Memory Limit Register (PHMLIMIT_REG_0_0_0_VTDBAR) — Offset 78h

Register to set up the limit address of DMA-protected high-memory region. This register must be set up before enabling protected memory through PMEN_REG, and must not be updated when protected memory regions are enabled

This register is always treated as RO for implementations not supporting protected high memory region (PHMR field reported as Clear in the Capability register)

The alignment of the protected high memory region limit depends on the number of reserved bits (N:0) of this register. Software may determine the value of N by writing all 1s to this register, and finding most significant zero bit position below host address width (HAW) in the value read back from the register. Bits N:0 of the limit register is decoded by hardware as all 1s

The protected high-memory base & limit registers functions as follows

- Programming the protected low-memory base and limit registers with the same value in bits HAW:(N+1) specifies a protected low-memory region of size 2(N+1) bytes
- Programming the protected high-memory limit register with a value less than the protected high-memory base register disables the protected high-memory region

Software must not modify this register when protected memory regions are enabled (PRS field Set in PMEN_REG).

Type	Size	Offset	Default
MMIO	64 bit	VTDPVC0BAR + 78h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:20	00000h RW	**Protected High-Memory Limit (PHML):** This register specifies the last host physical address of the DMA-protected high-memory region in system memory Hardware ignores and does not implement bits 63:HAW, where HAW is the host address width.
19:0	0h RO	**Reserved**

3.8.20 Invalidation Queue Head Register (IQH_REG_0_0_0_VTDBAR) — Offset 80h

Register indicating the invalidation queue head. This register is treated as RsvdZ by implementations reporting Queued Invalidation (QI) as not supported in the Extended Capability register.

Type	Size	Offset	Default
MMIO	64 bit	VTDPVC0BAR + 80h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:19	0h RO	**Reserved**
18:4	0000h RO/V	**Queue Head (QH):** Specifies the offset (128-bit aligned) to the invalidation queue for the command that will be fetched next by hardware Hardware resets this field to 0 whenever the queued invalidation is disabled (QIES field Clear in the Global Status register).
3:0	0h RO	**Reserved**

3.8.21 Invalidation Queue Tail Register (IQT_REG_0_0_0_VTDBAR) — Offset 88h

Register indicating the invalidation tail head. This register is treated as RsvdZ by implementations reporting Queued Invalidation (QI) as not supported in the Extended Capability register.

Type	Size	Offset	Default
MMIO	64 bit	VTDPVC0BAR + 88h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
63:19	0h RO	**Reserved**
18:4	0000h RW	**Queue Tail (QT):** Specifies the offset (128-bit aligned) to the invalidation queue for the command that will be written next by software.
3:0	0h RO	**Reserved**

3.8.22 Invalidation Queue Address Register (IQA_REG_0_0_0_VTDBAR) — Offset 90h

Register to configure the base address and size of the invalidation queue. This register is treated as RsvdZ by implementations reporting Queued Invalidation (QI) as not supported in the Extended Capability register.

Type	Size	Offset	Default
MMIO	64 bit	VTDPVC0BAR + 90h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:12	0000000h RW	**Invalidation Queue Base Address (IQA):** This field points to the base of 4KB aligned invalidation request queue. Hardware ignores and does not implement bits 63:HAW, where HAW is the host address width Reads of this field return the value that was last programmed to it.

Bit Range	Default & Access	Field Name (ID): Description
11:3	0h RO	**Reserved**
2:0	0h RW	**Queue Size (QS):** This field specifies the size of the invalidation request queue. A value of X in this field indicates an invalidation request queue of (2X) 4KB pages. The number of entries in the invalidation queue is 2(X + 8).

3.8.23 Invalidation Completion Status Register (ICS_REG_0_0_0_VTDBAR) — Offset 9Ch

Register to report completion status of invalidation wait descriptor with Interrupt Flag (IF) Set

This register is treated as RsvdZ by implementations reporting Queued Invalidation (QI) as not supported in the Extended Capability register.

Type	Size	Offset	Default
MMIO	32 bit	VTDPVC0BAR + 9Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:1	0h RO	**Reserved**
0	0h RW/1C	**Invalidation Wait Descriptor Complete (IWC):** Indicates completion of Invalidation Wait Descriptor with Interrupt Flag (IF) field Set. Hardware implementations not supporting queued invalidations implement this field as RsvdZ.

3.8.24 Invalidation Event Control Register (IECTL_REG_0_0_0_VTDBAR) — Offset A0h

Register specifying the invalidation event interrupt control bits

This register is treated as RsvdZ by implementations reporting Queued Invalidation (QI) as not supported in the Extended Capability register.

Type	Size	Offset	Default
MMIO	32 bit	VTDPVC0BAR + A0h	80000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	1h RW	**Interrupt Mask (IM):** • 0= No masking of interrupt. When a invalidation event condition is detected, hardware issues an interrupt message (using the Invalidation Event Data & Invalidation Event Address register values) • 1= This is the value on reset. Software may mask interrupt message generation by setting this field. Hardware is prohibited from sending the interrupt message when this field is Set.
30	0h RO/V	**Interrupt Pending (IP):** Hardware sets the IP field whenever it detects an interrupt condition. Interrupt condition is defined as: • An Invalidation Wait Descriptor with Interrupt Flag (IF) field Set completed, setting the IWC field in the Invalidation Completion Status register • If the IWC field in the Invalidation Completion Status register was already Set at the time of setting this field, it is not treated as a new interrupt condition The IP field is kept Set by hardware while the interrupt message is held pending. The interrupt message could be held pending due to interrupt mask (IM field) being Set, or due to other transient hardware conditions. The IP field is cleared by hardware as soon as the interrupt message pending condition is serviced. This could be due to either: • 0= Hardware issuing the interrupt message due to either change in the transient hardware condition that caused interrupt message to be held pending or due to software clearing the IM field • 1= Software servicing the IWC field in the Invalidation Completion Status register.
29:0	0h RO	**Reserved**

3.8.25 Invalidation Event Data Register (IEDATA_REG_0_0_0_VTDBAR) — Offset A4h

Register specifying the Invalidation Event interrupt message data

This register is treated as RsvdZ by implementations reporting Queued Invalidation (QI) as not supported in the Extended Capability register.

Type	Size	Offset	Default
MMIO	32 bit	VTDPVC0BAR + A4h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:16	0000h RW	**Extended Interrupt Message Data (EIMD):** This field is valid only for implementations supporting 32-bit interrupt data fields Hardware implementations supporting only 16-bit interrupt data treat this field as Rsvd.
15:0	0000h RW	**Interrupt Message Data (IMD):** Data value in the interrupt request.

3.8.26 Invalidation Event Address Register (IEADDR_REG_0_0_0_VTDBAR) — Offset A8h

Register specifying the Invalidation Event Interrupt message address

This register is treated as RsvdZ by implementations reporting Queued Invalidation (QI) as not supported in the Extended Capability register.

Note: Bit definitions are the same as FEADDR_REG_0_0_0_VTDBAR, offset 40h.

3.8.27 Invalidation Event Upper Address Register (IEUADDR_REG_0_0_0_VTDBAR) — Offset ACh

Register specifying the Invalidation Event interrupt message upper address.

Type	Size	Offset	Default
MMIO	32 bit	VTDPVC0BAR + ACh	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RW	**Message Upper Address (MUA):** Hardware implementations supporting Queued Invalidations and Extended Interrupt Mode are required to implement this register Hardware implementations not supporting Queued Invalidations or Extended Interrupt Mode may treat this field as RsvdZ.

3.8.28 Interrupt Remapping Table Address Register (IRTA_REG_0_0_0_VTDBAR) — Offset B8h

Register providing the base address of Interrupt remapping table. This register is treated as RsvdZ by implementations reporting Interrupt Remapping (IR) as not supported in the Extended Capability register.

Type	Size	Offset	Default
MMIO	64 bit	VTDPVC0BAR + B8h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
63:12	00000000 00000h RW	**Interrupt Remapping Table Address (IRTA):** This field points to the base of 4KB aligned interrupt remapping table Hardware ignores and does not implement bits 63:HAW, where HAW is the host address width Reads of this field returns value that was last programmed to it.
11	0h RW	**Extended Interrupt Mode Enable (EIME):** This field is used by hardware on Intel64 platforms as follows: • 0=xAPIC mode is active. Hardware interprets only low 8-bits of Destination-ID field in the IRTEs. The high 24-bits of the Destination-ID field are treated as reserved • 1= x2APIC mode is active. Hardware interprets all 32-bits of Destination-ID field in the IRTEs This field is implemented as RsvdZ on implementations reporting Extended Interrupt Mode (EIM) field as Clear in Extended Capability register.
10:4	0h RO	**Reserved**
3:0	0h RW	**S:** This field specifies the size of the interrupt remapping table. The number of entries in the interrupt remapping table is 2(X+1), where X is the value programmed in this field.

3.8.29 Page Request Status Register (PRESTS_REG_0_0_0_VTDBAR) — Offset DCh

Register to report pending page request in page request queue. This register is treated as RsvdZ by implementations reporting Page Request Support (PRS) as not supported in the Extended Capability register.

Type	Size	Offset	Default
MMIO	32 bit	VTDPVC0BAR + DCh	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:1	0h RO	**Reserved**
0	0h RO	**Pending Page Request (PPR):** Pending Page Request: Indicates pending page requests to be serviced by software in the page request queue. This field is Set by hardware when a streaming page request entry (page_stream_reg_dsc) or a page group request (page_grp_req_dsc) with Last Page in Group (LPG) field Set, is added to the page request queue.

3.8.30 Page Request Event Control Register (PRECTL_REG_0_0_0_VTDBAR) — Offset E0h

Register specifying the page request event interrupt control bits. This register is treated as RsvdZ by implementations reporting Page Request Support (PRS) as not supported in the Extended Capability register

Type	Size	Offset	Default
MMIO	32 bit	VTDPVC0BAR + E0h	80000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31	1h RO	**Interrupt Mask (IM):** Interrupt Mask • 0=No masking of interrupt. When a page request event condition is detected, hardware issues an interrupt message (using the Page Request Event Data and Page Request Event Address register values) • 1=This is the value on reset. Software may mask interrupt message generation by setting this field. Hardware is prohibited from sending the interrupt message when this field is Set.

Bit Range	Default & Access	Field Name (ID): Description
30	0h RO	**Interrupt Pending (IP):** Interrupt Pending: Hardware sets the IP field whenever it detects an interrupt condition. Interrupt condition is defined as: • A streaming page request entry (page_stream_req_dsc) or a page group request (page_grp_req_dsc) with Last Page in Group (LPG) field Set, was added to page request queue, resulting in hardware setting the Pending Page Request (PPR) field in Page Request Status register • If the PPR field in the Page Request Event Status register was already Set at the time of setting this field, it is not treated as a new interrupt condition The IP field is kept Set by hardware while the interrupt message is held pending. The interrupt message could be held pending due to interrupt mask (IM field) being Set, or due to other transient hardware conditions. The IP field is cleared by hardware as soon as the interrupt message pending condition is serviced. This could be due to either: • Hardware issuing the interrupt message due to either change in the transient hardware condition that caused interrupt message to be held pending or due to software clearing the IM field • Software servicing the PPR field in the Page Request Event Status register.
29:0	0h RO	**Reserved**

3.8.31 Page Request Event Data Register (PREDATA_REG_0_0_0_VTDBAR) — Offset E4h

Register specifying the Page Request Event interrupt message data. This register is treated as RsvdZ by implementations reporting Page Request Support (PRS) as not supported in the Extended Capability register.

Type	Size	Offset	Default
MMIO	32 bit	VTDPVC0BAR + E4h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:16	0000h RO	**Extended Interrupt Message Data (EIMD):** Extended Interrupt Message Data
15:0	0000h RO	**Interrupt Message Data (IMD):** Interrupt Message Data: Data value in the interrupt request. Software requirements for programming this register are described in VTd Spec

3.8.32 Page Request Event Address Register (PREADDR_REG_0_0_0_VTDBAR) — Offset E8h

Register specifying the Page Request Event Interrupt message address. This register is treated as RsvdZ by implementations reporting Page Request Support (PRS) as not supported in the Extended Capability register.

Type	Size	Offset	Default
MMIO	32 bit	VTDPVC0BAR + E8h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:2	00000000h RO	**Message Address (MA):** Message Address: When fault events are enabled, the contents of this register specify the DWORD-aligned address (bits 31:2) for the interrupt request.
1:0	0h RO	**Reserved**

3.8.33 Page Request Event Upper Address Register (PREUADDR_REG_0_0_0_VTDBAR) — Offset ECh

Register specifying the Page Request Event interrupt message upper address.

Type	Size	Offset	Default
MMIO	32 bit	VTDPVC0BAR + ECh	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RO	**Message Upper Address (MUA):** Message Upper Address: This field specifies the upper address (bits.. 63:32) for the page request event interrupt.

3.8.34 Fault Recording Register Low [0] (FRCDL_REG_0_0_0_VTDBAR) — Offset 400h

Register to record fault information when primary fault logging is active. Hardware reports the number and location of fault recording registers through the Capability register. This register is relevant only for primary fault logging

This register is sticky and can be cleared only through power good reset or by software clearing the RW1C fields by writing a 1.

Type	Size	Offset	Default
MMIO	64 bit	VTDPVC0BAR + 400h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:12	00000000 00000h RO/V	**Fault Info (FI):** When the Fault Reason (FR) field indicates one of the DMA-remapping fault conditions, bits 63:12 of this field contain the page address in the faulted DMA request. Hardware treats bits 63:N as reserved (0), where N is the maximum guest address width (MGAW) supported. When the Fault Reason (FR) field indicates one of the interrupt-remapping fault conditions, bits 63:48 of this field indicate the interrupt_index computed for the faulted interrupt request, and bits 47:12 are cleared. This field is relevant only when the F field is Set.
11:0	0h RO	**Reserved**

3.8.35 Fault Recording Register High [0] (FRCDH_REG_0_0_0_VTDBAR) — Offset 408h

Register to record fault information when primary fault logging is active. Hardware reports the number and location of fault recording registers through the Capability register. This register is relevant only for primary fault logging

This register is sticky and can be cleared only through power good reset or by software clearing the RW1C fields by writing a 1.

Type	Size	Offset	Default
MMIO	64 bit	VTDPVC0BAR + 408h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
63	0h RW/1C	**F:** Hardware sets this field to indicate a fault is logged in this Fault Recording register. The F field is set by hardware after the details of the fault is recorded in other fields. When this field is Set, hardware may collapse additional faults from the same source-id (SID)

Bit Range	Default & Access	Field Name (ID): Description
62	0h RO/V	**T:** Type of the faulted request: • 0=0: Write request • 1=1: Read request or AtomicOp request This field is relevant only when the F field is Set, and when the fault reason (FR) indicates one of the DMA-remapping fault conditions.
61:60	0h RO/V	**Address Type (AT):** This field captures the AT field from the faulted DMA request Hardware implementations not supporting Device-IOTLBs (DI field Clear in Extended Capability register) treat this field as RsvdZ When supported, this field is valid only when the F field is Set, and when the fault reason (FR) indicates one of the DMA-remapping fault conditions.
59:40	00000h RO/V	**PASID Value (PN):** PASID value in the faulted request. This field is relevant only when the PP field is set. Hardware implementations not supporting PASID (PASID field Clear in Extended Capability register) implement this field as RsvdZ.
39:32	00h RO/V	**Fault Reason (FR):** Reason for the fault This field is relevant only when the F field is set.
31	0h RO/V	**PASID Present (PP):** When set, indicates the faulted request has a PASID tag. The value of the PASID field is reported in the PASID Value (PV) field. This field is relevant only when the F field is Set, and when the fault reason (FR) indicates one of the non-recoverable address translation fault conditions. Hardware implementations not supporting PASID (PASID field Clear in Extended Capability register) implement this field as RsvdZ.
30	0h RO/V	**Execute Permission Requested (EXE):** When set, indicates Execute permission was requested by the faulted read request. This field is relevant only when the PP field and T field are both Set. Hardware implementations not supporting PASID (PASID field Clear in Extended Capability register) implement this field as RsvdZ.
29	0h RO/V	**Privilege Mode Requested (PRIV):** When set, indicates Supervisor privilege was requested by the faulted request. This field is relevant only when the PP field is Set. Hardware implementations not supporting PASID (PASID field Clear in Extended Capability register) implement this field as RsvdZ.
28:16	0h RO	**Reserved**
15:0	0000h RO/V	**Source Identifier (SID):** Requester-id associated with the fault condition This field is relevant only when the F field is set.

3.8.36 Invalidate Address Register (IVA_REG_0_0_0_VTDBAR) — Offset 500h

Register to provide the DMA address whose corresponding IOTLB entry needs to be invalidated through the corresponding IOTLB Invalidate register. This register is a write-only register.

Type	Size	Offset	Default
MMIO	64 bit	VTDPVC0BAR + 500h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
63:12	00000000 00000h RW	**ADDR:** Software provides the DMA address that needs to be page-selectively invalidated. To make a page-selective invalidation request to hardware, software must first write the appropriate fields in this register, and then issue the appropriate page-selective invalidate command through the IOTLB_REG. Hardware ignores bits 63:N, where N is the maximum guest address width (MGAW) supported. A value returned on a read of this field is undefined A value returned on a read of this field is undefined
11:7	0h RO	**Reserved**
6	0h RW	**Invalidation Hint (IH):** The field provides hint to hardware about preserving or flushing the non-leaf (page-directory) entries that may be cached in hardware: • 0 = Software may have modified both leaf and non-leaf page-table entries corresponding to mappings specified in the ADDR and AM fields. On a page-selective invalidation request, hardware must flush both the cached leaf and non-leaf page-table entries corresponding to the mappings specified by ADDR and AM fields. • 1 = Software has not modified any non-leaf page-table entries corresponding to mappings specified in the ADDR and AM fields. On a page-selective invalidation request, hardware may preserve the cached non-leaf page-table entries corresponding to mappings specified by ADDR and AM fields. A value returned on a read of this field is undefined
5:0	00h RW	**Address Mask (AM):** The value in this field specifies the number of low order bits of the ADDR field that must be masked for the invalidation operation. This field enables software to request invalidation of contiguous mappings for size-aligned regions. For example:..Mask ADDR bits Pages..Value masked invalidated.. 0 None 1.. 1 12 2.. 2 13:12 4.. 3 14:12 8.. 4 15:12 16 When invalidating mappings for super-pages, software must specify the appropriate mask value. For example, when invalidating mapping for a 2MB page, software must specify an address mask value of at least 9...Hardware implementations report the maximum supported mask value through the Capability register.

3.8.37 IOTLB Invalidate Register (IOTLB_REG_0_0_0_VTDBAR) — Offset 508h

Register to invalidate IOTLB. The act of writing the upper byte of the IOTLB_REG with IVT field Set causes the hardware to perform the IOTLB invalidation.

Type	Size	Offset	Default
MMIO	64 bit	VTDPVC0BAR + 508h	0200000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
63	0h RW/V	**Invalidate IOTLB (IVT):** Software requests IOTLB invalidation by setting this field. Software must also set the requested invalidation granularity by programming the IIRG field Hardware clears the IVT field to indicate the invalidation request is complete. Hardware also indicates the granularity at which the invalidation operation was performed through the IAIG field. Software must not submit another invalidation request through this register while the IVT field is Set, nor update the associated Invalidate Address register Software must not submit IOTLB invalidation requests when there is a context-cache invalidation request pending at this remapping hardware unit. Hardware implementations reporting write-buffer flushing requirement (RWBF=1 in Capability register) must implicitly perform a write buffer flushing before invalidating the IOTLB.
62	0h RO	**Reserved**
61:60	0h RW	**IOTLB Invalidation Request Granularity (IIRG):** When requesting hardware to invalidate the IOTLB (by setting the IVT field), software writes the requested invalidation granularity through this field. The following are the encodings for the field • 00 = Reserved • 01 = Global invalidation request • 10 = Domain-selective invalidation request. The target domain-id must be specified in the DID field • 11 = Page-selective invalidation request. The target address, mask and invalidation hint must be specified in the Invalidate Address register, and the domain-id must be provided in the DID field Hardware implementations may process an invalidation request by performing invalidation at a coarser granularity than requested. Hardware indicates completion of the invalidation request by clearing the IVT field. At this time, the granularity at which actual invalidation was performed is reported through the IAIG field
59	0h RO	**Reserved**
58:57	1h RO/V	**IOTLB Actual Invalidation Granularity (IAIG):** Hardware reports the granularity at which an invalidation request was processed through this field when reporting invalidation completion (by clearing the IVT field). The following are the encodings for this field • 00 = Reserved. This indicates hardware detected an incorrect invalidation request and ignored the request. Examples of incorrect invalidation requests include detecting an unsupported address mask value in Invalidate Address register for page-selective invalidation requests • 01 = Global Invalidation performed. This could be in response to a global, domain-selective, or page-selective invalidation request • 10 = Domain-selective invalidation performed using the domain-id specified by software in the DID field. This could be in response to a domain-selective or a page-selective invalidation request • 11 = Domain-page-selective invalidation performed using the address, mask and hint specified by software in the Invalidate Address register and domain-id specified in DID field. This can be in response to a page-selective invalidation request.

Bit Range	Default & Access	Field Name (ID): Description
56:50	0h RO	**Reserved**
49	0h RW	**Drain Reads (DR):** This field is ignored by hardware if the DRD field is reported as clear in the Capability register. When the DRD field is reported as Set in the Capability register, the following encodings are supported for this field: • 0 = Hardware may complete the IOTLB invalidation without draining any translated DMA read requests • 1 = Hardware must drain DMA read requests.
48	0h RW	**Drain Writes (DW):** This field is ignored by hardware if the DWD field is reported as Clear in the Capability register. When the DWD field is reported as Set in the Capability register, the following encodings are supported for this field: • 0 = Hardware may complete the IOTLB invalidation without draining DMA write requests • 1 = Hardware must drain relevant translated DMA write requests.
47:32	0000h RW	**DID:** Indicates the ID of the domain whose IOTLB entries need to be selectively invalidated. This field must be programmed by software for domain-selective and page-selective invalidation requests. The Capability register reports the domain-id width supported by hardware. Software must ensure that the value written to this field is within this limit. Hardware ignores and not implements bits 47:(32+N), where N is the supported domain-id width reported in the Capability register.
31:0	0h RO	**Reserved**

4 Processor Graphics (D2:F0)

This chapter documents the Processor Graphics Registers.

Table 4-1. Summary of Processor Graphics (D2:F0)

Processor Graphics Registers (D2:F0)
Graphics VT BAR (GFXVTBAR) Registers

4.1 Processor Graphics Registers (D2:F0)

This chapter documents the registers in Bus: 0, Device 2, Function 0.

Note: These registers apply to all processors.

4.1.1 Summary of Registers

Table 4-2. Summary of Bus: 0, Device: 2, Function: 0 Registers

Offset	Size (Bytes)	Register Name (Register Symbol)	Default Value
0h	2	Vendor ID (VID2_0_2_0_PCI)	8086h
2h	2	Device ID (DID2_0_2_0_PCI)	0A80h
4h	2	PCI Command (PCICMD_0_2_0_PCI)	0000h
6h	2	PCI Status (PCISTS2_0_2_0_PCI)	0010h
8h	4	Revision Identification and Class Code register (RID2_CC_0_2_0_PCI)	03000000h
Ch	1	Cache Line Size (CLS_0_2_0_PCI)	00h
Dh	1	Master Latency Timer (MLT2_0_2_0_PCI)	00h
Eh	1	Header Type (HDR2_0_2_0_PCI)	00h
Fh	1	Built In Self Test (BIST_0_2_0_PCI)	00h
10h	4	Graphics Translation Table Memory Mapped Range Address (GTTMMADR0_0_2_0_PCI)	00000004h
14h	4	Graphics Translation Table Memory Mapped Range Address (GTTMMADR1_0_2_0_PCI)	00000000h
18h	4	Graphics Memory Range Address (GMADR0_0_2_0_PCI)	0000000Ch
1Ch	4	Graphics Memory Range Address (GMADR1_0_2_0_PCI)	00000000h
20h	4	I/O Base Address (IOBAR_0_2_0_PCI)	00000001h
2Ch	2	Subsystem Vendor Identification (SVID2_0_2_0_PCI)	0000h
2Eh	2	Subsystem Identification (SID2_0_2_0_PCI)	0000h
30h	4	Video BIOS ROM Base Address (ROMADR_0_2_0_PCI)	00000000h
34h	1	Capabilities Pointer (CAPPOINT_0_2_0_PCI)	40h
3Ch	1	Interrupt Line (INTRLINE_0_2_0_PCI)	00h
3Dh	1	Interrupt Pin (INTRPIN_0_2_0_PCI)	01h
3Eh	1	Minimum Grant (MINGNT_0_2_0_PCI)	00h
3Fh	1	Maximum Latency (MAXLAT_0_2_0_PCI)	00h

Offset	Size (Bytes)	Register Name (Register Symbol)	Default Value
40h	2	Capability Identifier (CAPID0_0_2_0_PCI)	7009h
42h	2	Capabilities Control (CAPCTRL0_0_2_0_PCI)	010Ch
44h	4	Capabilities A (CAPID0_A_0_2_0_PCI)	00000000h
48h	4	Capabilities B (CAPID0_B_0_2_0_PCI)	00000000h
50h	2	PCI Mirror of GMCH Graphics Control (MGGC0_0_2_0_PCI)	0500h
54h	2	Mirror of Device Enable (DEVEN0_0_2_0_PCI)	00BFh
58h	1	Device 2 Control (DEV2CTL_0_2_0_PCI)	00h
60h	4	Multi Size Aperture Control (MSAC_0_2_0_PCI)	00010000h
68h	4	Push Aperture (PUSHAP_0_2_0_PCI)	00000000h
6Ch	1	VTd Status (VTD_STATUS_0_2_0_PCI)	00h
70h	2	PCI Express Capability Header (PCIECAPHDR_0_2_0_PCI)	AC10h
72h	2	PCI Express Capability (PCIECAP_0_2_0_PCI)	0092h
74h	4	Device Capabilities (DEVICECAP_0_2_0_PCI)	10008000h
78h	2	PCI Express Device Control (DEVICECTL_0_2_0_PCI)	0000h
7Ah	2	PCI Express Capability Structure (DEVICESTS_0_2_0_PCI)	0000h
ACh	2	Message Signaled Interrupts Capability ID (MSI_CAPID_0_2_0_PCI)	D005h
AEh	2	Message Control (MC_0_2_0_PCI)	0100h
B0h	4	Message Address (MA_0_2_0_PCI)	00000000h
B4h	2	Message Data (MD_0_2_0_PCI)	0000h
B8h	4	MSI Mask Bits (MSI_MASK_0_2_0_PCI)	00000000h
BCh	4	MSI Pending Bits (MSI_PEND_0_2_0_PCI)	00000000h
C0h	4	Mirror of Base Data of Stolen Memory (BDSM0_0_2_0_PCI)	00000000h
C4h	4	Mirror of Base Data of Stolen Memory (BDSM1_0_2_0_PCI)	00000000h
C8h	4	Graphics VTD Base Address LSB (GFXVTDBAR_LSB_0_2_0_PCI)	00000000h
CCh	4	Graphics VTD Base Address MSB (GFXVTDBAR_MSB_0_2_0_PCI)	00000000h
D0h	2	Power Management Capabilities ID (PMCAPID_0_2_0_PCI)	0001h
D2h	2	Power Management Capabilities (PMCAP_0_2_0_PCI)	0022h
D4h	2	Power Management Control and Status (PMCS_0_2_0_PCI)	0000h
E0h	2	Software SMI (SWSMI_0_2_0_PCI)	0000h
E4h	4	Graphics System Event (GSE_0_2_0_PCI)	00000000h
E8h	2	Software SCI (SWSCI_0_2_0_PCI)	0000h
F0h	4	Device 2 Mirror of Protected Audio Video Path Control (PAVPC0_0_2_0_PCI)	00000000h
F4h	4	Device 2 Mirror of Protected Audio Video Path Control (PAVPC1_0_2_0_PCI)	00000000h
F8h	4	Stepping Revision ID (SRID_0_2_0_PCI)	00000000h
FCh	4	ASL Storage (ASLS_0_2_0_PCI)	00000000h
100h	4	PASID Extended Capability Header (PASID_EXTCAP_0_2_0_PCI)	2001001Bh
104h	2	PASID Capability (PASID_CAP_0_2_0_PCI)	1400h
106h	2	PASID Control (PASID_CTRL_0_2_0_PCI)	0000h
200h	4	ATS Extended Capability Header (ATS_EXTCAP_0_2_0_PCI)	3001000Fh

Offset	Size (Bytes)	Register Name (Register Symbol)	Default Value
204h	2	ATS Capability (ATS_CAP_0_2_0_PCI)	0060h
206h	2	ATS Control (ATS_CTRL_0_2_0_PCI)	0000h
300h	4	Page Request Extended Capability Header (PR_EXTCAP_0_2_0_PCI)	00010013h
304h	2	Page Request Control (PR_CTRL_0_2_0_PCI)	0000h
306h	2	Page Request Status (PR_STATUS_0_2_0_PCI)	8100h
308h	4	Outstanding Page Request Capacity (OPRC_0_2_0_PCI)	00008000h
30Ch	4	Outstanding Page Request Allocation (OPRA_0_2_0_PCI)	00000000h
320h	4	SRIOV Extended Capability Header (SRIOV_ECAPHDR_0_2_0_PCI)	00010010h
324h	4	SRIOV Capabilities (SRIOV_CAP_0_2_0_PCI)	00000000h
328h	2	SRIOV Control (SRIOV_CTRL_0_2_0_PCI)	0000h
32Ah	2	SRIOV Status (SRIOV_STS_0_2_0_PCI)	0000h
32Ch	2	SRIOV Initial Virtual Functions (SRIOV_INITVFS_0_2_0_PCI)	0007h
32Eh	2	SRIOV Total Virtual Functions (SRIOV_TOTVFS_0_2_0_PCI)	0007h
330h	4	Number of Virtual Functions (SRIOV_NUMOFVFS_0_2_0_PCI)	00000000h
334h	2	First Virtual Function Offset (FIRST_VF_OFFSET_0_2_0_PCI)	0001h
336h	2	Virtual Function Stride (VF_STRIDE_0_2_0_PCI)	0001h
33Ah	2	Virtual Function Device ID (VF_DEVICEID_0_2_0_PCI)	0A80h
33Ch	4	Supported Page Sizes (SUPPORTED_PAGE_SIZES_0_2_0_PCI)	00000513h
340h	4	System Page Sizes (SYSTEM_PAGE_SIZES_0_2_0_PCI)	00000001h
344h	4	Virtual Function BAR0 Lower DWORD (VF_BAR0_LDW_0_2_0_PCI)	00000004h
348h	4	Virtual Function BAR0 Upper DWORD (VF_BAR0_UDW_0_2_0_PCI)	00000000h
34Ch	4	Virtual Function BAR1 LDW (VF_BAR1_LDW_0_2_0_PCI)	0000000Ch
350h	4	Virtual Function BAR1 UDW (VF_BAR1_UDW_0_2_0_PCI)	00000000h
35Ch	4	Virtual Function Migration State Array Offset (VF_MIGST_OFFSET_0_2_0_PCI)	00000000h

4.1.2 Vendor ID (VID2_0_2_0_PCI) — Offset 0h

This register combined with the Device Identification register uniquely identifies any PCI device.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:2, F:0] + 0h	8086h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
15:0	8086h RO	**Vendor ID (VID):** PCI standard identification for Intel.

4.1.3 Device ID (DID2_0_2_0_PCI) — Offset 2h

This register combined with the Vendor Identification register uniquely identifies any PCI device.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:2, F:0] + 2h	0A80h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
15:7	015h RO	**Device ID MSB (DID_MSB):** Upper byte of the Device ID.
6:0	00h RO/V	**Device ID LSB (DID_LSB):** Lower byte of the Device ID.

4.1.4 PCI Command (PCICMD_0_2_0_PCI) — Offset 4h

This 16-bit register provides basic control over the IGD's ability to respond to PCI cycles. The PCICMD Register in the IGD disables the IGD PCI compliant master accesses to main memory.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:2, F:0] + 4h	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:11	0h RO	**Reserved**
10	0h RW/V	**Interrupt Disable (INTDIS):** This bit disables the device from asserting INTx#. 0: Enable the assertion of this device's INTx# signal. 1: Disable the assertion of this device's INTx# signal. DO_INTx messages will not be sent to DMI.
9	0h RO	**Fast Back-To-Back (FB2B):** Not Implemented. Hardwired to 0.
8	0h RO	**SERR Enable (SEN):** Not Implemented. Hardwired to 0.
7	0h RO	**Wait Cycle Control (WCC):** Not Implemented. Hardwired to 0.

Bit Range	Default & Access	Field Name (ID): Description
6	0h RO	**Parity Error Enable (PER):** Not Implemented. Hardwired to 0. Since the IGD belongs to the category of devices that does not corrupt programs or data in system memory or hard drives, the IGD ignores any parity error that it detects and continues with normal operation.
5	0h RO	**Video Palette Snooping (VPS):** This bit is hardwired to 0 to disable snooping.
4	0h RO	**Memory Write and Invalidate Enable (MWIE):** Hardwired to 0. The IGD does not support memory write and invalidate commands.
3	0h RO	**Special Cycle Enable (SCE):** This bit is hardwired to 0. The IGD ignores Special cycles.
2	0h RW/V	**Bus Master Enable (BME):** 0: Disable IGD bus mastering. 1: Enable the IGD to function as a PCI compliant master.
1	0h RW/V	**Memory Access Enable (MAE):** This bit controls the IGD's response to memory space accesses. 0: Disable. 1: Enable.
0	0h RW/V/L	**I/O Access Enable (IOAE):** This bit controls the IGD's response to I/O space accesses. 0: Disable. 1: Enable. This field is read-only 0 if DEV2CTL[0].IOBARDIS at offset 58h is 1. **Locked by:** DEV2CTL_0_2_0_PCI.IOBARDIS

4.1.5 PCI Status (PCISTS2_0_2_0_PCI) — Offset 6h

PCISTS is a 16-bit status register that reports the occurrence of a PCI compliant master abort and PCI compliant target abort. PCISTS also indicates the DEVSEL# timing that has been set by the IGD.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:2, F:0] + 6h	0010h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
15	0h RO	**Detected Parity Error (DPE):** Since the IGD does not detect parity, this bit is always hardwired to 0.
14	0h RO	**Signaled System Error (SSE):** The IGD never asserts SERR#, therefore this bit is hardwired to 0.
13	0h RO	**Received Master Abort Status (RMAS):** The IGD never gets a Master Abort, therefore this bit is hardwired to 0.

Bit Range	Default & Access	Field Name (ID): Description
12	0h RO	**Received Target Abort Status (RTAS):** The IGD never gets a Target Abort, therefore this bit is hardwired to 0.
11	0h RO	**Signaled Target Abort Status (STAS):** Hardwired to 0. The IGD does not use target abort semantics.
10:9	0h RO	**Device Select Timing (DEVT):** Hardwired to 00.
8	0h RO	**Master Data Parity Error Detected (DPD):** Since Parity Error Response is hardwired to disabled, and the IGD does not do any parity detection, this bit is hardwired to 0.
7	0h RO	**Fast Back-To-Back (FB2B):** Hardwired to 0 to be compliant to PCI Express Base Spec (rev 3.0).
6	0h RO	**User Defined Format (UDF):** Hardwired to 0.
5	0h RO	**66MHz PCI Capable (C66):** Hardwired to 0.
4	1h RO	**Capability List (CLIST):** This bit is hardwired to 1 to indicate that the register at 34h provides an offset into the function's PCI Configuration Space containing a pointer to the location of the first item in the list.
3	0h RO/V	**Interrupt Status (INTSTS):** This bit reflects the state of the interrupt in the device. Only when the Interrupt Disable bit in the command register is a 0 and this Interrupt Status bit is a 1, will the devices INTx# signal be asserted.
2:0	0h RO	**Reserved**

4.1.6 Revision Identification and Class Code register (RID2_CC_0_2_0_PCI) — Offset 8h

This register contains the revision number for Device #2 Functions 0 and contains the device programming interface information related to the Sub-Class Code and Base Class Code definition for the IGD. This register also contains the Base Class Code and the function sub-class in relation to the Base Class Code.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + 8h	03000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:24	03h RO/V	**Base Class Code (BCC):** This is an 8-bit value that indicates the base class code. When MGGC0[VAMEN] is 0 this code has the value 03h, indicating a Display Controller. When MGGC0[VAMEN] is 1 this code has the value 03h, indicating a Display Controller Device.

Bit Range	Default & Access	Field Name (ID): Description
23:16	00h RO/V	**Sub-Class Code (SUBCC):** When MGGC0[VAMEN] is 0, this value is 00h. When MGGC0[VAMEN] is 1, this value is 80h, indicating other display device.
15:8	00h RO	**Programming Interface (PI):** When MGGC0[VAMEN] is 0 this value is 00h, indicating a Display Controller.When MGGC0[VAMEN] is 1 this value is 00h, indicating a NOP.
7:0	00h RO	**Revision ID (RID):** Revision ID of the device

4.1.7 Cache Line Size (CLS_0_2_0_PCI) — Offset Ch

PCI standard Cache Line Size register

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:2, F:0] + Ch	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
7:0	00h RW	**Cache Line Size Value (CLS):** This field is implemented by PCI Express devices as a read-write field for legacy compatibility purposes but has no effect on any PCI Express device behavior.

4.1.8 Master Latency Timer (MLT2_0_2_0_PCI) — Offset Dh

The IGD does not support the programmability of the master latency timer because it does not perform bursts.

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:2, F:0] + Dh	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:0	00h RO	**Master Latency Timer Count Value (MLTCV):** Hardwired to 0s.

4.1.9 Header Type (HDR2_0_2_0_PCI) — Offset Eh

This register contains the Header Type of the IGD.

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:2, F:0] + Eh	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7	0h RO	**Multi Function Status (MFUNC):** Indicates if the device is a Multi-Function Device. The Value of this register is hardwired to 0, internal graphics is a single function.
6:0	00h RO	**Header Code (H):** This is a 7-bit value that indicates the Header Code for the IGD. This code is hardwired to the value 00h, indicating a type 0 configuration space format.

4.1.10 Built In Self Test (BIST_0_2_0_PCI) — Offset Fh

This register is used for control and status of Built In Self Test (BIST).

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:2, F:0] + Fh	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
7	0h RO	**BIST Supported (BISTS):** BIST is not supported. This bit is hardwired to 0.
6:0	0h RO	**Reserved**

4.1.11 Graphics Translation Table Memory Mapped Range Address (GTTMMADR0_0_2_0_PCI) — Offset 10h

This register requests allocation for the combined Graphics Translation Table Modification Range and Memory Mapped Range. The range requires 16 MB combined for MMIO and Global GTT aperture, with 2MB of that used by MMIO, 6MB reserved, and 8MB used by GTT. GTTADR will begin at (GTTMMADR + 8 MB) while the MMIO base address will be the same as GTTMMADR. The region between (GTTMMADR + 2MB) - (GTTMMADR + 8MB) is reserved. For the Global GTT, this range is defined as a memory

BAR in graphics device configuration space. It is an alias into which software is required to write Page Table Entry values (PTEs). Software may read PTE values from the global Graphics Translation Table (GTT). PTEs cannot be written directly into the global GTT memory area. The device snoops writes to this region in order to invalidate any cached translations within the various TLBs implemented on-chip. The allocation is for 16MB and the base address is defined by bits [38:24].

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + 10h	00000004h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:24	00h RW/V	**Memory Base Address (MBA_0):** Set by the OS, these bits correspond to address signals [63:24].
23:4	00000h RO	**Address Mask (ADM):** Hardwired to 0s to indicate at least 16MB address range.
3	0h RO	**Prefetchable Memory (PREFMEM):** Hardwired to 0 to prevent prefetching.
2:1	2h RO	**Memory Type (MEMTYP):** Hardwired to 2h to indicate 64 bit base address.
0	0h RO	**Memory I/O Space (MIOS):** Hardwired to 0 to indicate memory space.

4.1.12 Graphics Translation Table Memory Mapped Range Address (GTTMMADR1_0_2_0_PCI) — Offset 14h

This register requests allocation for the combined Graphics Translation Table Modification Range and Memory Mapped Range. The range requires 16 MB combined for MMIO and Global GTT aperture, with 2MB of that used by MMIO, 6MB reserved, and 8MB used by GTT. GTTADR will begin at (GTTMMADR + 8 MB) while the MMIO base address will be the same as GTTMMADR. The region between (GTTMMADR + 2MB) - (GTTMMADR + 8MB) is reserved. For the Global GTT, this range is defined as a memory BAR in graphics device configuration space. It is an alias into which software is required to write Page Table Entry values (PTEs). Software may read PTE values from the global Graphics Translation Table (GTT). PTEs cannot be written directly into the global GTT memory area. The device snoops writes to this region in order to invalidate any cached translations within the various TLBs implemented on-chip. The allocation is for 16MB and the base address is defined by bits [38:24].

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + 14h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RW/V	**Memory Base Address (MBA_1):** Set by the OS, these bits correspond to address signals [63:24].

4.1.13 Graphics Memory Range Address (GMADR0_0_2_0_PCI) — Offset 18h

GMADR is the PCI aperture used by S/W to access tiled GFX surfaces in a linear fashion.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + 18h	0000000Ch

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RW/V/L	**4096MB Address Mask (ADMSK4096):** This bit is either part of the Memory Base Address (R/W) or part of Address Mask (RO) depending on the value of MSAC.APSZ.RO and forced to 0 when MSAC.APSZ >= 4096MB. (i.e. MSAC.APSZ[4]=1) **Locked by:** MSAC_0_2_0_PCI.APSZ4
30	0h RW/V/L	**2048MB Address Mask (ADMSK2048):** This bit is either part of the Memory Base Address (R/W) or part of the Address Mask (RO) depending on the value of MSAC.APSZ.RO and forced to 0 when MSAC.APSZ >= 2048MB. (i.e. MSAC.APSZ[3]=1) **Locked by:** MSAC_0_2_0_PCI.APSZ3
29	0h RW/V/L	**1024MB Address Mask (ADMSK1024):** This bit is either part of the Memory Base Address (R/W) or part of the Address Mask (RO) depending on the value of MSAC.APSZ.RO and forced to 0 when MSAC.APSZ >= 1024MB. (i.e. MSAC.APSZ[2]=1) **Locked by:** MSAC_0_2_0_PCI.APSZ2
28	0h RW/V/L	**512MB Address Mask (ADMSK512):** This bit is either part of the Memory Base Address (R/W) or part of the Address Mask (RO) depending on the value of MSAC.APSZ.RO and forced to 0 when MSAC.APSZ >= 512MB. (i.e. MSAC.APSZ[1]=1) **Locked by:** MSAC_0_2_0_PCI.APSZ1

Bit Range	Default & Access	Field Name (ID): Description
27	0h RW/V/L	**256MB Address Mask (ADMSK256):** This bit is either part of the Memory Base Address (R/W) or part of the Address Mask (RO) depending on the value of MSAC.APSZ.RO and forced to 0 when MSAC.APSZ >= 256MB. (i.e. MSAC.APSZ[0]=1) **Locked by:** MSAC_0_2_0_PCI.APSZ0
26:4	000000h RO	**Address Mask (ADM):** Hardwired to 0s to indicate at least 128MB address range.
3	1h RO	**Prefetchable Memory (PREFMEM):** Hardwired to 1 to enable prefetching.
2:1	2h RO	**Memory Type (MEMTYP):** Hardwired to 2h to indicate 64 bit base address.
0	0h RO	**Memory I/O Space (MIOS):** Hardwired to 0 to indicate memory space.

4.1.14 Graphics Memory Range Address (GMADR1_0_2_0_PCI) — Offset 1Ch

GMADR is the PCI aperture used by S/W to access tiled GFX surfaces in a linear fashion.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + 1Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RW/V	**Memory Base Address (MBA):** Set by the OS, these bits correspond to address signals [63:32].

4.1.15 I/O Base Address (IOBAR_0_2_0_PCI) — Offset 20h

This register provides the Base offset of the I/O registers within Device #2.

Bits 15:6 are programmable allowing the I/O Base to be located anywhere in 16bit I/O Address Space.

Bits 2:1 are fixed and return zero

Bit 0 is hardwired to a one indicating that 8 bytes of I/O space are decoded.

Access to the 8Bs of IO space is allowed in PM state D0 when IO Enable (PCICMD bit 0) set.

Access is disallowed in PM states D1-D3 or if IO Enable is clear or if Device #2 is turned off or if Internal graphics is disabled.

Note that access to this IO BAR is independent of VGA functionality within Device #2.

If accesses to this IO bar is allowed then all 8, 16 or 32 bit IO cycles from IA cores that falls within the 8B are claimed.

This IO BAR can be disabled and hidden from system software via DEV2CTL[0] IOBARDIS at offset 0x58.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + 20h	00000001h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:16	0h RO	**Reserved**
15:6	000h RW/V/L	**IO Base Address (IOBASE):** Set by the OS, these bits correspond to address signals [15:6]. Note: This field is RO 0's if DEV2CTL[0] IOBARDIS is 1b. **Locked by:** DEV2CTL_0_2_0_PCI.IOBARDIS
5:3	0h RO	**Reserved**
2:1	0h RO	**Memory Type (MEMTYPE):** Hardwired to 0s to indicate 32-bit address.
0	1h RO	**Memory I/O Space (MIOS):** Hardwired to '1' to indicate IO space. Note: This field is RO 0's if DEV2CTL[0] IOBARDIS is 1b.

4.1.16 Subsystem Vendor Identification (SVID2_0_2_0_PCI) — Offset 2Ch

This register is used to uniquely identify the subsystem where the PCI device resides.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:2, F:0] + 2Ch	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:0	0000h RW/O	**Subsystem Vendor Id (SUBVID):** This value is used to identify the vendor of the subsystem.

4.1.17 Subsystem Identification (SID2_0_2_0_PCI) — Offset 2Eh

This register is used to uniquely identify the subsystem where the PCI device resides.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:2, F:0] + 2Eh	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:0	0000h RW/O	**Subsystem ID (SUBID):** This value is used to identify a particular subsystem. This field should be programmed by BIOS during boot-up.

4.1.18 Video BIOS ROM Base Address (ROMADR_0_2_0_PCI) — Offset 30h

The IGD does not use a separate BIOS ROM, therefore this register is hardwired to 0s.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + 30h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:18	0000h RO	**ROM Base Address (RBA):** Hardwired to 0's.
17:11	00h RO	**Address Mask (ADMSK):** Hardwired to 0s to indicate 256 KB address range.
10:1	0h RO	**Reserved**
0	0h RO	**ROM BIOS Enable (RBE):** Hardwired to 0 to indicate ROM not accessible.

4.1.19 Capabilities Pointer (CAPPOINT_0_2_0_PCI) — Offset 34h

This register points to a linked list of capabilities implemented by this device.

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:2, F:0] + 34h	40h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:0	40h RO	**Capabilities Pointer Value (CPV):** This field contains an offset into the function's PCI Configuration Space for the first item in the New Capabilities Linked List, the CAPID0 register at offset 40h.

4.1.20 Interrupt Line (INTRLINE_0_2_0_PCI) — Offset 3Ch

This register is used to communicate interrupt line routing information. The device itself does not use this value, rather it is used by device drivers and operating systems to determine priority and vector information.

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:2, F:0] + 3Ch	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
7:0	00h RW	**Interrupt Connection (INTCON):** Used to communicate interrupt line routing information. POST software writes the routing information into this register as it initializes and configures the system. The value in this register indicates to which input of the system interrupt controller the device's interrupt pin is connected.

4.1.21 Interrupt Pin (INTRPIN_0_2_0_PCI) — Offset 3Dh

This register tells which interrupt pin the device uses.

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:2, F:0] + 3Dh	01h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:0	01h RO	**Interrupt Pin Value (INTPIN):** As a single function device, the IGD specifies INTA# as its interrupt pin. Hardwired to 01h = INTA#.

4.1.22 Minimum Grant (MINGNT_0_2_0_PCI) — Offset 3Eh

The Integrated Graphics Device has no requirement for the settings of Latency Timers.

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:2, F:0] + 3Eh	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:0	00h RO	**Minimum Grant Value (MGV):** Hardwired to 0s because the IGD does not burst as a PCI compliant master.

4.1.23 Maximum Latency (MAXLAT_0_2_0_PCI) — Offset 3Fh

The Integrated Graphics Device has no requirement for the settings of Latency Timers.

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:2, F:0] + 3Fh	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:0	00h RO	**Maximum Latency Value (MLV):** Hardwired to 0s because the IGD has no specific requirements for how often it needs to access the PCI bus.

4.1.24 Capability Identifier (CAPID0_0_2_0_PCI) — Offset 40h

PCI standard Capability Identifier

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:2, F:0] + 40h	7009h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
15:8	70h RO	**Next Capability Pointer (NEXT_CAP):** This field is hardwired to point to the next PCI Capability structure, the PCIe Capabilities structure at 70h.
7:0	09h RO	**Capability Identifier (CAP_ID):** This field is hardwired to the value 09h to identify the CAP_ID assigned by the PCI SIG for vendor dependent capability pointers.

4.1.25 Capabilities Control (CAPCTRL0_0_2_0_PCI) — Offset 42h

Capabilities Control

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:2, F:0] + 42h	010Ch

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:12	0h RO	**Reserved**
11:8	1h RO	**CAPID Version (CAPID_VER):** This field is hardwired to the value 1h to identify the first revision of the CAPID register definition.
7:0	0Ch RO	**CAPID Length (CAPIDLEN):** This field is hardwired to the value 0Ch to indicate the structure length (12 bytes).

4.1.26 Capabilities A (CAPID0_A_0_2_0_PCI) — Offset 44h

Various Capabilities of the device.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + 44h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:4	0h RO	**Reserved**
3	0h RO/V	**VGT Enabled (VGT_EN):** 0: VGT is disabled 1: VGT is enabled
2	0h RO	**Reserved**
1	0h RO/V	**SVM Disabled (SVMD):** 0: SVM is enabled 1: SVM is disabled
0	0h RO/V	**VTD Disable (VTDD):** 0: VTD is enabled 1: VTD is disabled

4.1.27 Capabilities B (CAPID0_B_0_2_0_PCI) — Offset 48h

Various Capabilities of the device.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + 48h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:0	0h RO	**Reserved**

4.1.28 PCI Mirror of GMCH Graphics Control (MGGC0_0_2_0_PCI) — Offset 50h

Mirror of GGC register from GTTMMADR Space at offset 0x108040.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:2, F:0] + 50h	0500h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:8	05h RO/V	**Graphics Memory Size (GMS):** This field is used to select the amount of Main Memory that is pre-allocated to support the Internal Graphics device in VGA (non-linear) and Native (linear) modes. It corresponds to DSM (Data Stolen Memory region) region. The BIOS ensures that memory is pre-allocated only when Internal graphics is enabled. Hardware does not clear or set any of these bits automatically based on IGD being disabled/enabled. BIOS Requirement: BIOS must not set this field to 0h if IVD (bit 1 of this register) is 0. BIOS Requirement: Given new sizes allow down to 8MB allocation, BIOS has to ensure there is sufficient space for WOPCM and basic GFX Stolen functions. 00h: 0MB 01h - 10h: 32MB, 64MB, 96MB, ..., 512MB 11h - 1Fh: Reserved 20h: 1024MB 21h - 2Fh: Reserved 30h: 1536MB 31h - 3Fh: Reserved 40h: 2048MB 41h - EFh: Reserved F0h - FEh: 4MB, 8MB, 12MB, ..., 60MB FFh: Reserved Hardware functionality in case of programming this value to Reserved is not guaranteed.

Bit Range	Default & Access	Field Name (ID): Description
7:6	0h RO/V	**Graphics Translation Table Memory Size (GGMS):** This field is used to select the amount of Main Memory that is pre-allocated to support the Internal Graphics Translation Table. The BIOS ensures that memory is pre-allocated only when Internal graphics is enabled. GSM is assumed to be a contiguous physical DRAM space with DSM, and BIOS needs to allocate a contiguous memory chunk. Hardware will derive the base of GSM from DSM only using the GSM size programmed in the register. Hardware functionality in case of programming this value to Reserved is not guaranteed. 0x0:No Preallocated Memory 0x1:2MB of Preallocated Memory 0x2:4MB of Preallocated Memory 0x3:8MB of Preallocated Memory
5:3	0h RO	**Reserved**
2	0h RO/V	**Versatile Acceleration Mode Enable (VAMEN):** Enables the use of the iGFX engines for Versatile Acceleration. 0: iGFX engines are in iGFX Mode. Device 2 Class Code is 030000h. 1: iGFX engines are in Versatile Acceleration Mode. Device 2 Class Code is 038000h.
1	0h RO/V	**IVD:** 0: Enable. Device 2 (IGD) claims VGA memory and IO cycles, the Sub-Class Code within Device 2 Class Code register is 00. 1: Disable. Device 2 (IGD) does not claim VGA cycles (Mem and IO), and the Sub-Class Code field within Device 2 function 0 Class Code register is 80. BIOS Requirement: BIOS must not set this bit to 0 if the GMS field (bits 7:3 of this register) pre-allocates no memory.
0	0h RO	**Reserved**

4.1.29 Mirror of Device Enable (DEVEN0_0_2_0_PCI) — Offset 54h

Mirror of DEVEN_0_0_0_PCI.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:2, F:0] + 54h	00BFh

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15	0h RO	**Reserved**
14	0h RO/V	**CHAP Enable (D7EN):** 0: Device 7 is disabled 1: Device 7 is enabled
13	0h RO	**Device 6 Enable (D6EN):** 0: Device 6 is disabled 1: Device 6 is enabled
12:11	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
10	0h RO	**Device 5 Enable (D5EN):** 0: Device 5 is disabled 1: Device 5 is enabled
9:8	0h RO	**Reserved**
7	1h RO/V	**Device 4 Enable (D4EN):** 0: Device 4 is disabled 1: Device 4 is enabled
6	0h RO	**Reserved**
5	1h RO/V	**Device 3 Enable For Display HD Audio (D3EN):** 0: Device 3 is disabled 1: Device 3 is enabled
4	1h RO/V	**Internal Graphics Engine (D2EN):** 0: Bus 0 Device 2 is disabled and hidden 1: Bus 0 Device 2 is enabled and visible. This bit will be set to 0b and remain 0b if Device 2 capability is disabled.
3	1h RO/V	**PEG10 Enable (D1F0EN):** Device 1, Function 0 is enabled
2	1h RO/V	**PEG11 Enable (D1F1EN):** Device 1, Function 1 is enabled
1	1h RO/V	**PEG12 Enable (D1F2EN):** Device 1, Function 2 is enabled
0	1h RO	**Host Bridge Enable (D0EN):** Device 0, Function 0 is enabled

4.1.30 Device 2 Control (DEV2CTL_0_2_0_PCI) — Offset 58h

This register implements a control bit to disable and hide the IOBAR register in systems that do not require legacy IOBAR access to Gfx MMIO registers.

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:2, F:0] + 58h	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
7:1	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
0	0h RW	**IO BAR Disable (IOBARDIS):** System BIOS can choose to disable and hide the IOBAR for systems that do not require legacy IOBAR access to GFX MMIO registers. 0b: IOBAR is enabled and exposed at offset 0x20 in Device 2 Configuration space (Default). 1b: IOBAR is disabled and not visible in PCI Configuration Space. Behaves as if hardwired to zeros.

4.1.31 Multi Size Aperture Control (MSAC_0_2_0_PCI) — Offset 60h

This register contains MSAC register which determines the size of the graphics memory aperture (GMADR) in function 0 and in the trusted space, and affects certain bits of the GMADR register. Bits [20:16] 00000b: 128MB, GMADR[26:4] is hardwired to all 0 Bits [20:16] 00001b: 256MB, GMADR[27:4] overridden to all 0 Bits [20:16] 00010b: illegal (hardware will treat this as 00011b) Bits [20:16] 00011b: 512MB, GMADR[28:27] overridden to all 0 Bits [20:16] 00100-00110b: illegal (hardware will treat this as 00111b) Bits [20:16] 00111b: 1024MB, GMADR[29:27] overridden to all 0 Bits [20:16] 01000-01110b: illegal (hardware will treat this as 01111b) Bits [20:16] 01111b: 2048MB, GMADR[30:27] overridden to all 0 Bits [20:16] 10000-11110b: illegal (hardware will treat this as 11111b) Bits [20:16] 11111b: 4096MB, GMADR[31:27] overridden to all 0

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + 60h	00010000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:21	0h RO	**Reserved**
20	0h RW/V	**Untrusted Aperture Size Bit 4 (APSZ4):** Untrusted Aperture Size Bit 4
19	0h RW/V	**Untrusted Aperture Size Bit 3 (APSZ3):** Untrusted Aperture Size Bit 3
18	0h RW/V	**Untrusted Aperture Size Bit 2 (APSZ2):** Untrusted Aperture Size Bit 2
17	0h RW/V	**Untrusted Aperture Size Bit 1 (APSZ1):** Untrusted Aperture Size Bit 1
16	1h RW/V	**Untrusted Aperture Size Bit 0 (APSZ0):** Untrusted Aperture Size Bit 0
15:0	0h RO	**Reserved**

4.1.32 Push Aperture (PUSHAP_0_2_0_PCI) — Offset 68h

GT writes this Push Aperture register to ensure aperture writes have been pushed to DRAM.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + 68h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RW/V	**Token Value (TOKEN_VALUE):** 32 bit Token Value. GT (GuC) writes a DWORD Token value to this field. A write to this register triggers a write response to GT. The response write will use the value written into this register.

4.1.33 VTd Status (VTD_STATUS_0_2_0_PCI) — Offset 6Ch

This register contains indicator bits for Graphics VTd mode.

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:2, F:0] + 6Ch	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:1	0h RO	**Reserved**
0	0h RO	**GFX VTd Active (VTACT):** Reflects GFX VTd Mode is active. 1: GFX VTd Mode is active 0: GFX VTd Mode is inactive.

4.1.34 PCI Express Capability Header (PCIECAPHDR_0_2_0_PCI) — Offset 70h

PCI Express Capability Header

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:2, F:0] + 70h	AC10h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
15:8	ACh RO	**Next Capability Pointer (NEXT_PTR):** This field is hardwired to point to the next PCI Capability structure, the MSI Capabilities at ACh.
7:0	10h RO	**Capability Identifier (CAP_ID):** This field is hardwired to 10h to indicate that this is a PCI Express Capability structure.

4.1.35 PCI Express Capability (PCIECAP_0_2_0_PCI) — Offset 72h

PCI Express Capability

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:2, F:0] + 72h	0092h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:14	0h RO	**Reserved**
13:9	00h RO	**Interrupt Message Number (INTRMSG):** This field indicates which MSI vector is used for the interrupt message generated in association with any of the status bits of this Capability structure.Since this device only supports one MSI vector, this field is hardwired to 0.
8	0h RO	**Slot Implemented (SLOTIMP):** This field is hardwired to 0 for an endpoint device.
7:4	9h RO	**Device Type (DEV_TYPE):** This field is hardwired to 9h to indicate a Root Complex Integrated Endpoint.
3:0	2h RO	**Capability Version (CAP_VER):** This field is hardwired to 2h to indicate Functions compliant to PCI Express 3.0 Base Specification.

4.1.36 Device Capabilities (DEVICECAP_0_2_0_PCI) — Offset 74h

PCI Express Device Capabilities

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + 74h	10008000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:29	0h RO	**Reserved**
28	1h RO	**Functional Level Reset Capability (FLRCAP):** Hardwired to 1b to indicate the Function supports the optional Function Level Reset mechanism.
27:26	0h RO	**Captured Slot Power Limit Scale (PWR_LIM_SCALE):** Not applicable for a Root Complex Integrated Endpoint with no Link or Slot. Hardwired to 00b
25:18	00h RO	**Captured Slot Power Limit Value (CSPLS):** Not applicable for a Root Complex Integrated Endpoint with no Link or Slot. Hardwired to 00h
17:16	0h RO	**Reserved**
15	1h RO	**Role-Based Error Reporting (RBER):** When Set, this bit indicates that the Function implements the functionality originally defined in the Error Reporting ECN for PCI Express Base Specification, Revision 1.0a, and later incorporated into PCI Express Base Specification, Revision 1.1.Hardwired to 1b as this bit must be Set by all Functions conforming to the ECN, PCI Express Base Specification, Revision 1.1, or subsequent PCI Express Base Specification revisions.
14:12	0h RO	**Reserved**
11:9	0h RO	**Endpoint L1 Acceptable Latency (EPL1AL):** This field indicates the acceptable total latency that an Endpoint can withstand due to the transition from the L1 state to the L0 state.This does not apply to the integrated graphics device, so it is hardwired to 000b (Maximum of 1 us).
8:6	0h RO	**Endpoint L0S Acceptable Latency (EPL0AL):** This field indicates the acceptable total latency that an Endpoint can withstand due to the transition from the L0s state to the L0 state.This does not apply to the integrated graphics device, so it is hardwired to 000b (Maximum of 64 ns).
5	0h RO	**Extended Tag Field Supported (ETFS):** This bit indicates the maximum supported size of the Tag field as a Requester.This does not apply to the integrated graphics device, so it is hardwired to 0b (5-bit Tag field supported).
4:3	0h RO	**Phantom Functions Supported (PFS):** This field indicates the support for use of unclaimed Function Numbers to extend the number of outstanding transactions for PCIe devices.This does not apply to the integrated graphics device, so it is hardwired to 00b to indicate no Function Number bits are used for Phantom Functions.
2:0	0h RO	**Max Payload Size Supported (MPSS):** This field indicates the maximum payload size that the Function can support for TLPs.Hardwired to 000b to represents 128 bytes, the minimum allowed value.

4.1.37 PCI Express Device Control (DEVICECTL_0_2_0_PCI) — Offset 78h

PCI Express Device Control

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:2, F:0] + 78h	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15	0h RW/V	**Initiate Function Level Reset (INIT_FLR):** A write of 1b initiates Function Level Reset to the Function.During FLR, a read will return 1b since device 2 reads abort. If a local panel is powered on and configured to power down on reset, the FLR will typically take several hundred milliseconds to complete. The worst possible, although unrealistic, delay is 5 seconds.
14:12	0h RO	**Max Read Request Size (MRRS):** Functions that do not generate Read Requests larger than 128 bytes and Functions that do not generate Read Requests on their own behalf are permitted to implement this field as Read Only (RO) with a value of 000b.
11	0h RO	**Enable No Snoop (ENS):** This bit is permitted to be hardwired to 0b if a Function would never Set the No Snoop attribute in transactions it initiates.The graphics device never generates a PCI Express TLP.
10	0h RO	**Aux Power PM Enable (APPME):** Functions that do not implement this capability hardwire this bit to 0b.
9	0h RO	**Phantom Functions Enable (PFE):** Functions that do not implement this capability hardwire this bit to 0b.
8	0h RO	**Extended Tag Field Enable (ETFE):** Functions that do not implement this capability hardwire this bit to 0b.
7:5	0h RO	**Max Payload Size (MPS):** Functions that support only the 128-byte max payload size are permitted to hardwire this field to 000b.
4	0h RO	**Enable Relaxed Ordering (ERO):** A Function is permitted to hardwire this bit to 0b if it never sets the Relaxed Ordering attribute in transactions it initiates as a Requester.The graphics device never generates a PCI Express TLP.
3	0h RO	**Unsupported Request Response Enable (URRE):** A Root Complex Integrated Endpoint that is not associated with a Root Complex Event Collector is permitted to hardwire this bit to 0b.
2	0h RO	**Fatal Error Enable (FEE):** This bit, in conjunction with other bits, controls sending ERR_FATAL Messages.
1	0h RO	**Non-Fatal Error Enable (NFEE):** This bit, in conjunction with other bits, controls sending ERR_NONFATAL Messages.
0	0h RO	**Correctable Error Enable (CEE):** This bit, in conjunction with other bits, controls sending ERR_COR Messages.

4.1.38 PCI Express Capability Structure (DEVICESTS_0_2_0_PCI) — Offset 7Ah

PCI Express Capability Structure

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:2, F:0] + 7Ah	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:6	0h RO	**Reserved**
5	0h RO	**Transactions Pending (TP):** When Set, this bit indicates that the Function has issued Non-Posted Requests that have not been completed.A Function reports this bit is cleared only when all outstanding Non-Posted Requests have completed or have been terminated by the Completion Timeout mechanism. This bit must also be cleared upon the completion of an FLR.
4	0h RO	**Aux Power Detected (APD):** Functions that require Aux power report this bit as Set if Aux power is detected by the Function. Hardwired to 0b, the integrated graphics device does not require Aux power.
3	0h RO	**Unsupported Request Detected (URD):** This bit indicates the Function received an Unsupported Request.Hardwired to 0b, the Root Complex Integrated Endpoint graphics device does not use the PCI Express error reporting mechanism.
2	0h RO	**Fatal Error Detected (FED):** This bit indicates the status of Fatal errors detected.Hardwired to 0b, the Root Complex Integrated Endpoint graphics device does not use the PCI Express error reporting mechanism.
1	0h RO	**Non-Fatal Error Detected (NFED):** This bit indicates the status of Non-Fatal errors detected.Hardwired to 0b, the Root Complex Integrated Endpoint graphics device does not use the PCI Express error reporting mechanism.
0	0h RO	**Correctable Error Detected (CED):** This bit indicates status of correctable errors detected. Errors are logged in this register regardless of whether error reporting is enabled or not in the Device Control Register.

4.1.39 Message Signaled Interrupts Capability ID (MSI_CAPID_0_2_0_PCI) — Offset ACh

When a device supports MSI it can generate an interrupt request to the processor by writing a predefined data item (a message) to a predefined memory address.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:2, F:0] + ACh	D005h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
15:8	D0h RO	**Pointer To Next Capability (POINTNEXT):** This is a hardwired pointer to the next item in the capabilities list.
7:0	05h RO	**Capability ID (CAPID):** This field is hardwired to the value 05h to identify the CAP_ID as being for MSI registers.

4.1.40 Message Control (MC_0_2_0_PCI) — Offset AEh

Message Signaled Interrupt control register. System software can modify bits in this register, but the device is prohibited from doing so. If the device writes the same message multiple times, only one of those messages is guaranteed to be serviced. If all of them must be serviced, the device must not generate the same message again until the driver services the earlier one.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:2, F:0] + AEh	0100h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:9	0h RO	**Reserved**
8	1h RO	**Per Vector Mask Capable (PVMASKCAP):** SR-IOV requires this capability.
7	0h RO	**64BIT Capable (CAP64B):** Hardwired to 0 to indicate that the function does not implement the upper 32 bits of the Message address register and is incapable of generating a 64-bit memory address.
6:4	0h RW/V	**Multiple Message Enable (MME):** System software programs this field to indicate the actual number of messages allocated to this device. This number will be equal to or less than the number actually requested.Value: Number of requests000: 1001: 2010: 4011: 8100: 16101: 32110: Reserved111: Reserved
3:1	0h RO	**Multiple Message Capable (MMC):** System Software reads this field to determine the number of messages being requested by this device. Hardwired to 000b to indicate number of requests is 1.

Bit Range	Default & Access	Field Name (ID): Description
0	0h RW/V	**MSI Enable (MSIEN):** Controls the ability of this device to generate MSIs.

4.1.41 Message Address (MA_0_2_0_PCI) — Offset B0h

This register contains the Message Address for MSIs sent by the device.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + B0h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:2	00000000h RW/V	**Message Address Field (MESSADD):** Used by system software to assign an MSI address to the device.The device handles an MSI by writing the padded contents of the MD register to this address.
1:0	0h RO	**Force DWORD Align (FDWORD):** Hardwired to 0 so that addresses assigned by system software are always aligned on a DWORD address boundary.

4.1.42 Message Data (MD_0_2_0_PCI) — Offset B4h

This register contains the Message Data for MSIs sent by the device.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:2, F:0] + B4h	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:0	0000h RW/V	**Message Data (MESSDATA):** Base message data pattern assigned by system software and used to handle an MSI from the device.When the device must generate an interrupt request, it writes a 32-bit value to the memory address specified in the MA register. The upper 16 bits are always set to 0. The lower 16 bits are supplied by this register.

4.1.43 MSI Mask Bits (MSI_MASK_0_2_0_PCI) — Offset B8h

This register contains the MSI Mask Bits

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + B8h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:1	0h RO	**Reserved**
0	0h RW/V	**Mask Bit For Vector 0 (MASKBIT):** For each Mask bit that is set, the function is prohibited from sending the associated message.

4.1.44 MSI Pending Bits (MSI_PEND_0_2_0_PCI) — Offset BCh

This register contains the MSI Pending Bits

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + BCh	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:1	0h RO	**Reserved**
0	0h RO/V	**Pending Bit For Vector 0 (PENDBIT):** For each Pending bit that is set, the function has a pending associated message. If this bit is set when the corresponding vector's Mask bit is cleared, the function will send an MSI and then clear the Pending bit.

4.1.45 Mirror of Base Data of Stolen Memory (BDSM0_0_2_0_PCI) — Offset C0h

Mirror of BSDM from GTTMMADR space. This register contains the base address of graphics data stolen DRAM memory.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + C0h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:20	000h RO/V	**Graphics Base Of Stolen Memory LSB (BDSM_LSB):** This register contains bits 63 to 20 of the base address of stolen DRAM memory. BIOS is now able to allocate GDSM above 4GB.
19:0	0h RO	**Reserved**

4.1.46 Mirror of Base Data of Stolen Memory (BDSM1_0_2_0_PCI) — Offset C4h

Mirror of BSDM from GTTMMADR space. This register contains the base address of graphics data stolen DRAM memory.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + C4h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RO/V	**Graphics Base Of Stolen Memory MSB (BDSM_MSB):** This register contains bits 63 to 20 of the base address of stolen DRAM memory. BIOS is now able to allocate GDSM above 4GB.

4.1.47 Graphics VTD Base Address LSB (GFXVTDBAR_LSB_0_2_0_PCI) — Offset C8h

This is the base address for the Graphics VTD configuration space.

There is no physical memory within this 4KB window that can be addressed.

The 4KB reserved by this register does not alias to any PCI 2.3 compliant memory mapped space.

On reset, the GFX-VTD configuration space is disabled and must be enabled by writing a 1 to GFXVTDBAREN.

None of the bits in this register are writable in Intel TXT mode.

BIOS programs this register, after which the register cannot be altered.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + C8h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:12	00000h RW	**GFX-VTD Base Address Lower DWORD (GFXVTDBAR):** This field corresponds to bits 31 to 12 of the base address GFX-VTD configuration space. BIOS will program this register resulting in a base address for a 4KB block of contiguous memory address space. This register ensures that a naturally aligned 4KB space is allocated within the first 512GB of addressable memory space. System Software uses this base address to program the GFX-VTD register set.
11:1	0h RO	**Reserved**
0	0h RW/V	**GFX-VTBAR Enable (GFXVTDBAREN):** 0: GFX-VTBAR is disabled and does not claim any memory. 1: GFX-VTBAR memory mapped accesses are claimed and decoded appropriately This bit will remain 0 if VTd capability is disabled.

4.1.48 Graphics VTD Base Address MSB (GFXVTDBAR_MSB_0_2_0_PCI) — Offset CCh

This is the base address for the Graphics VTD configuration space.

There is no physical memory within this 4KB window that can be addressed.

The 4KB reserved by this register does not alias to any PCI 2.3 compliant memory mapped space.

On reset, the GFX-VTD configuration space is disabled and must be enabled by writing a 1 to GFXVTDBAREN.

None of the bits in this register are writable in Intel TXT mode.

BIOS programs this register, after which the register cannot be altered.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + CCh	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RW	**GFX-VTD Base Address Upper DWORD (GFXVTDBAR):** This field corresponds to bits 63 to 32 of the base address GFX-VTD configuration space. BIOS will program this register, resulting in a base address for a 4KB block of contiguous memory address space. This register ensures that a naturally aligned 4KB space is allocated within the first 512GB of addressable memory space. System Software uses this base address to program the GFX-VTD register set.

4.1.49 Power Management Capabilities ID (PMCAPID_0_2_0_PCI) — Offset D0h

This register contains the PCI Power Management Capability ID and the next capability pointer.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:2, F:0] + D0h	0001h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
15:8	00h RO	**Next Capability Pointer (NEXT_PTR):** This is a hardwired pointer to the next item in the capabilities list.
7:0	01h RO	**Capability Identifier (CAP_ID):** Hardwired to 01h for power management.

4.1.50 Power Management Capabilities (PMCAP_0_2_0_PCI) — Offset D2h

This register provides information on the capabilities of the function related to power management.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:2, F:0] + D2h	0022h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:11	00h RO	**PME Support (PMES):** This field indicates the power states in which the IGD may assert PME#. Hardwired to 0 to indicate that the IGD does not assert the PME# signal.
10	0h RO	**D2 Support (D2):** Hardwired to 0 to indicate the D2 power management state is not supported.
9	0h RO	**D1 Support (D1):** Hardwired to 0 to indicate that the D1 power management state is not supported.
8:6	0h RO	**Reserved**
5	1h RO	**Device Specific Initialization (DSI):** Hardwired to 1 to indicate that special initialization of the IGD is required before generic class device driver is to use it.
4	0h RO	**Reserved**
3	0h RO	**PME Clock (PMECLK):** Hardwired to 0 to indicate IGD does not support PME# generation.
2:0	2h RO	**Power Management Interface Version (VER):** Hardwired to 010b to indicate that there are 4 bytes of power management registers implemented and that this device complies with revision 1.1 of the PCI Power Management Interface Specification.

4.1.51 Power Management Control and Status (PMCS_0_2_0_PCI) — Offset D4h

Power Management Control and Status

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:2, F:0] + D4h	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15	0h RO	**PME Status (PMESTS):** This bit is hardwired to 0 to indicate that IGD does not support PME# generation from D3 (cold).

Bit Range	Default & Access	Field Name (ID): Description
14:13	0h RO	**Data Scale (DSCALE):** This field is hardwired to 00 to indicate IGD does not support data register.
12:9	0h RO	**Data Select (DSEL):** This field is hardwired to 0h to indicate IGD does not support data register.
8	0h RO	**PME Enable (PMEEN):** This bit is hardwired to 0 to indicate that PME# assertion from D3 (cold) is disabled.
7:2	0h RO	**Reserved**
1:0	0h RW/V	**Power State (PWRSTAT):** This field indicates the current power state of the IGD and can be used to set the IGD into a new power state. If software attempts to write an unsupported state to this field, write operation must complete normally on the bus, but the data is discarded and no state change occurs. Behavior of the graphics controller in supported states is detailed in the power management section of the Bspec.Bits[1:0]Power state00:D0Default01:D1Not Supported10:D2Not Supported11:D3

4.1.52 Software SMI (SWSMI_0_2_0_PCI) — Offset E0h

As long as there is the potential that DVO port legacy drivers exist which expect this register at this address, Dev#2F0 address E0h-E1h must be reserved for this register.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:2, F:0] + E0h	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:8	00h RW	**Software Scratch Bits (SWSB):** Software Scratch Bits
7:1	00h RW	**Software Flag (SWF):** Used to indicate caller and SMI function desired, as well as return result.
0	0h RW	**Software SMI Event (GSSMIE):** When Set this bit will trigger an SMI. Software must write a '0' to clear this bit.SMI will be triggered only if SWSCI[SMISCISEL] is set to select SMI.

4.1.53 Graphics System Event (GSE_0_2_0_PCI) — Offset E4h

This register can be accessed by either Byte, Word, or DWORD PCI configuration cycles. A write to this register will cause the Graphics System Event display interrupt if it is enabled and unmasked in the display interrupt registers.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + E4h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:24	00h RW	**Graphics System Event Scratch Trigger 3 (GSE3):** Graphics System Event Scratch Trigger 3
23:16	00h RW	**Graphics System Event Scratch Trigger 2 (GSE2):** Graphics System Event Scratch Trigger 2
15:8	00h RW	**Graphics System Event Scratch Trigger 1 (GSE1):** Graphics System Event Scratch Trigger 1
7:0	00h RW	**Graphics System Event Scratch Trigger 0 (GSE0):** Graphics System Event Scratch Trigger 0

4.1.54 Software SCI (SWSCI_0_2_0_PCI) — Offset E8h

This register serves 2 purposes: 1) Support selection of SMI or SCI event source (SMISCISEL - bit15) 2) SCI Event trigger (GSSCIE - bit 0). To generate a SW SCI event, software should program bit 15 (SMISCISEL) to 1. This is typically programmed once (assuming SMIs are never triggered). On a '0' to '1' subsequent transition in bit 0 of this register (caused by a software write operation), a SCI message will be sent to cause the TCOSCI_STS bit in GPE0 register to be set to 1. The corresponding SCI event handler in BIOS is to be defined as a _Lxx method, indicating level trigger to the operating system. Once written as 1, software must write a '0' to this bit to clear it, and all other write transitions (1-0, 0-0, 1-1) will not cause a SCI message to be sent. To generate a SW SMI event, software should program bit 15 to 0 and trigger SMI via writes to SWSMI register (See SWSMI register for programming details).

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:2, F:0] + E8h	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15	0h RW	**SMI Or SCI Event Select (SMISCISEL):** 0 = SMI (default)1 = SCI If selected event source is SMI, SMI trigger and associated scratch bits accesses are performed via SWSMI register. If SCI event source is selected, the rest of the bits in this register provide SCI trigger capability and associated SW scratch pad area.
14:1	0000h RW	**Software Scratch Bits (SCISB):** Read/write bits not used by hardware.

Bit Range	Default & Access	Field Name (ID): Description
0	0h RW	**Software SCI Event (GSSCIE):** If SCI event is selected (SMISCISEL = 1), on a 0 to 1 transition of GSSCIE bit, a SCI message will be sent to cause the TCOSCI_STS bit in GPE0 register to be set to 1. Software must write a 0 to clear this bit.

4.1.55 Device 2 Mirror of Protected Audio Video Path Control (PAVPC0_0_2_0_PCI) — Offset F0h

Device 2 Mirror of Protected Audio Video Control.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + F0h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:20	000h RO/V	**WOPCM Base LSB (WOPCMBASE_LSB):** Base value programmed (from Top of Stolen Memory). The programmed value must be consistent with the WOPCM Size programming.
19:9	0h RO	**Reserved**
8:7	0h RO/V	**WOPCM Size (WOPCMSIZE):** This register determines the WOPCM size. The programmed value must be consistent with the WOPCM base programming. 00b: 1MB (default) 01b: 2MB 10b: 4MB 11b: 8MB
6	0h RO/V	**ASMF Method Enable (ASMFEN):** 0: Disable ASMF 1: Enable ASMF
5	0h RO	**Reserved**
4	0h RO/V	**Override Terminate Attack (OVTATTACK):** Override of unsolicited connection state attack and terminate 0: Disable override; attack terminate allowed 1: Enable override; attack terminate disallowed
3	0h RO/V	**Heavy Mode Select (HVYMODSEL):** Heavy/light encryption mode select 0: Surface encryption is disabled - Light mode 1: Surface encryption is enabled
2	0h RO/V	**Lock Bit (LOCK):** BIOS will set this bit with bit 0 and/or bit 1.
1	0h RO/V	**PAVP Enable (PAVPE):** 0: PAVP functionality disabled 1: PAVP functionality enabled

Bit Range	Default & Access	Field Name (ID): Description
0	0h RO/V	**PCM Enable (PCME):** Protected content memory enable.

4.1.56 Device 2 Mirror of Protected Audio Video Path Control (PAVPC1_0_2_0_PCI) — Offset F4h

Device 2 Mirror of Protected Audio Video Control.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + F4h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RO/V	**WOPCM Base MSB (WOPCMBASE_MSB):** Base value programmed (from Top of Stolen Memory). The programmed value must be consistent with the WOPCM Size programming.

4.1.57 Stepping Revision ID (SRID_0_2_0_PCI) — Offset F8h

Stepping Revision ID of this device

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + F8h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:20	000h RO	**Stepping Revision ID MSB (SRID_MSB):** Upper 4 bit of the Stepping Revision ID.
19:16	0h RO	**Stepping Revision ID LSB (SRID_LSB):** Lower 4 bit of the Stepping Revision ID.
15:0	0h RO	**Reserved**

4.1.58 ASL Storage (ASLS_0_2_0_PCI) — Offset FCh

This is a software scratch register.

The exact bit register usage must be worked out in common between System BIOS and driver software.

For each device, the ASL control method requires two bits for DOD (BIOS detectable yes or no, VGA/Non-VGA), one bit for DGS (enable/disable requested), and two bits for DCS (enabled now/disabled now, connected or not).

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + FCh	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RW	**Device Switching Storage (DSS):** Software controlled usage to support device switching.

4.1.59 PASID Extended Capability Header (PASID_EXTCAP_0_2_0_PCI) — Offset 100h

PASID capability reports support for Process Address Space ID(PASID) on Device-2, compliant to PCI-Express PASID ECN.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + 100h	2001001Bh

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:20	200h RO	**Next Capability Offset (NCO):** This is a hardwired pointer to the next item in the capabilities list.
19:16	1h RO	**Version ID (V):** Hardwired to capability version 1.
15:0	001Bh RO	**Capability ID (CAPID):** Hardwired to the PASID Extended Capability ID

4.1.60 PASID Capability (PASID_CAP_0_2_0_PCI) — Offset 104h

PASID capability reports support for Process Address Space ID(PASID) on Device-2, compliant to PCI-Express PASID ECN.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:2, F:0] + 104h	1400h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:13	0h RO	**Reserved**
12:8	14h RO	**Maximum PASID Width (MPW):** Indicates the width of the PASID field supported by the Endpoint. Hardwired to 14h to indicate support for all PASID values (20 bits).
7:3	0h RO	**Reserved**
2	0h RO	**Privilege Mode Supported (PMS):** Hardwired to 0, the Endpoint supports operating in Non-privileged mode only, and will never request privileged mode in requests-with-PASID.
1	0h RO	**Execute Permission Supported (EPS):** Hardwired to 0, the Endpoint supports requests-with-PASID that requests execute permission.
0	0h RO	**Reserved**

4.1.61 PASID Control (PASID_CTRL_0_2_0_PCI) — Offset 106h

Process Address Space ID (PASID) control for Device-2.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:2, F:0] + 106h	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:3	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
2	0h RO	**Privileged Mode Enable (PME):** Hardwired to 0, the Endpoint is not permitted to request privileged mode in requests-with-PASID.
1	0h RW	**Execute Permission Enable (EPE):** If Set, the Endpoint is permitted to request execute permission in requests-with-PASID. If Clear, the Endpoint is not permitted to do so. Behavior is undefined if this bit changes value when ATS Enable field in ATS Capability is Set.Processor graphics does not use this field. Software is expected to Set this field before configuring extended-context-entry for Device-2 with the Execute Request Enable field Set.
0	0h RW	**PASID Enable (PE):** If Set, the Endpoint is permitted to generate requests-with-PASID. If Clear, the Endpoint is not permitted to do so. Behavior is undefined if this bit changes value when ATS Enable field in ATS Capability is Set. If privileged Mode Supported field in PASID Capability register is Clear, then this field is treated as Reserved(0).Processor graphics does not use this field. Software is expected to Set this field before configuring extended-context-entry for Device-2 with Supervisor Request Enable field Set. For compatibility reasons, this field is implemented as RW.

4.1.62 ATS Extended Capability Header (ATS_EXTCAP_0_2_0_PCI) — Offset 200h

ATS Capability reports support for Device-TLBs on Device-2, compliant to PCI Express ATS specification.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + 200h	3001000Fh

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:20	300h RO	**Next Capability Offset (NCO):** This is a hardwired pointer to the next item in the capabilities list. Value 300h in this field provides the offset for Page-Request Capability.
19:16	1h RO	**Version ID (V):** Hardwired to capability version 1.
15:0	000Fh RO	**Capability ID (CAPID):** Hardwired to the ATS Extended Capability ID

4.1.63 ATS Capability (ATS_CAP_0_2_0_PCI) — Offset 204h

ATS Capability reports support for Device-TLBs on Device-2, compliant to PCI Express ATS specification.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:2, F:0] + 204h	0060h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:7	0h RO	**Reserved**
6	1h RO	**Global Invalidate Supported (GIS):** If Set, the Function supports Invalidation Requests that have the Global Invalidate bit Set. If Clear, the Function ignores the Global Invalidate bit in all Invalidate requests.Reserved
5	1h RO	**Page Aligned Request (PAR):** Hardwired to 1, the Untranslated Address is always aligned to a 4096 byte boundary. Processor Graphics reports value of 1b indicating all VT-d and SVM translations are page-aligned.
4:0	00h RO	**Invalidate Queue Depth (IQE):** The number of Invalidate Requests that the endpoint can accept before putting back pressure on the upstream connection. Hardwired to 0h, the function can accept 32 Invalidate Requests.

4.1.64 ATS Control (ATS_CTRL_0_2_0_PCI) — Offset 206h

ATS Control register

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:2, F:0] + 206h	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15	0h RW	**ATS Enable (AE):** When Set, the function is enabled to cache translations. Processor graphics ignores this field, as GT uses GTLB as IOTLB and only pretends to software that it has a Device-TLB. Software is expected to Set this field before configuring extended context-entry for Device2 with Page Request Enable field Set. For compatibility, this field is implemented as RW as software can read it to determine ATS enable status.
14:5	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
4:0	00h RW	**Smallest Translation Unit (STU):** This value indicates to the Endpoint the minimum number of 4096-byte blocks that is indicated in a Translation Completion or Invalidate Request. This is a power of 2 multiple and the number of blocks is 2^STU. A value of 0 indicates one block and value 1F indicates 2^31 blocks. For IGD this must be programmed to 0h for 4KB as smallest translation unit.

4.1.65 Page Request Extended Capability Header (PR_EXTCAP_0_2_0_PCI) — Offset 300h

Page Request Extended Capability reports support for page-faults on Device-2, compliant to PCI-Express ATS 1.1 Specification

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + 300h	00010013h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:20	000h RO/V	**Next Capability Offset (NCO):** This is a hardwired pointer to the next item in the capabilities list. Value 000h (Default) indicates that this is the end of the PCI-Express Extended capability Linked List. When Graphics Virtualization is enabled, this field is hardwired to point to the next PCI Capability structure, the SRIOV Extended Capability Header at 320h. When Graphics Virtualization is disabled, this field will be hardwired to 000h to indicate the end of PCI-Express Extended capability Linked List.
19:16	1h RO	**Version ID (V):** Hardwired to capability version 1.
15:0	0013h RO	**Capability ID (CAPID):** Hardwired to the Page Request Extended Capability ID

4.1.66 Page Request Control (PR_CTRL_0_2_0_PCI) — Offset 304h

Page Request Control

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:2, F:0] + 304h	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:2	0h RO	**Reserved**
1	0h RO	**RST:** When the Enable field is clear, or is being cleared in the same register update that sets this field, writing a 1b to this field, clears the associated implementation dependent page request credit Counter and pending request state for the associated Page Request Interface. No action is initiated if this field is written to 0b or if this field is written with any value when the PRE field is set. Processor graphics does not use this field, and hardwires it as read-only (0).
0	0h RW	**Page-Request Enable (PRE):** When Set, indicates that the page request interface on the endpoint is allowed to make page requests. If both this field and the Stopped field in Page Request Status register are Clear, then the Page request interface will not issue new page requests, but has outstanding page requests for which page responses is not yet received. When this field transitions from 0 to 1, all the status fields in the Page-Request Status register are cleared. Enabling a page request interface that has not successfully stopped has indeterminate results.

4.1.67 Page Request Status (PR_STATUS_0_2_0_PCI) — Offset 306h

Page Request Status

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:2, F:0] + 306h	8100h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15	1h RO	**PRG Response PASID Required (PRPR):** If set, the Function expects a PASID TLP Prefix on PRG Response Messages when the corresponding page requests had a PASID TLP Prefix. If Clear, the function does not expect PASID TLP Prefixes on any PRG Response Message. Function behavior is undefined if this bit is Clear and the Function receives a PRG Response Message with a PASID TLP Prefix. Function behavior is undefined if this bit is Set and the Function receives a PRG Response Message with no PASID TLP Prefix when the corresponding Page Requests had a PASID TLP Prefix. This bit is RsvdZ if the Function does not support the PASID TLP Prefix.
14:9	0h RO	**Reserved**
8	1h RO	**S:** When this field is Set, the associated page request interface has stopped issuing additional Page requests and that all previously issued Page requests have completed. When this field is clear the associate Page request interface either has not stopped or has stopped issuing new Page requests but has outstanding Page requests.
7:2	0h RO	**Reserved**
1	0h RW/V	**Unexpected Page Request Group Index (UPGRI):** When Set, indicates the function received a PRG response message containing a PRG index that has no matching request, a response failure. This field is Set by the Function and cleared when a 1b is written to the field.
0	0h RW/V	**Response Failure (RF):** When Set, indicates the function received a PRG response message indicating a response failure. The function expects no further response from the host (any received are ignored). This field is Set by the Function and cleared when a 1b is written to this field.

4.1.68 Outstanding Page Request Capacity (OPRC_0_2_0_PCI) — Offset 308h

Outstanding Page Request Capacity

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + 308h	00008000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:0	00008000h RO	**Outstanding Page Request Capacity (OPRC):** This register contains the number of outstanding page request messages the associated Page Request Interface physically supports. This is the upper limit on the number of pages that can be usefully allocated to the Page Request Interface. Hardwired to 32,768 requests.

4.1.69 Outstanding Page Request Allocation (OPRA_0_2_0_PCI) — Offset 30Ch

Outstanding Page Request Allocation

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + 30Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RW	**Outstanding Page Request Allocation (OPRA):** This register contains the number of outstanding page request messages the associated Page Request Interface is allowed to issue.

4.1.70 SRIOV Extended Capability Header (SRIOV_ECAPHDR_0_2_0_PCI) — Offset 320h

SR-IOV Extended Capability Header.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + 320h	00010010h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:20	000h RO	**Next Capability Offset (NEXT):** Next capability Offset. Value = 0x000 to indicate the end of the Extended Capability List
19:16	1h RO	**Capability Version (CAP_VER):** Capability Version
15:0	0010h RO	**PCIE Extended Capability ID (PCIE_ECAP_ID):** PCIE Extended capability ID

4.1.71 SRIOV Capabilities (SRIOV_CAP_0_2_0_PCI) — Offset 324h

Defines SR-IOV Capabilities

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + 324h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:21	000h RO	**Virtual Function Migration Interrupt Message Number (VF_MIG_INTR_MSG_NUM):** Value: 0. Virtual Function Migration is not supported.
20:2	0h RO	**Reserved**
1	0h RO	**ARI Capable Hierarchy Preserved (ARI_CAP_HIER_PRESERVED):** Value: Always 0. ARI is not supported.
0	0h RO	**Virtual Function Migration Capable (VF_MIG_CAP):** Value:0. Virtual Function Migration not supported.

4.1.72 SRIOV Control (SRIOV_CTRL_0_2_0_PCI) — Offset 328h

SR-IOV Control Register.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:2, F:0] + 328h	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:5	0h RO	**Reserved**
4	0h RO	**ARI Capable Hierarchy (ARI_CAPHIER):** Hardwired to 0. ARI capability is not supported
3	0h RW/V	**Virtual Function Memory Space Enable (VF_MSE):** SW shall set this bit before setting Virtual Function Enable. (to allow Virtual Function memory space response)
2	0h RO	**Virtual Function Migration Interrupt Enable (VF_MIG_INTR_EN):** Virtual Function migration is not supported.
1	0h RO	**Virtual Function Migration Enable (VF_MIG_EN):** Virtual Function migration is not supported.
0	0h RW/V	**Virtual Function Enable (VF_EN):** System SW shall set this bit to enable Virtual Functions. Setting/Clearing this bit shall result in an interrupt to GUC. This allows the GuC and subsequently the PF to take appropriate action to comprehend virtualization.

4.1.73 SRIOV Status (SRIOV_STS_0_2_0_PCI) — Offset 32Ah

SR-IOV Status Register.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:2, F:0] + 32Ah	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:1	0h RO	**Reserved**
0	0h RO	**Virtual Function Migration Status (VF_MIG_STS):** Virtual Function Migration Status

4.1.74 SRIOV Initial Virtual Functions (SRIOV_INITVFS_0_2_0_PCI) — Offset 32Ch

Defines Initial number of Virtual Functions available to the VMM.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:2, F:0] + 32Ch	0007h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
15:0	0007h RO/V	**Initial Virtual Functions (INITIAL_VFS):** For SR-IOV implementation, this value must exactly match the Total Virtual Functions

4.1.75 SRIOV Total Virtual Functions (SRIOV_TOTVFS_0_2_0_PCI) — Offset 32Eh

Defines the Total number of Virtual Functions available to the VMM.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:2, F:0] + 32Eh	0007h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
15:0	0007h RO	**Total Virtual Functions (TOTAL_VFS):** Indicates the maximum number of Virtual Functions that could be associated with the PF

4.1.76 Number of Virtual Functions (SRIOV_NUMOFVFS_0_2_0_PCI) — Offset 330h

Number of Virtual Functions enabled by the VMM.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + 330h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:24	0h RO	**Reserved**
23:16	00h RO	**Function Dependency Link (FUN_DPNDNCY_LINK):** Same value as the Physical function number, indicating no Dependency
15:0	0000h RW/V	**Number of Virtual functions (NUMOF_VFS):** System SW shall set this field to control the number of Virtual Functions that are visible. This field must be programmed before setting Virtual Function Enable. Changing this field when Virtual Function Enable is set will produced undefined behavior as per the SR-IOV specification. HW will ignore the new value programmed.

4.1.77 First Virtual Function Offset (FIRST_VF_OFFSET_0_2_0_PCI) — Offset 334h

Defines the offset of the function number from the PF to the first Virtual Function.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:2, F:0] + 334h	0001h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
15:0	0001h RO	**First Virtual Function Offset Value (FIRST_VF_OFFSET):** Defines the routing ID offset of the first Virtual Function that is associated with the PF that contains this Capability structure. The first Virtual Functions 16-bit Routing ID is calculated by adding the contents of this field to the Routing ID of the PF containing this field ignoring any carry, using unsigned, 16-bit arithmetic. The value of this field is hardwired to 0001h.

4.1.78 Virtual Function Stride (VF_STRIDE_0_2_0_PCI) — Offset 336h

Defines the stride of the function number from one Virtual Function to the next.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:2, F:0] + 336h	0001h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
15:0	0001h RO	**Virtual Function Stride Value (VF_STRIDE):** Defines the Routing ID offset from one Virtual Function to the next one for all Virtual Functions associated with the PF that contains this Capability structure. The next Virtual Functions 16-bit Routing ID is calculated by adding the contents of this field to the Routing ID of the current Virtual Function, ignoring any carry, using unsigned 16-bit arithmetic. The value of this field is hardwired to 0001h.

4.1.79 Virtual Function Device ID (VF_DEVICEID_0_2_0_PCI) — Offset 33Ah

Defines the Device ID to be used by all Virtual Functions

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:2, F:0] + 33Ah	0A80h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
15:0	0A80h RO/V	**Virtual Function Device ID (VF_DEVICEID):** Mirror the same device ID as the PF

4.1.80 Supported Page Sizes (SUPPORTED_PAGE_SIZES_0_2_0_PCI) — Offset 33Ch

Defines the System Page Sizes supported by this SR-IOV implementation.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + 33Ch	00000513h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000513h RO	**Supported Page Sizes Value (PAGE_SIZES):** This field indicates the page sizes supported by the PF. This PF supports a page size of 2^(n+12) if bit n is Set. For example, if bit 0 is Set, the PF supports 4-KB page sizes. PFs are required to support 4-KB, 8-KB, 64-KB, 256-KB, 1-MB, and 4-MB page sizes. All other page sizes are optional, and not supported in this implementation.

4.1.81 System Page Sizes (SYSTEM_PAGE_SIZES_0_2_0_PCI) — Offset 340h

Defines the System Page Size chosen by the VMM.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + 340h	00000001h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000001h RO	**Graphics System Event Scratch Trigger (SYS_PAGE_SIZES):** This field defines the page size the system will use to map the Virtual Functions memory addresses. Software must set the value of the System Page Size to one of the page sizes set in the Supported Page Sizes field. As with Supported Page Sizes, if bit nis Set in System Page Size, the Virtual Functions associated with this PF are required to support a page size of 2^(n+12). For example, if bit 1 is Set, the system is using an 8-KB page size. The results are undefined if System Page Size is zero. The results are undefined if more than one bit is set in System Page Size. The results are undefined if a bit is Set in System Page Size that is not Set in Supported Page Sizes. When System Page Size is set, the Virtual Function associated with this PF is required to align all BAR resources 20 on a System Page Size boundary. Each Virtual Function BARn or Virtual Function BARn pair shall be aligned on a System Page Size boundary. Each Virtual Function BARn or Virtual Function BARn pair defining a non-zero address space shall be sized to consume an integer multiple of System Page Size bytes. All data structures requiring page size alignment within a Virtual Function shall be aligned on a System Page Size boundary. Virtual Function Enable must be zero when System Page Size is written. The results are undefined if System Page Size is written when Virtual Function Enable is Set. Default value is 1h (i.e., 4 KB), and that is the only value allowed for this implementation

4.1.82 Virtual Function BAR0 Lower DWORD (VF_BAR0_LDW_0_2_0_PCI) — Offset 344h

Lower DWORD of the BAR that defines the base Host Physical Address (HPA) of GTTMMADR for all Virtual Functions.

The HPA of the GTTMMADR for Virtual Function n = Virtual Function GTTMMADDR (Upper and Lower DWORD) + (n - 1) * (16MB * num Tiles)

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + 344h	00000004h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:24	00h RW/V	**Virtual Function GTTMMADDR Lower DWORD (VF_GTTMMADDR_LDW):** Virtual Function GTTMMADDR Lower DWORD
23:4	00000h RO	**Virtual Function GTTMMADDR Lower DWORD Mask (VF_GTTMMADDR_LDW_MASK):** Virtual Function GTTMMADDR Lower DWORD Mask
3	0h RO	**BAR is Prefetchable (PREFETCHABLE):** BAR is Prefetchable
2:1	2h RO	**BAR Type (BAR_TYPE):** A value of 10 indicates a 64 bit BAR.
0	0h RO	**Memory Space Indicator (MEM_SPACE_IND):** A value 0 indicates a memory space.

4.1.83 Virtual Function BAR0 Upper DWORD (VF_BAR0_UDW_0_2_0_PCI) — Offset 348h

Upper DWORD of the BAR that defines the base Host Physical Address of the GTTMMADR for all Virtual Functions

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + 348h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RW/V	**Virtual Function GTTMMADDR Upper DWORD (VF_GTTMMADDR_UDW):** Virtual Function GTTMMADDR Upper DWORD

4.1.84 Virtual Function BAR1 LDW (VF_BAR1_LDW_0_2_0_PCI) — Offset 34Ch

Lower DWORD of the BAR that defines the base Host Physical Address of GMADR for all Virtual Functions.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + 34Ch	0000000Ch

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:29	0h RW/V	**Virtual Function GMADDR Lower DWORD (VF_GMADDR_LDW):** Virtual Function GMADDR Lower DWORD
28:4	0000000h RO	**Virtual Function GMADDR Lower DWORD Mask (VF_GMADDR_LDW_MASK):** Virtual Function GMADDR Lower DWORD Mask
3	1h RO	**BAR is Prefetchable (PREFETCHABLE):** BAR is Prefetchable
2:1	2h RO	**BAR Type (BAR_TYPE):** A value of 10 indicates a 64 bit BAR.
0	0h RO	**Memory Space Indicator (MEM_SPACE_IND):** A value 0 indicates a memory space.

4.1.85 Virtual Function BAR1 UDW (VF_BAR1_UDW_0_2_0_PCI) — Offset 350h

Upper DWORD of the BAR that defines the base Host Physical Address of GMADR for all Virtual Functions

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + 350h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RW/V	**Virtual Function GMADDR Upper DWORD (VF_GMADDR_UDW):** Virtual Function GMADDR Upper DWORD

4.1.86 Virtual Function Migration State Array Offset (VF_MIGST_OFFSET_0_2_0_PCI) — Offset 35Ch

Defines offset from a PF BAR to the Virtual Function Migration State Array. Virtual Function Migration not supported in this implementation

Note: Bit definitions are the same as CAPID0_B_0_2_0_PCI, offset 48h.

4.2 Graphics VT BAR (GFXVTBAR) Registers

This chapter documents the GFXVTBAR registers. Base address of these registers are defined in the GFXVTBAR_0_0_0_MCHBAR_NCU register which resides in the MCHBAR register collection.

Note: These registers apply to all processors.

4.2.1 Summary of Registers

Table 4-3. Summary of GFXVTBAR Registers

Offset	Size (Bytes)	Register Name (Register Symbol)	Default Value
0h	4	Version Register (VER_REG_0_0_0_VTDBAR)	00000040h
8h	8	Capability Register (CAP_REG_0_0_0_VTDBAR)	09C0000C406F0466h
10h	8	Extended Capability Register (ECAP_REG_0_0_0_VTDBAR)	0000059E2FF050DFh
18h	4	Global Command Register (GCMD_REG_0_0_0_VTDBAR)	00000000h
1Ch	4	Global Status Register (GSTS_REG_0_0_0_VTDBAR)	00000000h
20h	8	Root Table Address Register (RTADDR_REG_0_0_0_VTDBAR)	0000000000000000h
28h	8	Context Command Register (CCMD_REG_0_0_0_VTDBAR)	0800000000000000h
34h	4	Fault Status Register (FSTS_REG_0_0_0_VTDBAR)	00000000h
38h	4	Fault Event Control Register (FECTL_REG_0_0_0_VTDBAR)	80000000h
3Ch	4	Fault Event Data Register (FEDATA_REG_0_0_0_VTDBAR)	00000000h
40h	4	Fault Event Address Register (FEADDR_REG_0_0_0_VTDBAR)	00000000h
44h	4	Fault Event Upper Address Register (FEUADDR_REG_0_0_0_VTDBAR)	00000000h
58h	8	Advanced Fault Log Register (AFLOG_REG_0_0_0_VTDBAR)	0000000000000000h
64h	4	Protected Memory Enable Register (PMEN_REG_0_0_0_VTDBAR)	00000000h
68h	4	Protected Low Memory Base Register (PLMBASE_REG_0_0_0_VTDBAR)	00000000h
6Ch	4	Protected Low-Memory Limit Register (PLMLIMIT_REG_0_0_0_VTDBAR)	00000000h
70h	8	Protected High-Memory Base Register (PHMBASE_REG_0_0_0_VTDBAR)	0000000000000000h
78h	8	Protected High-Memory Limit Register (PHMLIMIT_REG_0_0_0_VTDBAR)	0000000000000000h
80h	8	Invalidation Queue Head Register (IQH_REG_0_0_0_VTDBAR)	0000000000000000h
88h	8	Invalidation Queue Tail Register (IQT_REG_0_0_0_VTDBAR)	0000000000000000h
90h	8	Invalidation Queue Address Register (IQA_REG_0_0_0_VTDBAR)	0000000000000000h
9Ch	4	Invalidation Completion Status Register (ICS_REG_0_0_0_VTDBAR)	00000000h
A0h	4	Invalidation Event Control Register (IECTL_REG_0_0_0_VTDBAR)	80000000h
A4h	4	Invalidation Event Data Register (IEDATA_REG_0_0_0_VTDBAR)	00000000h

Offset	Size (Bytes)	Register Name (Register Symbol)	Default Value
A8h	4	Invalidation Event Address Register (IEADDR_REG_0_0_0_VTDBAR)	00000000h
ACh	4	Invalidation Event Upper Address Register (IEUADDR_REG_0_0_0_VTDBAR)	00000000h
B8h	8	Interrupt Remapping Table Address Register (IRTA_REG_0_0_0_VTDBAR)	0000000000000000h
C0h	8	Page Request Queue Head Register (PQH_REG_0_0_0_VTDBAR)	0000000000000000h
C8h	8	Page Request Queue Tail Register (PQT_REG_0_0_0_VTDBAR)	0000000000000000h
D0h	8	Page Request Queue Address Register (PQA_REG_0_0_0_VTDBAR)	0000000000000000h
DCh	4	Page Request Status Register (PRS_REG_0_0_0_VTDBAR)	00000000h
E0h	4	Page Request Event Control Register (PECTL_REG_0_0_0_VTDBAR)	80000000h
E4h	4	Page Request Event Data Register (PEDATA_REG_0_0_0_VTDBAR)	00000000h
E8h	4	Page Request Event Address Register (PEADDR_REG_0_0_0_VTDBAR)	00000000h
ECh	4	Page Request Event Upper Address Register (PEUADDR_REG_0_0_0_VTDBAR)	00000000h
100h	8	MTRR Capability Register (MTRRCAP_0_0_0_VTDBAR)	0000000000000000h
108h	8	MTRR Default Type Register (MTRRDEFAULT_0_0_0_VTDBAR)	0000000000000000h
120h	8	Fixed-Range MTRR Format 64K-00000 (MTRR_FIX64K_00000_REG_0_0_0_VTDBAR)	0000000000000000h
128h	8	Fixed-Range MTRR Format 16K-80000 (MTRR_FIX16K_80000_REG_0_0_0_VTDBAR)	0000000000000000h
130h	8	Fixed-Range MTRR Format 16K-A0000 (MTRR_FIX16K_A0000_REG_0_0_0_VTDBAR)	0000000000000000h
138h	8	Fixed-Range MTRR Format 4K-C0000 (MTRR_FIX4K_C0000_REG_0_0_0_VTDBAR)	0000000000000000h
140h	8	Fixed-Range MTRR Format 4K-C8000 (MTRR_FIX4K_C8000_REG_0_0_0_VTDBAR)	0000000000000000h
148h	8	Fixed-Range MTRR Format 4K-D0000 (MTRR_FIX4K_D0000_REG_0_0_0_VTDBAR)	0000000000000000h
150h	8	Fixed-Range MTRR Format 4K-D8000 (MTRR_FIX4K_D8000_REG_0_0_0_VTDBAR)	0000000000000000h
158h	8	Fixed-Range MTRR Format 4K-E0000 (MTRR_FIX4K_E0000_REG_0_0_0_VTDBAR)	0000000000000000h
160h	8	Fixed-Range MTRR Format 4K-E8000 (MTRR_FIX4K_E8000_REG_0_0_0_VTDBAR)	0000000000000000h
168h	8	Fixed-Range MTRR Format 4K-F0000 (MTRR_FIX4K_F0000_REG_0_0_0_VTDBAR)	0000000000000000h
170h	8	Fixed-Range MTRR Format 4K-F8000 (MTRR_FIX4K_F8000_REG_0_0_0_VTDBAR)	0000000000000000h
180h	8	Variable-Range MTRR Format Physical Base 0 (MTRR_PHYSBASE0_REG_0_0_0_VTDBAR)	0000000000000000h
188h	8	Variable-Range MTRR Format Physical Mask 0 (MTRR_PHYSMASK0_REG_0_0_0_VTDBAR)	0000000000000000h
190h	8	Variable-Range MTRR Format Physical Base 1 (MTRR_PHYSBASE1_REG_0_0_0_VTDBAR)	0000000000000000h

Offset	Size (Bytes)	Register Name (Register Symbol)	Default Value
198h	8	Variable-Range MTRR Format Physical Mask 1 (MTRR_PHYSMASK1_REG_0_0_0_VTDBAR)	0000000000000000h
1A0h	8	Variable-Range MTRR Format Physical Base 2 (MTRR_PHYSBASE2_REG_0_0_0_VTDBAR)	0000000000000000h
1A8h	8	Variable-Range MTRR Format Physical Mask 2 (MTRR_PHYSMASK2_REG_0_0_0_VTDBAR)	0000000000000000h
1B0h	8	Variable-Range MTRR Format Physical Base 3 (MTRR_PHYSBASE3_REG_0_0_0_VTDBAR)	0000000000000000h
1B8h	8	Variable-Range MTRR Format Physical Mask 3 (MTRR_PHYSMASK3_REG_0_0_0_VTDBAR)	0000000000000000h
1C0h	8	Variable-Range MTRR Format Physical Base 4 (MTRR_PHYSBASE4_REG_0_0_0_VTDBAR)	0000000000000000h
1C8h	8	Variable-Range MTRR Format Physical Mask 4 (MTRR_PHYSMASK4_REG_0_0_0_VTDBAR)	0000000000000000h
1D0h	8	Variable-Range MTRR Format Physical Base 5 (MTRR_PHYSBASE5_REG_0_0_0_VTDBAR)	0000000000000000h
1D8h	8	Variable-Range MTRR Format Physical Mask 5 (MTRR_PHYSMASK5_REG_0_0_0_VTDBAR)	0000000000000000h
1E0h	8	Variable-Range MTRR Format Physical Base 6 (MTRR_PHYSBASE6_REG_0_0_0_VTDBAR)	0000000000000000h
1E8h	8	Variable-Range MTRR Format Physical Mask 6 (MTRR_PHYSMASK6_REG_0_0_0_VTDBAR)	0000000000000000h
1F0h	8	Variable-Range MTRR Format Physical Base 7 (MTRR_PHYSBASE7_REG_0_0_0_VTDBAR)	0000000000000000h
1F8h	8	Variable-Range MTRR Format Physical Mask 7 (MTRR_PHYSMASK7_REG_0_0_0_VTDBAR)	0000000000000000h
200h	8	Variable-Range MTRR Format Physical Base 8 (MTRR_PHYSBASE8_REG_0_0_0_VTDBAR)	0000000000000000h
208h	8	Variable-Range MTRR Format Physical Mask 8 (MTRR_PHYSMASK8_REG_0_0_0_VTDBAR)	0000000000000000h
210h	8	Variable-Range MTRR Format Physical Base 9 (MTRR_PHYSBASE9_REG_0_0_0_VTDBAR)	0000000000000000h
218h	8	Variable-Range MTRR Format Physical Mask 9 (MTRR_PHYSMASK9_REG_0_0_0_VTDBAR)	0000000000000000h
400h	8	Fault Recording Register Low [0] (FRCDL_REG_0_0_0_VTDBAR)	0000000000000000h
408h	8	Fault Recording Register High [0] (FRCDH_REG_0_0_0_VTDBAR)	0000000000000000h
500h	8	Invalidate Address Register (IVA_REG_0_0_0_VTDBAR)	0000000000000000h
508h	8	IOTLB Invalidate Register (IOTLB_REG_0_0_0_VTDBAR)	0200000000000000h

4.2.2 Version Register (VER_REG_0_0_0_VTDBAR) — Offset 0h

Register to report the architecture version supported. Backward compatibility for the architecture is maintained with new revision numbers, allowing software to load remapping hardware drivers written for prior architecture versions.

Type	Size	Offset	Default
MMIO	32 bit	GFXVTBAR + 0h	00000040h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:8	0h RO	**Reserved**
7:4	4h RO	**Major Version Number (MAJOR):** Indicates supported architecture version.
3:0	0h RO	**Minor Version Number (MINOR):** Indicates supported architecture minor version.

4.2.3 Capability Register (CAP_REG_0_0_0_VTDBAR) — Offset 8h

Register to report general remapping hardware capabilities.

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + 8h	09C0000C406F0466h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:60	0h RO	**Reserved**
59	1h RO	**Posted Interrupt Support (PI):** • 0 = Hardware does not support Posting of Interrupts. • 1 = Hardware supports Posting of Interrupts. Hardware implementations reporting this field as Set must also report Interrupt Remapping support (IR field in Extended Capability Register)
58:57	0h RO	**Reserved**
56	1h RO	**First Level 1-GByte Page Support (FL1GP):** A value of 1 in this field indicates 1-GByte page size is supported for first-level translation.
55	1h RO	**Read Draining (DRD):** • 0 = Hardware does not support draining of DMA read requests. • 1 = Hardware supports draining of DMA read requests.

Bit Range	Default & Access	Field Name (ID): Description
54	1h RO	**Write Draining (DWD):** • 0 = Hardware does not support draining of DMA write requests. • 1 = Hardware supports draining of DMA write requests.
53:48	00h RO	**Maximum Address Mask Value (MAMV):** The value in this field indicates the maximum supported value for the Address Mask (AM) field in the Invalidation Address register (IVA_REG) and IOTLB Invalidation Descriptor (iotlb_inv_dsc) used for invalidations of second-level translation. This field is valid only when the PSI field in Capability register is reported as Set.
47:40	00h RO	**Number of Fault-Recording Registers (NFR):** Number of fault recording registers is computed as N+1, where N is the value reported in this field. Implementations must support at least one fault recording register (NFR = 0) for each remapping hardware unit in the platform. The maximum number of fault recording registers per remapping hardware unit is 256.
39	0h RO	**Page Selective Invalidation (PSI):** • 0 = Hardware supports only domain and global invalidates for IOTLB. • 1 = Hardware supports page selective, domain and global invalidates for IOTLB. Hardware implementations reporting this field as set are recommended to support a Maximum Address Mask Value (MAMV) value of at least 9 (or 18 if supporting 1GB pages with second level translation).
38	0h RO	**Reserved**
37:34	3h RO	**Second Level Large Page Support (SLLPS):** This field indicates the super page sizes supported by hardware. A value of 1 in any of these bits indicates the corresponding super-page size is supported. The super-page sizes corresponding to various bit positions within this field are: • 0 = 21-bit offset to page frame (2MB) • 1 = 30-bit offset to page frame (1GB) • 2 = 39-bit offset to page frame (512GB) • 3 = 48-bit offset to page frame (1TB) Hardware implementations supporting a specific super-page size must support all smaller super-page sizes, i.e. only valid values for this field are 0000b, 0001b, 0011b, 0111b, 1111b.
33:24	040h RO	**Fault-Recording Register Offset (FRO):** This field specifies the location to the first fault recording register relative to the register base address of this remapping hardware unit. If the register base address is X, and the value reported in this field is Y, the address for the first fault recording register is calculated as X+(16*Y).
23	0h RO	**Reserved**
22	1h RO	**Zero Length Read (ZLR):** • 0 = Indicates the remapping hardware unit blocks (and treats as fault) zero length DMA read requests to write-only pages. • 1 = Indicates the remapping hardware unit supports zero length DMA read requests to write-only pages. DMA remapping hardware implementations are recommended to report ZLR field as Set.

Bit Range	Default & Access	Field Name (ID): Description
21:16	2Fh RO	**Maximum Guest Address Width (MGAW):** This field indicates the maximum DMA virtual addressability supported by remapping hardware. The Maximum Guest Address Width (MGAW) is computed as (N+1), where N is the value reported in this field. For example, a hardware implementation supporting 48-bit MGAW reports a value of 47 (101111b) in this field. If the value in this field is X, untranslated and translated DMA requests to addresses above 2(x+1)-1 are always blocked by hardware. Translations requests to address above 2(x+1)-1 from allowed devices return a null Translation Completion Data Entry with R=W=0. Guest addressability for a given DMA request is limited to the minimum of the value reported through this field and the adjusted guest address width of the corresponding page-table structure. (Adjusted guest address widths supported by hardware are reported through the SAGAW field). Implementations are recommended to support MGAW at least equal to the physical addressability (host address width) of the platform.
15:13	0h RO	**Reserved**
12:8	04h RO	**Supported Adjusted Guest Address Widths (SAGAW):** This 5-bit field indicates the supported adjusted guest address widths (which in turn represents the levels of page-table walks for the 4KB base page size) supported by the hardware implementation. A value of 1 in any of these bits indicates the corresponding adjusted guest address width is supported. The adjusted guest address widths corresponding to various bit positions within this field are: • 0 = 30-bit AGAW (2-level page table) • 1 = 39-bit AGAW (3-level page table) • 2 = 48-bit AGAW (4-level page table) • 3 = 57-bit AGAW (5-level page table) • 4 = 64-bit AGAW (6-level page table) Software must ensure that the adjusted guest address width used to setup the page tables is one of the supported guest address widths reported in this field.
7	0h RO	**Caching Mode (CM):** • 0 = Not-present and erroneous entries are not cached in any of the renmapping caches. Invalidations are not required for modifications to individual not present or invalid entries. However, any modifications that result in decreasing the effective permissions or partial permission increases require invalidations for them to be effective. • 1 = Not-present and erroneous mappings may be cached in the remapping caches. Any software updates to the remapping structures (including updates to not-present or erroneous entries) require explicit invalidation. Hardware implementations of this architecture must support a value of 0 in this field.
6	1h RO	**Protected High-Memory Region (PHMR):** • 0 = Indicates protected high-memory region is not supported. • 1 = Indicates protected high-memory region is supported.
5	1h RO	**Protected Low-Memory Region (PLMR):** • 0 = Indicates protected low-memory region is not supported. • 1 = Indicates protected low-memory region is supported.
4	0h RO	**Required Write-Buffer Flushing (RWBF):** • 0 = Indicates no write-buffer flushing is needed to ensure changes to memory-resident structures are visible to hardware. • 1 = Indicates software must explicitly flush the write buffers to ensure updates made to memory-resident remapping structures are visible to hardware.
3	0h RO	**Advanced Fault Logging (AFL):** • 0 = Indicates advanced fault logging is not supported. Only primary fault logging is supported. • 1 = Indicates advanced fault logging is supported.

Bit Range	Default & Access	Field Name (ID): Description
2:0	6h RO	**Number of Domains Supported (ND):** • 000b = Hardware supports 4-bit domain-ids with support for up to 16 domains. • 001b = Hardware supports 6-bit domain-ids with support for up to 64 domains. • 010b = Hardware supports 8-bit domain-ids with support for up to 256 domains. • 011b = Hardware supports 10-bit domain-ids with support for up to 1024 domains. • 100b = Hardware supports 12-bit domain-ids with support for up to 4K domains. • 100b = Hardware supports 14-bit domain-ids with support for up to 16K domains. • 110b = Hardware supports 16-bit domain-ids with support for up to 64K domains. • 111b = Reserved.

4.2.4 Extended Capability Register (ECAP_REG_0_0_0_VTDBAR) — Offset 10h

Register to report remapping hardware extended capabilities.

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + 10h	0000059E2FF050DFh

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:43	0h RO	**Reserved**
42	1h RO	**Page Request Draining Support (PDS):** • 0 = Hardware does not support Page-Request Drain (PD) flag in Inv_wait_dsc. • 1 = Hardware supports Page-Request Drain (PD) flag in Inv_wait_dsc. This field is valid only when Device-TLB support field is reported as Set.
41	0h RO	**Reserved**
40	1h RO	**Process Address Space ID Support (PASID):** • 0 = Hardware does not support requests tagged with Process Address Space IDs. • 1 = Hardware supports requests tagged with Process Address Space IDs.
39:35	13h RO	**PASID Size Supported (PSS):** This field reports the PASID size supported by the remapping hardware for requests-with-PASID. A value of N in this field indicates hardware supports PASID field of N+1 bits (For example, value of 7 in this field, indicates 8-bit PASIDs are supported). Requests-with-PASID with PASID value beyond the limit specified by this field are treated as error by the remapping hardware. This field is valid only when PASID field is reported as Set.
34	1h RO	**Extended Accessed Flag Support (EAFS):** • 0 = Hardware does not support the extended-accessed (EA) bit in first-level paging-structure entries. • 1 = Hardware supports the extended accessed (EA) bit in first-level paging-structure entries. This field is valid only when PASID field is reported as Set.

Bit Range	Default & Access	Field Name (ID): Description
33	1h RO	**No Write Flag Support (NWFS):** • 0 = Hardware ignores the No Write (NW) flag in Device-TLB translationrequests, and behaves as if NW is always 0. • 1 = Hardware supports the No Write (NW) flag in Device-TLB translationrequests. This field is valid only when Device-TLB support (DT) field is reported as Set.
32	0h RO	**Reserved**
31	0h RO	**Supervisor Request Support (SRS):** • 0 = H/W does not support requests-with-PASID seeking supervisor privilege. • 1 = H/W supports requests-with-PASID seeking supervisor privilege. The field is valid only when PASID field is reported as Set.
30	0h RO	**Execute Request Support (ERS):** • 0 = H/W does not support requests-with-PASID seeking execute permission. • 1 = H/W supports requests-with-PASID seeking execute permission. This field is valid only when PASID field is reported as Set.
29	1h RO	**Page Request Support (PRS):** • 0 = Hardware does not support Page Requests. • 1 = Hardware supports Page Requests This field is valid only when Device-TLB (DT) field is reported as Set.
28	0h RO	**IGN:** Ignore this field
27	1h RO	**Deferred Invalidate Support (DIS):** • 0 = Hardware does not support deferred invalidations of IOTLB and Device-TLB. • 1 = Hardware supports deferred invalidations of IOTLB and Device-TLB. This field is valid only when PASID field is reported as Set.
26	1h RO	**Nested Translation Support (NEST):** • 0 = Hardware does not support nested translations. • 1 = Hardware supports nested translations. This field is valid only when PASID field is reported as Set.
25	1h RO	**Memory Type Support (MTS):** • 0 = Hardware does not support Memory Type in first-level translation and Extended Memory type in second-level translation. • 1 = Hardware supports Memory Type in first-level translation and Extended Memory type in second-level translation. This field is valid only when PASID and ECS fields are reported as Set. Remapping hardware units with, one or more devices that operate in processor coherency domain, under its scope must report this field as Set.
24	1h RO	**Extended Context Support (ECS):** • 0 = Hardware does not support extended-root-entries and extended-context-entries. • 1 = Hardware supports extended-root-entries and extended-context-entries. Implementations reporting PASID or PRS fields as Set, must report this field as Set.
23:20	Fh RO	**Maximum Handle Mask Value (MHMV):** The value in this field indicates the maximum supported value for the Handle Mask (HM) field in the interrupt entry cache invalidation descriptor (iec_inv_dsc). This field is valid only when the IR field in Extended Capability register is reported as Set.
19:18	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
17:8	050h RO	**IOTLB Register Offset (IRO):** This field specifies the offset to the IOTLB registers relative to the register base address of this remapping hardware unit. If the register base address is X, and the value reported in this field is Y, the address for the first IOTLB invalidation register is calculated as X+(16*Y).
7	1h RO	**Snoop Control (SC):** • 0 = Hardware does not support 1-setting of the SNP field in the page-table entries. • 1 = Hardware supports the 1-setting of the SNP field in the page-table entries.
6	1h RO	**Pass Through (PT):** • 0 = Hardware does not support pass-through translation type in context entries and extended-context-entries. • 1 = Hardware supports pass-through translation type in context entries and extended-context-entries. Pass-through translation is specified through Translation-Type (T) field value of 10b in context-entries, or T field value of 010b in extended-context-entries. Hardware implementations supporting PASID must report a value of 1b in this field.
5	0h RO	**Reserved**
4	1h RO	**Extended Interrupt Mode (EIM):** • 0 = On Intel64 platforms, hardware supports only 8-bit APIC-IDs (xAPIC mode). • 1 = On Intel64 platforms, hardware supports 32-bit APIC-IDs (x2APIC mode). This field is valid only on Intel64 platforms reporting Interrupt Remapping support (IR field Set).
3	1h RO	**Interrupt Remapping support (IR):** • 0 = Hardware does not support interrupt remapping. • 1 = Hardware supports interrupt remapping. Implementations reporting this field as Set must also support Queued Invalidation (QI).
2	1h RO	**Device-TLB Support (DT):** • 0 = Hardware does not support device-IOTLBs. • 1 = Hardware supports Device-IOTLBs. Implementations reporting this field as Set must also support Queued Invalidation (QI). Hardware implementations supporting I/O Page Requests (PRS field Set in Extended Capability register) must report a value of 1b in this field.
1	1h RO	**Queued Invalidation Support (QI):** • 0 = Hardware does not support queued invalidations. • 1 = Hardware supports queued invalidations.
0	1h RO	**Page-Walk Coherency (C):** This field indicates if hardware access to the root, context, extended-context and interrupt-remap tables, and second-level paging structures for requests-without-PASID, are coherent (snooped) or not. • 0 = Indicates hardware accesses to remapping structures are non-coherent. • 1 = Indicates hardware accesses to remapping structures are coherent. Hardware access to advanced fault log, invalidation queue, invalidation semaphore, page-request queue, PASID-table, PASID-state table, and first-level page-tables are always coherent.

4.2.5 Global Command Register (GCMD_REG_0_0_0_VTDBAR) — Offset 18h

Register to control remapping hardware. If multiple control fields in this register need to be modified, software must serialize the modifications through multiple writes to this register.

Type	Size	Offset	Default
MMIO	32 bit	GFXVTBAR + 18h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RW	**Translation Enable (TE):** Software writes to this field to request hardware to enable/disable DMA-remapping: • 0 = Disable DMA remapping. • 1 = Enable DMA remapping. Hardware reports the status of the translation enable operation through the TES field in the Global Status register. There may be active DMA requests in the platform when software updates this field. Hardware must enable or disable remapping logic only at deterministic transaction boundaries, so that any in-flight transaction is either subject to remapping or not at all. Hardware implementations supporting DMA draining must drain any in-flight DMA read/write requests queued within the Root-Complex before completing the translation enable command and reflecting the status of the command through the TES field in the Global Status register. The value returned on a read of this field is undefined.
30	0h WO	**Set Root Table Pointer (SRTP):** Software sets this field to set/update the root-entry table pointer used by hardware. The root-entry table pointer is specified through the Root-entry Table Address (RTA_REG) register. Hardware reports the status of the Set Root Table Pointer operation through the RTPS field in the Global Status register. The Set Root Table Pointer operation must be performed before enabling or re-enabling (after disabling) DMA remapping through the TE field. .After a Set Root Table Pointer operation, software must globally invalidate the context cache and then globally invalidate of IOTLB. This is required to ensure hardware uses only the remapping structures referenced by the new root table pointer, and not stale cached entries. While DMA remapping hardware is active, software may update the root table pointer through this field. However, to ensure valid in-flight DMA requests are deterministically remapped, software must ensure that the structures referenced by the new root table pointer are programmed to provide the same remapping results as the structures referenced by the previous root-table pointer. Clearing this bit has no effect. The value returned on read of this field is undefined.
29	0h RO	**Set Fault Log (SFL):** This field is valid only for implementations supporting advanced fault logging. Software sets this field to request hardware to set/update the fault-log pointer used by hardware. The fault-log pointer is specified through Advanced Fault Log register. Hardware reports the status of the Set Fault Log operation through the FLS field in the Global Status register. The fault log pointer must be set before enabling advanced fault logging (through EAFL field). Once advanced fault logging is enabled, the fault log pointer may be updated through this field while DMA remapping is active. Clearing this bit has no effect. The value returned on read of this field is undefined.

Bit Range	Default & Access	Field Name (ID): Description
28	0h RO	**Enable Advanced Fault Logging (EAFL):** This field is valid only for implementations supporting advanced fault logging. Software writes to this field to request hardware to enable or disable advanced fault logging: • 0 = Disable advanced fault logging. In this case, translation faults are reported through the Fault Recording registers. • 1 = Enable use of memory-resident fault log. When enabled, translation faults are recorded in the memory-resident log. The fault log pointer must be set in hardware (through the SFL field) before enabling advanced fault logging. Hardware reports the status of the advanced fault logging enable operation through the AFLS field in the Global Status register. The value returned on read of this field is undefined.
27	0h RO	**Write Buffer Flush (WBF):** This bit is valid only for implementations requiring write buffer flushing. Software sets this field to request that hardware flush the Root-Complex internal write buffers. This is done to ensure any updates to the memory-resident remapping structures are not held in any internal write posting buffers. Hardware reports the status of the write buffer flushing operation through the WBFS field in the Global Status register. Clearing this bit has no effect. The value returned on a read of this field is undefined.
26	0h RW	**Queued Invalidation Enable (QIE):** This field is valid only for implementations supporting queued invalidations. Software writes to this field to enable or disable queued invalidations. • 0 = Disable queued invalidations. • 1 = Enable use of queued invalidations. Hardware reports the status of queued invalidation enable operation through QIES field in the Global Status register. The value returned on a read of this field is undefined.
25	0h RW	**Interrupt Remapping Enable (IRE):** This field is valid only for implementations supporting interrupt remapping. • 0 = Disable interrupt-remapping hardware. • 1 = Enable interrupt-remapping hardware. Hardware reports the status of the interrupt remapping enable operation through the IRES field in the Global Status register. There may be active interrupt requests in the platform when software updates this field. Hardware must enable or disable interrupt-remapping logic only at deterministic transaction boundaries, so that any in-flight interrupts are either subject to remapping or not at all. Hardware implementations must drain any in-flight interrupts requests queued in the Root-Complex before completing the interrupt-remapping enable command and reflecting the status of the command through the IRES field in the Global Status register. The value returned on a read of this field is undefined.

Bit Range	Default & Access	Field Name (ID): Description
24	0h WO	**Set Interrupt Remap Table Pointer (SIRTP):** This field is valid only for implementations supporting interrupt-remapping. Software sets this field to set/update the interrupt remapping table pointer used by hardware. The interrupt remapping table pointer is specified through the Interrupt Remapping Table Address (IRTA_REG) register. Hardware reports the status of the Set Interrupt Remap Table Pointer operation through the IRTPS field in the Global Status register. The Set Interrupt Remap Table Pointer operation must be performed before enabling or re-enabling (after disabling) interrupt-remapping hardware through the IRE field. After a Set Interrupt Remap Table Pointer operation, software must globally invalidate the interrupt entry cache. This is required to ensure hardware uses only the interrupt-remapping entries referenced by the new interrupt remap table pointer, and not any stale cached entries. While interrupt remapping is active, software may update the interrupt remapping table pointer through this field. However, to ensure valid in-flight interrupt requests are deterministically remapped, software must ensure that the structures referenced by the new interrupt remap table pointer are programmed to provide the same remapping results as the structures referenced by the previous interrupt remap table pointer. Clearing this bit has no effect. The value returned on a read of this field is undefined.
23	0h RW	**Compatibility Format Interrupt (CFI):** This field is valid only for Intel64 implementations supporting interrupt-remapping. Software writes to this field to enable or disable Compatibility Format interrupts on Intel64 platforms. The value in this field is effective only when interrupt-remapping is enabled and Extended Interrupt Mode (x2APIC mode) is not enabled. • 0 = Block Compatibility format interrupts. • 1 = Process Compatibility format interrupts as pass-through (bypass interrupt remapping). Hardware reports the status of updating this field through the CFIS field in the Global Status register. The value returned on a read of this field is undefined.
22:0	0h RO	**Reserved**

4.2.6 Global Status Register (GSTS_REG_0_0_0_VTDBAR) — Offset 1Ch

Register to report general remapping hardware status.

Type	Size	Offset	Default
MMIO	32 bit	GFXVTBAR + 1Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31	0h RO/V	**Translation Enable Status (TES):** This field indicates the status of DMA-remapping hardware. • 0 = DMA-remapping hardware is not enabled. • 1 = DMA-remapping hardware is enabled

Bit Range	Default & Access	Field Name (ID): Description
30	0h RO/V	**Root Table Pointer Status (RTPS):** This field indicates the status of the root- table pointer in hardware. This field is cleared by hardware when software sets the SRTP field in the Global Command register. This field is set by hardware when hardware completes the Set Root Table Pointer operation using the value provided in the Root-Entry Table Address register.
29	0h RO	**Fault Log Status (FLS):** This field: • Is cleared by hardware when software Sets the SFL field in the Global Command register. • Is Set by hardware when hardware completes the Set Fault Log Pointer operation using the value provided in the Advanced Fault Log register.
28	0h RO	**Advanced Fault Logging Status (AFLS):** This field is valid only for implementations supporting advanced fault logging. It indicates the advanced fault logging status: • 0 = Advanced Fault Logging is not enabled. • 1 = Advanced Fault Logging is enabled.
27	0h RO	**Write Buffer Flush Status (WBFS):** This field is valid only for implementations requiring write buffer flushing. This field indicates the status of the write buffer flush command. It is: • Set by hardware when software sets the WBF field in the Global Command register. • Cleared by hardware when hardware completes the write buffer flushing operation.
26	0h RO/V	**Queued Invalidation Enable Status (QIES):** This field indicates queued invalidation enable status. • 0 = queued invalidation is not enabled. • 1 = queued invalidation is enabled
25	0h RO/V	**Interrupt Remapping Enable Status (IRES):** This field indicates the status of Interrupt-remapping hardware. • 0 = Interrupt-remapping hardware is not enabled. • 1 = Interrupt-remapping hardware is enabled
24	0h RO/V	**Interrupt Remapping Pointer Status (IRTPS):** This field indicates the status of the interrupt remapping table pointer in hardware. This field is cleared by hardware when software sets the SIRTP field in the Global Command register. This field is Set by hardware when hardware completes the set interrupt remap table pointer operation using the value provided in the Interrupt Remapping Table Address register.
23	0h RO/V	**Compatibility Format Interrupt Status (CFIS):** This field indicates the status of Compatibility format interrupts on Intel64 implementations supporting interrupt-remapping. The value reported in this field is applicable only when interrupt-remapping is enabled and Extended Interrupt Mode (x2APIC mode) is not enabled. • 0 = Compatibility format interrupts are blocked. • 1 = Compatibility format interrupts are processed as pass-through (bypassing interrupt remapping).
22:0	0h RO	**Reserved**

4.2.7 Root Table Address Register (RTADDR_REG_0_0_0_VTDBAR) — Offset 20h

Register providing the base address of root-entry table.

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + 20h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
63:52	0h RO	**Reserved**
51:12	0000000000h RW	**Root Table Address (RTA):** This register points to base of page aligned, 4KB-sized root-entry table in system memory. Hardware ignores and not implements bits 63:HAW, where HAW is the host address width. Software specifies the base address of the root-entry table through this register, and programs it in hardware through the SRTP field in the Global Command register. Reads of this register returns value that was last programmed to it.
11	0h RW	**Root Table Type (RTT):** This field specifies the type of root-table referenced by the Root Table Address (RTA) field: • 0 = Root Table. • 1 = Extended Root Table
10:0	0h RO	**Reserved**

4.2.8 Context Command Register (CCMD_REG_0_0_0_VTDBAR) — Offset 28h

Register to manage context cache. The act of writing the uppermost byte of the CCMD_REG with the ICC field Set causes the hardware to perform the context-cache invalidation.

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + 28h	0800000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
63	0h RW/V	**Invalidate Context Cache (ICC):** Software requests invalidation of context-cache by setting this field. Software must also set the requested invalidation granularity by programming the CIRG field. Software must read back and check the ICC field is Clear to confirm the invalidation is complete. Software must not update this register when this field is set. Hardware clears the ICC field to indicate the invalidation request is complete. Hardware also indicates the granularity at which the invalidation operation was performed through the CAIG field. Software must submit a context-cache invalidation request through this field only when there are no invalidation requests pending at this remapping hardware unit. Since information from the context-cache may be used by hardware to tag IOTLB entries, software must perform domain-selective (or global) invalidation of IOTLB after the context cache invalidation has completed. Hardware implementations reporting write-buffer flushing requirement (RWBF=1 in Capability register) must implicitly perform a write buffer flush before invalidating the context cache.
62:61	0h RW	**Context Invalidation Request Granularity (CIRG):** Software provides the requested invalidation granularity through this field when setting the ICC field: • 00: Reserved. • 01: Global Invalidation request. • 10: Domain-selective invalidation request. The target domain-id must be specified in the DID field. • 11: Device-selective invalidation request. The target source-id(s) must be specified through the SID and FM fields, and the domain-id (that was programmed in the context-entry for these device(s)) must be provided in the DID field. Hardware implementations may process an invalidation request by performing invalidation at a coarser granularity than requested. Hardware indicates completion of the invalidation request by clearing the ICC field. At this time, hardware also indicates the granularity at which the actual invalidation was performed through the CAIG field.
60:59	1h RO/V	**Context Actual Invalidation Granularity (CAIG):** Hardware reports the granularity at which an invalidation request was processed through the CAIG field at the time of reporting invalidation completion (by clearing the ICC field). The following are the encodings for this field: • 00: Reserved. • 01: Global Invalidation performed. This could be in response to a global, domain-selective or device-selective invalidation request. • 10: Domain-selective invalidation performed using the domain-id specified by software in the DID field. This could be in response to a domain-selective or device-selective invalidation request. • 11: Device-selective invalidation performed using the source-id and domain-id specified by software in the SID and FM fields. This can only be in response to a device-selective invalidation request.
58:34	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
33:32	0h RW	**Function Mask (FM):** Software may use the Function Mask to perform device-selective invalidations on behalf of devices supporting PCI Express Phantom Functions...This field specifies which bits of the function number portion (least significant three bits) of the SID field to mask when performing device-selective invalidations. The following encodings are defined for this field: • 00: No bits in the SID field masked. • 01: Mask most significant bit of function number in the SID field. • 10: Mask two most significant bit of function number in the SID field. • 11: Mask all three bits of function number in the SID field. The context-entries corresponding to all the source-ids specified through the FM and SID fields must have to the domain-id specified in the DID field.
31:16	0000h RW	**SID:** Indicates the source-id of the device whose corresponding context-entry needs to be selectively invalidated. This field along with the FM field must be programmed by software for device-selective invalidation requests.
15:0	0000h RW	**DID:** Indicates the id of the domain whose context-entries need to be selectively invalidated. This field must be programmed by software for both domain-selective and device-selective invalidation requests. The Capability register reports the domain-id width supported by hardware. Software must ensure that the value written to this field is within this limit. Hardware may ignore and not implement bits15:N, where N is the supported domain-id width reported in the Capability register.

4.2.9 Fault Status Register (FSTS_REG_0_0_0_VTDBAR) — Offset 34h

Register indicating the various error status.

Type	Size	Offset	Default
MMIO	32 bit	GFXVTBAR + 34h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:16	0h RO	**Reserved**
15:8	00h RO	**Fault Record Index (FRI):** This field is valid only when the PPF field is Set. The FRI field indicates the index (from base) of the fault recording register to which the first pending fault was recorded when the PPF field was Set by hardware. The value read from this field is undefined when the PPF field is clear.
7	0h RW/1C	**Page Request Overflow (PRO):** Hardware detected a Page Request Overflow error. Hardware implementations not supporting the Page Request Queue implement this bit as RsvdZ.

Bit Range	Default & Access	Field Name (ID): Description
6	0h RW/1C	**Invalidation Time-out Error (ITE):** Hardware detected a Device-IOTLB invalidation completion time-out. At this time, a fault event may be generated based on the programming of the Fault Event Control register. Hardware implementations not supporting device Device-IOTLBs implement this bit as RsvdZ.
5	0h RW/1C	**Invalidation Completion Error (ICE):** Hardware received an unexpected or invalid Device-IOTLB invalidation completion. This could be due to either an invalid ITag or invalid source-id in an invalidation completion response. At this time, a fault event may be generated based on the programming of hte Fault Event Control register. Hardware implementations not supporting Device-IOTLBs implement this bit as RsvdZ.
4	0h RW/1C	**Invalidation Queue Error (IQE):** Hardware detected an error associated with the invalidation queue. This could be due to either a hardware error while fetching a descriptor from the invalidation queue, or hardware detecting an erroneous or invalid descriptor in the invalidation queue. At this time, a fault event may be generated based on the programming of the Fault Event Control register. Hardware implementations not supporting queued invalidations implement this bit as RsvdZ.
3	0h RO	**Advanced Pending Fault (APF):** When this field is Clear, hardware sets this field when the first fault record (at index 0) is written to a fault log. At this time, a fault event is generated based on the programming of the Fault Event Control register. Software writing 1 to this field clears it. Hardware implementations not supporting advanced fault logging implement this bit as RsvdZ.
2	0h RO	**Advanced Fault Overflow (AFO):** Hardware sets this field to indicate advanced fault log overflow condition. At this time, a fault event is generated based on the programming of the Fault Event Control register. Software writing 1 to this field clears it. Hardware implementations not supporting advanced fault logging implement this bit as RsvdZ.
1	0h RO/V	**Primary Pending Fault (PPF):** This field indicates if there are one or more pending faults logged in the fault recording registers. Hardware computes this field as the logical OR of Fault (F) fields across all the fault recording registers of this remapping hardware unit. • 0 = No pending faults in any of the fault recording registers. • 1 = One or more fault recording registers has pending faults. The FRI field is updated by hardware whenever the PPF field is set by hardware. Also, depending on the programming of Fault Event Control register, a fault event is generated when hardware sets this field.
0	0h RW/1C	**Primary Fault Overflow (PFO):** Hardware sets this field to indicate overflow of fault recording registers. Software writing 1 clears this field. When this field is Set, hardware does not record any new faults until software clears this field.

4.2.10 Fault Event Control Register (FECTL_REG_0_0_0_VTDBAR) — Offset 38h

Register specifying the fault event interrupt message control bits.

Type	Size	Offset	Default
MMIO	32 bit	GFXVTBAR + 38h	80000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	1h RW	**Interrupt Mask (IM):** • 0 = No masking of interrupt. When an interrupt condition is detected, hardware issues an interrupt message (using the Fault Event Data and Fault Event Address register values). • 1 = This is the value on reset. Software may mask interrupt message generation by setting this field. Hardware is prohibited from sending the interrupt message when this field is set.
30	0h RO/V	**Interrupt Pending (IP):** Hardware sets the IP field whenever it detects an interrupt condition, which is defined as: • When primary fault logging is active, an interrupt condition occurs when hardware records a fault through one of the Fault Recording registers and sets the PPF field in Fault Status register. • When advanced fault logging is active, an interrupt condition occurs when hardware records a fault in the first fault record (at index 0) of the current fault log and sets the APF field in the Fault Status register. • Hardware detected error associated with the Invalidation Queue, setting the IQE field in the Fault Status register. • Hardware detected invalid Device-IOTLB invalidation completion, setting the ICE field in the Fault Status register. • Hardware detected Device-IOTLB invalidation completion time-out, setting the ITE field in the Fault Status register. If any of the status fields in the Fault Status register was already Set at the time of setting any of these fields, it is not treated as a new interrupt condition. The IP field is kept set by hardware while the interrupt message is held pending. The interrupt message could be held pending due to interrupt mask (IM field) being Set or other transient hardware conditions. The IP field is cleared by hardware as soon as the interrupt message pending condition is serviced. This could be due to either: • Hardware issuing the interrupt message due to either change in the transient hardware condition that caused interrupt message to be held pending, or due to software clearing the IM field. • Software servicing all the pending interrupt status fields in the Fault Status register as follows: - When primary fault logging is active, software clearing the Fault (F) field in all the Fault Recording registers with faults, causing the PPF field in Fault Status register to be evaluated as clear. - Software clearing other status fields in the Fault Status register by writing back the value read from the respective fields.
29:0	0h RO	**Reserved**

4.2.11 Fault Event Data Register (FEDATA_REG_0_0_0_VTDBAR) — Offset 3Ch

Register specifying the interrupt message data

Type	Size	Offset	Default
MMIO	32 bit	GFXVTBAR + 3Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:16	0000h RW	**Extended Interrupt Message Data (EIMD):** This field is valid only for implementations supporting 32-bit interrupt data fields. Hardware implementations supporting only 16-bit interrupt data may treat this field as RsvdZ.
15:0	0000h RW	**Interrupt Message Data (IMD):** Data value in the interrupt request.

4.2.12 Fault Event Address Register (FEADDR_REG_0_0_0_VTDBAR) — Offset 40h

Register specifying the interrupt message address.

Type	Size	Offset	Default
MMIO	32 bit	GFXVTBAR + 40h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:2	00000000h RW	**Message Address (MA):** When fault events are enabled, the contents of this register specify the DWORD-aligned address (bits 31:2) for the interrupt request.
1:0	0h RO	**Reserved**

4.2.13 Fault Event Upper Address Register (FEUADDR_REG_0_0_0_VTDBAR) — Offset 44h

Register specifying the interrupt message upper address.

Type	Size	Offset	Default
MMIO	32 bit	GFXVTBAR + 44h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RW	**Message Upper Address (MUA):** Hardware implementations supporting Extended Interrupt Mode are required to implement this register. Hardware implementations not supporting Extended Interrupt Mode may treat this field as RsvdZ.

4.2.14 Advanced Fault Log Register (AFLOG_REG_0_0_0_VTDBAR) — Offset 58h

Register to specify the base address of the memory-resident fault-log region. This register is treated as RsvdZ for implementations not supporting advanced translation fault logging (AFL field reported as 0 in the Capability register).

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + 58h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:12	0000000000000h RO	**Fault Log Address (FLA):** This field specifies the base of 4KB aligned fault-log region in system memory. Hardware ignores and does not implement bits 63:HAW, where HAW is the host address width. Software specifies the base address and size of the fault log region through this register, and programs it in hardware through the SFL field in the Global Command register. When implemented, reads of this field return the value that was last programmed to it.
11:9	0h RO	**Fault Log Size (FLS):** This field specifies the size of the fault log region pointed by the FLA field. The size of the fault log region is 2X * 4KB, where X is the value programmed in this register. When implemented, reads of this field return the value that was last programmed to it.
8:0	0h RO	**Reserved**

4.2.15 Protected Memory Enable Register (PMEN_REG_0_0_0_VTDBAR) — Offset 64h

Register to enable the DMA-protected memory regions setup through the PLMBASE,..PLMLIMT, PHMBASE, PHMLIMIT registers. This register is always treated as RO for implementations not supporting protected memory regions (PLMR and PHMR fields reported as Clear in the Capability register).

Protected memory regions may be used by software to securely initialize remapping structures in memory. To avoid impact to legacy BIOS usage of memory, software is recommended to not overlap protected memory regions with any reserved memory regions of the platform reported through the Reserved Memory Region Reporting (RMRR) structures.

Type	Size	Offset	Default
MMIO	32 bit	GFXVTBAR + 64h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RW	**Enable Protected Memory (EPM):** This field controls DMA accesses to the protected low-memory and protected high-memory regions. • 0 = Protected memory regions are disabled. • 1 = Protected memory regions are enabled.DMA requests accessing protected memory regions are handled as follows: - When DMA remapping is not enabled, all DMA requests accessing protected memory regions are blocked. - When DMA remapping is enabled: • DMA requests processed as pass-through (Translation Type value of 10b in Context-Entry) and accessing the protected memory regions are blocked. • DMA requests with translated address (AT=10b) and accessing the protected memory regions are blocked. • DMA requests that are subject to address remapping, and accessing the protected memory regions may or may not be blocked by hardware. For such requests, software must not depend on hardware protection of the protected memory regions, and instead program the DMA-remapping page-tables to not allow DMA to protected memory regions. Remapping hardware access to the remapping structures are not subject to protected memory region checks. DMA requests blocked due to protected memory region violation are not recorded or reported as remapping faults. Hardware reports the status of the protected memory enable/disable operation through the PRS field in this register.Hardware implementations supporting DMA draining must drain any in-flight translated DMA requests queued within the Root-Complex before indicating the protected memory region as enabled through the PRS field.
30:1	0h RO	**Reserved**
0	0h RO/V	**Protected Region Status (PRS):** This field indicates the status of protected memory region(s): • 0 = Protected memory region(s) disabled. • 1 = Protected memory region(s) enabled.

4.2.16 Protected Low Memory Base Register (PLMBASE_REG_0_0_0_VTDBAR) — Offset 68h

Register to set up the base address of DMA-protected low-memory region below 4GB. This register must be set up before enabling protected memory through PMEN_REG, and must not be updated when protected memory regions are enabled.

This register is always treated as RO for implementations not supporting protected low memory region (PLMR field reported as Clear in the Capability register).

The alignment of the protected low memory region base depends on the number of reserved bits (N:0) of this register. Software may determine N by writing all 1s to this register, and finding the most significant zero bit position with 0 in the value read back from the register. Bits N:0 of this register is decoded by hardware as all 0s...Software must setup the protected low memory region below 4GB.

Software must not modify this register when protected memory regions are enabled (PRS field Set in PMEN_REG).

Type	Size	Offset	Default
MMIO	32 bit	GFXVTBAR + 68h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:20	000h RW	**Protected Low-Memory Base (PLMB):** This register specifies the base of protected low-memory region in system memory.
19:0	0h RO	**Reserved**

4.2.17 Protected Low-Memory Limit Register (PLMLIMIT_REG_0_0_0_VTDBAR) — Offset 6Ch

Register to set up the limit address of DMA-protected low-memory region below 4GB. This register must be set up before enabling protected memory through PMEN_REG, and must not be updated when protected memory regions are enabled

This register is always treated as RO for implementations not supporting protected low memory region (PLMR field reported as Clear in the Capability register)

The alignment of the protected low memory region limit depends on the number of reserved bits (N:0) of this register. Software may determine N by writing all 1s to this register, and finding most significant zero bit position with 0 in the value read back from the register. Bits N:0 of the limit register is decoded by hardware as all 1s

The Protected low-memory base and limit registers functions as follows:

- Programming the protected low-memory base and limit registers with the same value in bits 31: (N+1) specifies a protected low-memory region of size 2(N+1) bytes

- Programming the protected low-memory limit register with a value less than the protected low-memory base register disables the protected low-memory region

Software must not modify this register when protected memory regions are enabled (PRS field Set in PMEN_REG).

Type	Size	Offset	Default
MMIO	32 bit	GFXVTBAR + 6Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:20	000h RW	**Protected Low-Memory Limit (PLML):** This register specifies the last host physical address of the DMA-protected low-memory region in system memory.
19:0	0h RO	**Reserved**

4.2.18 Protected High-Memory Base Register (PHMBASE_REG_0_0_0_VTDBAR) — Offset 70h

Register to set up the base address of DMA-protected high-memory region. This register must be set up before enabling protected memory through PMEN_REG, and must not be updated when protected memory regions are enabled

This register is always treated as RO for implementations not supporting protected high memory region (PHMR field reported as Clear in the Capability register)

The alignment of the protected high memory region base depends on the number of reserved bits (N:0) of this register. Software may determine N by writing all 1s to this register, and finding most significant zero bit position below host address width (HAW) in the value read back from the register. Bits N:0 of this register are decoded by hardware as all 0s

Software may setup the protected high memory region either above or below 4GB

Software must not modify this register when protected memory regions are enabled (PRS field Set in PMEN_REG).

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + 70h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:20	00000h RW	**Protected High-Memory Base (PHMB):** This register specifies the base of protected (high) memory region in system memory Hardware ignores, and does not implement, bits 63:HAW, where HAW is the host address width.
19:0	0h RO	**Reserved**

4.2.19 Protected High-Memory Limit Register (PHMLIMIT_REG_0_0_0_VTDBAR) — Offset 78h

Register to set up the limit address of DMA-protected high-memory region. This register must be set up before enabling protected memory through PMEN_REG, and must not be updated when protected memory regions are enabled

This register is always treated as RO for implementations not supporting protected high memory region (PHMR field reported as Clear in the Capability register)

The alignment of the protected high memory region limit depends on the number of reserved bits (N:0) of this register. Software may determine the value of N by writing all 1s to this register, and finding most significant zero bit position below host address width (HAW) in the value read back from the register. Bits N:0 of the limit register is decoded by hardware as all 1s

The protected high-memory base & limit registers functions as follows

- Programming the protected low-memory base and limit registers with the same value in bits HAW:(N+1) specifies a protected low-memory region of size 2(N+1) bytes
- Programming the protected high-memory limit register with a value less than the protected high-memory base register disables the protected high-memory region

Software must not modify this register when protected memory regions are enabled (PRS field Set in PMEN_REG).

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + 78h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:20	00000h RW	**Protected High-Memory Limit (PHML):** This register specifies the last host physical address of the DMA-protected high-memory region in system memory Hardware ignores and does not implement bits 63:HAW, where HAW is the host address width.
19:0	0h RO	**Reserved**

4.2.20 Invalidation Queue Head Register (IQH_REG_0_0_0_VTDBAR) — Offset 80h

Register indicating the invalidation queue head. This register is treated as RsvdZ by implementations reporting Queued Invalidation (QI) as not supported in the Extended Capability register.

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + 80h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:19	0h RO	**Reserved**
18:4	0000h RO/V	**Queue Head (QH):** Specifies the offset (128-bit aligned) to the invalidation queue for the command that will be fetched next by hardware Hardware resets this field to 0 whenever the queued invalidation is disabled (QIES field Clear in the Global Status register).
3:0	0h RO	**Reserved**

4.2.21 Invalidation Queue Tail Register (IQT_REG_0_0_0_VTDBAR) — Offset 88h

Register indicating the invalidation tail head. This register is treated as RsvdZ by implementations reporting Queued Invalidation (QI) as not supported in the Extended Capability register.

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + 88h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
63:19	0h RO	**Reserved**
18:4	0000h RW	**Queue Tail (QT):** Specifies the offset (128-bit aligned) to the invalidation queue for the command that will be written next by software.
3:0	0h RO	**Reserved**

4.2.22 Invalidation Queue Address Register (IQA_REG_0_0_0_VTDBAR) — Offset 90h

Register to configure the base address and size of the invalidation queue. This register is treated as RsvdZ by implementations reporting Queued Invalidation (QI) as not supported in the Extended Capability register.

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + 90h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:12	0000000h RW	**Invalidation Queue Base Address (IQA):** This field points to the base of 4KB aligned invalidation request queue. Hardware ignores and does not implement bits 63:HAW, where HAW is the host address width Reads of this field return the value that was last programmed to it.

Bit Range	Default & Access	Field Name (ID): Description
11:3	0h RO	**Reserved**
2:0	0h RW	**Queue Size (QS):** This field specifies the size of the invalidation request queue. A value of X in this field indicates an invalidation request queue of (2^X) 4KB pages. The number of entries in the invalidation queue is 2^(X + 8).

4.2.23 Invalidation Completion Status Register (ICS_REG_0_0_0_VTDBAR) — Offset 9Ch

Register to report completion status of invalidation wait descriptor with Interrupt Flag (IF) Set

This register is treated as RsvdZ by implementations reporting Queued Invalidation (QI) as not supported in the Extended Capability register.

Type	Size	Offset	Default
MMIO	32 bit	GFXVTBAR + 9Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:1	0h RO	**Reserved**
0	0h RW/1C	**Invalidation Wait Descriptor Complete (IWC):** Indicates completion of Invalidation Wait Descriptor with Interrupt Flag (IF) field Set. Hardware implementations not supporting queued invalidations implement this field as RsvdZ.

4.2.24 Invalidation Event Control Register (IECTL_REG_0_0_0_VTDBAR) — Offset A0h

Register specifying the invalidation event interrupt control bits

This register is treated as RsvdZ by implementations reporting Queued Invalidation (QI) as not supported in the Extended Capability register.

Type	Size	Offset	Default
MMIO	32 bit	GFXVTBAR + A0h	80000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	1h RW	**Interrupt Mask (IM):** • 0= No masking of interrupt. When a invalidation event condition is detected, hardware issues an interrupt message (using the Invalidation Event Data & Invalidation Event Address register values) • 1= This is the value on reset. Software may mask interrupt message generation by setting this field. Hardware is prohibited from sending the interrupt message when this field is Set.
30	0h RO/V	**Interrupt Pending (IP):** Hardware sets the IP field whenever it detects an interrupt condition. Interrupt condition is defined as: • An Invalidation Wait Descriptor with Interrupt Flag (IF) field Set completed, setting the IWC field in the Invalidation Completion Status register • If the IWC field in the Invalidation Completion Status register was already Set at the time of setting this field, it is not treated as a new interrupt condition The IP field is kept Set by hardware while the interrupt message is held pending. The interrupt message could be held pending due to interrupt mask (IM field) being Set, or due to other transient hardware conditions. The IP field is cleared by hardware as soon as the interrupt message pending condition is serviced. This could be due to either: • 0= Hardware issuing the interrupt message due to either change in the transient hardware condition that caused interrupt message to be held pending or due to software clearing the IM field • 1= Software servicing the IWC field in the Invalidation Completion Status register.
29:0	0h RO	**Reserved**

4.2.25 Invalidation Event Data Register (IEDATA_REG_0_0_0_VTDBAR) — Offset A4h

Register specifying the Invalidation Event interrupt message data

This register is treated as RsvdZ by implementations reporting Queued Invalidation (QI) as not supported in the Extended Capability register.

Type	Size	Offset	Default
MMIO	32 bit	GFXVTBAR + A4h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:16	0000h RW	**Extended Interrupt Message Data (EIMD):** This field is valid only for implementations supporting 32-bit interrupt data fields Hardware implementations supporting only 16-bit interrupt data treat this field as Rsvd.
15:0	0000h RW	**Interrupt Message Data (IMD):** Data value in the interrupt request.

4.2.26 Invalidation Event Address Register (IEADDR_REG_0_0_0_VTDBAR) — Offset A8h

Register specifying the Invalidation Event Interrupt message address

This register is treated as RsvdZ by implementations reporting Queued Invalidation (QI) as not supported in the Extended Capability register.

Note: Bit definitions are the same as FEADDR_REG_0_0_0_VTDBAR, offset 40h.

4.2.27 Invalidation Event Upper Address Register (IEUADDR_REG_0_0_0_VTDBAR) — Offset ACh

Register specifying the Invalidation Event interrupt message upper address.

Type	Size	Offset	Default
MMIO	32 bit	GFXVTBAR + ACh	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RW	**Message Upper Address (MUA):** Hardware implementations supporting Queued Invalidations and Extended Interrupt Mode are required to implement this register Hardware implementations not supporting Queued Invalidations or Extended Interrupt Mode may treat this field as RsvdZ.

4.2.28 Interrupt Remapping Table Address Register (IRTA_REG_0_0_0_VTDBAR) — Offset B8h

Register providing the base address of Interrupt remapping table. This register is treated as RsvdZ by implementations reporting Interrupt Remapping (IR) as not supported in the Extended Capability register.

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + B8h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
63:12	0000000000000h RW	**Interrupt Remapping Table Address (IRTA):** This field points to the base of 4KB aligned interrupt remapping table Hardware ignores and does not implement bits 63:HAW, where HAW is the host address width Reads of this field returns value that was last programmed to it.
11	0h RW	**Extended Interrupt Mode Enable (EIME):** This field is used by hardware on Intel64 platforms as follows: • 0=xAPIC mode is active. Hardware interprets only low 8-bits of Destination-ID field in the IRTEs. The high 24-bits of the Destination-ID field are treated as reserved • 1= x2APIC mode is active. Hardware interprets all 32-bits of Destination-ID field in the IRTEs This field is implemented as RsvdZ on implementations reporting Extended Interrupt Mode (EIM) field as Clear in Extended Capability register.
10:4	0h RO	**Reserved**
3:0	0h RW	**S:** This field specifies the size of the interrupt remapping table. The number of entries in the interrupt remapping table is 2(X+1), where X is the value programmed in this field.

4.2.29 Page Request Queue Head Register (PQH_REG_0_0_0_VTDBAR) — Offset C0h

Register indicating the page request queue head. This register is treated as RsvdZ by implementations reporting Page Request Support (PRS) as not supported in the Extended Capability register.

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + C0h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
63:19	0h RO	**Reserved**
18:4	0000h RW	**Page Queue Head (PQH):** Specifies the offset (16-bytes aligned) to the page request queue for the request that will be processed next by software.
3:0	0h RO	**Reserved**

4.2.30 Page Request Queue Tail Register (PQT_REG_0_0_0_VTDBAR) — Offset C8h

Register indicating the page request queue tail. This register is treated as RsvdZ by implementations reporting Page Request Support (PRS) as not supported in the Extended Capability register.

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + C8h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
63:19	0h RO	**Reserved**
18:4	0000h RW/V	**Page Queue Tail (PQT):** Specifies the offset (16-bytes aligned) to the page request queue for the request that will be written next by hardware.
3:0	0h RO	**Reserved**

4.2.31 Page Request Queue Address Register (PQA_REG_0_0_0_VTDBAR) — Offset D0h

Register to configure the base address and size of the page request queue. This register is treated as RsvdZ by implementations reporting Page Request Support (PRS) as not supported in the Extended Capability register.

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + D0h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
63:46	0h RO	**Reserved**
45:12	00000000 0h RW	**Page Request Queue Base Address (PQA):** This field points to the base of 4KB aligned page request queue. Hardware may ignore and not implement bits 63:HAW, where HAW is the host address width. Software must configure this register before enabling page requests in any extended-context-entries.
11:3	0h RO	**Reserved**
2:0	0h RW	**Page Request Queue Size (PQS):** This field specifies the size of the page request queue. A value of X in this field indicates an invalidation request queue of (2^X) 4KB pages. The number of entries in the page request queue is 2^(X + 8)

4.2.32 Page Request Status Register (PRS_REG_0_0_0_VTDBAR) — Offset DCh

Register to report pending page request in page request queue. This register is treated as RsvdZ by implementations reporting Page Request Support (PRS) as not supported in the Extended Capability register.

Type	Size	Offset	Default
MMIO	32 bit	GFXVTBAR + DCh	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:1	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
0	0h RW/1C	**Pending Page Request (PPR):** Pending Page Request: Indicates pending page requests to be serviced by software in the page request queue. This field is Set by hardware when a streaming page request entry (page_stream_reg_dsc) or a page group request (page_grp_req_dsc) with Last Page in Group (LPG) field Set, is added to the page request queue.

4.2.33 Page Request Event Control Register (PECTL_REG_0_0_0_VTDBAR) — Offset E0h

Register specifying the page request event interrupt control bits. This register is treated as RsvdZ by implementations reporting Page Request Support (PRS) as not supported in the Extended Capability register

Type	Size	Offset	Default
MMIO	32 bit	GFXVTBAR + E0h	80000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	1h RW	**Interrupt Mask (IM):** Interrupt Mask • 0=No masking of interrupt. When a page request event condition is detected, hardware issues an interrupt message (using the Page Request Event Data and Page Request Event Address register values) • 1=This is the value on reset. Software may mask interrupt message generation by setting this field. Hardware is prohibited from sending the interrupt message when this field is Set.
30	0h RO/V	**Interrupt Pending (IP):** Interrupt Pending: Hardware sets the IP field whenever it detects an interrupt condition. Interrupt condition is defined as: • A streaming page request entry (page_stream_req_dsc) or a page group request (page_grp_req_dsc) with Last Page in Group (LPG) field Set, was added to page request queue, resulting in hardware setting the Pending Page Request (PPR) field in Page Request Status register • If the PPR field in the Page Request Event Status register was already Set at the time of setting this field, it is not treated as a new interrupt condition The IP field is kept Set by hardware while the interrupt message is held pending. The interrupt message could be held pending due to interrupt mask (IM field) being Set, or due to other transient hardware conditions. The IP field is cleared by hardware as soon as the interrupt message pending condition is serviced. This could be due to either: • Hardware issuing the interrupt message due to either change in the transient hardware condition that caused interrupt message to be held pending or due to software clearing the IM field • Software servicing the PPR field in the Page Request Event Status register.
29:0	0h RO	**Reserved**

4.2.34 Page Request Event Data Register (PEDATA_REG_0_0_0_VTDBAR) — Offset E4h

Register specifying the Page Request Event interrupt message data. This register is treated as RsvdZ by implementations reporting Page Request Support (PRS) as not supported in the Extended Capability register.

Type	Size	Offset	Default
MMIO	32 bit	GFXVTBAR + E4h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:16	0000h RW	**Extended Interrupt Message Data (EIMD):** Extended Interrupt Message Data
15:0	0000h RW	**Interrupt Message Data (IMD):** Interrupt Message Data: Data value in the interrupt request. Software requirements for programming this register are described in VTd Spec

4.2.35 Page Request Event Address Register (PEADDR_REG_0_0_0_VTDBAR) — Offset E8h

Register specifying the Page Request Event Interrupt message address. This register is treated as RsvdZ by implementations reporting Page Request Support (PRS) as not supported in the Extended Capability register.

Type	Size	Offset	Default
MMIO	32 bit	GFXVTBAR + E8h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:2	00000000h RW	**Message Address (MA):** Message Address: When fault events are enabled, the contents of this register specify the DWORD-aligned address (bits 31:2) for the interrupt request.
1:0	0h RO	**Reserved**

4.2.36 Page Request Event Upper Address Register (PEUADDR_REG_0_0_0_VTDBAR) — Offset ECh

Register specifying the Page Request Event interrupt message upper address.

Type	Size	Offset	Default
MMIO	32 bit	GFXVTBAR + ECh	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RW	**Message Upper Address (MUA):** Message Upper Address: This field specifies the upper address (bits.. 63:32) for the page request event interrupt.

4.2.37 MTRR Capability Register (MTRRCAP_0_0_0_VTDBAR) — Offset 100h

Register reporting the Memory Type Range Register Capability. This register is treated as RsvdZ by implementations reporting Memory Type Support (MTS) as not supported in the Extended Capability register.

When implemented, value reported in this register must match IA32_MTRRCAP Model Specific Register (MSR) value reported by the host IA-32 processor(s).

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + 100h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:11	0h RO	**Reserved**
10	0h RO	**Write Combining (WC):** • 0 = Write-combining (WC) memory type is not supported. • 1 = Write-combining (WC) memory type is supported.Indicates whether the Write Combining memory type is supported.
9	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
8	0h RO	**Fixed Range MTRRs Supported (FIX):** • 0 = No fixed range MTRRs are supported • 1 = Fixed range MTRRs (MTRR_FIX64K_00000 through MTRR_FIX4K_0F8000) are supported
7:0	00h RO	**Variable MTRR Count (VCNT):** Indicates number of variable range MTRRs are supported.

4.2.38 MTRR Default Type Register (MTRRDEFAULT_0_0_0_VTDBAR) — Offset 108h

Register for enabling/configuring Memory Type Range Registers. This register is treated as RsvdZ by implementations reporting Memory Type Support (MTS) as not supported in the Extended Capability register.

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + 108h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:12	0h RO	**Reserved**
11	0h RO	**MTRR Enable (E):** • 0 = Disable MTRRs; UC memory type is applied. FE field has no effect. • 1 = Enable MTRRs. FE field can disable the fixed-range MTRRs. Type specified in the default memory type field is used for areas of memory not already mapped by either fixed or variable MTRR
10	0h RO	**Fixed Range MTRR Enable (FE):** • 0 = Disable fixed range MTRRs. • 1 = Enable fixed range MTRRs. When fixed range MTRRs are enabled, they take priority over the variable range MTRRs when overlaps in ranges occur. If the fixed-range MTRRs are disabled, the variable range MTRRs can still be used and can map the range ordinarily covered by the fixed range MTRRs.
9:8	0h RO	**Reserved**
7:0	00h RO	**Default Memory Type (MEMTYPE):** Indicates default memory type used for physical memory address ranges that do not have a memory type specified for them by an MTRR. Legal values for this field are 0,1,4, 5 and 6.

4.2.39 Fixed-Range MTRR Format 64K-00000 (MTRR_FIX64K_00000_REG_0_0_0_VTDBAR) — Offset 120h

Fixed Range MTRR covering the 64K memory space from 0x00000 - 0x7FFFF.

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + 120h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:56	00h RO	**R7:** Register Field 7
55:48	00h RO	**R6:** Register Field 6
47:40	00h RO	**R5:** Register Field 5
39:32	00h RO	**R4:** Register Field 4
31:24	00h RO	**R3:** Register Field 3
23:16	00h RO	**R2:** Register Field 2
15:8	00h RO	**R1:** Register Field 1
7:0	00h RO	**R0:** Register Field 0

4.2.40 Fixed-Range MTRR Format 16K-80000 (MTRR_FIX16K_80000_REG_0_0_0_VTDBAR) — Offset 128h

Fixed Range MTRR covering the 16K memory space from 0x80000 - 0x9FFFF.

Note: Bit definitions are the same as MTRR_FIX64K_00000_REG_0_0_0_VTDBAR, offset 120h.

4.2.41 Fixed-Range MTRR Format 16K-A0000 (MTRR_FIX16K_A0000_REG_0_0_0_VTDBAR) — Offset 130h

Fixed Range MTRR covering the 16K memory space from 0xA0000 - 0xBFFFF.

Note: Bit definitions are the same as MTRR_FIX64K_00000_REG_0_0_0_VTDBAR, offset 120h.

4.2.42 Fixed-Range MTRR Format 4K-C0000 (MTRR_FIX4K_C0000_REG_0_0_0_VTDBAR) — Offset 138h

Fixed Range MTRR covering the 4K memory space 0xC0000 - 0xC7FFF.

Note: Bit definitions are the same as MTRR_FIX64K_00000_REG_0_0_0_VTDBAR, offset 120h.

4.2.43 Fixed-Range MTRR Format 4K-C8000 (MTRR_FIX4K_C8000_REG_0_0_0_VTDBAR) — Offset 140h

Fixed Range MTRR covering the 4K memory space from 0xC8000 - 0xCFFFF.

Note: Bit definitions are the same as MTRR_FIX64K_00000_REG_0_0_0_VTDBAR, offset 120h.

4.2.44 Fixed-Range MTRR Format 4K-D0000 (MTRR_FIX4K_D0000_REG_0_0_0_VTDBAR) — Offset 148h

Fixed Range MTRR covering the 4K memory space from 0xD0000 - 0xD7FFF.

Note: Bit definitions are the same as MTRR_FIX64K_00000_REG_0_0_0_VTDBAR, offset 120h.

4.2.45 Fixed-Range MTRR Format 4K-D8000 (MTRR_FIX4K_D8000_REG_0_0_0_VTDBAR) — Offset 150h

Fixed Range MTRR covering the 4K memory space from 0xD80000 - 0xDFFFF.

Note: Bit definitions are the same as MTRR_FIX64K_00000_REG_0_0_0_VTDBAR, offset 120h.

4.2.46 Fixed-Range MTRR Format 4K-E0000 (MTRR_FIX4K_E0000_REG_0_0_0_VTDBAR) — Offset 158h

Fixed Range MTRR covering the 4K memory space from 0xE0000 - 0xE7FFF.

Note: Bit definitions are the same as MTRR_FIX64K_00000_REG_0_0_0_VTDBAR, offset 120h.

4.2.47 Fixed-Range MTRR Format 4K-E8000 (MTRR_FIX4K_E8000_REG_0_0_0_VTDBAR) — Offset 160h

Fixed Range MTRR covering the 4K memory space from 0xE8000 - 0xEFFFF.

Note: Bit definitions are the same as MTRR_FIX64K_00000_REG_0_0_0_VTDBAR, offset 120h.

4.2.48 Fixed-Range MTRR Format 4K-F0000 (MTRR_FIX4K_F0000_REG_0_0_0_VTDBAR) — Offset 168h

Fixed Range MTRR covering the 4K memory space from 0xF0000 - 0xF7FFF.

Note: Bit definitions are the same as MTRR_FIX64K_00000_REG_0_0_0_VTDBAR, offset 120h.

4.2.49 Fixed-Range MTRR Format 4K-F8000 (MTRR_FIX4K_F8000_REG_0_0_0_VTDBAR) — Offset 170h

Fixed Range MTRR covering the 4K memory space from 0xF8000 - 0xFFFFF.

Note: Bit definitions are the same as MTRR_FIX64K_00000_REG_0_0_0_VTDBAR, offset 120h.

4.2.50 Variable-Range MTRR Format Physical Base 0 (MTRR_PHYSBASE0_REG_0_0_0_VTDBAR) — Offset 180h

Variable-Range MTRR BASE0

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + 180h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:12	0000000h RO	**Physical Base (PHYSBASE):** Base Address for variable memory type range 0
11:8	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
7:0	00h RO	**MEMTYPE:** Memory type for variable memory type range 0

4.2.51 Variable-Range MTRR Format Physical Mask 0 (MTRR_PHYSMASK0_REG_0_0_0_VTDBAR) — Offset 188h

Variable-Range MTRR MASK0

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + 188h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:12	0000000h RO	**Physical Mask (PHYSMASK):** Address mask for variable memory type range 0
11	0h RO	**VALID:** Valid bit for variable range 0 mask
10:0	0h RO	**Reserved**

4.2.52 Variable-Range MTRR Format Physical Base 1 (MTRR_PHYSBASE1_REG_0_0_0_VTDBAR) — Offset 190h

Variable-Range MTRR BASE1

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + 190h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
38:12	0000000h RO	**Physical Base (PHYSBASE):** Base Address for variable memory type range 1
11:8	0h RO	**Reserved**
7:0	00h RO	**MEMTYPE:** Memory type for variable memory type range 1

4.2.53 Variable-Range MTRR Format Physical Mask 1 (MTRR_PHYSMASK1_REG_0_0_0_VTDBAR) — Offset 198h

Variable-Range MTRR MASK1

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + 198h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:12	0000000h RO	**Physical Mask (PHYSMASK):** Address mask for variable memory type range 1
11	0h RO	**VALID:** Valid bit for variable range 1 mask
10:0	0h RO	**Reserved**

4.2.54 Variable-Range MTRR Format Physical Base 2 (MTRR_PHYSBASE2_REG_0_0_0_VTDBAR) — Offset 1A0h

Variable-Range MTRR BASE2

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + 1A0h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:12	0000000h RO	**Physical Base (PHYSBASE):** Base Address for variable memory type range 2
11:8	0h RO	**Reserved**
7:0	00h RO	**MEMTYPE:** Memory type for variable memory type range 2

4.2.55 Variable-Range MTRR Format Physical Mask 2 (MTRR_PHYSMASK2_REG_0_0_0_VTDBAR) — Offset 1A8h

Variable-Range MTRR MASK2

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + 1A8h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:12	0000000h RO	**Physical Mask (PHYSMASK):** Address mask for variable memory type range 2
11	0h RO	**VALID:** Valid bit for variable range 2 mask
10:0	0h RO	**Reserved**

4.2.56 Variable-Range MTRR Format Physical Base 3 (MTRR_PHYSBASE3_REG_0_0_0_VTDBAR) — Offset 1B0h

Variable-Range MTRR BASE3

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + 1B0h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:12	0000000h RO	**Physical Base (PHYSBASE):** Base Address for variable memory type range 3
11:8	0h RO	**Reserved**
7:0	00h RO	**MEMTYPE:** Memory type for variable memory type range 3

4.2.57 Variable-Range MTRR Format Physical Mask 3 (MTRR_PHYSMASK3_REG_0_0_0_VTDBAR) — Offset 1B8h

Variable-Range MTRR MASK3

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + 1B8h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:12	0000000h RO	**Physical Mask (PHYSMASK):** Address mask for variable memory type range 3
11	0h RO	**VALID:** Valid bit for variable range 3 mask
10:0	0h RO	**Reserved**

4.2.58 Variable-Range MTRR Format Physical Base 4 (MTRR_PHYSBASE4_REG_0_0_0_VTDBAR) — Offset 1C0h

Variable-Range MTRR BASE4

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + 1C0h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:12	0000000h RO	**Physical Base (PHYSBASE):** Base Address for variable memory type range 4
11:8	0h RO	**Reserved**
7:0	00h RO	**MEMTYPE:** Memory type for variable memory type range 4

4.2.59 Variable-Range MTRR Format Physical Mask 4 (MTRR_PHYSMASK4_REG_0_0_0_VTDBAR) — Offset 1C8h

Variable-Range MTRR MASK4

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + 1C8h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:12	0000000h RO	**Physical Mask (PHYSMASK):** Address mask for variable memory type range 4
11	0h RO	**VALID:** Valid bit for variable range 4 mask
10:0	0h RO	**Reserved**

4.2.60 Variable-Range MTRR Format Physical Base 5 (MTRR_PHYSBASE5_REG_0_0_0_VTDBAR) — Offset 1D0h

Variable-Range MTRR BASE5

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + 1D0h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:12	0000000h RO	**Physical Base (PHYSBASE):** Base Address for variable memory type range 5
11:8	0h RO	**Reserved**
7:0	00h RO	**MEMTYPE:** Memory type for variable memory type range 5

4.2.61 Variable-Range MTRR Format Physical Mask 5 (MTRR_PHYSMASK5_REG_0_0_0_VTDBAR) — Offset 1D8h

Variable-Range MTRR MASK5

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + 1D8h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:12	0000000h RO	**Physical Mask (PHYSMASK):** Address mask for variable memory type range 5
11	0h RO	**VALID:** Valid bit for variable range 5 mask
10:0	0h RO	**Reserved**

4.2.62 Variable-Range MTRR Format Physical Base 6 (MTRR_PHYSBASE6_REG_0_0_0_VTDBAR) — Offset 1E0h

Variable-Range MTRR BASE6

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + 1E0h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:12	0000000h RO	**Physical Base (PHYSBASE):** Base Address for variable memory type range 6
11:8	0h RO	**Reserved**
7:0	00h RO	**MEMTYPE:** Memory type for variable memory type range 6

4.2.63 Variable-Range MTRR Format Physical Mask 6 (MTRR_PHYSMASK6_REG_0_0_0_VTDBAR) — Offset 1E8h

Variable-Range MTRR MASK6

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + 1E8h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:12	0000000h RO	**Physical Mask (PHYSMASK):** Address mask for variable memory type range 6
11	0h RO	**VALID:** Valid bit for variable range 6 mask
10:0	0h RO	**Reserved**

4.2.64 Variable-Range MTRR Format Physical Base 7 (MTRR_PHYSBASE7_REG_0_0_0_VTDBAR) — Offset 1F0h

Variable-Range MTRR BASE7

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + 1F0h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:12	0000000h RO	**Physical Base (PHYSBASE):** Base Address for variable memory type range 7
11:8	0h RO	**Reserved**
7:0	00h RO	**MEMTYPE:** Memory type for variable memory type range 7

4.2.65 Variable-Range MTRR Format Physical Mask 7 (MTRR_PHYSMASK7_REG_0_0_0_VTDBAR) — Offset 1F8h

Variable-Range MTRR MASK7

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + 1F8h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:12	0000000h RO	**Physical Mask (PHYSMASK):** Address mask for variable memory type range 7
11	0h RO	**VALID:** Valid bit for variable range 7 mask
10:0	0h RO	**Reserved**

4.2.66 Variable-Range MTRR Format Physical Base 8 (MTRR_PHYSBASE8_REG_0_0_0_VTDBAR) — Offset 200h

Variable-Range MTRR BASE8

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + 200h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:12	0000000h RO	**Physical Base (PHYSBASE):** Base Address for variable memory type range 8
11:8	0h RO	**Reserved**
7:0	00h RO	**MEMTYPE:** Memory type for variable memory type range 8

4.2.67 Variable-Range MTRR Format Physical Mask 8 (MTRR_PHYSMASK8_REG_0_0_0_VTDBAR) — Offset 208h

Variable-Range MTRR MASK8

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + 208h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:12	0000000h RO	**Physical Mask (PHYSMASK):** Address mask for variable memory type range 8
11	0h RO	**VALID:** Valid bit for variable range 8 mask
10:0	0h RO	**Reserved**

4.2.68 Variable-Range MTRR Format Physical Base 9 (MTRR_PHYSBASE9_REG_0_0_0_VTDBAR) — Offset 210h

Variable-Range MTRR BASE9

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + 210h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:12	0000000h RO	**Physical Base (PHYSBASE):** Base Address for variable memory type range 9
11:8	0h RO	**Reserved**
7:0	00h RO	**MEMTYPE:** Memory type for variable memory type range 9

4.2.69 Variable-Range MTRR Format Physical Mask 9 (MTRR_PHYSMASK9_REG_0_0_0_VTDBAR) — Offset 218h

Variable-Range MTRR MASK9

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + 218h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:12	0000000h RO	**Physical Mask (PHYSMASK):** Address mask for variable memory type range 9
11	0h RO	**VALID:** Valid bit for variable range 9 mask
10:0	0h RO	**Reserved**

4.2.70 Fault Recording Register Low [0] (FRCDL_REG_0_0_0_VTDBAR) — Offset 400h

Register to record fault information when primary fault logging is active. Hardware reports the number and location of fault recording registers through the Capability register. This register is relevant only for primary fault logging

This register is sticky and can be cleared only through power good reset or by software clearing the RW1C fields by writing a 1.

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + 400h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63:12	00000000 00000h RO/V	**Fault Info (FI):** When the Fault Reason (FR) field indicates one of the DMA-remapping fault conditions, bits 63:12 of this field contain the page address in the faulted DMA request. Hardware treats bits 63:N as reserved (0), where N is the maximum guest address width (MGAW) supported When the Fault Reason (FR) field indicates one of the interrupt-remapping fault conditions, bits 63:48 of this field indicate the interrupt_index computed for the faulted interrupt request, and bits 47:12 are cleared This field is relevant only when the F field is Set.
11:0	0h RO	**Reserved**

4.2.71 Fault Recording Register High [0] (FRCDH_REG_0_0_0_VTDBAR) — Offset 408h

Register to record fault information when primary fault logging is active. Hardware reports the number and location of fault recording registers through the Capability register. This register is relevant only for primary fault logging

This register is sticky and can be cleared only through power good reset or by software clearing the RW1C fields by writing a 1.

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + 408h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
63	0h RW/1C	**F:** Hardware sets this field to indicate a fault is logged in this Fault Recording register. The F field is set by hardware after the details of the fault is recorded in other fields When this field is Set, hardware may collapse additional faults from the same source-id (SID) Software writes the value read from this field to Clear it.
62	0h RO/V	**T:** Type of the faulted request: • 0=0: Write request • 1=1: Read request or AtomicOp request This field is relevant only when the F field is Set, and when the fault reason (FR) indicates one of the DMA-remapping fault conditions.
61:60	0h RO/V	**Address Type (AT):** This field captures the AT field from the faulted DMA request Hardware implementations not supporting Device-IOTLBs (DI field Clear in Extended Capability register) treat this field as RsvdZ When supported, this field is valid only when the F field is Set, and when the fault reason (FR) indicates one of the DMA-remapping fault conditions.
59:40	00000h RO/V	**PASID Value (PV):** PASID value in the faulted request. This field is relevant only when the PP field is set. Hardware implementations not supporting PASID (PASID field Clear in Extended Capability register) implement this field as RsvdZ.
39:32	00h RO/V	**Fault Reason (FR):** Reason for the fault This field is relevant only when the F field is set.
31	0h RO/V	**PASID Present (PP):** When set, indicates the faulted request has a PASID tag. The value of the PASID field is reported in the PASID Value (PV) field. This field is relevant only when the F field is Set, and when the fault reason (FR) indicates one of the non-recoverable address translation fault conditions. Hardware implementations not supporting PASID (PASID field Clear in Extended Capability register) implement this field as RsvdZ.
30	0h RO/V	**Execute Permission Requested (EXE):** When set, indicates Execute permission was requested by the faulted read request. This field is relevant only when the PP field and T field are both Set. Hardware implementations not supporting PASID (PASID field Clear in Extended Capability register) implement this field as RsvdZ.
29	0h RO/V	**Privilege Mode Requested (PRIV):** When set, indicates Supervisor privilege was requested by the faulted request. This field is relevant only when the PP field is Set. Hardware implementations not supporting PASID (PASID field Clear in Extended Capability register) implement this field as RsvdZ.
28:16	0h RO	**Reserved**
15:0	0000h RO/V	**Source Identifier (SID):** Requester-id associated with the fault condition This field is relevant only when the F field is set.

4.2.72 Invalidate Address Register (IVA_REG_0_0_0_VTDBAR) — Offset 500h

Register to provide the DMA address whose corresponding IOTLB entry needs to be invalidated through the corresponding IOTLB Invalidate register. This register is a write-only register.

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + 500h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
63:12	0000000000000h RW	**ADDR:** Software provides the DMA address that needs to be page-selectively invalidated. To make a page-selective invalidation request to hardware, software must first write the appropriate fields in this register, and then issue the appropriate page-selective invalidate command through the IOTLB_REG. Hardware ignores bits 63:N, where N is the maximum guest address width (MGAW) supported. A value returned on a read of this field is undefined A value returned on a read of this field is undefined
11:7	0h RO	**Reserved**
6	0h RW	**Invalidation Hint (IH):** The field provides hint to hardware about preserving or flushing the non-leaf (page-directory) entries that may be cached in hardware: • 0 = Software may have modified both leaf and non-leaf page-table entries corresponding to mappings specified in the ADDR and AM fields. On a page-selective invalidation request, hardware must flush both the cached leaf and non-leaf page-table entries corresponding to the mappings specified by ADDR and AM fields. • 1 = Software has not modified any non-leaf page-table entries corresponding to mappings specified in the ADDR and AM fields. On a page-selective invalidation request, hardware may preserve the cached non-leaf page-table entries corresponding to mappings specified by ADDR and AM fields. A value returned on a read of this field is undefined
5:0	00h RW	**Address Mask (AM):** The value in this field specifies the number of low order bits of the ADDR field that must be masked for the invalidation operation. This field enables software to request invalidation of contiguous mappings for size-aligned regions. For example:..Mask ADDR bits Pages..Value masked invalidated.. 0 None 1.. 1 12 2.. 2 13:12 4.. 3 14:12 8.. 4 15:12 16 When invalidating mappings for super-pages, software must specify the appropriate mask value. For example, when invalidating mapping for a 2MB page, software must specify an address mask value of at least 9...Hardware implementations report the maximum supported mask value through the Capability register.

4.2.73 IOTLB Invalidate Register (IOTLB_REG_0_0_0_VTDBAR) — Offset 508h

Register to invalidate IOTLB. The act of writing the upper byte of the IOTLB_REG with IVT field Set causes the hardware to perform the IOTLB invalidation.

Type	Size	Offset	Default
MMIO	64 bit	GFXVTBAR + 508h	0200000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
63	0h RW/V	**Invalidate IOTLB (IVT):** Software requests IOTLB invalidation by setting this field. Software must also set the requested invalidation granularity by programming the IIRG field Hardware clears the IVT field to indicate the invalidation request is complete. Hardware also indicates the granularity at which the invalidation operation was performed through the IAIG field. Software must not submit another invalidation request through this register while the IVT field is Set, nor update the associated Invalidate Address register Software must not submit IOTLB invalidation requests when there is a context-cache invalidation request pending at this remapping hardware unit. Hardware implementations reporting write-buffer flushing requirement (RWBF=1 in Capability register) must implicitly perform a write buffer flushing before invalidating the IOTLB.
62	0h RO	**Reserved**
61:60	0h RW	**IOTLB Invalidation Request Granularity (IIRG):** When requesting hardware to invalidate the IOTLB (by setting the IVT field), software writes the requested invalidation granularity through this field. The following are the encodings for the field • 00 = Reserved • 01 = Global invalidation request • 10 = Domain-selective invalidation request. The target domain-id must be specified in the DID field • 11 = Page-selective invalidation request. The target address, mask and invalidation hint must be specified in the Invalidate Address register, and the domain-id must be provided in the DID field Hardware implementations may process an invalidation request by performing invalidation at a coarser granularity than requested. Hardware indicates completion of the invalidation request by clearing the IVT field. At this time, the granularity at which actual invalidation was performed is reported through the IAIG field
59	0h RO	**Reserved**
58:57	1h RO/V	**IOTLB Actual Invalidation Granularity (IAIG):** Hardware reports the granularity at which an invalidation request was processed through this field when reporting invalidation completion (by clearing the IVT field). The following are the encodings for this field • 00 = Reserved. This indicates hardware detected an incorrect invalidation request and ignored the request. Examples of incorrect invalidation requests include detecting an unsupported address mask value in Invalidate Address register for page-selective invalidation requests • 01 = Global Invalidation performed. This could be in response to a global, domain-selective, or page-selective invalidation request • 10 = Domain-selective invalidation performed using the domain-id specified by software in the DID field. This could be in response to a domain-selective or a page-selective invalidation request • 11 = Domain-page-selective invalidation performed using the address, mask and hint specified by software in the Invalidate Address register and domain-id specified in DID field. This can be in response to a page-selective invalidation request.

Bit Range	Default & Access	Field Name (ID): Description
56:50	0h RO	**Reserved**
49	0h RW	**Drain Reads (DR):** This field is ignored by hardware if the DRD field is reported as clear in the Capability register. When the DRD field is reported as Set in the Capability register, the following encodings are supported for this field: • 0 = Hardware may complete the IOTLB invalidation without draining any translated DMA read requests • 1 = Hardware must drain DMA read requests.
48	0h RW	**Drain Writes (DW):** This field is ignored by hardware if the DWD field is reported as Clear in the Capability register. When the DWD field is reported as Set in the Capability register, the following encodings are supported for this field: • 0 = Hardware may complete the IOTLB invalidation without draining DMA write requests • 1 = Hardware must drain relevant translated DMA write requests.
47:32	0000h RW	**DID:** Indicates the ID of the domain whose IOTLB entries need to be selectively invalidated. This field must be programmed by software for domain-selective and page-selective invalidation requests. The Capability register reports the domain-id width supported by hardware. Software must ensure that the value written to this field is within this limit. Hardware ignores and not implements bits 47:(32+N), where N is the supported domain-id width reported in the Capability register.
31:0	0h RO	**Reserved**

5 Dynamic Power Performance Management Registers (D4:F0)

This chapter documents the registers in Bus: 0, Device 4, Function 0.

Note: These registers apply to all processors.

Table 5-1. Summary of Bus: 0, Device: 4, Function: 0 Registers

Offset	Size (Bytes)	Register Name (Register Symbol)	Default Value
0h	2	Vendor ID (VID_0_4_0_PCI)	8086h
2h	2	Device ID (DID_0_4_0_PCI)	8A03h
4h	2	PCI Command (PCICMD_0_4_0_PCI)	0000h
6h	2	PCI Status (PCISTS_0_4_0_PCI)	0090h
8h	1	Revision ID (RID_0_4_0_PCI)	00h
9h	1	Class Code (CC_0_4_0_PCI)	00h
Ah	2	Extended Class Code (CC_0_4_0_NOPI_PCI)	1180h
Ch	1	Cache Line Size Register (CLS_0_4_0_PCI)	00h
Dh	1	Master Latency Timer (MLT_0_4_0_PCI)	00h
Eh	1	Header Type (HDR_0_4_0_PCI)	00h
Fh	1	Built In Self Test (BIST_0_4_0_PCI)	00h
10h	8	Thermal Controller Base Address (TMBAR_0_4_0_PCI)	0000000000000004h
2Ch	2	Subsystem Vendor ID (SVID_0_4_0_PCI)	0000h
2Eh	2	Subsystem ID (SID_0_4_0_PCI)	0000h
34h	1	Capability Pointer (CAPPOINT_0_4_0_PCI)	90h
3Ch	1	Interrupt Line Register (INTRLINE_0_4_0_PCI)	00h
3Dh	1	Interrupt Pin Register (INTRPIN_0_4_0_PCI)	01h
3Eh	1	Minimum Guaranteed (MINGNT_0_4_0_PCI)	00h
3Fh	1	Maximum Latency (MAXLAT_0_4_0_PCI)	00h
54h	4	Device Enable (DEVEN_0_4_0_PCI)	0000F49Fh
E4h	4	Capabilities A (CAPID0_A_0_4_0_PCI)	00000000h
E8h	4	Capabilities B (CAPID0_B_0_4_0_PCI)	00000000h

5.1 Vendor ID (VID_0_4_0_PCI) — Offset 0h

This register combined with the Vendor Identification register uniquely identifies any PCI

device.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:4, F:0] + 0h	8086h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
15:0	8086h RO	**VID:** PCI standard identification for Intel.

5.2 Device ID (DID_0_4_0_PCI) — Offset 2h

This register combined with the Device Identification register uniquely identifies any PCI

device.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:4, F:0] + 2h	8A03h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:0	8A03h RW/V/L	**DID:** Identifier assigned to the Thermal Management Controller.

5.3 PCI Command (PCICMD_0_4_0_PCI) — Offset 4h

This register provides basic control over the DTT devices ability to respond to PCI cycles.

The PCICMD Register in the DTT disables the DTT PCI compliant master accesses to main memory.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:4, F:0] + 4h	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:11	0h RO	**Reserved**
10	0h RW	**INTDIS:** This bit, when set, disables the device from asserting INTA#.
9	0h RO	**FB2B:** The DTT device does not implement this bit and it is hardwired to a 0.
8	0h RO	**SERRE:** The DTT device does not implement this bit and it is hardwired to a 0.
7	0h RO	**ADSTEP:** The DTT device does not implement this bit and it is hardwired to a 0.
6	0h RO	**PERRE:** This bit is hardwired to 0. The DTT Device belongs to the category of devices that does not corrupt programs or data in system memory or hard drives. It therefore ignores any parity error that it detects and continues with normal operation.
5	0h RO	**VGASNOOP:** The DTT device does not implement this bit and it is hardwired to a 0.
4	0h RO	**MWIE:** This bit is hardwired to 0. The DTT Device will never issue memory write and invalidate commands, and therefore has no need to implement this bit.
3	0h RO	**SCE:** The DTT device does not implement this bit and it is hardwired to a 0.
2	0h RW	**BME:** The DTT Device is enabled to function as a PCI-compliant bus master when this bit is set. If it is not set, bus mastering is disabled.
1	0h RW	**MAE:** The DTT Device will allow access to thermal registers when this bit is set. If it is not set, access to memory mapped thermal registers is disabled.
0	0h RO	**IOAE:** The DTT device does not implement this bit and it is hardwired to a 0.

5.4 PCI Status (PCISTS_0_4_0_PCI) — Offset 6h

PCISTS is a 16-bit status register that reports the occurrence of a PCI compliant Master Abort (MA) and PCI compliant Target Abort (TA).

PCISTS also indicates the DEVSEL# timing that has been set by the DTT Device.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:4, F:0] + 6h	0090h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15	0h RO	**DPE:** The DTT device does not implement this bit and it is hardwired to a 0.
14	0h RO	**SSE:** This bit is hardwired to zero. The DTT Device never asserts SERR#, and therefore it has no need to implement this bit.
13	0h RO	**RURS:** The DTT device does not implement this bit and it is hardwired to a 0.
12	0h RO	**RCAS:** The DTT device does not implement this bit and it is hardwired to a 0.
11	0h RO	**STAS:** This bit is hardwired to 0. The DTT Device will not generate a Target Abort DMI completion packet or Special Cycle, and therefore it has no need to implement this bit.
10:9	0h RO	**DEVT:** These bits are hardwired to 0. Device 4 does not physically connect to PCI_A.
8	0h RO	**DPD:** This bit is hardwired to 0. PERR signaling and messaging are not implemented by the DTT Device, and therefore it has no need to implement this bit.
7	1h RO	**FB2B:** This bit is hardwired to 1. Device 4 does not physically connect to PCI_A, so this bit is set to 1 (indicating fast back-to-back capability) so that the optimum setting for PCI_A is not limited by the DTT Device.
6	0h RO	**Reserved**
5	0h RO	**PCI66M:** The DTT device does not implement this bit and it is hardwired to a 0.
4	1h RO	**CLIST:** This bit is set to 1 to indicate that the register at 34h provides an offset into the function. PCI Configuration Space containing a pointer to the location of the first item in the list.
3	0h RW/V/L	**IS:** Reflects the state of the INTA# signal at the input of the enable/disable circuit. This bit is set by HW to 1 when the INTA# is asserted and reset by HW to 0 after the interrupt is cleared (independent of the state of the Interrupt Disable bit in the 0.4.0.PCICMD register).
2:0	0h RO	**Reserved**

5.5 Revision ID (RID_0_4_0_PCI) — Offset 8h

This register contains the revision number of the DTT Device.

This is an 8-bit value that indicates the revision identification number for the device.

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:4, F:0] + 8h	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
7:4	0h RW/L	**Revision ID Upper Bits (RID_MSB):** DTT device Revision ID 4 upper bits.
3:0	0h RW/L	**Revision ID Lower Bits (RID):** DTT device Revision ID 4 lower bits.

5.6 Class Code (CC_0_4_0_PCI) — Offset 9h

This register contains the device programming interface information related to the Sub-Class Code and

Base Class Code definition for the DTT Device. This register also contains the Base Class Code and the

function sub-class in relation to the Base Class Code.

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:4, F:0] + 9h	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:0	00h RO	**PI:** This is an 8-bit value that indicates the programming interface of this device. This value does not specify a particular register set layout and provides no practical use for this device.

5.7 Extended Class Code (CC_0_4_0_NOPI_PCI) — Offset Ah

This register contains the device programming interface information related to the Sub-Class Code and Base Class Code definition for the DTT Device.

This register also contains the Base Class Code and the function sub-class in relation to the Base Class Code.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:4, F:0] + Ah	1180h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
15:8	11h RO	**BCC:** This is an 8-bit value that indicates the base class code for the DTT Thermal Controller. This code has the value 11h, indicating a device that is used for data acquisition and signal processing.
7:0	80h RO	**SUBCC:** The code is 80h which indicates Other Data Acquisition and Signal Processing Controllers.

5.8 Cache Line Size Register (CLS_0_4_0_PCI) — Offset Ch

The DTT Device does not support this register as a PCI slave.

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:4, F:0] + Ch	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:0	00h RO	**CLS:** This field is hardwired to 0. The DTT as a PCI compliant master does not use the Memory Write and Invalidate command and, in general, does not perform operations based on cache line size.

5.9 Master Latency Timer (MLT_0_4_0_PCI) — Offset Dh

The DTT Device does not support the programmability of the master latency timer because it does

not perform bursts.

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:4, F:0] + Dh	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:0	00h RO	**MLT:** This field is hardwired to 0. The DTT Device does not support perform bursts.

5.10 Header Type (HDR_0_4_0_PCI) — Offset Eh

This register identifies the header layout of the configuration space. No physical register exists at

this location.

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:4, F:0] + Eh	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:0	00h RO	**HDR:** This field always returns 0 to indicate that the DTT device is a single function device with standard header layout.

5.11 Built In Self Test (BIST_0_4_0_PCI) — Offset Fh

This register is used for control and status of Built In Self Test (BIST).

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:4, F:0] + Fh	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7	0h RO	**BS:** This bit is hardwired to zero. The DTT Device does not support BIST.
6:0	0h RO	**Reserved**

5.12 Thermal Controller Base Address (TMBAR_0_4_0_PCI) — Offset 10h

This is the base address for the Thermal Controller Memory Mapped space. There is no physical memory

within this 32KB window that can be addressed. The 32KB reserved by this register does not alias to any PCI 2.2

compliant memory mapped space. All TMBAR space maps the access to this memory space towards MCHBAR space. For

details of this BAR, refer to the MCHBAR specifications.

Type	Size	Offset	Default
PCI	64 bit	[B:0, D:4, F:0] + 10h	0000000000000004h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
63:39	0h RO	**Reserved**
38:16	000000h RW	**TMMBA:** This field corresponds to bits 38 to 16 of the base address TMBAR address space. BIOS will program this register resulting in a base address for a 64KB block of contiguous memory address space. This register ensures that a naturally aligned 64KB space is allocated within total addressable memory space. The DTT driver uses this base address to program all Thermal and Throttling control register set.

Bit Range	Default & Access	Field Name (ID): Description
15	0h RO	**Reserved**
14:4	000h RO	**ADM:** Hardwired to 0s to indicate at least 32KB address range.
3	0h RO	**PM:** Hardwired to 0 to prevent prefetching.
2:1	2h RO	**MT:** Hardwired to 10 to indicate 64-bit address.
0	0h RO	**MIOS:** Hardwired to 0 to indicate memory space.

5.13 Subsystem Vendor ID (SVID_0_4_0_PCI) — Offset 2Ch

This value is used to identify the vendor of the subsystem.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:4, F:0] + 2Ch	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:0	0000h RW/L	**SUBVID:** This field should be programmed during boot-up to indicate the vendor of the system board. After it has been written once, it becomes read only. **Locked by:** WRITE_ONCE_LOCK.SUBVID_WOL

5.14 Subsystem ID (SID_0_4_0_PCI) — Offset 2Eh

This value is used to identify a particular subsystem.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:4, F:0] + 2Eh	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:0	0000h RW/L	**SUBID:** This field should be programmed during BIOS initialization. After it has been written once, it becomes read only. **Locked by:** WRITE_ONCE_LOCK.SUBID_WOL

5.15 Capability Pointer (CAPPOINT_0_4_0_PCI) — Offset 34h

CAPPOINT provides the offset that is the pointer to the location of the first device capability in

the capability list.

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:4, F:0] + 34h	90h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
7:0	90h RW/V/L	**CAPPV:** This field contains an offset into the functions PCI Configuration Space for the first item in the New Capabilities Linked List which is the MSI Capabilities ID register at address 90h or the Power Management Capabilities ID registers at address D0h. The value is determined by CAPL[0].

5.16 Interrupt Line Register (INTRLINE_0_4_0_PCI) — Offset 3Ch

Used to communicate interrupt line routing information.

BIOS Requirement: POST software writes the routing information into this register as it initializes and configures the system.

The value indicates to which input of the system interrupt controller this devices interrupt pin is connected.

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:4, F:0] + 3Ch	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
7:0	00h RW	**INTCON:** Used to communicate interrupt line routing information. BIOS Requirement: POST software writes the routing information into this register as it initializes and configures the system. The value indicates to which input of the system interrupt controller this devices interrupt pin is connected.

5.17 Interrupt Pin Register (INTRPIN_0_4_0_PCI) — Offset 3Dh

This register specifies which interrupt pin this device uses.

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:4, F:0] + 3Dh	01h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:0	01h RO	**INTPIN:** As a single function device, the DTT device specifies INTA as its interrupt pin. 01h = INTA.

5.18 Minimum Guaranteed (MINGNT_0_4_0_PCI) — Offset 3Eh

This register is hardwired to zero.

The DTT Device does not burst as a PCI compliant master.

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:4, F:0] + 3Eh	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:0	00h RO	**MGV:** These bits are hardwired to zero. The DTT Device does not burst as a PCI compliant master.

5.19 Maximum Latency (MAXLAT_0_4_0_PCI) — Offset 3Fh

This register are hardwired to zero.

The DTT Device has no specific requirements for how often it needs to access the PCI bus.

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:4, F:0] + 3Fh	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:0	00h RO	**MLV:** These bits are hardwired to zero. The DTT Device has no specific requirements for how often it needs to access the PCI bus.

5.20 Device Enable (DEVEN_0_4_0_PCI) — Offset 54h

Allows for enabling/disabling of PCI devices and functions that are within the CPU package. The table below the bit definitions describes the behavior of all combinations of transactions to devices controlled by this register. All the bits in this register are Intel TXT Lockable.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:4, F:0] + 54h	0000F49Fh

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:16	0h RO	**Reserved**
15	1h RW/L	**D8EN:** 0: Bus 0 Device 8 is disabled and not visible. 1: Bus 0 Device 8 is enabled and visible. This bit will be set to 0b and remain 0b if Device 8 capability is disabled. **Locked by:** CAPID0_B_0_0_0_PCI.GMM_DIS
14	1h RW/L	**D14F0EN:** VMD Enable - 0: Bus 0 Device 14 Function 0 is disabled and hidden. 1: Bus 0 Device 14 Function 0 is enabled and visible. **Locked by:** CAPID0_B_0_0_0_PCI.VMD_DIS
13	1h RW/L	**D6EN:** 0: Bus 0 Device 6 Function 0 is disabled and not visible. 1: Bus 0 Device 6 Function 0 is enabled and visible. This bit will be set to 0b and remain 0b if Device 6 Function 0 capability is disabled. **Locked by:** CAPID0_A_0_0_0_PCI.PEG60D
12	1h RW/L	**D9EN:** 0: Bus 0 Device 9 is disabled and not visible. 1: Bus 0 Device 9 is enabled and visible. This bit will be set to 0b and remain 0b if Device 9 capability is disabled. **Locked by:** CAPID0_B_0_0_0_PCI.NPK_DIS
11	0h RO	**Reserved**
10	1h RW/L	**D5EN:** 0: Bus 0 Device 5 is disabled and not visible. 1: Bus 0 Device 5 is enabled and visible. This bit will be set to 0b and remain 0b if Device 5 capability is disabled. **Locked by:** CAPID0_B_0_0_0_PCI.IMGU_DIS
9:8	0h RO	**Reserved**
7	1h RW/L	**D4EN:** 0: Bus 0 Device 4 is disabled and not visible. 1: Bus 0 Device 4 is enabled and visible. This bit will be set to 0b and remain 0b if Device 4 capability is disabled. **Locked by:** CAPID0_A_0_0_0_PCI.CDD
6:5	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
4	1h RW/L	**D2EN:** 0: Bus 0 Device 2 is disabled and hidden 1: Bus 0 Device 2 is enabled and visible This bit will be set to 0b and remain 0b if Device 2 capability is disabled. **Locked by:** CAPID0_A_0_0_0_PCI.IGD
3	1h RW/L	**D1F0EN:** 0: Bus 0 Device 1 Function 0 is disabled and hidden. 1: Bus 0 Device 1 Function 0 is enabled and visible. This bit will be set to 0b and remain 0b if PEG10 capability is disabled. **Locked by:** CAPID0_A_0_0_0_PCI.PEG10D
2	1h RW/L	**D1F1EN:** 0: Bus 0 Device 1 Function 1 is disabled and hidden. 1: Bus 0 Device 1 Function 1 is enabled and visible. **Locked by:** CAPID0_A_0_0_0_PCI.PEG11D
1	1h RW/L	**D1F2EN:** 0: Bus 0 Device 1 Function 2 is disabled and hidden. 1: Bus 0 Device 1 Function 2 is enabled and visible. **Locked by:** CAPID0_A_0_0_0_PCI.PEG12D
0	1h RO	**D0EN:** Bus 0 Device 0 Function 0 may not be disabled and is therefore hardwired to 1.

5.21 Capabilities A (CAPID0_A_0_4_0_PCI) — Offset E4h

Processor capability enumeration

.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:4, F:0] + E4h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RW/L	**NVME Disabled (NVME_DIS):** 0: NVMe Enabled 1: NVMe Disabled
30	0h RW/L	**PCIe Device 1 Function 2 Disable (PEG12D):** 0: Device 1 Function 2 and associated memory spaces are accessible. 1: Device 1 Function 2 and associated memory and IO spaces are disabled by hardwiring the D1F2EN field, bit 1 of the Device Enable register, (DEVEN Dev 0 Offset 54h) to 0.

Bit Range	Default & Access	Field Name (ID): Description
29	0h RW/L	**PCIe Device 1 Function 1 Disable (PEG11D):** 0: Device 1 Function 1 and associated memory spaces are accessible. 1: Device 1 Function 1 and associated memory and IO spaces are disabled by hardwiring the D1F1EN field, bit 2 of the Device Enable register, (DEVEN Dev 0 Offset 54h) to 0.
28	0h RW/L	**PCIe Device 1 Function 0 Disable (PEG10D):** 0: Device 1 Function 0 and associated memory spaces are accessible. 1: Device 1 Function 0 and associated memory and IO spaces are disabled by hardwiring the D1F0EN field, bit 3 of the Device Enable register, (DEVEN Dev 0 Offset 54h) to 0.
27	0h RW/L	**PCIe Link Width Up-config Disable (PELWUD):** 0: Link width upconfig is supported. The Processor advertises upconfig capability using the data rate symbol in its TS2 training ordered sets during Configuration.Complete. The CPU responds to link width upconfigs initiated by the downstream device. 1: Link width upconfig is NOT supported. The Processor does not advertise upconfig capability using the data rate field in TS2 training ordered sets during Configuration.Complete. The CPU does not respond to link width upconfigs initiated by the downstream device.
26	0h RW/L	**DMI Width (DW):** 0: DMI x4 1: DMI x2
25	0h RW/L	**DRAM ECC Disable (ECCDIS):** 0: ECC is supported 1: ECC is not supported
24	0h RW/L	**Force DRAM ECC Enable (FDEE):** 0: DRAM ECC optional via software. 1: DRAM ECC enabled. MCHBAR C0MISCCTL bit [0] and C1MISCCTL bit [0] are forced to 1 and Read-Only. Note that FDEE and ECCDIS must not both be set to 1.
23	0h RW/L	**VT-d Disable (VTDD):** 0: VT-d is supported 1: VT-d is not supported
22	0h RW/L	**DMI GEN2 Disable (DMIG2DIS):** 0: Capable of running DMI in Gen 2 mode 1: Not capable of running DMI in Gen 2 mode
21	0h RW/L	**PCIe Controller Gen 2 Disable (PEGG2DIS):** 0: Capable of running any of the PEG controllers in Gen 2 mode 1: Not capable of running any of the PEG controllers in Gen 2 mode
20:19	0h RW/L	**DRAM Maximum Size per Channel (DDRSZ):** This field defines the maximum allowed memory size per channel. • 0: Unlimited (64GB per channel) • 1: Maximum 8GB per channel • 2: Maximum 4GB per channel • 3: Maximum 2GB per channel
18	0h RO	**Reserved**
17	0h RW/L	**DRAM 1N Timing Disable (D1NM):** 0: Part is capable of supporting 1n mode timings on the DDR interface. 1: Part is not capable of supporting 1n mode. Only supported timings are 2n or greater.
16	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
15	0h RW/L	**DTT Device Disable (CDD):** 0: DTT Device enabled. 1: DTT Device disabled.
14	0h RW/L	**2 DIMMs Per Channel Enable (DDPCD):** Allows Dual Channel operation but only supports 1 DIMM per channel. 0: 2 DIMMs per channel enabled 1: 2 DIMMs per channel disabled. This setting hardwires bits 2 and 3 of the rank population field for each channel to zero. (MCHBAR offset 260h, bits 22-23 for channel 0 and MCHBAR offset 660h, bits 22-23 for channel 1)
13	0h RW/L	**X2APIC Enable (X2APIC_EN):** Extended Interrupt Mode. 0b: Hardware does not support Extended APIC mode. 1b: Hardware supports Extended APIC mode.
12	0h RW/L	**Dual Memory Channel Support (PDCD):** 0: Capable of Dual Channel 1: Not Capable of Dual Channel - only single channel capable.
11	0h RW/L	**Internal Graphics Disable (IGD):** 0: There is a graphics engine within this CPU. Internal Graphics Device (Device 2) is enabled and all of its memory and I/O spaces are accessible. Configuration cycles to Device 2 will be completed within the CPU. All non-SMM memory and IO accesses to VGA will be handled based on Memory and IO enables of Device 2 and IO registers within Device 2 and VGA Enable of the PCI to PCI bridge control register in Devices 1 and 6 (If PCI Express GFX attach is supported). A selected amount of Graphics Memory space is pre-allocated from the main memory based on Graphics Mode Select (GMS in the GGC Register). Graphics Memory is pre-allocated above TSEG Memory. 1: There is no graphics engine within this CPU. Internal Graphics Device (Device 2) and all of its memory and I/O functions are disabled. Configuration cycle targeted to Device 2 will be passed on to DMI. In addition, all clocks to internal graphics logic are turned off. All non-SMM memory and IO accesses to VGA will be handled based on VGA Enable of the PCI to PCI bridge control register in Devices 1 and 6. DEVEN [4:3] (Device 0, offset 54h) have no meaning. Device 2 Functions 0 and 1 are disabled and hidden.
10	0h RW/L	**DID0 Override Enable (DID0OE):** 0: Disable ability to override DID0 - For production 1: Enable ability to override DID - For debug and samples only
9:8	0h RO	**Reserved**
7:4	0h RW/L	**Compatibility Revision ID (CRID):** Compatibility Revision ID
3	0h RW/L	**Memory Overclocking (DDR_OVERCLOCK):** Memory Overclocking support 0: Memory Overclocking is not supported 1: Memory Overclocking is supported
2:0	0h RO	**Reserved**

5.22 Capabilities B (CAPID0_B_0_4_0_PCI) — Offset E8h

Processor capability enumeration

.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:4, F:0] + E8h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RW/L	**Image Processing Unit (IPU) Disable (IPU_DIS):** 0: Device 5 associated memory spaces are accessible. 1: Device 5 associated memory and IO spaces are disabled by hardwiring the D1F2EN field, bit 1 of the Device Enable register, (DEVEN Dev 0 Offset 54h) to 0.
30	0h RW/L	**Processor Trace Disable (PT_DIS):** 0: Processor Trace associated memory spaces are accessible. 1: Processor Trace associated memory and IO spaces are disabled by hardwiring the D1F2EN field, bit 1 of the Device Enable register, (DEVEN Dev 0 Offset 54h) to 0.
29	0h RW/L	**Overclocking Enabled (OC_ENABLED):** 0: Overclocking is Disabled 1: Overclocking is Enabled If overclocking is enabled, MSR FLEX_RATIO.OC_BINS contains how many bits of over-clocking are supported. The encoding is as follows: 0: Overclocking is Disabled 1-6: Turbo ratio limits can be incremented by this amount 7: Unlimited If overclocking is disabled, FLEX_RATIO.OC_BINS is meaningless.
28	0h RW/L	**SMT Capability (SMT):** This setting indicates whether the processor is SMT (HyperThreading) capable.
27:25	0h RW/L	**Cache Size (CACHESZ):** This setting indicates the supporting cache sizes.
24	0h RW/L	**SVM Disable (SVM_DISABLE):** 0: SVM enabled 1: SVM disabled
23:21	0h RW/L	**Memory 100MHz Reference Clock (PLL_REF100_CFG):** DDR Maximum Frequency Capability with 100MHz memory reference clock (ref_clk). 0: 100 MHz memory reference clock is not supported 1-6: Reserved 7: Unlimited
20	0h RW/L	**PCIe Gen 3 Disable (PEGG3_DIS):** 0: Capable of running any of the Gen 3-compliant PCIe controllers in Gen 3 mode (Devices 0/1/0, 0/1/1, 0/1/2, 0/6/0) 1: Not capable of running any of the PCIe controllers in Gen 3 mode
19	0h RW/L	**Processor Package Type (PKGTYP):** This setting indicates the CPU Package Type.
18	0h RW/L	**Additive Graphics Enabled (ADDGFXEN):** 0: Additive Graphics is disabled 1: Additive Graphics is enabled
17	0h RW/L	**Additive Graphics Capability Disable (ADDGFXCAP):** 0: Capable of Additive Graphics 1: Not capable of Additive Graphics

Bit Range	Default & Access	Field Name (ID): Description
16	0h RW/L	**PCIe x16 Disable (PEGX16D):** 0: Capable of x16 PCIe Port 1: Not Capable of x16 PCIe port, instead PCIe limited to x8 and below. Causes PCIe port to enable and train logical lanes 7:0 only. Logical lanes 15:8 are powered down (unless in use by the other PEG port or the embedded Display Port), and the Max Link Width field of the Link Capability register reports x8 instead of x16. (In the case of lane reversal, lanes 15:8 are active and lanes 7:0 are powered down.)
15	0h RW/L	**DMI Gen 3 Disable (DMIG3DIS):** DMI Gen 3 Disable
14:12	0h RW/L	**2 Level Memory Technology Support (LTECH):** 0: 1LM 1: EDRAM0 3: EDRAM0+1 4: 2LM Other values are reserved.
11	0h RW/L	**HDCP Disable (HDCPD):** 0: Capable of HDCP 1: HDCP Disabled
10:9	0h RO	**Reserved**
8	0h RW/L	**GNA (GMM) Disable (GNA_DIS):** 0: Device 8 associated memory spaces are accessible. 1: Device 8 associated memory and IO spaces are disabled by hardwiring the D8EN field, bit 1 of the Device Enable register, (DEVEN Dev 0 Offset 54h) to 0.
7	0h RW/L	**DDD:** 0: Debug mode 1: Production mode
6:4	0h RO	**Reserved**
3	0h RW/L	**S/H OPI Enable (SH_OPI_EN):** Specifies if OPI or DMI are enabled for S/H models. 0: DMI is enabled 1: OPI is enabled
2	0h RW/L	**VMD Disable (VMD_DIS):** Indicates if VMD is disabled.
1	0h RW/L	**Global Single PCIe Lane (DPEGFX1):** This bit has no effect on Device 1 unless Device 1 is configured for at least two ports via PEG0CFGSEL strap. 0: All PCIe port widths do not depend on their respective BCTRL[VGAEN]. 1: Each PCIe port width is limited to x1 operation when its respective BCTRL[VGAEN] is set to 1b.
0	0h RW/L	**Single PCIe Lane (SPEGFX1):** This bit has no effect on Device 1 unless Device 1 is configured for a single port via PEG0CFGSEL strap. 0: Device 1 Function 0 width does not depend on its BCTRL[VGAEN]. 1: Device 1 Function 0 width is limited to x1 operation when its respective BCTRL[VGAEN] is set to 1.

6 Image Processing Unit Registers (D5:F0)

This chapter documents the registers in Bus: 0, Device 5, Function 0.

Note: These registers apply to all processors.

Table 6-1. Summary of Bus: 0, Device: 5, Function: 0 Registers

Offset	Size (Bytes)	Register Name (Register Symbol)	Default Value
0h	4	Vendor ID and Device ID (VID_DID)	00008086h
4h	4	Command and Status (PCICMD_PCISTS)	00100000h
8h	4	Revision ID and Class Code (RID_CC)	04800000h
Ch	4	Cache Line Size, Master Latency Timer, Header Type and BIST (CLS_MLT_HT_BIST)	00000000h
10h	4	ISPMMADR LSB (ISPMMADR_LOW)	00000004h
14h	4	ISPMMADR MSB (ISPMMADR_HIGH)	00000000h
2Ch	4	Subsystem Vendor ID and Subsystem ID (SVID_SID)	00000000h
34h	4	Capabilities Pointer (CAPPOINT)	00000070h
3Ch	4	Interrupt Properties (INTR)	00000100h
70h	4	PCIe Capabilities (PCIECAPHDR_PCIECAP)	0092AC10h
74h	4	Device Capabilities (DEVICECAP)	10008000h
78h	4	Device Capabilities and Control (DEVICECTL_DEVICESTS)	00000000h
ACh	4	MSI Capabilities and MSI Control (MSI_CAPID)	0080D005h
B0h	4	MSI Address Low (MSI_ADDRESS_LO)	00000000h
B4h	4	MSI Address High (MSI_ADDRESS_HI)	00000000h
B8h	4	MSI Data (MSI_DATA)	00000000h
D0h	4	Power Management Capabilities (PMCAP)	00030001h
D4h	4	Power Management Control and Status (PMCS)	00000008h
F0h	4	IPUVTDBAR Base Address Register (IPUVTDBAR_LOW)	00000000h
F4h	4	IPUVTDBAR Base Address Register (IPUVTDBAR_HIGH)	00000000h

6.1 Vendor ID and Device ID (VID_DID) — Offset 0h

VID_DID - Vendor ID and Device ID Register

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:5, F:0] + 0h	00008086h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:16	0000h RO/V	**Device ID (DID):** Device Identification Number.
15:0	8086h RO	**Vendor ID (VENDOR_ID):** Vendor Identification Number (VID): PCI standard identification for Intel.

6.2 Command and Status (PCICMD_PCISTS) — Offset 4h

Command and Status Register

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:5, F:0] + 4h	00100000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RO	**Reserved**
30	0h RO/V	**SERR Status (SERR_STS):** SERR status
29	0h RW/1C/V	**RMA:** Received Master Abort (MA): Set when IUNIT receive UR
28	0h RW/1C/V	**RTA:** Received Target Abort (RTA): Set when IUNIT receive CA
27	0h RW/1C/V	**STA:** Signaled Target Abort (STA): Set when IUNIT receive P/NP transaction which is CA
26:21	0h RO	**Reserved**
20	1h RO	**Capability List (CAP):** Indicates that the CAPPOINT register at 34h provides an offset into PCI Configuration Space containing a pointer to the location of the first item in the list.

Bit Range	Default & Access	Field Name (ID): Description
19	0h RO/V	**Interrupt Status (IS):** Reflects the state of the interrupt in the camera device. Is set to 1 if IER and IIR are both set. Otherwise is set to 0.
18:11	0h RO	**Reserved**
10	0h RW	**Interrupt Disable (INTA_DISABLE):** When set, blocks the sending of ASSERT_INTA and DEASSERT_INTA messages to the Intel Legacy Block (ILB). The interrupt status is not blocked from being reflected in PCICMDSTS.IS. When 0, permits the sending of ASSERT_INTA and DEASSERT_INTA messages to the ILB.
9	0h RW	**Fast Back To Back Enable (FASTB2B):** Hardwired to 0
8	0h RW	**SERR Reporting Enable (SERR_EN):** SERR Reporting Enable.
7	0h RO	**Reserved**
6	0h RW	**Parity Error (PARITY_ERR):** Parity Error Reporting Enable.
5	0h RW	**VGA Snoop (VGA_SNP):** Not applicable to internal IIO devices. Hardwired to 0.
4	0h RW	**Memory Write and Invalidate Enable (MWRINV):** Memory Write and Invalidate Enable Not applicable to internal IIO devices. Hardwired to 0.
3	0h RW	**Special Cycle (SPECIAL_CYCLE):** Special Cycle Enable. Hardwired to 0
2	0h RW	**Bus Master Enable (BME):** Enables ISP to function as a PCI compliant master. When 0, blocks the sending of MSI interrupts. When 1, permits the sending of MSI interrupts.
1	0h RW	**Memory Space Enable (MSE):** When set, accesses to this device's memory space is enabled.
0	0h RW	**IO Space Enable (IOAE):** The IPU doesn't support IO commands.

6.3 Revision ID and Class Code (RID_CC) — Offset 8h

RID_CC - Revision ID and Class Code Register

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:5, F:0] + 8h	04800000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:24	04h RO	**Base-Class Code (BASECLASS_CODE):** 04h indicates a multimedia device
23:16	80h RO	**Sub-Class Code (SUBCLASS_CODE):** 80h indicates a video device
15:8	00h RO	**Programming Interface (PROGRAMMING_INTERFACE):** Default programming interface
7:0	00h RO/V	**Revision ID (REVISION_ID):** The value in this field is set by the setIDValue message

6.4 Cache Line Size, Master Latency Timer, Header Type and BIST (CLS_MLT_HT_BIST) — Offset Ch

Cache Line Size, Master Latency Timer, Header Type and BIST Register

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:5, F:0] + Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:24	00h RO	**Built In Self Test (BIST):** Built In Self Test
23:16	00h RO	**Header Type (HEADER_TYPE):** Indicates a type 0 header format.
15:8	00h RO	**Master Latency Timer (LATENCY_TIMER):** Master Latency Timer
7:0	00h RW	**Cache Line Size (CACHELINE_SIZE):** Value is ignored. This field is implemented by PCI Express devices as a read-write field for legacy compatibility purposes but has no effect on any PCI Express device behavior.

6.5 ISPMMADR LSB (ISPMMADR_LOW) — Offset 10h

Lower Part of the ISPMMADR Base Address Register

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:5, F:0] + 10h	00000004h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:24	00h RW	**Base Address (BASE_ADDR):** Set by the OS, these bits correspond to address signals (31:24).
23:4	00000h RO	**Address Mask (ADDR_MASK):** Hardwired to 0s to indicate at least 16MB address range
3	0h RO	**Prefetchable Memory (PREFETCHABLE):** Hardwired to 0 to prevent prefetching
2:1	2h RO	**Memory Type (TYPE):** 2h indicates 64 bit wide addressing
0	0h RO	**Message Space (MESSAGE_SPACE):** 0h indicates memory space

6.6 ISPMMADR MSB (ISPMMADR_HIGH) — Offset 14h

Higher Part of Base Address Register

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:5, F:0] + 14h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:7	0h RO	**Reserved**
6:0	00h RW	**Base Address MSB (BASE_ADDR):** Base Address MSB

6.7 Subsystem Vendor ID and Subsystem ID (SVID_SID) — Offset 2Ch

Subsystem Vendor ID and Subsystem ID Register

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:5, F:0] + 2Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:16	0000h RW/O	**Subsystem ID (SUBSYSTEM_ID):** Written by BIOS after reset, can be changed only after a reset cycle
15:0	0000h RW/O	**Subsystem Vendor ID (SUBSYSTEM_VENDOR_ID):** Written by BIOS after reset, can be changed only after a reset cycle

6.8 Capabilities Pointer (CAPPOINT) — Offset 34h

Capabilities Pointer Register

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:5, F:0] + 34h	00000070h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:8	0h RO	**Reserved**
7:0	70h RO	**Capabilities Pointer (CAPABILITY_PTR):** This field contains an offset into the function's PCI Configuration Space for the first item in the New Capabilities Linked List, the CAPID0 register at offset 70h

6.9 Interrupt Properties (INTR) — Offset 3Ch

Interrupt Properties Register

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:5, F:0] + 3Ch	00000100h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:24	00h RO	**Maximum Latency (MAXLAT):** Maximum latency
23:16	00h RO	**Minimum Latency (MINLAT):** Minimum latency
15:8	01h RO	**Interrupt Pin (INTERRUPT_PIN):** PCI Device 0/5/0 (IPU) is a single function device. If INTx is used, the PCI spec requires that it use INTA# This field is hardcoded to 1 - signifies INTa is used.
7:0	00h RW	**Interrupt Line (INTERRUPT_LINE):** BIOS written value to communicate interrupt line routing information to the ISP device driver.

6.10 PCIe Capabilities (PCIECAPHDR_PCIECAP) — Offset 70h

PCIe Capabilities Register

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:5, F:0] + 70h	0092AC10h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:16	0092h RO	**PCIe Capability (PCIE_CAP):** Bits 15:14: Reserved, 0 Bits 13:9: Interrupt Message Number (INTMSG): Since this device only supports one MSI vector, this field is hardwired to 0. Bit 8: Slot Implemented (SLOTIMP): Hardwired to 0 for any endpoint device. Bits 7:4: DevicePort Type: Indicates the specific type of this PCI Express function. 1001b indicates a Root Complex Integrated Endpoint Bits 3:0 Capability Version: Must be hardwired to 2h for Functions compliant to PCI Express 3.0 Base Specification.
15:8	ACh RO	**Next Capability Pointer (NEXT_PTR):** Indicates the next item in the capabilities list or 00h if no other items exist in the linked list of capabilities.

Bit Range	Default & Access	Field Name (ID): Description
7:0	10h RO	**Capability ID (CAPABILITY_ID):** Indicates the PCI Express Capability structure. This field must return a Capability ID of 10h indicating that this is a PCI Express Capability structure

6.11 Device Capabilities (DEVICECAP) — Offset 74h

Capabilities Register

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:5, F:0] + 74h	10008000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:29	0h RO	**Reserved**
28	1h RO/V	**Functional Level Reset (FLRCAP):** A value of 1b indicates the Function supports the optional Function Level Reset mechanism.
27:0	0008000h RO	**Device Capabilities (DEVICECAP):** Bits 31:29: Reserved, 0 Bits 27:26: Power Limit Scale: Not applicable, hardwired to 00b Bits 25:18: Power Limit Value: Not applicable, hardwired to 00b Bits 17:16: Reserved, 0. Bit 15: Role-base Error Reporting (RBER): When Set, this bit indicates that the Function implements the functionality originally defined in the Error Reporting ECN for PCI Express Base Specification, Revision 1.0a, and later incorporated into PCI Express Base Specification, Revision 1.1 Bits 14:12: Reserved, 0. Bits 11:9: Endpoint L1 Acceptable Latency: This field indicates the acceptable total latency that an Endpoint can withstand due to the transition from the L1 state to the L0 state. Bits 8:6: Endpoint L0s Acceptable Latency: This field indicates the acceptable total latency that an Endpoint can withstand due to the transition from the L0s state to the L0 state. Bit 5: Extended Tag Field Supported: This bit indicates the maximum supported size of the Tag field as a Requester. Bits 4:3: Phantom Functions Supported: This field indicates the support for use of unclaimed Function Numbers to extend the number of outstanding transactions for PCIe devices. Bits 2:0: Max_Payload_Size Supported: This field indicates the maximum payload size that the Function can support for TLPs. 000b represents 128 bytes, the minimum allowed value.

6.12 Device Capabilities and Control (DEVICECTL_DEVICESTS) — Offset 78h

PCI Express Device Capabilities and Control Register

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:5, F:0] + 78h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:22	0h RO	**Reserved**
21	0h RO/V	**Transaction Pending (DEVICESTS):** When Set, this bit indicates that the Function has issued Non-Posted Requests that have not been completed. A Function reports this bit is cleared only when all outstanding Non-Posted Requests have completed or have been terminated by the Completion Timeout mechanism. This bit must also be cleared upon the completion of an FLR.
20	0h RO	**AUX Power Detected (RELAX_ORD_EN):** Not used, always 0
19	0h RW/1C/V	**Unsupported Request Detected (UR_REQ_DET):** Unsupported Request Detected - set when IUNIT receive P/NP transaction which is UR
18:16	0h RO	**Misc Errors (DEVICECTL_MISC_STS):** Bits 2:0: Various error detected bits: The Root Complex Integrated Endpoint does not use the PCI Express error reporting mechanism. Always return 0.
15	0h RW	**Initiate Function Level Reset (INIT_FLR):** A write of 1b initiates Function Level Reset to the Function. The value read by software from this bit is always 0b.
14:0	0000h RO	**Misc Device Control (DEVICECTL_MISC_CTRL):** The only bit set reflect Unsupported-Request-Reporting Enable

6.13 MSI Capabilities and MSI Control (MSI_CAPID) — Offset ACh

MSI Capabilities and MSI Control Register

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:5, F:0] + ACh	0080D005h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:24	0h RO	**Reserved**
23	1h RO	**64-bit Address Capable (AC64):** 64-bit Address Capable (C64): PCIe devices must support 64b MSI addressing.
22:20	0h RW	**Multiple Message Enable (MME):** Multiple Message Enable (MME): This field is RW for software compatibility, but only a single message is ever generated.
19:17	0h RO	**Multiple Message Capable (MMC):** 3'h0 indicates one outstanding message is supported
16	0h RW	**MSI Enable (MSIEN):** If set, MSI is enabled. PCICMDSTS.BME must be set for an MSI to be generated. When 0, blocks the sending of a MSI interrupt. The interrupt status is not blocked from being reflected in the PCICMDSTS.IS bit. When 1, permits sending of a MSI interrupt.
15:8	D0h RO	**Next Capability Pointer (NEXT_PTR):** This contains a pointer to the next item in the capabilities list which is the Power Management capability
7:0	05h RO	**MSI Capability (CAPABILITY_ID):** Indicates an MSI capability.

6.14 MSI Address Low (MSI_ADDRESS_LO) — Offset B0h

MSI Address Register

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:5, F:0] + B0h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:2	00000000h RW	**MSI Address (MSI_ADDR):** System specified message address, always DW aligned.

Bit Range	Default & Access	Field Name (ID): Description
1:0	0h RO	**Reserved**

6.15 MSI Address High (MSI_ADDRESS_HI) — Offset B4h

MSI Address Register

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:5, F:0] + B4h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:7	0h RO	**Reserved**
6:0	00h RW	**MSI Address (MSI_ADDR):** MSI Address: Upper 32 bits of the system specified message address.

6.16 MSI Data (MSI_DATA) — Offset B8h

MSI Data Register

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:5, F:0] + B8h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:16	0h RO	**Reserved**
15:0	0000h RW	**MSI Data (MSI_DATA):** This 16-bit field is programmed by system software and is driven onto the lower word of data during the data phase of the MSI write transaction.

6.17 Power Management Capabilities (PMCAP) — Offset D0h

Power Management Capabilities

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:5, F:0] + D0h	00030001h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:16	0003h RO	**PM Capability (PMCAP):** Bits 31:27: PME Support (PMES): The camera controller does not generate PME#. Bit 26: D2_SUPPORT (D2S): The D2 power management state is not supported. Bit 25: D1_SUPPORT (D1S): The D1 power management state is not supported. Bits 24:22: Reserved Bit 21: Device Specific Initialization (DSI): Hardwired to 0 to indicate that no special initialization of the camera controller is required before generic class device driver is to use it. Bits 20:19: Reserved Bits 18:16: Version (VS): Indicates compliance with revision 1.2 of the PCI Power Management Specification.
15:8	00h RO	**Next Capability Pointer (NEXT_PTR):** End of List
7:0	01h RO	**PM Capability ID (CAPABILITY_ID):** PCI SIG defines this ID is 01h for power management

6.18 Power Management Control and Status (PMCS) — Offset D4h

Power Management Control and Status

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:5, F:0] + D4h	00000008h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:16	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
15	0h RW/1C/V	**Power Management Event Status (PMES):** Not used in this product. No PME from D3cold.
14:13	0h RO	**Data Scale (DS):** Not used
12:9	0h RO	**Data Select (DSEL):** Not used
8	0h RO	**Power Management Event Enable (PMEEN):** Power Management Event Enable
7:4	0h RO	**Reserved**
3	1h RO	**No Soft Reset (NSR):** This read-only bit indicates that the device does not lose internal state on a D3hot to D0 transition. This means that the internal state is not reset on a D3 (D3hot actually) to D0 transition and no additional operating system intervention is required to preserve the state A transition from D3 to D0 will NOT cause the IP to return to D0uninitialized. The Iunit+PUnit will restore the state of the IP configuration and MMIO registers .
2	0h RO	**Reserved**
1:0	0h RW/V	**Power State (PS):** Power management is implemented by writing to control registers in the PUNIT. This field may be programmed by the software driver, but no action is taken based on writing to this field

6.19 IPUVTDBAR Base Address Register (IPUVTDBAR_LOW) — Offset F0h

This is the lower part of the base address for the IPU's VTDBAR register group

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:5, F:0] + F0h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	None	None

Bit Range	Default & Access	Field Name (ID): Description
31:12	00000h RW	**IPUVTDBAR Base Address LSB (VTD_BAR_LOW):** VTD BAR bits 31:12
11:1	0h RO	**Reserved**
0	0h RW/V	**IPUVTDBAR Enable (VTD_ENABLE):** BIOS can write VTD_ENABLE only if VTD_ENABLE_LOCK is 0

6.20 IPUVTDBAR Base Address Register (IPUVTDBAR_HIGH) — Offset F4h

This is the upper part of the base address for the IPU's VTDBAR register group

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:5, F:0] + F4h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	None	None

Bit Range	Default & Access	Field Name (ID): Description
31:7	0h RO	**Reserved**
6:0	00h RW	**IPUVTDBAR Base Address MSB (VTD_BAR_HIGH):** VTD BAR bits 38:32

7 Gauss Newton Algorithm Registers (D8:F0)

Gaussian Mixture Model and Neural Network Accelerator. This chapter documents the registers in Bus: 0, Device 8, Function 0.

Note: These registers apply to all processors.

Table 7-1. Summary of Bus: 0, Device: 8, Function: 0 Registers

Offset	Size (Bytes)	Register Name (Register Symbol)	Default Value
0h	4	Vendor & Device ID (IDENTIFICATION)	00008086h
4h	2	Device Control (DCTRL)	0000h
6h	2	Device Status (DSTS)	0010h
8h	4	Revision ID & Class Codes (RID_DLCO)	08800000h
Ch	1	Cache Line Size (CLS)	00h
Eh	1	Header Type (HTYPE)	00h
Fh	1	Built-in Self Test (BIST)	00h
10h	4	GNA Base Address Low (GNABAL)	00000004h
14h	4	GNA Base Address High (GNABAH)	00000000h
2Ch	2	Sub System Vendor Identifiers (SSVI)	0000h
2Eh	2	Sub System Identifiers (SSI)	0000h
34h	4	Capabilities Pointers (CAPP)	00000090h
3Ch	1	Interrupt Line (INTL)	00h
3Dh	1	Interrupt Pin Register (INTP)	01h
3Eh	2	Min Grant And Min Latency Register (MINGNTLAT)	0000h
40h	4	Override Configuration Control (OVRCFGCTL)	00000000h
90h	2	Message Signaled Interrupt Capability ID (MSICAPID)	A005h
92h	2	Message Signaled Interrupt Message Control (MC)	0000h
94h	4	Message Signaled Interrupt Message Address (MA)	00000000h
98h	4	Message Signaled Interrupt Message Data (MD)	00000000h
A0h	2	D0i3 Capability ID (D0I3CAPID)	DC09h
A2h	2	D0i3 Capability (D0I3CAP)	F014h
A4h	4	D0i3 Vendor Extended Capability Register (D0I3VSEC)	01400010h
A8h	4	D0i3 SW LTR Pointer Register (D0I3SWLTRPTR)	00000000h
ACh	4	D0i3 DevIdle Pointer Register (D0I3DEVIDLEPTR)	00000A81h
B0h	2	D0i3 DevIdle Power On Latency (D0I3DEVIDLEPOL)	0800h
B2h	2	D0i3 Power Control Enables Register (PCE)	0028h
DCh	2	Power Management Capability ID (PMCAPID)	F001h
DEh	2	Power Management Capability (PMCAP)	0002h
E0h	2	Power Management Control Status (PMCS)	0000h

Offset	Size (Bytes)	Register Name (Register Symbol)	Default Value
F0h	2	FLR Capability ID (FLRCAPID)	0013h
F2h	2	FLR Capability Length And Version (FLRMISC)	0306h
F4h	1	FLR Control Register (FLRCTL)	00h
F5h	1	FLR Status Register (FLRSTS)	00h

7.1 Vendor & Device ID (IDENTIFICATION) — Offset 0h

Device ID assigned to GNA and Vendor ID

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:8, F:0] + 0h	00008086h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:16	0000h RO/V	**Device Identification Number (DID):** Indicates the device ID assigned to the GNA.
15:0	8086h RO	**Vendor Identification Number (VID):** Indicates Intel's identification

7.2 Device Control (DCTRL) — Offset 4h

The Command register provides coarse control over GMM's abilities such as:

- Unsupported Request Error Reporting Enable
- Poisoned TLP Error Reporting Enable
- Interrupt Disable
- Max Aligned Payload Size
- Max Aligned Read Request Size
- Special Cycle Enable
- Bus Master Enable
- Memory Space Enable

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:8, F:0] + 4h	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15	0h RO	**Reserved**
14	0h RO	**Unsupported Request Error Reporting Enable (UNSPREQERREN):** Unsupported Request Error Reporting Enable
13	0h RO	**Poisoned TLP Error Reporting Enable (PTLPERREN):** Poisoned TLP Error Reporting Enable
12:11	0h RO	**Reserved**
10	0h RW	**Interrupt Disable (INTDIS):** Interrupt Disable: Controls the ability of the function to generate INTx interrupts. 0: INTx allowed 1: INTx disabled
9:6	0h RO	**Reserved**
5	0h RO	**Max Aligned Payload Size (MXAPAYLDSZ):** Max Aligned Payload Size - Reserved
4	0h RO	**Max Aligned Read Request Size (MXARDREQSZ):** Max Aligned Read Request Size - Reserved
3	0h RO	**Special Cycle Enable (SCEN):** Special Cycle Enable - Reserved
2	0h RW	**Bus Master Enable (BME):** Bus Master Enable: 0: Disable (default). 1: Enabled. Device may generate bus master transactions depending on its mode of operation.
1	0h RW	**Memory Space Enable (MSE):** Memory Space Enable Controls the GMM devices response to memory space accesses. 0: Disabled (default) 1: Enabled. Device will respond to memory space accesses.
0	0h RO	**IO Space Enable (IOSE):** IO Space Enable. Not implemented.

7.3 Device Status (DSTS) — Offset 6h

The Status register to record status information for PCI related events

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:8, F:0] + 6h	0010h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15	0h RO	**Detected Parity Error (DPE):** This bit is set by a function whenever it receives a Poisoned TLP, regardless of the state the parity Error Response bit in the Command register. On a Function with a Type 1 Configuration header, the bit is set when the Poisoned TLP is received by its primary side. Note: some implementations use this error type as non-fatal error indication This bit is typically RWC. Change to RO as this bit is not in use.
14	0h RO	**Signaled System Error (SSE):** This bit is set when a function sends an ERR_FATAL or ERR_NONFATAL Message, and the SERR# enable bit in the command register is 1. Note: some implementations use this error for fatal. When received all operations are aborted. This bit is typically RWC. Change to RO as this bit is not in use
13	0h RW/1C/V	**Received Master Abort (RMA):** This bit is set when a requester receives a completion with Unsupported Request Completion status. On a function with a Type 1 configuration header, the bit is set when the Unsupported Request is received by its primary side.
12	0h RW/1C/V	**Received Target Abort (RTA):** This bit is set when a transaction abort is received to a GMM initiated transaction.
11	0h RW/1C/V	**Signaled Target Abort (STA):** This bit is set when a Function completes a Posted or Non-Posted Request as a Completer Abort Error. This applies to a function with a type 1 configuration header when the Completer Abort was generated by its primary side.
10:8	0h RO	**Reserved**
7	0h RO	**Fast Back-to-Back (FB2B):** Fast Back-to-Back (ignored by SW)
6:5	0h RO	**Reserved**
4	1h RO	**Capability List (CLIST):** Capability List 0: no capability list 1: the GMM contains a linked list of capabilities which is accessed via the CAPPTR register at offset 34h
3	0h RO/V	**Interrupt Status (INTSTS):** Reflects the state of the interrupt in the device. Only when the Interrupt Disable bit in the command register is a 0 and this Interrupt Status bit is a 1, will this device send a virtual INTA. Setting the Interrupt Disable bit to a 1 has no effect on the state of this bit. This bit is controlled by HW. 0: No interrupt pending 1: Interrupt pending

Bit Range	Default & Access	Field Name (ID): Description
2:0	0h RO	**Reserved**

7.4 Revision ID & Class Codes (RID_DLCO) — Offset 8h

RID: This register indicates the stepping of this device.

DLCO: This register identify the type of device.

The values are as defined in PCI 3.0 bus specification in Appendix D.

The GMM is identified as an Other system Peripheral

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:8, F:0] + 8h	08800000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:24	08h RO	**Base Class Code (BCC):** Base Class (Generic system Peripherals)
23:16	80h RO	**Sub Class Code (SCC):** Code for Sub Class
15:8	00h RO	**Peripheral Interface (PROGINTERFACE):** Interface (other system peripheral)
7:0	00h RO/V	**Revision ID (RID):** Indicates the stepping of this device.

7.5 Cache Line Size (CLS) — Offset Ch

The system cache-line size in units of DWORDS

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:8, F:0] + Ch	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
7:0	00h RW	**Cache Line Size (CLS):** Implemented by PCI Express devices as a read-write field for legacy compatibility purposes but has no impact on any PCI Express device functionality.

7.6 Header Type (HTYPE) — Offset Eh

This byte identifies the layout of the second part of the predefined header and whether or not the device contains multiple functions (GMM is a single-function device of basic configuration space format, so this register is Read-Only and hardwired to 0).

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:8, F:0] + Eh	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7	0h RO	**Multi Function Device (MFD):** Hardwired to 0 indicating this device is not a multi-function device.
6:0	00h RO	**Header Type (HT):** The value 00h, indicates a basic (i.e. single function) configuration space format.

7.7 Built-in Self Test (BIST) — Offset Fh

This register describes the BIST capability of GMM and since GMM doesn't support BIST, the register is configured as Read Only.

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:8, F:0] + Fh	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7	0h RO	**BIST Capable (BISTCAP):** BIST Capable. Hardwired to 0 since this device does not implement BIST.
6	0h RO	**Start BIST (BISTST):** Start BIST. Hardwired to 0 since this device does not implement BIST.
5:4	0h RO	**Reserved**
3:0	0h RO	**BIST Completion Code (BISTCC):** Hardwired to 0 since this device does not implement BIST.

7.8 GNA Base Address Low (GNABAL) — Offset 10h

GNA Base Address Low:

Lower 32-bits of the GNA Base Address register.

The GMM Base Address register may be accessed with Double Word (32bit) read/write operations.

In 32-bit OS, the address specified may be limited by 32-bit of space, and the renaming bits must stay with their default values.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:8, F:0] + 10h	00000004h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:12	00000h RW	**Memory Base Address Low (BAL):** Base address of this device's memory mapped IO space. A page of 4KB of address is used.
11:4	00h RO	**Address Mask (ADDRMSK):** Hardwired to 0s to indicate at least 4KB address range
3	0h RO	**Prefetchable Memory (PREF):** Hardwired to 0 indicating that this range is not prefetchable.

Bit Range	Default & Access	Field Name (ID): Description
2:1	2h RO	**Memory Type (MEMTY):** Memory Type: 00: 32 bit base address 01: reserved 10: 64-bit base address 11: reserved
0	0h RO	**Space Type (SPTY):** Space Type: Memory/IO Space Hardwired to 0 indicating that this is a Memory BAR.

7.9 GNA Base Address High (GNABAH) — Offset 14h

Upper 32-bits of the GNA Base Address register.

The GNA Base Address register may be accessed with Double Word (32bit) read/write operations.

In 32-bit OS, the address specified may be limited by 32-bit of space, and the renaming bits must stay with their default values.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:8, F:0] + 14h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:7	0000000h RW	**Memory Base Address High (Reserved) (BAR):** These bits must be loaded with zeros.
6:0	00h RW	**Memory Base Address High (BAH):** Includes the high bits of the base address used by 64-bit OS. Must hold zero for 32-bit OS.

7.10 Sub System Vendor Identifiers (SSVI) — Offset 2Ch

This register is initialized to logic 0 by the assertion of reset. This register can be written only once after reset de-assertion it is locked for writes after that.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:8, F:0] + 2Ch	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:0	0000h RW/O	**Subsystem Vendor ID (SSVID):** Subsystem Vendor ID (SSVID): This is written by BIOS. No hardware action taken on this value.

7.11 Sub System Identifiers (SSI) — Offset 2Eh

This register is initialized to logic 0 by the assertion of reset. This register can be written only once after reset de-assertion it is locked for writes after that.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:8, F:0] + 2Eh	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:0	0000h RW/O	**Subsystem ID (SSID):** Subsystem ID (SSID): This is written by BIOS. No hardware action taken on this value.

7.12 Capabilities Pointers (CAPP) — Offset 34h

This register gives MSI capability pointer offset.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:8, F:0] + 34h	00000090h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:8	0h RO	**Reserved**
7:0	90h RO	**Capability Pointer (CAPP):** Indicates that the MSI capability pointer offset is offset 90h.

7.13 Interrupt Line (INTL) — Offset 3Ch

This register contains interrupt line routing information. The device itself does not use this value, rather it is used by device drivers and operating systems to determine priority and vector information.

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:8, F:0] + 3Ch	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
7:0	00h RW	**Interrupt Connection (INTCON):** Communicate interrupt line routing information. BIOS Requirement: POST software writes the routing information into this register as it initializes and configures the system. The value indicates to which input of the system interrupt controller this device's interrupt pin is connected.

7.14 Interrupt Pin Register (INTP) — Offset 3Dh

Tells which PCI legacy interrupt pin a device will use (GMM uses only IntA).

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:8, F:0] + 3Dh	01h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:3	0h RO	**Reserved**
2:0	1h RO	**Legacy Interrupt (LEGINT):** When Legacy interrupts are used, function use legacy interrupt INTA.

7.15 Min Grant And Min Latency Register (MINGNTLAT) — Offset 3Eh

Specifies a device's desired settings for Latency Timer values.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:8, F:0] + 3Eh	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
15:8	00h RO	**Min Latency (MINLAT):** Reserved
7:0	00h RO	**Min Grant (MINGNT):** Reserved

7.16 Override Configuration Control (OVRCFGCTL) — Offset 40h

This register holds bits that may be used internal mechanisms in the GMM during debug operations. Special notes will be made to BIOS writers, if any 5 of these bits will need to be set to value other than default.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:8, F:0] + 40h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:9	0h RO	**Reserved**
8	0h RW	**Sideband Clock Gating Enable (SBDCGEN):** This bit, when set, enables the sideband interface clock used for GMM bus interface operations (gated_side_clk) to be gated when conditions are met. When clear, clock gating is disabled.
7:0	0h RO	**Reserved**

7.17 Message Signaled Interrupt Capability ID (MSICAPID) — Offset 90h

This register contains a pointer to the next item in the capabilities list which is the Power Management Capability and also helps to identify linked list item (capability structure) as being for MSI registers.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:8, F:0] + 90h	A005h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
15:8	A0h RO	**Pointer to Next Capability (NXTPTR):** This contains a pointer to the next item in the capabilities list which is the Power Management Capability
7:0	05h RO	**Capability ID (CAPID):** Capability ID Value of 05h identifies this linked list item (capability structure) as being for MSI registers.

7.18 Message Signaled Interrupt Message Control (MC) — Offset 92h

This register is defined to meet PCI Local Bus Specification 3.0 Section 6.8 definition of MSI messages.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:8, F:0] + 92h	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:9	0h RO	**Reserved**
8	0h RO	**Per-Vector Masking Capable (PVMCAP):** Per-Vector Masking Capable. 0: not supported by GMM.
7	0h RO	**64-bit Address Capable (ADDR64CAP):** Hardwired to 0 to indicate that the function does not implement the upper 32 bits of the Message Address register and is incapable of generating a 64-bit memory address. This may need to change in future implementations when addressable system memory exceeds the 32bit/4GB limit.
6:4	0h RW	**Multiple Message Enable (MMEN):** System software program this field to indicate the number of vectors allocated to the GMM. At least one vector must be allocated when the MSI interrupts are enabled. This value is ignored by HW as only a single vector is in use by GMM.
3:1	0h RO	**Multiple Message Capable (MMCAP):** Indicates to SW the number of vectors that the GMM module is requesting for use. Value Number of Messages requested 000 1 001 2 (reserved) 010 4 (reserved) 011 8 (reserved) 100 16(reserved) 101 32(reserved) Other reserved
0	0h RW	**MSI Enable (MSIEN):** MSI Enable Controls the ability of GMM to generate MSI Messages. A device driver is prohibited from writing this bit to mask a functions service request. 0: MSI will not be generated 1: MSI will be generated. INTA will not be generated and INTA status is not set.

7.19 Message Signaled Interrupt Message Address (MA) — Offset 94h

This register is defined to meet PCI Local Bus Specification 3.0 Section 6.8 definition of MSI messages.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:8, F:0] + 94h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:2	00000000h RW	**Message Address (MADDR):** Used by system software to assign an MSI address to the device. The device handles an MSI by writing the padded contents of the MD register to this address.
1:0	0h RO	**Reserved**

7.20 Message Signaled Interrupt Message Data (MD) — Offset 98h

This register is defined to meet PCI Local Bus Specification 3.0 Section 6.8 definition of MSI messages

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:8, F:0] + 98h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:16	0h RO	**Reserved**
15:0	0000h RW	**Message Data (MDAT):** Base message data pattern assigned by system software and used to handle an MSI from the device. When the device must generate an interrupt request, it writes a 32-bit value to the memory address specified in the MA register. The upper 16 bits are always set to 0. The lower 16 bits are supplied by this register.

7.21 D0i3 Capability ID (D0I3CAPID) — Offset A0h

Pointer to next capability and capability ID.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:8, F:0] + A0h	DC09h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
15:8	DCh RO	**Pointer to Next Capability (NXTPTR):** This contains a pointer to the next item in the capabilities list which is the Power Management Capability.
7:0	09h RO	**Capability ID (CAPID):** Value of 09h identifies this linked list item (capability structure) is a vendor specific capability.

7.22 D0i3 Capability (D0I3CAP) — Offset A2h

Vendor-Specific Capability ID.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:8, F:0] + A2h	F014h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
15:12	Fh RO	**Vendor-Specific Capability ID (VSID):** Indicates that this Vendor Specific Capability is an Extended Capability, which use a VSEC 16-bit Extended Vendor Capability in the subsequent 4B., differentiating this from other vendor specific capabilities.
11:8	0h RO	**Vendor Specific Capability Revision (VSREV):** Reserved
7:0	14h RO	**Vendor Specific Capability Length (VSLEN):** This field indicates the number of bytes in this capability including the CapID and Cap registers.

7.23 D0i3 Vendor Extended Capability Register (D0I3VSEC) — Offset A4h

Vendor Specific Extended Capability Length.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:8, F:0] + A4h	01400010h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:20	014h RO	**Vendor Specific Extended Capability Length (VSECLEN):** Indicates that this Vendor Specific Capability is an Extended Capability, which use a VSEC 16-bit Extended Vendor Capability in the subsequent 4B., differentiating this from other vendor specific capabilities.
19:16	0h RO	**Vendor Specific Extended Capability Revision (VSREV):** For this revision of DevIdle, this field is 0h.
15:0	0010h RO	**Vendor Specific Extended Capability ID (VSECID):** DevIdle has been assigned the Intel VSEC ID of 10h.

7.24 D0i3 SW LTR Pointer Register (D0I3SWLTRPTR) — Offset A8h

SW LTR Update MMIO Offset Location.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:8, F:0] + A8h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:4	0000000h RO	**SW LTR Update MMIO Offset Location (SWLTRLOC):** The value in this field is ignored as GMM does not support SW LTR.
3:1	0h RO	**Base Address Register Number (BARNUM):** The value in this field is ignored as GMM does not support SW LTR.
0	0h RO	**Valid Indicator (VALID):** Indicates the use of SW LTR by the function.GMM does not use SW LTR.

7.25 D0i3 DevIdle Pointer Register (D0I3DEVIDLEPTR) — Offset ACh

DevIdle MMIO Offset Location.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:8, F:0] + ACh	00000A81h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:4	00000A8h RO	**DevIdle MMIO Offset Location (DEVIDLELOC):** This location pointer to the DevIdle register in MMIO space, as an offset from the BAR base.
3:1	0h RO	**Base Address Register Number (BARNUM):** The DevIdle is located in BAR0.
0	1h RO	**Valid Indicator (VALID):** GMM has a DevIdle register.

7.26 D0i3 DevIdle Power On Latency (D0I3DEVIDLEPOL) — Offset B0h

D0idle_5 Max_Power_On_Latency is set by BIOS at boot and read by device driver SW to calculate approximate cost of a D0idle entry + exit cycle. This allows driver to avoid idle entry in cases where device duty cycle is larger than D0idle entry + exit cycle.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:8, F:0] + B0h	0800h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
15:13	0h RO	**Reserved**
12:10	2h RO	**Power On Latency Scale (POLS):** Latency Scale multiplier: 010: 1us 011: 32us All other settings are reserved. This field is a RO as there is no need for BIOS programing of it.
9:0	000h RO	**Power On Latency Value (POLV):** A value of 0 indicates a power on latency of less than 1us. This field is a RO as there is no need for BIOS programing of it.

7.27 D0i3 Power Control Enables Register (PCE) — Offset B2h

This register controls the D0i3 features like Hardware Autonomous Enable, sleep enable, D3-Hot Enable, I3 Enable and PMC Request Enable.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:8, F:0] + B2h	0028h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:6	0h RO	**Reserved**
5	1h RW	**Hardware Autonomous Enable (HAE):** If set, then the IP may request a PG whenever it is idle. NOTE: If this bit is set, then bits[2:0] must be 000.
4	0h RO	**Reserved**
3	1h RW	**Sleep Enable (SE):** If clear, then IP will never assert Sleep to the retention flops. If set, then IP may assert Sleep during PGing. Note that some platforms may default this bit to 0, others to 1.
2	0h RW	**D3-Hot Enable (D3HE):** If set, then IP will PG when idle and the PMCSR[1:0] register in the IP =11.
1	0h RW	**I3 Enable (I3E):** If set, then IP will PG when idle and the D0i3 register (D0i3C[2] = 1) is set. NOTE: If bits [2:1] = 11, then the IP would PG whenever either PMCSR = 11 or the D0i3C.i3 bit is set.
0	0h RW	**PMC Request Enable (PMCRE):** If set, then IP will PG when idle and the PMC requests power gating by asserting the pmc_*_sw_pg_req_b signal.

7.28 Power Management Capability ID (PMCAPID) — Offset DCh

This register contains a pointer to next item in capabilities list and also helps to identify linked list item as being for

PCI Power Management registers.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:8, F:0] + DCh	F001h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
15:8	F0h RO	**Next Pointer (NXTPTR):** This contains a pointer to next item in capabilities list. This is the final capability in the list and must be set to 00h.
7:0	01h RO	**Capability Identifier (CAPID):** Identifies this linked list item as being for PCI Power Management registers. This is compliant with the PCI Power Management Interface Specification (section 3.2).

7.29 Power Management Capability (PMCAP) — Offset DEh

This register describes the Power Management Capability of GMM.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:8, F:0] + DEh	0002h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
15:11	00h RO	**PME Support (PMES):** This device does not support PMEB signal.
10	0h RO	**D2 Support (D2S):** This device does not support D2.
9	0h RO	**D1 Support (D1S):** This device does not support D1.
8:6	0h RO	**Auxiliary Current (AUXC):** Reserved
5	0h RO	**Device Specific Initialization (DSI):** Indicates that this device requires device specific initialization before generic class device driver is to use it.
4	0h RO	**Auxiliary Power (AUXP):** This device does not use Aux power.
3	0h RO	**PME Clock (PMEC):** Indicate this device does NOT support PMEB generation.

Bit Range	Default & Access	Field Name (ID): Description
2:0	2h RO	**Power Management Version (VER):** Hardwired to 010b to indicate there are 4 bytes of power management registers implemented and that this device complies with revision 1.1 of the PCI Power Management Interface Specification.

7.30 Power Management Control Status (PMCS) — Offset E0h

This register has the status of PME Generation from D3(cold), Data Scale, Data Select, PME Enable and Power State.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:8, F:0] + E0h	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15	0h RO	**PME Generation from D3 (cold) (PMEGD3):** Not supported.
14:13	0h RO	**Data Scale (DATSC):** No support for Power Management Data register.
12:9	0h RO	**Data Select (DATSEL):** No support for Power Management Data register.
8	0h RO	**PME Enable (PMEE):** PMEB is not supported.
7:2	0h RO	**Reserved**
1:0	0h RW	**Power State (PS):** Indicates the current power state of this device and can be used to set the device into a new power state. If software attempts to write an unsupported state to this field, write operation must complete normally on the bus, but the data is discarded and no state change occurs. 00: D0 01: D1 (Not supported in this device.) 10: D2 (Not supported in this device.) 11: D3 Write of reserved values is ignored and state will not change. Support of D3cold does not require any special action. While in the D3hot state, this device can only act as the target of PCI configuration transactions (for power management control). This device also cannot generate interrupts or respond to MMR cycles in the D3 state. The device must return to the D0 state in order to be fully-functional.

7.31 FLR Capability ID (FLRCAPID) — Offset F0h

This register contains a pointer to next item in capabilities list and capability of Advanced Features.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:8, F:0] + F0h	0013h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
15:8	00h RO	**Next Pointer (NXTPTR):** This contains a pointer to next item in capabilities list. This is the final capability in the list and must be set to 00h.
7:0	13h RO	**Capability Identifier (CAPID):** A value that indicates FLR (Vendor specific value). 0: 09h (FLR in use) A value of 09h in this register indicates that this is a FLR capabilities field.

7.32 FLR Capability Length And Version (FLRMISC) — Offset F2h

This register describes the FLR Capability, TXP Capability and Capability Length.

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:8, F:0] + F2h	0306h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
15:10	0h RO	**Reserved**
9	1h RO	**FLR Capability (FLRCAP):** Indicates support for Function Level Reset (FLR).
8	1h RO	**TXP Capability (TXPCAP):** Indicates that TP bit is supported.
7:0	06h RO	**Capability Length (CAPLEN):** This bit indicates the number of bytes this vendor specified capability requires. it has a value of 06h for the FLR capability.

7.33 FLR Control Register (FLRCTL) — Offset F4h

This register controls the Functional Level reset operation of GMM.

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:8, F:0] + F4h	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
7:1	0h RO	**Reserved**
0	0h WO	**Initiate FLR (INITFLR):** Writing 1 to this field starts the Functional Level Reset.This will act similar to the Abort + will bring all non-CFG registers to their reset value. The FLR is completed when the FLR status bit is cleared.

7.34 FLR Status Register (FLRSTS) — Offset F5h

This register helps to identify whether FLR is in progress.

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:8, F:0] + F5h	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:1	0h RO	**Reserved**
0	0h RO/V	**Transaction Pending (XPEND):** 0: FLR not in progress. 1: FLR is in progress (due to internal operation or waiting for the completion of a non-posted transaction).

8 Type C Subsystem (TCSS)

This chapter documents the Type C Subsystem Registers.

Table 8-1. Summary of Type C Subsystem (TCSS)

Thunderbolt DMA Device Registers (D13:F2-3)
USB Host Controller (xHCI) Registers (D13:F0)
USB Host Controller MBAR Registers (D13:F0)
USB Device Controller (xDCI) Configuration Registers (D13:F1)
Thunderbolt PCI Express* Controller Registers (D7:F0-3)

8.1 Thunderbolt DMA Device Registers (D13:F2-3)

This chapter documents the registers of the Thunderbolt DMA devices. There are two Thunderbolt DMA devices:

- Bus: 0, Device: 13, Function: 2 (TBT_DMA0)
- Bus: 0, Device: 13, Function: 3 (TBT_DMA1)

Note: Register default values are taken from device TBT_DMA0 only. Consult the Ice Lake EDS Vol1 for Device IDs

8.1.1 Summary of Registers

Table 8-2. Summary of Bus: 0, Device: 13, Function: 2 Registers

Offset	Size (Bytes)	Register Name (Register Symbol)	Default Value
0h	4	Vendor ID and Device ID (DMA_CFG_FIRST16DWORD_DW0_INST)	15778086h
4h	4	PCIE Config Space Header 1: Command and Status (DMA_CFG_FIRST16DWORD_DW1_INST)	00100000h
8h	4	PCIE Config Space Header 2: Revision ID and Class Code (DMA_CFG_FIRST16DWORD_DW2_INST)	08800000h
Ch	4	PCIE Config Space Header 3: MISC (DMA_CFG_FIRST16DWORD_DW3_INST)	00000000h
10h	4	PCIE Config Space Header 4: BAR0 (DMA_CFG_FIRST16DWORD_DW4_INST)	FFFC0000h
14h	4	PCIE Config Space Header 5: BAR1 (DMA_CFG_FIRST16DWORD_DW5_INST)	00000000h
18h	4	PCIE Config Space Header 6: BAR2 (DMA_CFG_FIRST16DWORD_DW6_INST)	00000000h
1Ch	4	PCIE Config Space Header 7: BAR3 (DMA_CFG_FIRST16DWORD_DW7_INST)	00000000h
28h	4	PCIE Config Space Header 10: Cardbus CIS Pointer (DMA_CFG_FIRST16DWORD_DW10_INST)	00000000h
2Ch	4	PCIE Config Space Header 11: Subsystem IDs (DMA_CFG_FIRST16DWORD_DW11_INST)	11112222h
30h	4	PCIE Config Space Header 12: Expansion ROM Base Address (DMA_CFG_FIRST16DWORD_DW12_INST)	00000000h

Offset	Size (Bytes)	Register Name (Register Symbol)	Default Value
34h	4	PCIE Config Space Header 13: PCIE Capabilities Pointer (DMA_CFG_FIRST16DWORD_DW13_INST)	00000080h
3Ch	4	PCIE Config Space Header 15: Interrupt Config (DMA_CFG_FIRST16DWORD_DW15_INST)	000001FFh
80h	4	Power Management Capability Configuration (DMA_CFG_PM_CAP_0)	F8038801h
84h	4	PM Capability 1 Control and Status (DMA_CFG_PM_CAP_1)	00000000h
88h	4	MSI Capability 0: MSI Capability Config (DMA_CFG_MSIREG_DW0_INST)	0080A005h
8Ch	4	MSI Capability 1: Message Address Low (DMA_CFG_MSIREG_DW1_INST)	00000000h
90h	4	MSI Capability 2: Message Address High (DMA_CFG_MSIREG_DW2_INST)	00000000h
94h	4	MSI Capability 3: Message Data (DMA_CFG_MSIREG_DW3_INST)	00000000h
98h	4	MSI Capability 4: Interrupt Mask (DMA_CFG_MSIREG_DW4_INST)	00000000h
9Ch	4	MSI Capability 5: Interrupt Pending (DMA_CFG_MSIREG_DW5_INST)	00000000h
A0h	4	MSIX Capability 0: MSIX Capability Config (DMA_CFG_MSIXREG_DW0_INST)	000F0011h
A4h	4	MSIX Capability 1: Table Offset and Table BIR (DMA_CFG_MSIXREG_DW1_INST)	00000000h
A8h	4	MSIX Capability 2: PBA Offset and PBA BIR (DMA_CFG_MSIXREG_DW2_INST)	00000FA0h
D4h	4	VS CAP 12 Thunderbolt Access Through PCIE Command Register (DMA_CFG_VS_CAP_12)	00000000h
D8h	4	VS CAP 13 Thunderbolt Access Through PCIE Write Data Register (DMA_CFG_VS_CAP_13)	00000000h
DCh	4	VS CAP 14 Thunderbolt Access Through PCIERead Data Register (DMA_CFG_VS_CAP_14)	00000000h
FCh	4	VS CAP 22: YFL Vendor Configuration Bits (DMA_CFG_VS_CAP_22)	06061000h

8.1.2 Vendor ID and Device ID (DMA_CFG_FIRST16DWORD_DW0_INST) — Offset 0h

PCIE Config Space Header 0 Vendor ID and Device ID

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:2] + 0h	15778086h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:16	1577h RO/V	**Device ID (DEVID):** See Description in PCI Local Bus Specification

Bit Range	Default & Access	Field Name (ID): Description
15:0	8086h RO	**Vendor ID (VENDOR_ID):** See Description in PCI Local Bus Specification

8.1.3 PCIE Config Space Header 1: Command and Status (DMA_CFG_FIRST16DWORD_DW1_INST) — Offset 4h

Command and Status

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:2] + 4h	00100000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RW/1C	**Detected Parity Error (DETECTEDPARERR):** See Description in PCI Local Bus Specification
30	0h RW/1C	**Signaled System Error (SYSERROR):** See Description in PCI Local Bus Specification
29	0h RW/1C	**Received Master Abort (RCVDMASABORT):** See Description in PCI Local Bus Specification
28	0h RW/1C	**Received Taret Abort (RCVDTARABORT):** See Description in PCI Local Bus Specification
27	0h RW/1C	**Signaled Target Abort (SIGNALEDTARABORT):** See Description in PCI Local Bus Specification
26:25	0h RO	**Reserved**
24	0h RW/1C	**Master Data Parity Error (MASTDATPARERR):** See Description in PCI Local Bus Specification
23:21	0h RO	**Reserved**
20	1h RO	**New Capability List Exists (CAPLIST):** See Description in PCI Local Bus Specification
19	0h RO	**Interrupt Status (INTRPTSTATUS):** See Description in PCI Local Bus Specification
18:11	0h RO	**Reserved**
10	0h RW	**Interrupt Disable (INTRPTDISAB):** See Description in PCI Local Bus Specification
9	0h RO	**Reserved**
8	0h RW	**Serr# Enable (SERREN):** See Description in PCI Local Bus Specification

Bit Range	Default & Access	Field Name (ID): Description
7	0h RO	**Reserved**
6	0h RW	**Parity Error Resp (PARERRRESP):** See Description in PCI Local Bus Specification
5:3	0h RO	**Reserved**
2	0h RW	**Bus Master Enable (BUSMASEN):** See Description in PCI Local Bus Specification
1	0h RW	**Mem Space Enable (MEMSPACEEN):** See Description in PCI Local Bus Specification
0	0h RW	**IO space Enable (IOSPACEEN):** See Description in PCI Local Bus Specification

8.1.4 PCIE Config Space Header 2: Revision ID and Class Code (DMA_CFG_FIRST16DWORD_DW2_INST) — Offset 8h

Revision ID and Class Code

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:2] + 8h	08800000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:8	088000h RO	**Class Code (CLASS_CODE):** See Description in PCI Local Bus Specification
7:0	00h RO/V	**Revision ID (REVID):** See Description in PCI Local Bus Specification

8.1.5 PCIE Config Space Header 3: MISC (DMA_CFG_FIRST16DWORD_DW3_INST) — Offset Ch

Contains various Config fields

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:2] + Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:24	00h RO	**Built-in Self test (BIST):** See Description in PCI Local Bus Specification
23:16	00h RO	**Header Type (HEADER_TYPE):** See Description in PCI Local Bus Specification
15:8	00h RO	**Master Latency Timer (MASTER_LATENCY_TIMER):** See Description in PCI Local Bus Specification
7:0	00h RW	**Cache Line Size (CACHE_LINE_SIZE):** See Description in PCI Local Bus Specification

8.1.6 PCIE Config Space Header 4: BAR0 (DMA_CFG_FIRST16DWORD_DW4_INST) — Offset 10h

Contains BAR0 in 32 bit addressing and BAR0_LOW in 64 bit addressing. BAR0 is used for DMA Memory Access.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:2] + 10h	FFFC0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:18	3FFFh RW	**BAR0: RW (BAR0_4):** BAR0[31:18]: RW field.
17:4	0000h RO	**BAR0: RO (BAR0_3):** BAR0[17:4]: RO field.
3	0h RO	**BAR0: Prefetchable (BAR0_2):** BAR0[3]: Set to 1 if there are no side affects on reads; zero otherwise.
2	0h RO	**BAR0: Type (BAR0_1):** BAR0[2]: 0 - Locate anywhere in 32-bit access space;1 - Locate anywhere in 64-bit access space.
1:0	0h RO	**BAR0: Memory Space Indicator (BAR0_0):** BAR0[1:0]: 00b.

8.1.7 PCIE Config Space Header 5: BAR1 (DMA_CFG_FIRST16DWORD_DW5_INST) — Offset 14h

Contains BAR1 in 32 bit addressing and BAR0_HIGH in 64 bit addressing. BAR0 is used for DMA Memory Access. BAR1 is used for MSIX Memory accessing.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:2] + 14h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:12	00000h RW	**BAR1: RW (BAR1_3):** If 64 bit addressing: BAR0_HIGH[31:12]. Otherswise If 32 bit addressing and MSIX enabled: BAR1[31:12]: RW for MSIX BAR. Otherwise not used.
11:4	00h RO	**BAR1: RO (BAR1_2):** If 64 bit addressing: BAR0_HIGH[11:4]. Otherwise If 32 bit addressing and MSIX is enabled: BAR1[11:4]: RO for MSIX BAR. Otherwise not used.
3	0h RO	**BAR1: Prefetchable (BAR1_1):** If 64 bit addressing: BAR0_HIGH[3]. Otherwise if 32 bit addressing and MSIX enabled: BAR1[3]: 0 - Locate anywhere in 32-bit access space;1 - Locate anywhere in 64-bit access space. Otherwise not used.
2:0	0h RO	**BAR1: Memory Space Enable and Type (BAR1_0):** If 64 bit addressing: BAR0_HIGH[2:0] otherwise If 32 bit addressing and MSIX enabled: BAR1[2:0]: 3'b000. Otherwise not used.

8.1.8 PCIE Config Space Header 6: BAR2 (DMA_CFG_FIRST16DWORD_DW6_INST) — Offset 18h

Not used when using in 32 bit addressing and BAR1_LOW when using 64 bit addressing. BAR1 is used for MSIX Memory accessing.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:2] + 18h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:12	00000h RO	**BAR2 4 (BAR2_4):** If 64 bit addressing and MSIX enabled: BAR1[31:12]: MSIX RW field. Otherwise not used.

Bit Range	Default & Access	Field Name (ID): Description
11:4	00h RO	**BAR2 3 (BAR2_3):** If 64 bit addressing and MSIX enabled: BAR1[11:4]: MSIX RO field. Otherwise not used.
3	0h RO	**BAR2 2 (BAR2_2):** If 64 bit addressing and MSIX enabled: BAR1[3]: Set to 1 if there are no side affects on reads; zero otherwise. Otherwise not used.
2	0h RO	**BAR2 1 (BAR2_1):** If 64 bit addressing and MSIX enabled: BAR1[2]: 0 - Locate anywhere in 32-bit access space;1 - Locate anywhere in 64-bit access space. Otherwise not used.
1:0	0h RO	**BAR2 0 (BAR2_0):** If 64 bit addressing and MSIX enabled: BAR1[1:0]: 2'b00. Otherwise not used.

8.1.9 PCIE Config Space Header 7: BAR3 (DMA_CFG_FIRST16DWORD_DW7_INST) — Offset 1Ch

Not used when using in 32 bit addressing and BAR1_HIGH when using 64 bit addressing. BAR1 is used for MSIX Memory accessing.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:2] + 1Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RO	**BAR 3 (BAR3):** If 64 bit addressing and MSIX enabled: BAR1_HIGH

8.1.10 PCIE Config Space Header 10: Cardbus CIS Pointer (DMA_CFG_FIRST16DWORD_DW10_INST) — Offset 28h

Cardbus CIS Pointer

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:2] + 28h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RO	**Cardbus CIS Pointer (CARDBUS_CIS_POINTER):** See Description in PCI Local Bus Specification

8.1.11 PCIE Config Space Header 11: Subsystem IDs (DMA_CFG_FIRST16DWORD_DW11_INST) — Offset 2Ch

Subsystem IDs Used.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:2] + 2Ch	11112222h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:16	1111h RO	**Subsystem ID (SUBSYS_ID):** See Description in PCI Local Bus Specification
15:0	2222h RO	**Subsystem Vendor ID (SUBSYS_VENDORID):** See Description in PCI Local Bus Specification

8.1.12 PCIE Config Space Header 12: Expansion ROM Base Address (DMA_CFG_FIRST16DWORD_DW12_INST) — Offset 30h

Expansion ROM Base Address

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:2] + 30h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RO	**Expansion ROM Base Address (EXPANSION_ROM_BASE_ADDRESS):** See Description in PCI Local Bus Specification

8.1.13 PCIE Config Space Header 13: PCIE Capabilities Pointer (DMA_CFG_FIRST16DWORD_DW13_INST) — Offset 34h

Capabilities Pointer

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:2] + 34h	00000080h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:8	0h RO	**Reserved**
7:0	80h RO	**New Capabilities Pointer (CAPABILITIES_POINTER):** See Description in PCI Local Bus Specification

8.1.14 PCIE Config Space Header 15: Interrupt Config (DMA_CFG_FIRST16DWORD_DW15_INST) — Offset 3Ch

Interrupt configuration fields.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:2] + 3Ch	000001FFh

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:24	00h RO	**Maximum Latency gaining access to PCI bus (MAX_LAT):** See Description in PCI Local Bus Specification
23:16	00h RO	**Minimum Grant for device burst period (MIN_GNT):** See Description in PCI Local Bus Specification
15:8	01h RO	**Interrupt Pin (INTERRUPT_PIN):** See Description in PCI Local Bus Specification
7:0	FFh RW	**Interrupt Line (INTERRUPT_LINE):** See Description in PCI Local Bus Specification

8.1.15 Power Management Capability Configuration (DMA_CFG_PM_CAP_0) — Offset 80h

Power Management capability Configuration

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:2] + 80h	F8038801h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:27	1Fh RO	**PME Support (PME_SUPPORT):** See Description in PCI Local Bus Specification
26:20	0h RO	**Reserved**
19	0h RO	**PME Clock (PME_CLOCK):** See Description in PCI Local Bus Specification
18:16	3h RO	**VERSION:** See Description in PCI Local Bus Specification
15:8	88h RO	**Next Capability Pointer (NEXT_CAPABILITY_POINTER):** See Description in PCI Local Bus Specification
7:0	01h RO	**Capability ID (CAPABILITY_ID):** See Description in PCI Local Bus Specification

8.1.16 PM Capability 1 Control and Status (DMA_CFG_PM_CAP_1) — Offset 84h

Power management Control and Status

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:2] + 84h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:24	00h RO	**PM Data Reg (PM_DATA_REG):** See Description in PCI Local Bus Specification
23:16	00h RO	**BSE:** See Description in PCI Local Bus Specification
15	0h RW/1C	**PME Status (PME_STATUS):** See Description in PCI Local Bus Specification
14:13	0h RO	**Data Scale (DATA_SCALE):** See Description in PCI Local Bus Specification
12:9	0h RO	**Data Select (DATA_SEL):** See Description in PCI Local Bus Specification
8	0h RW	**PME Enable (PME_EN):** See Description in PCI Local Bus Specification
7:4	0h RO	**Reserved**
3	0h RO	**No Soft Reset (NO_SOFT_RESET):** See Description in PCI Local Bus Specification
2	0h RO	**Reserved**
1:0	0h RW	**PM State (PM_STATE):** See Description in PCI Local Bus Specification

8.1.17 MSI Capability 0: MSI Capability Config (DMA_CFG_MSIREG_DW0_INST) — Offset 88h

MSI Capability Config

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:2] + 88h	0080A005h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:25	0h RO	**Reserved**
24	0h RO	**Per vector masking capable (PER_VECTOR_MASKING_CAPABLE):** See Description in PCI Local Bus Specification
23	1h RO	**b64 address capable (B64_ADDRESS_CAPABLE):** See Description in PCI Local Bus Specification
22:20	0h RW	**Multiple Message Enable (MULTIPLE_MESSAGE_ENABLE):** See Description in PCI Local Bus Specification
19:17	0h RO	**Multiple Message Capable (MULTIPLE_MESSAGE_CAPABLE):** See Description in PCI Local Bus Specification
16	0h RW	**MSI Enable (MSI_ENABLE):** See Description in PCI Local Bus Specification
15:8	A0h RO	**NextCapability Pointer (NEXT_CAPABILITY_POINTER):** See Description in PCI Local Bus Specification
7:0	05h RO	**Capability ID (CAPABILITY_ID):** See Description in PCI Local Bus Specification

8.1.18 MSI Capability 1: Message Address Low (DMA_CFG_MSIREG_DW1_INST) — Offset 8Ch

MSI Message Address Low

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:2] + 8Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:2	00000000h RW	**Message Address Low (MESSAGE_ADDRESS_LOW):** See Description in PCI Local Bus Specification
1:0	0h RO	**Reserved**

8.1.19 MSI Capability 2: Message Address High (DMA_CFG_MSIREG_DW2_INST) — Offset 90h

MSI Message Address High

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:2] + 90h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RW	**Message Address High (MSG_ADDR_HI):** See Description in PCI Local Bus Specification

8.1.20 MSI Capability 3: Message Data (DMA_CFG_MSIREG_DW3_INST) — Offset 94h

MSI Message Data

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:2] + 94h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:16	0h RO	**Reserved**
15:0	0000h RW	**Message Data (MSG_DATA):** See Description in PCI Local Bus Specification

8.1.21 MSI Capability 4: Interrupt Mask (DMA_CFG_MSIREG_DW4_INST) — Offset 98h

MSI Interrupt Mask

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:2] + 98h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RW	**Mask Bits (MSI_MASK):** See Description in PCI Local Bus Specification

8.1.22 MSI Capability 5: Interrupt Pending (DMA_CFG_MSIREG_DW5_INST) — Offset 9Ch

MSI Interrupt Pending

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:2] + 9Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RO/V	**Pending Bits (MSI_PENDING):** See Description in PCI Local Bus Specification

8.1.23 MSIX Capability 0: MSIX Capability Config (DMA_CFG_MSIXREG_DW0_INST) — Offset A0h

MSIX Capability Config

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:2] + A0h	000F0011h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RW	**MSIX Enable (MSIX_EN):** See Description in PCI Local Bus Specification
30	0h RW	**MSIX FUN MASK (MSIX_FUN_MASK):** See Description in PCI Local Bus Specification
29:27	0h RO	**Reserved**
26:16	00Fh RO	**MSIX Table Size (MSIX_TABLE_SIZE):** See Description in PCI Local Bus Specification
15:8	00h RO	**Next to MSIX Ptr (NEXT_TO_MSIX_PTR):** See Description in PCI Local Bus Specification
7:0	11h RO	**MSIX Cap ID (MSIX_CAP_ID):** See Description in PCI Local Bus Specification

8.1.24 MSIX Capability 1: Table Offset and Table BIR (DMA_CFG_MSIXREG_DW1_INST) — Offset A4h

Table Offset and Table BIR

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:2] + A4h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:3	00000000h RO	**MSIX Table Offset (MSIX_TABLE_OFFSET):** See Description in PCI Local Bus Specification
2:0	0h RO	**MSIX Table BIR (MSIX_TABLE_BIR):** See Description in PCI Local Bus Specification

8.1.25 MSIX Capability 2: PBA Offset and PBA BIR (DMA_CFG_MSIXREG_DW2_INST) — Offset A8h

PBA Offset and PBA BIR

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:2] + A8h	00000FA0h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:3	000001F4h RO	**MSIX PBA Offset (MSIX_PBA_OFFSET):** See Description in PCI Local Bus Specification
2:0	0h RO	**MSIX PBA BIR (MSIX_PBA_BIR):** See Description in PCI Local Bus Specification

8.1.26 VS CAP 12 Thunderbolt Access Through PCIE Command Register (DMA_CFG_VS_CAP_12) — Offset D4h

VS CAP 12 PCIE Mailbox feature TBT access through PCIE Command register

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:2] + D4h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RW	**Time Out (TIMEOUT):** Set by Hardware in case of timeout
30	0h RW	**Command In Progress (COMMAND_IN_PROGRESS):** Set by Software to start wr/rd command and cleared by Hardware when command is finished or timeouts
29:24	0h RO	**Reserved**
23	0h RW	**CMD 2 (CMD_2):** 1'b0: Regular Target bus access 1'b1: Access to PCIe Switch registers
22	0h RW	**CMD 1 (CMD_1):** 1'b0: Regular Target bus access 1'b1: Access to CIO Switch registers

Bit Range	Default & Access	Field Name (ID): Description
21	0h RW	**CMD 0 (CMD_0):** 1'b0 - Read 1'b1 - Write
20:19	0h RW	**Configuration Space (CS):** Sets CS Target bus value 2'b00 - Path Configuration Space 2'b01 - Port Configuration Space 2'b10 - Device Configuration Space 2'b11 - Counters Configuration Space
18:13	00h RW	**Port ID (PORT):** Sets Port# Target bus value
12:0	0000h RW	**DW Index (DW_INDEX):** Sets DW Index Target bus value

8.1.27 VS CAP 13 Thunderbolt Access Through PCIE Write Data Register (DMA_CFG_VS_CAP_13) — Offset D8h

VS CAP 13 PCIE Mailbox feature Thunderbolt access through PCIE Write Data register

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:2] + D8h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RW	**Write Data (WRITE_DATA):** Software puts required data before performing wr command

8.1.28 VS CAP 14 Thunderbolt Access Through PCIERead Data Register (DMA_CFG_VS_CAP_14) — Offset DCh

VS CAP 14 PCIE Mailbox feature Thunderbolt access through Read data register

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:2] + DCh	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RO/V	**Read Data (READ_DATA):** Hardware puts read data for Software to read.

8.1.29 VS CAP 22: YFL Vendor Configuration Bits (DMA_CFG_VS_CAP_22) — Offset FCh

YFL Vendor Configuration Bits

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:2] + FCh	06061000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:24	06h RW	**dma active delay (DMA_ACTIVE_DELAY):** Initial value for DMA delay counter before stopping clock request.
23:16	06h RW	**D3 Reset Counter Length (D3_RESET_COUNTER_LENGTH):** Initial Value for D3 reset counter.
15:13	0h RO	**Reserved**
12:8	10h RW	**Idle Request Timeout Value (CFG_SCR_IDLE_REQ_TOUT_VAL):** IDLE_REQ TimeOUT VALue (16 ... 31).
7:3	0h RO	**Reserved**
2	0h RW	**Force Reread Imr (CB_FORCE_REREAD_IMR):** Force reread of IMR
1	0h RW	**Force Power (FORCE_POWER):** Force Power cycle. Sets IMR load needed.
0	0h RW	**RTD3 Enable (RTD3_ENABLE):** 0: Disable TRD3 1: Enable RTD3

8.2 USB Host Controller (xHCI) Registers (D13:F0)

This chapter documents the registers in Bus: 0, Device 13, Function 0.

Note: These registers do not apply to S/H processors.

8.2.1 Summary of Registers

Table 8-3. Summary of Bus: 0, Device: 13, Function: 0 Registers

Offset	Size (Bytes)	Register Name (Register Symbol)	Default Value
0h	2	Vendor ID (VID)	8086h
2h	2	Device ID (DID)	8C31h
4h	2	Command Reg (CMD)	0000h
6h	2	Device Status (STS)	0290h
8h	1	Revision ID (RID)	00h
9h	1	Programming Interface (PI)	30h
Ah	1	Sub Class Code (SCC)	03h
Bh	1	Base Class Code (BCC)	0Ch
Dh	1	Master Latency Timer (MLT)	00h
Eh	1	Header Type (HT)	80h
10h	8	Memory Base Address (MBAR)	00000000000000004h
2Ch	2	USB Subsystem Vendor ID (SSVID)	0000h
2Eh	2	USB Subsystem ID (SSID)	0000h
34h	1	Capabilities Pointer (CAP_PTR)	70h
3Ch	1	Interrupt Line (ILINE)	00h
3Dh	1	Interrupt Pin (IPIN)	00h
44h	4	XHC System Bus Configuration 2 (XHCC2)	0003C000h
58h	4	Audio Time Synchronization (AUDSYNC)	00000000h
60h	1	Serial Bus Release Number (SBRN)	31h
61h	1	Frame Length Adjustment (FLADJ)	60h
62h	1	Best Effort Service Latency (BESL)	00h
70h	1	PCI Power Management Capability ID (PM_CID)	01h
71h	1	Next Item Pointer 1 (PM_NEXT)	80h
72h	2	Power Management Capabilities (PM_CAP)	C1C2h
74h	2	Power Management Control/Status (PM_CS)	0008h
80h	1	Message Signaled Interrupt CID (MSI_CID)	05h
81h	1	Next Item Pointer (MSI_NEXT)	00h
82h	2	Message Signaled Interrupt Message Control (MSI_MCTL)	0086h
84h	4	Message Signaled Interrupt Message Address (MSI_MAD)	00000000h
88h	4	Message Signaled Interrupt Upper Address (MSI_MUAD)	00000000h
8Ch	2	Message Signaled Interrupt Message Data (MSI_MD)	0000h
A4h	4	High Speed Configuration 2 (HSCFG2)	00002000h

Offset	Size (Bytes)	Register Name (Register Symbol)	Default Value
B0h	4	XHCI USB2 Overcurrent Pin Mapping (U2OCM1)	00000000h
B4h	4	XHCI USB2 Overcurrent Pin Mapping (U2OCM2)	00000000h
B8h	4	XHCI USB2 Overcurrent Pin Mapping (U2OCM3)	00000000h
BCh	4	XHCI USB2 Overcurrent Pin Mapping (U2OCM4)	00000000h
D0h	4	XHCI USB3 Overcurrent Pin Mapping (U3OCM1)	00000000h
D4h	4	XHCI USB3 Overcurrent Pin Mapping (U3OCM2)	00000000h
D8h	4	XHCI USB3 Overcurrent Pin Mapping (U3OCM3)	00000000h
DCh	4	XHCI USB3 Overcurrent Pin Mapping (U3OCM4)	00000000h

8.2.2 Vendor ID (VID) — Offset 0h

Vendor ID

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:13, F:0] + 0h	8086h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
15:0	8086h RO	**Vendor ID (VID):** Vendor ID

8.2.3 Device ID (DID) — Offset 2h

Device ID

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:13, F:0] + 2h	8C31h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
15:0	8C31h RO/V	**Device ID (DID):** See Global Device ID table in Chap. 6 for value

8.2.4 Command Reg (CMD) — Offset 4h

Command Reg

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:13, F:0] + 4h	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:11	0h RO	**Reserved**
10	0h RW	**Interrupt Disable (INTR_DIS):** When cleared to 0, the function is capable of generating interrupts. When 1, the function can not generate its interrupt to the interrupt controller. Note that the corresponding Interrupt Status bit is not affected by the interrupt enable.
9	0h RO	**Fast Back to Back Enable (FBE):** Fast Back to Back Enable
8	0h RW	**SERR# Enable (SERR):** When set to 1, the XHC is capable of generating (internally) SERR#.
7	0h RO	**Wait Cycle Control (WCC):** Wait Cycle Control
6	0h RW	**Parity Error Response (PER):** When set to 1, the XHCI Host Controller will check for correct parity (on its internal interface) and halt operation when bad parity is detected during the data phase as recommended by the XHCI specification. Note that this applies to both requests and completions from the system interface. This bit must be set in order for the parity errors to generate SERR#.
5	0h RO	**VGA Palette Snoop (VPS):** VGA Palette Snoop
4	0h RO	**Memory Write Invalidate (MWI):** Memory Write Invalidate
3	0h RO	**Special Cycle Enable (SCE):** Special Cycle Enable
2	0h RW	**Bus Master Enable (BME):** When set, it allows XHC to act as a bus master. When cleared, it disable XHC from initiating transactions on the system bus.
1	0h RW	**Memory Space Enable (MSE):** This bit controls access to the XHC Memory Space registers. If this bit is set, accesses to the XHC registers are enabled. The Base Address register for the XHC should be programmed before this bit is set.
0	0h RO	**I/O Space Enable (IOSE):** Reserved

8.2.5 Device Status (STS) — Offset 6h

Device Status

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:13, F:0] + 6h	0290h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15	0h RW/1C	**Detected Parity Error (DPE):** This bit is set by the Intel PCH whenever a parity error is seen on the internal interface to the XHC host controller, regardless of the setting of bit 6 or bit 8 in the Command register or any other conditions. Software clears this bit by writing a 1 to this bit location.
14	0h RW/1C	**Signaled System Error (SSE):** This bit is set by the Intel PCH whenever it signals SERR# (internally). The SERR_EN bit (bit 8 in the Command Register) must be 1 for this bit to be set. Software clears this bit by writing a 1 to this bit location.
13	0h RW/1C	**Received Master-Abort Status (RMA):** This bit is set when XHC, as a master, receives a master-abort status on a memory access. This is treated as a Host Error and halts the DMA engines. Software clears this bit by writing a 1 to this bit location.
12	0h RW/1C	**Received Target Abort Status (RTA):** This bit is set when XHC, as a master, receives a target abort status on a memory access. This is treated as a Host Error and halts the DMA engines. Software clears this bit by writing a 1 to this bit location.
11	0h RW/1C	**Signaled Target-Abort Status (STA):** This bit is used to indicate when the XHC function responds to a cycle with a target abort.
10:9	1h RO	**DEVSEL# Timing Status (DEVT):** This 2-bit field defines the timing for DEVSEL# assertion. Read-Only.
8	0h RW/1C	**Master Data Parity Error Detected (MDPED):** This bit is set by the Intel PCH whenever a data parity error is detected on a XHC read completion packet on the internal interface to the XHC host controller and bit 6 of the Command register is set to 1. Software clears this bit by writing a 1 to this bit location.
7	1h RO	**Fast Back-to-Back Capable (FBBC):** Reserved
6	0h RO	**User Definable Features (UDF):** Reserved
5	0h RO	**66 MHz Capable (MC):** Reserved
4	1h RO	**Capabilities List (CL):** Hardwired to 1 indicating that offset 34h contains a valid capabilities pointer.
3	0h RO/V	**Interrupt Status (INTR_STS):** This read-only bit reflects the state of this function's interrupt at the input of the enable/disable logic. This bit is a 1 when the interrupt is asserted. This bit will be 0 when the interrupt is deasserted. The value reported in this bit is independent of the value in the Interrupt Enable bit.
2:0	0h RO	**Reserved**

8.2.6 Revision ID (RID) — Offset 8h

Revision ID

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:13, F:0] + 8h	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:0	00h RO/V	**Revision ID (RID):** See Chap 6 for value.

8.2.7 Programming Interface (PI) — Offset 9h

Programming Interface

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:13, F:0] + 9h	30h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:0	30h RO	**Programming Interface (PI):** A value of 30h indicates that this USB Host Controller conforms to the XHCI specification.

8.2.8 Sub Class Code (SCC) — Offset Ah

Sub Class Code

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:13, F:0] + Ah	03h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:0	03h RO	**Sub Class Code (SCC):** A value of 03h indicates that this is a Universal Serial Bus Host Controller.

8.2.9 Base Class Code (BCC) — Offset Bh

Base Class Code

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:13, F:0] + Bh	0Ch

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:0	0Ch RO	**Base Class Code (BCC):** A value of 0Ch indicates that this is a Serial Bus controller.

8.2.10 Master Latency Timer (MLT) — Offset Dh

Master Latency Timer

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:13, F:0] + Dh	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:0	00h RO	**Master Latency Timer (MLT):** Because the XHC controller is internally implemented with arbitration on an internal interface, it does not need a master latency timer. The bits will be fixed at 0.

8.2.11 Header Type (HT) — Offset Eh

Header Type

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:13, F:0] + Eh	80h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7	1h RO	**Multi-Function Bit (MFB):** Read only indicating single function device.
6:0	00h RO	**Configuration layout (CL):** Hardwired to 0 to indicate a standard PCI configuration layout.

8.2.12 Memory Base Address (MBAR) — Offset 10h

Value in this register will be different after the enumeration process.

Type	Size	Offset	Default
PCI	64 bit	[B:0, D:13, F:0] + 10h	0000000000000004h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
63:16	0000000000000h RW	**Base Address (BA):** Bits (63:16) correspond to memory address signals (63:16), respectively. This gives 64 KB of relocatable memory space aligned to 64 KB boundaries.
15:4	0h RO	**Reserved**
3	0h RO	**PREFETCHABLE:** This bit is hardwired to 0 indicating that this range should not be prefetched.
2:1	2h RO	**Memory BAR Type (MBAR_TYPE):** If this field is hardwired to 00 it indicates that this range can be mapped anywhere within 32-bit address space. If this field is hardwired to 10 it indicates that this range can be mapped anywhere within 64-bit address space.
0	0h RO	**Resource Type Indicator (RTE):** This bit is hardwired to 0 indicating that the base address field in this register maps to memory space

8.2.13 USB Subsystem Vendor ID (SSVID) — Offset 2Ch

This register is modified and maintained by BIOS

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:13, F:0] + 2Ch	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:0	0000h RW/L	**USB Subsystem Vendor ID (SSVID):** This register, in combination with the USB Subsystem ID register, enables the operating system to distinguish each subsystem from the others. **Locked by:** XHCC1.ACCTRL

8.2.14 USB Subsystem ID (SSID) — Offset 2Eh

This register is modified and maintained by BIOS

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:13, F:0] + 2Eh	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:0	0000h RW/L	**USB Subsystem ID (SSID):** BIOS sets the value in this register to identify the Subsystem ID. This register, in combination with the Subsystem Vendor ID register, enables the operating system to distinguish each subsystem from other(s). **Locked by:** XHCC1.ACCTRL

8.2.15 Capabilities Pointer (CAP_PTR) — Offset 34h

Capabilities Pointer

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:13, F:0] + 34h	70h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:0	70h RO	**Capabilities Pointer (CAP_PTR):** This register points to the starting offset of the capabilities ranges.

8.2.16 Interrupt Line (ILINE) — Offset 3Ch

Interrupt Line

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:13, F:0] + 3Ch	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
7:0	00h RW	**Interrupt Line (ILINE):** This data is not used by the Intel PCH. It is used as a scratchpad register to communicate to software the interrupt line that the interrupt pin is connected to.

8.2.17 Interrupt Pin (IPIN) — Offset 3Dh

This register is modified and maintained by BIOS

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:13, F:0] + 3Dh	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
7:0	00h RW/L	**Interrupt pin (IPIN):** Bits 7:0 reflect the Interrupt Pin assigned to the host controller by the platform (and are hardwired). **Locked by:** XHCC1.ACCTRL

8.2.18 XHC System Bus Configuration 2 (XHCC2) — Offset 44h

XHC System Bus Configuration.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:0] + 44h	0003C000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RW	**OC Configuration Done (OCCFGDONE):** This bit is used by BIOS to prevent spurious switching during OC configuration. It must be set by BIOS after configuration of the OC mapping bits is complete. Once this bit is set, OC mapping shall not be changed by SW.
30	0h RW	**Enable Relaxed Ordering (RO_EN):** This bit is used to assert Relaxed Ordering bit
29:28	0h RW	**MMIO Back to Back Rd/Wr Delay Count (RW_DLY_CNT):** This field controls the delay in PRIM_CLK clocks applied to the delay inserted between the MMIO Rd/Wr or Wr/Wr back to back scenarios if enabled via XHCC2[11:10] 0x0 - 64 clocks 0x1 - 128 clocks 0x2 - 256 clocks 0x3 - N/A
27:26	0h RO	**Reserved**
25	0h RW	**DMA Request Boundary Crossing Control (DREQBCC):** This bit controls the boundary crossing limit of each Read/Write Request. 0: 4KB 1: 64B

Bit Range	Default & Access	Field Name (ID): Description
24:22	0h RW	**IDMA Write Request Size Control (WRREQSZCTRL):** Write Request Size Control: This bit controls the maximum size of each Write Request. 000: 128B 001: 256B 011 - 110: Reserved 111: 64B
21	0h RW	**XHC Upstream Read Relaxed Ordering Enable (XHCUPRDROE):** Setting this to 1 disable downstream completion resource checking and allow upstream NP ready beyond Non-posed pre-allocation limit set by bits 20:14
20:14	0Fh RW	**Upstream Non-Posted Pre-Allocation (UNPPA):** This field reserves data sizes, in 64 byte chunks, of the downstream completion resource. This value is zero based. 000000 - 111111: Pre-allocate 64 bytes - 4096 bytes If set greater than the default allows over-allocation If set less than default allows under-allocation Only allowed to be programmed when BME = 0 and no outstanding downstream completion
13:12	0h RW	**Software Assisted xHC Idle Policy (SWAXHCIP):** Note: Irrespective of the setting of this field, a software write of 0 to SWAXHCI will clear the bit. 00b (default): xHC HW clears SWAXHCI bit upon: n MMIO access to Host Controller OR n xHC HW exits Idle state 01b: xHC HW does not autonomously clear SWAXHCI bit. The bit could be cleared only by SW. 10b: xHC HW clears SWAXHCI upon MMIO access to Host Controller. xHC HW exit from Idle state will not clear SWAXHCI. 11b: Reserved
11	0h RW	**MMIO Read After MMIO Write Delay Disable (RAWDD):** This field controls delay on MMIO Read after MMIO Write. 0b (Default): Delay MMIO Read after MMIO Write 1b: Do not delay MMIO Read after MMIO Write
10	0h RW	**MMIO Write After MMIO Write Delay Enable (WAWDE):** This field controls delay on MMIO Write after previous MMIO Write. 0b (Default): Do not delay MMIO Write after previous MMIO Write 1b: Delay MMIO Write after previous MMIO Write
9:8	0h RW	**SW Assisted Cx Inhibit (SWACXIHB):** This field controls how the DMI L1 inhibit signal from USB3 to PMC will behave. 00: Never inhibit Cx 01: Inhibit Cx when Isochronous Endpoint is active (PPT Behavior) 10: Inhibit Cx when Periodic Active as defined in 40.4.3.2.1 11: Always inhibit Cx
7:6	0h RW	**SW Assisted DMI L1 Inhibit (SWADMIL1IHB):** This field controls how the DMI L1 inhibit signal from USB3 to DMI will behave. 00: Never inhibit DMI L1. 01: Inhibit DMI L1 when Isochronous Endpoint is active (PPT Behavior). 10: Inhibit DMI L1 when periodic Active as defined in 40.4.3.2.1. 11: Inhibit DMI L1 if XHCC1.SWAXHCI = 0.

Bit Range	Default & Access	Field Name (ID): Description
5:3	0h RW	**L1 Force P2 Clock Gating Wait Count (L1FP2CGWC):** If programmed to non zero, it allows L1 force P2 gating off the clock to be delayed after the time-out period specified. If wake up event is detected before the time-out, pclk remains alive and trigger L1 exit as though CPU host is causing the wake, 000: Disabled 001: 128 bb_cclk 010: 256 bb_cclk 011: 512 bb_cclk 100: 1024 bb_cclk 101: 2048 bb_cclk 110: 4096 bb_cclk 111: 131072 bb_cclk
2:0	0h RW	**Read Request Size Control (RDREQSZCTRL):** Read Request Size Control: This bit controls the maximum size of each Read Request. 000: 128B 001: 256B 010: 512B 011 - 110: Reserved 111: 64B

8.2.19 Audio Time Synchronization (AUDSYNC) — Offset 58h

This 32 bit register is used for audio stream synchronization across different devices. Global signal sample_now captures a value in AUDSYNC register.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:0] + 58h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:30	0h RO	**Reserved**
29:16	0000h RO/V	**Captured Frame List Current Index/Frame Number (CMFI):** The value in this register is updated in response to sample_now signal. Bits (29:16) reflect state of bits (13:0) of FRINDEX
15:13	0h RO	**Reserved**
12:0	0000h RO/V	**Captured Micro-frame BLIF (CMFB):** The value is updated in response to sample_now signal and provides information about offset within micro-frame. Captured value represents number of 8 high-speed bit time units from start of micro-frame. At the beginning of micro-frame captured value will be 0 and increase to maximum value at the end. Default maximum value is 7499 but it may be changed as result of adjustment done in FLA.

8.2.20 Serial Bus Release Number (SBRN) — Offset 60h

Serial Bus Release Number

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:13, F:0] + 60h	31h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:0	31h RO	**Serial Bus Release Number (SBRN):** A value of 30h indicates that this controller follows USB release 3.0.

8.2.21 Frame Length Adjustment (FLADJ) — Offset 61h

This feature is used to adjust any offset from the clock source that generates the clock that drives the SOF counter. When a new value is written into these six bits, the length of the frame is adjusted. Its initial programmed value is system dependent based on the accuracy of hardware USB clock and is initialized by system BIOS. This register should only be modified when the HChalted bit in the USBSTS register is a one. Changing value of this register while the host controller is operating yields undefined results.

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:13, F:0] + 61h	60h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7	0h RO	**Reserved**
6	1h RO	**No Frame Length Timing Capability (NO_FRAME_LENGTH_TIMING_CAP):** This flag is set to 1 to indicate that the host controller does not support a programmable Frame Length Timing Value field.

Bit Range	Default & Access	Field Name (ID): Description
5:0	20h RO	**Frame Length Timing Value (FLTV):** SOF micro-frame length) is equal to 59488 + value in this field. The default value is decimal 32 (20h), which gives a SOF cycle time of 60000. Frame Length (number of High Speed bit times) FLADJ Value (decimal) (decimal) 59488 0 (00h) 59504 1 (01h) 59520 2 (02h) ... 59984 31 (1Fh) 60000 32 (20h) ... 60480 62 (3Eh) 60496 63 (3Fh) Each decimal value change to this register corresponds to 16 high-speed bit times. The SOF cycle time (number of SOF counter clock periods to generate a SOF micro-frame length) is equal to 59488 + value in this field. The default value is decimal 32 (20h), which gives a SOF cycle time of 60000. Frame Length (# High Speed bit times) FLADJ Value

8.2.22 Best Effort Service Latency (BESL) — Offset 62h

Best Effort Service Latency.

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:13, F:0] + 62h	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
7:4	0h RW/L	**Default Best Effort Service Latency Deep (DBESLD):** Default Best Effort Service Latency (DBESLD) If the value of this field is non-zero, it defines the recommended value for programming the PORTPMSC register BESLD field. This is programmed by BIOS based on platform parameters. **Locked by:** XHCC1.ACCTRL
3:0	0h RW/L	**Default Best Effort Service Latency (DBESL):** If the value of this field is non-zero, it defines the recommended value for programming the PORTPMSC register BESL field. This is programmed by BIOS based on platform parameters. **Locked by:** XHCC1.ACCTRL

8.2.23 PCI Power Management Capability ID (PM_CID) — Offset 70h

PCI Power Management Capability ID

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:13, F:0] + 70h	01h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:0	01h RO	**PCI Power Management Capability ID (PM_CID):** A value of 01h indicates that this is a PCI Power Management capabilities field.

8.2.24 Next Item Pointer 1 (PM_NEXT) — Offset 71h

This register is modified and maintained by BIOS

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:13, F:0] + 71h	80h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
7:0	80h RW/L	**Next Item Pointer 1 (PM_NEXT):** This register defaults to 80h, which indicates that the next capability registers begin at configuration offset 80h. This register is writable when the Access Control bit is set to '0'. This allows BIOS to effectively hide the next capability registers, if necessary. This register should only be written during system initialization before the plug-and-play software has enabled any master-initiated traffic. Values of: 80h implies next capability is MSI 00h implies that MSI capability is hidden. Note: This value is never expected to be programmed. **Locked by:** XHCC1.ACCTRL

8.2.25 Power Management Capabilities (PM_CAP) — Offset 72h

Normally, this register is read-only to report capabilities to the power management software. In order to report different power management capabilities depending on the system in which the Intel PCH is used, the write access to this register is controlled by the Access Control bit (ACCTRL). The value written to this register does not affect the hardware other than changing the value returned during a read.

This register is modified and maintained by BIOS

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:13, F:0] + 72h	C1C2h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:11	18h RW/L	**PME Support (PME_SUPPORT):** This 5-bit field indicates the power states in which the function may assert PME#. The Intel PCH XHC does not support the D1 or D2 states. For all other states, the Intel PCH XHC is capable of generating PME#. Software should never need to modify this field. **Locked by:** XHCC1.ACCTRL
10	0h RW/L	**D2 Support (D2_SUPPORT):** The D2 state is not supported. **Locked by:** XHCC1.ACCTRL
9	0h RW/L	**D1 Support (D1_SUPPORT):** The D1 state is not supported. **Locked by:** XHCC1.ACCTRL
8:6	7h RW/L	**Auxiliary Current (AUX_CURRENT):** The Intel PCH XHC reports 375mA maximum Suspend well current required when in the D3cold state. This value can be written by BIOS when a more accurate value is known. **Locked by:** XHCC1.ACCTRL
5	0h RW/L	**DSI:** The Intel PCH reports 0, indicating that no device-specific initialization is required. **Locked by:** XHCC1.ACCTRL
4	0h RO	**Reserved**
3	0h RW/L	**PME Clock (PMECLOCK):** The Intel PCH reports 0, indicating that no PCI clock is required to generate PME#. **Locked by:** XHCC1.ACCTRL
2:0	2h RW/L	**VERSION:** The Intel PCH reports 010, indicating that it complies with Revision 1.1 of the PCI Power Management Specification. **Locked by:** XHCC1.ACCTRL

8.2.26 Power Management Control/Status (PM_CS) — Offset 74h

Power Management Control/Status

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:13, F:0] + 74h	0008h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15	0h RW/1C	**PME Status (PME_STATUS):** This bit is set when the Intel PCH XHC would normally assert the PME# signal independent of the state of the PME_En bit. Writing a 1 to this bit will clear it and cause the internal PME to deassert (if enabled). Writing a 0 has no effect. This bit must be explicitly cleared by the operating system each time the operating system is loaded.
14:13	0h RO	**Data Scale (DATA_SCALE):** The Intel PCH hardwires these bits to 00 because it does not support the associated Data register.
12:9	0h RO	**Data Select (DATA_SELECT):** The Intel PCH hardwires these bits to 0000 because it does not support the associated Data register.
8	0h RW	**PME Enable (PME_EN):** A 1 enables the Intel PCH XHC to generate an internal PME signal when PME_Status is 1. This bit must be explicitly cleared by the operating system each time it is initially loaded.
7:4	0h RO	**Reserved**
3	1h RO	**No Soft Reset (NSR):** No_Soft_Reset - When set ("1"), this bit indicates that devices transitioning from D3hot to D0 because of PowerState commands do not perform an internal reset. Configuration Context is preserved. Upon transition from the D3hot to the D0 Initialized state, no additional operating system intervention is required to preserve Configuration Context beyond writing the PowerState bits. Transition from D3hot to D0 by a system or bus segment reset will return to the device state D0 Uninitialized with only PME context preserved if PME is supported and enabled.
2	0h RO	**Reserved**
1:0	0h RW	**POWERSTATE:** This 2-bit field is used both to determine the current power state of XHC function and to set a new power state. The definition of the field values are: 00b - D0 state 11b - D3hot state If software attempts to write a value of 10b or 01b in to this field, the write operation must complete normally, however, the data is discarded and no state change occurs. When in the D3hot state, the Intel PCH must not accept accesses to the XHC memory range, but the configuration space must still be accessible.

8.2.27 Message Signaled Interrupt CID (MSI_CID) — Offset 80h

Message Signaled Interrupt CID

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:13, F:0] + 80h	05h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:0	05h RO	**Capability ID (CID):** Indicates that this is an MSI capability

8.2.28 Next Item Pointer (MSI_NEXT) — Offset 81h

Next Item Pointer

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:13, F:0] + 81h	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
7:0	00h RW/L	**Next Pointer (NEXT_POINTER):** Indicates that this is the last item on the capability list **Locked by:** XHCC1.ACCTRL

8.2.29 Message Signaled Interrupt Message Control (MSI_MCTL) — Offset 82h

Message Signaled Interrupt Message Control

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:13, F:0] + 82h	0086h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:9	0h RO	**Reserved**
8	0h RO	**Per-Vector Masking Capable (PVM):** Specifies whether controller supports MSI per vector masking. Not supported
7	1h RO	**64 Bit Address Capable (C64):** Specifies whether capable of generating 64-bit messages. This device is 64-bit capable.
6:4	0h RW	**Multiple Message Enable (MME):** Indicates the number of messages the controller should assert. This device supports multiple message MSI.
3:1	3h RO	**Multiple Message Capable (MMC):** Indicates the number of messages the controller wishes to assert. This field must be set by HW to reflect the number of Interrupters supported. Encoding number of Vectors requested (number of Interrupters) 000 1 001 2 010 4 011 8 100 16 101 32 110-111 Reserved
0	0h RW	**MSI Enable (MSIE):** If set to 1, MSI is enabled and the traditional interrupt pins are not used to generate interrupts. If cleared to 0, MSI operation is disabled and the traditional interrupt pins are used.

8.2.30 Message Signaled Interrupt Message Address (MSI_MAD) — Offset 84h

Message Signaled Interrupt Message Address

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:0] + 84h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:2	00000000h RW	**ADDR:** Lower DW of system specified message address, always DWORD aligned
1:0	0h RO	**Reserved**

8.2.31 Message Signaled Interrupt Upper Address (MSI_MUAD) — Offset 88h

Message Signaled Interrupt Upper Address

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:0] + 88h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RW	**Upper Addr (UPPERADDR):** Upper DW of system specified message address.

8.2.32 Message Signaled Interrupt Message Data (MSI_MD) — Offset 8Ch

Message Signaled Interrupt Message Data

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:13, F:0] + 8Ch	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:0	0000h RW	**DATA:** This 16-bit field is programmed by system software if MSI is enabled. Its content is driven onto the lower word (PCI AD(15:0)) during the data phase of the MSI memory write transaction. The Multiple Message Enable field (bits 6-4 of the Message Control register) defines the number of low order message data bits the function is permitted to modify to generate its system software allocated vectors. For example, a Multiple Message Enable encoding of 010 indicates the function has been allocated four vectors and is permitted to modify message data bits 1 and 0 (a function modifies the lower message data bits to generate the allocated number of vectors). If the Multiple Message Enable field is 000, the function is not permitted to modify the message data.

8.2.33 High Speed Configuration 2 (HSCFG2) — Offset A4h

High Speed Configuration 2

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:0] + A4h	00002000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:19	0h RO	**Reserved**
18	0h RW	**Port1 Host Mode Override (PORT1_HOST_MODE_OVERRIDE):** When set, this bit causes the Host_Device mux on port 1 to be forced into the Host mode.
17:16	0h RW	**EUSB2SEL:** The two bits are associate with USB2 ports 1 - bit 16 and 2 - bit 2 0: Port is mapped to USB2 1: Port is mapped to eUSB2
15	0h RW	**HS ASYNC Active IN Mask (HSAAIM):** Determines if the Async Active will mask/ignore IN EP s. 0 HS ASYNC Active will include IN EP s. 1 HS ASYNC Active will mask/ignore IN EP s.

Bit Range	Default & Access	Field Name (ID): Description
14	0h RW	**HS OUT ASYNC Active Polling EP Mask (HSOAAPEPM):** Determines if the Async Active for OUT HS/FS/LS masks/ignores EP s that are polling/PINGing (HS) due to NAK. 0 HS OUT ASYNC Active will include EP s that are polling. 1 HS OUT ASYNC Active will mask/ignore EP s that are polling.
13	1h RW	**HS IN ASYNC Active Polling EP Mask (HSIAAPEPM):** Determines if the Async Active for IN HS/FS/LS masks/ignores EP s that are polling due to NAK. 0 HS IN ASYNC Active will include EP s that are polling. 1 HS IN ASYNC Active will mask/ignore EP s that are polling.
12:11	0h RW	**HS INTR IN Periodic Active Policy Control (HSIIPAPC):** Controls how the HS INTR IN periodic active is used to generate the global periodic active. This will determine how the smallest service interval among active EP s and number of active EP s are used. 0 HS INTR IN periodic active will be used to generate periodic active if Service Interval Threshold OR Numb of EP Threshold values meet the requirement. 1 HS INTR IN periodic active will be used to generate periodic active if Service Interval Threshold AND Numb of EP Threshold values meet the requirement. 2 Always allow HS INTR EP s to be used in the generation of the global Periodic Active indication. 3 Never allow HS INTR EP s to be used in the generation of the global Periodic Active indication
10:4	00h RW	**HS INTR IN Periodic Active Num of EP Threshold (HSIIPANEPT):** Defines the threshold used to determine if Periodic active may include HS/FS/LS INTR IN EP active indication. If there are more than NumEPThreshold active HS/FS/LS INTR EP s then they may be included as part of the periodic active generation.
3:0	0h RW	**HS INTR IN Periodic Active Service Interval Threshold (HSIIPASIT):** Defines the Service Interval threshold used to determine if Periodic active will include HS/FS/LS INTR IN EP active indication. If there are any active HS/FS/LS INTR EP s with a service interval less than or equal to this threshold then they may be included as part of the periodic active generation.

8.2.34 XHCI USB2 Overcurrent Pin Mapping (U2OCM1) — Offset B0h

The RW/L property of this register is controlled by OCCFDONE bit.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:0] + B0h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:1	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
0	0h RW/L	**OC Mapping (OCM):** USB2 Port assignment When Set to 1, Bit 0 maps the OC pin N to USB2 std. port 1 Bit 1 maps the OC pin N to USB2 std port 2 ... Bit (NumUSB2std-1) maps the OC pin N to USB2 Std port NumUSB2std Note: The USB-R port which is the most significant USB2 port does not have an OC pin. Thus the OC assignment for the USB-R port is ignored. **Locked by:** XHCC2.OCCFGDONE

8.2.35 XHCI USB2 Overcurrent Pin Mapping (U2OCM2) — Offset B4h

The RW/L property of this register is controlled by OCCFDONE bit.

Note: Bit definitions are the same as U2OCM1, offset B0h.

8.2.36 XHCI USB2 Overcurrent Pin Mapping (U2OCM3) — Offset B8h

The RW/L property of this register is controlled by OCCFDONE bit.

Note: Bit definitions are the same as U2OCM1, offset B0h.

8.2.37 XHCI USB2 Overcurrent Pin Mapping (U2OCM4) — Offset BCh

The RW/L property of this register is controlled by OCCFDONE bit.

Note: Bit definitions are the same as U2OCM1, offset B0h.

8.2.38 XHCI USB3 Overcurrent Pin Mapping (U3OCM1) — Offset D0h

The RW/L property of this register is controlled by OCCFDONE bit.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:0] + D0h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:4	0h RO	**Reserved**
3:0	0h RW/L	**OC Mapping (OCM):** USB3 Port assignment When Set to 1, Bit 0 maps the OC pin N to USB3 std. port 1 Bit 1 maps the OC pin N to USB3 std port 2 ... Bit (NumUSB3std-1) maps the OC pin N to USB3 Std port NumUSB3std **Locked by:** XHCC2.OCCFGDONE

8.2.39 XHCI USB3 Overcurrent Pin Mapping (U3OCM2) — Offset D4h

The RW/L property of this register is controlled by OCCFDONE bit.

Note: Bit definitions are the same as U3OCM1, offset D0h.

8.2.40 XHCI USB3 Overcurrent Pin Mapping (U3OCM3) — Offset D8h

The RW/L property of this register is controlled by OCCFDONE bit.

Note: Bit definitions are the same as U3OCM1, offset D0h.

8.2.41 XHCI USB3 Overcurrent Pin Mapping (U3OCM4) — Offset DCh

The RW/L property of this register is controlled by OCCFDONE bit.

Note: Bit definitions are the same as U3OCM1, offset D0h.

8.3 USB Host Controller MBAR Registers (D13:F0)

This chapter documents the USB Host Controller MBAR registers. The Base address of these registers is defined in the MBAR register which resides in the USB Host Controller register collection (D13:F0).

Note: These registers apply to all processors.

8.3.1 Summary of Registers

Table 8-4. Summary of MBAR Registers

Offset	Size (Bytes)	Register Name (Register Symbol)	Default Value
0h	1	Capability Registers Length (CAPLENGTH)	80h
2h	2	Host Controller Interface Version Number (HCIVERSION)	0101h
4h	4	Structural Parameters 1 (HCSPARAMS1)	05000840h
8h	4	Structural Parameters 2 (HCSPARAMS2)	14200054h
Ch	4	Structural Parameters 3 (HCSPARAMS3)	00040001h
10h	4	Capability Parameters (HCCPARAMS)	200077C1h
14h	4	Doorbell Offset (DBOFF)	00003000h
18h	4	Runtime Register Space Offset (RTSOFF)	00002000h
80h	4	USB Command (USBCMD)	00000000h
84h	4	USB Status (USBSTS)	00000001h
88h	4	Page Size (PAGESIZE)	00000001h
94h	4	Device Notification Control (DNCTRL)	00000000h
98h	4	Command Ring Low (CRCR_LO)	00000000h
9Ch	4	Command Ring High (CRCR_HI)	00000000h
B0h	4	Device Context Base Address Array Pointer Low (DCBAAP_LO)	00000000h
B4h	4	Device Context Base Address Array Pointer High (DCBAAP_HI)	00000000h
B8h	4	Configure Reg (CONFIG)	00000000h
480h	4	Port Status AndControl USB2 (PORTSC1)	000002A0h
484h	4	Port Power Management Status Aand Control USB2 (PORTPMSC1)	00000000h
48Ch	4	Port X Hardware LPM Control Register (PORTHLPMC1)	00000000h
490h	4	Port Status And Control USB3 (PORTSC2)	000002A0h
494h	4	Port Power Management Status And Control USB3 (PORTPMSC2)	00000000h
498h	4	USB3 Port Link Info (PORTLI2)	00000000h
4A0h	4	Port Status And Control USB3 (PORTSC3)	000002A0h
4A4h	4	Port Power Management Status And Control USB3 (PORTPMSC3)	00000000h
4A8h	4	USB3 Port Link Info (PORTLI3)	00000000h
4B0h	4	Port Status And Control USB3 (PORTSC4)	000002A0h
4B4h	4	Port Power Management Status And Control USB3 (PORTPMSC4)	00000000h
4B8h	4	USB3 Port Link Info (PORTLI4)	00000000h
4C0h	4	Port Status And Control USB3 (PORTSC5)	000002A0h
4C4h	4	Port Power Management Status And Control USB3 (PORTPMSC5)	00000000h
4C8h	4	USB3 Port Link Info (PORTLI5)	00000000h

Offset	Size (Bytes)	Register Name (Register Symbol)	Default Value
2000h	4	Microframe Index (RTMFINDEX)	00000000h
2020h	4	Interrupter Management (IMAN0)	00000000h
2024h	4	Interrupter Moderation (IMOD0)	00000FA0h
2028h	4	Event Ring Segment Table Size (ERSTSZ0)	00000000h
2030h	4	Event Ring Segment Table Base Address Low (ERSTBA_LO0)	00000000h
2034h	4	Event Ring Segment Table Base Address High (ERSTBA_HI0)	00000000h
2038h	4	Event Ring Dequeue Pointer Low (ERDP_LO0)	00000000h
203Ch	4	Event Ring Dequeue Pointer High (ERDP_HI0)	00000000h
2040h	4	Interrupter Management (IMAN1)	00000000h
2044h	4	Interrupter Moderation (IMOD1)	00000FA0h
2048h	4	Event Ring Segment Table Size (ERSTSZ1)	00000000h
2050h	4	Event Ring Segment Table Base Address Low (ERSTBA_LO1)	00000000h
2054h	4	Event Ring Segment Table Base Address High (ERSTBA_HI1)	00000000h
2058h	4	Event Ring Dequeue Pointer Low (ERDP_LO1)	00000000h
205Ch	4	Event Ring Dequeue Pointer High (ERDP_HI1)	00000000h
2060h	4	Interrupter Management (IMAN2)	00000000h
2064h	4	Interrupter Moderation (IMOD2)	00000FA0h
2068h	4	Event Ring Segment Table Size (ERSTSZ2)	00000000h
2070h	4	Event Ring Segment Table Base Address Low (ERSTBA_LO2)	00000000h
2074h	4	Event Ring Segment Table Base Address High (ERSTBA_HI2)	00000000h
2078h	4	Event Ring Dequeue Pointer Low (ERDP_LO2)	00000000h
207Ch	4	Event Ring Dequeue Pointer High (ERDP_HI2)	00000000h
2080h	4	Interrupter Management (IMAN3)	00000000h
2084h	4	Interrupter Moderation (IMOD3)	00000FA0h
2088h	4	Event Ring Segment Table Size (ERSTSZ3)	00000000h
2090h	4	Event Ring Segment Table Base Address Low (ERSTBA_LO3)	00000000h
2094h	4	Event Ring Segment Table Base Address High (ERSTBA_HI3)	00000000h
2098h	4	Event Ring Dequeue Pointer Low (ERDP_LO3)	00000000h
209Ch	4	Event Ring Dequeue Pointer High (ERDP_HI3)	00000000h
20A0h	4	Interrupter Management (IMAN4)	00000000h
20A4h	4	Interrupter Moderation (IMOD4)	00000FA0h
20A8h	4	Event Ring Segment Table Size (ERSTSZ4)	00000000h
20B0h	4	Event Ring Segment Table Base Address Low (ERSTBA_LO4)	00000000h
20B4h	4	Event Ring Segment Table Base Address High (ERSTBA_HI4)	00000000h
20B8h	4	Event Ring Dequeue Pointer Low (ERDP_LO4)	00000000h
20BCh	4	Event Ring Dequeue Pointer High (ERDP_HI4)	00000000h
20C0h	4	Interrupter Management (IMAN5)	00000000h
20C4h	4	Interrupter Moderation (IMOD5)	00000FA0h
20C8h	4	Event Ring Segment Table Size (ERSTSZ5)	00000000h
20D0h	4	Event Ring Segment Table Base Address Low (ERSTBA_LO5)	00000000h
20D4h	4	Event Ring Segment Table Base Address High (ERSTBA_HI5)	00000000h

Offset	Size (Bytes)	Register Name (Register Symbol)	Default Value
20D8h	4	Event Ring Dequeue Pointer Low (ERDP_LO5)	00000000h
20DCh	4	Event Ring Dequeue Pointer High (ERDP_HI5)	00000000h
20E0h	4	Interrupter Management (IMAN6)	00000000h
20E4h	4	Interrupter Moderation (IMOD6)	00000FA0h
20E8h	4	Event Ring Segment Table Size (ERSTSZ6)	00000000h
20F0h	4	Event Ring Segment Table Base Address Low (ERSTBA_LO6)	00000000h
20F4h	4	Event Ring Segment Table Base Address High (ERSTBA_HI6)	00000000h
20F8h	4	Event Ring Dequeue Pointer Low (ERDP_LO6)	00000000h
20FCh	4	Event Ring Dequeue Pointer High (ERDP_HI6)	00000000h
2100h	4	Interrupter Management (IMAN7)	00000000h
2104h	4	Interrupter Moderation (IMOD7)	00000FA0h
2108h	4	Event Ring Segment Table Size (ERSTSZ7)	00000000h
2110h	4	Event Ring Segment Table Base Address Low (ERSTBA_LO7)	00000000h
2114h	4	Event Ring Segment Table Base Address High (ERSTBA_HI7)	00000000h
2118h	4	Event Ring Dequeue Pointer Low (ERDP_LO7)	00000000h
211Ch	4	Event Ring Dequeue Pointer High (ERDP_HI7)	00000000h
3000h	4	Door Bell (DB0)	00000000h
3004h	4	Door Bell (DB1)	00000000h
3008h	4	Door Bell (DB2)	00000000h
300Ch	4	Door Bell (DB3)	00000000h
3010h	4	Door Bell (DB4)	00000000h
3014h	4	Door Bell (DB5)	00000000h
3018h	4	Door Bell (DB6)	00000000h
301Ch	4	Door Bell (DB7)	00000000h
3020h	4	Door Bell (DB8)	00000000h
3024h	4	Door Bell (DB9)	00000000h
3028h	4	Door Bell (DB10)	00000000h
302Ch	4	Door Bell (DB11)	00000000h
3030h	4	Door Bell (DB12)	00000000h
3034h	4	Door Bell (DB13)	00000000h
3038h	4	Door Bell (DB14)	00000000h
303Ch	4	Door Bell (DB15)	00000000h
3040h	4	Door Bell (DB16)	00000000h
3044h	4	Door Bell (DB17)	00000000h
3048h	4	Door Bell (DB18)	00000000h
304Ch	4	Door Bell (DB19)	00000000h
3050h	4	Door Bell (DB20)	00000000h
3054h	4	Door Bell (DB21)	00000000h
3058h	4	Door Bell (DB22)	00000000h
305Ch	4	Door Bell (DB23)	00000000h
3060h	4	Door Bell (DB24)	00000000h

Offset	Size (Bytes)	Register Name (Register Symbol)	Default Value
3064h	4	Door Bell (DB25)	00000000h
3068h	4	Door Bell (DB26)	00000000h
306Ch	4	Door Bell (DB27)	00000000h
3070h	4	Door Bell (DB28)	00000000h
3074h	4	Door Bell (DB29)	00000000h
3078h	4	Door Bell (DB30)	00000000h
307Ch	4	Door Bell (DB31)	00000000h
3080h	4	Door Bell (DB32)	00000000h
3084h	4	Door Bell (DB33)	00000000h
3088h	4	Door Bell (DB34)	00000000h
308Ch	4	Door Bell (DB35)	00000000h
3090h	4	Door Bell (DB36)	00000000h
3094h	4	Door Bell (DB37)	00000000h
3098h	4	Door Bell (DB38)	00000000h
309Ch	4	Door Bell (DB39)	00000000h
30A0h	4	Door Bell (DB40)	00000000h
30A4h	4	Door Bell (DB41)	00000000h
30A8h	4	Door Bell (DB42)	00000000h
30ACh	4	Door Bell (DB43)	00000000h
30B0h	4	Door Bell (DB44)	00000000h
30B4h	4	Door Bell (DB45)	00000000h
30B8h	4	Door Bell (DB46)	00000000h
30BCh	4	Door Bell (DB47)	00000000h
30C0h	4	Door Bell (DB48)	00000000h
30C4h	4	Door Bell (DB49)	00000000h
30C8h	4	Door Bell (DB50)	00000000h
30CCh	4	Door Bell (DB51)	00000000h
30D0h	4	Door Bell (DB52)	00000000h
30D4h	4	Door Bell (DB53)	00000000h
30D8h	4	Door Bell (DB54)	00000000h
30DCh	4	Door Bell (DB55)	00000000h
30E0h	4	Door Bell (DB56)	00000000h
30E4h	4	Door Bell (DB57)	00000000h
30E8h	4	Door Bell (DB58)	00000000h
30ECh	4	Door Bell (DB59)	00000000h
30F0h	4	Door Bell (DB60)	00000000h
30F4h	4	Door Bell (DB61)	00000000h
30F8h	4	Door Bell (DB62)	00000000h
30FCh	4	Door Bell (DB63)	00000000h
3100h	4	Door Bell (DB64)	00000000h
8004h	4	XECP USB2 Support (XECP_SUPP_USB2_1)	20425355h

Offset	Size (Bytes)	Register Name (Register Symbol)	Default Value
800Ch	4	XECP SUPP USB3_3 (XECP_SUPP_USB2_3)	00000000h
8010h	4	XECP SUPP USB2_4 Full Speed (XECP_SUPP_USB2_4)	000C0021h
8014h	4	XECP_SUPP USB2_5 Low Speed (XECP_SUPP_USB2_5)	05DC0012h
8018h	4	XECP SUPP USB2_6 High Speed (XECP_SUPP_USB2_6)	01E00023h
8020h	4	XECP SUPP USB3_0 (XECP_SUPP_USB3_0)	03101402h
8024h	4	XECP USB3.1 Support (XECP_SUPP_USB3_1)	20425355h
8028h	4	XECP USB3.2 Support (XECP_SUPP_USB3_2)	80000402h
802Ch	4	XECP SUPP USB3_3 (XECP_SUPP_USB3_3)	00000000h
8030h	4	XECP SUPP USB3_4 (XECP_SUPP_USB3_4)	00050134h
8034h	4	XECP SUPP USB3_5 (XECP_SUPP_USB3_5)	000A0135h
8038h	4	XECP SUPP USB3_6 (XECP_SUPP_USB3_6)	04E00126h
803Ch	4	XECP SUPP USB3_7 (XECP_SUPP_USB3_7)	09C00127h
8040h	4	XECP SUPP USB3_8 (XECP_SUPP_USB3_8)	13800128h
8044h	4	XECP SUPP USB3_9 (XECP_SUPP_USB3_9)	05B10129h
8048h	4	XECP SUPP USB3_10 (XECP_SUPP_USB3_10)	0B63012Ah
804Ch	4	XECP SUPP USB3_11 (XECP_SUPP_USB3_11)	16C6012Bh
8094h	4	Host Control Scheduler (HOST_CTRL_SCH_REG)	00008100h
80A4h	4	Power Management Control (PMCTRL_REG)	012DFF94h
80B0h	4	Host Controller Misc Reg (HOST_CTRL_MISC_REG)	0001037Fh
80B4h	4	Host Controller Misc Reg2 (HOST_CTRL_MISC_REG2)	00000100h
80B8h	4	Super Speed Port Enable (SSPE_REG)	80000000h
80E0h	4	AUX Power Management Control (AUX_CTRL_REG1)	8081BCE0h
80ECh	4	SuperSpeed Port Link Control (HOST_CTRL_PORT_LINK_REG)	18000000h
80F0h	4	USB2 Port Link Control 1 (USB2_LINK_MGR_CTRL_REG1)	310803A0h
80F4h	4	USB2 Port Link Control 2 (USB2_LINK_MGR_CTRL_REG2)	80C40620h
80F8h	4	USB2 Port Link Control 3 (USB2_LINK_MGR_CTRL_REG3)	F865EB6Bh
80FCh	4	USB2 Port Link Control 4 (USB2_LINK_MGR_CTRL_REG4)	00008003h
8140h	4	Power Scheduler Control 0 (PWR_SCHED_CTRL0)	0A019132h
8144h	4	Power Scheduler Control 1 (PWR_SCHED_CTRL2)	0000033Fh
8154h	4	AUX Power Management Control (AUX_CTRL_REG2)	81390206h
8164h	4	USB2 PHY Power Management Control (USB2_PHY_PMC)	000000FCh
816Ch	4	XHCI Aux Clock Control Register (XHCI_AUX_CCR)	00000400h
8174h	4	XHC Latency Tolerance Parameters LTV Control (XLTP_LTV1)	0040047Dh
8178h	4	XHC Latency Tolerance Parameters LTV Control 2 (XLTP_LTV2)	000017FFh
817Ch	4	XHC Latency Tolerance Parameters High Idle Time Control (XLTP_HITC)	00000000h
8180h	4	XHC Latency Tolerance Parameters Medium Idle Time Control (XLTP_MITC)	00000000h
8184h	4	XHC Latency Tolerance Parameters Low Idle Time Control (XLTP_LITC)	00000000h
81B8h	4	LFPS On Count (LFPSONCOUNT_REG)	000400C8h
81C4h	4	USB2 Power Management Control (USB2PMCTRL_REG)	00000900h

Offset	Size (Bytes)	Register Name (Register Symbol)	Default Value
846Ch	4	USB Legacy Support Capability (USBLEGSUP)	00002201h
8470h	4	USB Legacy Support Control Status (USBLEGCTLSTS)	00000000h
84F4h	4	Port Disable Override Capability Register (PDO_CAPABILITY)	000003C6h
8604h	2	Command Reg (CMD_MMIO)	0000h
8606h	2	Device Status (STS_MMIO)	0290h
8608h	1	Revision ID (RID_MMIO)	00h
8609h	1	Programming Interface (PI_MMIO)	30h
860Ah	1	Sub Class Code (SCC_MMIO)	03h
860Bh	1	Base Class Code (BCC_MMIO)	0Ch
860Dh	1	Master Latency Timer (MLT_MMIO)	00h
860Eh	1	Header Type (HT_MMIO)	80h
8610h	8	Memory Base Address (MBAR_MMIO)	0000000000000004h
862Ch	2	USB Subsystem Vendor ID (SSVID_MMIO)	0000h
862Eh	2	USB Subsystem ID (SSID_MMIO)	0000h
8634h	1	Capabilities Pointer (CAP_PTR_MMIO)	70h
863Ch	1	Interrupt Line (ILINE_MMIO)	00h
863Dh	1	Interrupt Pin (IPIN_MMIO)	00h
8660h	1	Serial Bus Release Number (SBRN_MMIO)	31h
8661h	1	Frame Length Adjustment (FLADJ_MMIO)	60h
8662h	1	Best Effort Service Latency (BESL_MMIO)	00h
8670h	1	PCI Power Management Capability ID (PM_CID_MMIO)	01h
8671h	1	Next Item Pointer 1 (PM_NEXT_MMIO)	80h
8672h	2	Power Management Capabilities (PM_CAP_MMIO)	C1C2h
8674h	2	Power Management Control/Status (PM_CS_MMIO)	0008h
8680h	1	Message Signaled Interrupt CID (MSI_CID_MMIO)	05h
8681h	1	Next Item Pointer (MSI_NEXT_MMIO)	00h
8682h	2	Message Signaled Interrupt Message Control (MSI_MCTL_MMIO)	0086h
8684h	4	Message Signaled Interrupt Message Address (MSI_MAD_MMIO)	00000000h
8688h	4	Message Signaled Interrupt Upper Address (MSI_MUAD_MMIO)	00000000h
868Ch	2	Message Signaled Interrupt Message Data (MSI_MD_MMIO)	0000h
86A4h	4	High Speed Configuration 2 (HSCFG2_MMIO)	00002000h
86B0h	4	XHCI USB2 Overcurrent Pin Mapping (U2OCM1_MMIO)	00000000h
86B4h	4	XHCI USB2 Overcurrent Pin Mapping (U2OCM2_MMIO)	00000000h
86B8h	4	XHCI USB2 Overcurrent Pin Mapping (U2OCM3_MMIO)	00000000h
86BCh	4	XHCI USB2 Overcurrent Pin Mapping (U2OCM4_MMIO)	00000000h
86D0h	4	XHCI USB3 Overcurrent Pin Mapping (U3OCM1_MMIO)	00000000h
86D4h	4	XHCI USB3 Overcurrent Pin Mapping (U3OCM2_MMIO)	00000000h
86D8h	4	XHCI USB3 Overcurrent Pin Mapping (U3OCM3_MMIO)	00000000h
86DCh	4	XHCI USB3 Overcurrent Pin Mapping (U3OCM4_MMIO)	00000000h
8700h	4	Debug Capability ID Register (DCID)	0005100Ah

Offset	Size (Bytes)	Register Name (Register Symbol)	Default Value
8704h	4	Debug Capability Doorbell Register (DCDB)	00000000h
8708h	4	Debug Capability Event Ring Segment Table Size Register (DCERSTSZ)	00000000h
8710h	8	Debug Capability Event Ring Segment Table Base Address Register (DCERSTBA)	0000000000000000h
8718h	8	Debug Capability Event Ring Dequeue Pointer Register (DCERDP)	0000000000000000h
8720h	4	Debug Capability Control Register (DCCTRL)	00000000h
8724h	4	Debug Capability Status Register (DCST)	00000000h
8728h	4	Debug Capability Port Status And Control Register (DCPORTSC)	00000080h
8730h	8	Debug Capability Context Pointer Register (DCCP)	0000000000000000h
8E10h	4	GLOBAL TIME SYNC CAP REG (GLOBAL_TIME_SYNC_CAP_REG)	000012C9h
8E14h	4	GLOBAL TIME SYNC CTRL REG (GLOBAL_TIME_SYNC_CTRL_REG)	00000000h
8E18h	4	MICROFRAME TIME REG (MICROFRAME_TIME_REG)	00000000h
8E20h	4	Global Time Low (GLOBAL_TIME_LOW_REG)	00000000h
8E24h	4	Global Time High (GLOBAL_TIME_HI_REG)	00000000h

8.3.2 Capability Registers Length (CAPLENGTH) — Offset 0h

This register is modified and maintained by BIOS

Type	Size	Offset	Default
MMIO	8 bit	MBAR + 0h	80h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
7:0	80h RW/L	**Capability Registers Length (CAPLENGTH):** Capability Registers Length (CAPLENGTH) **Locked by:** XHCC1.ACCTRL

8.3.3 Host Controller Interface Version Number (HCIVERSION) — Offset 2h

This register is modified and maintained by BIOS

Type	Size	Offset	Default
MMIO	16 bit	MBAR + 2h	0101h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:0	0101h RW/L	**Host Controller Interface Version Number (HCIVERSION):** Host Controller Interface Version Number (HCIVERSION) **Locked by:** XHCC1.ACCTRL

8.3.4 Structural Parameters 1 (HCSPARAMS1) — Offset 4h

This register is modified and maintained by BIOS

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 4h	05000840h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:24	05h RW/L	**Number of Ports (MAXPORTS):** Number of Ports (MaxPorts): The value in this field reflects the highest numbered port in the controller, not the actual count of the number of ports. This allows for gaps in the port numbering, between USB2 and USB3 protocol capabilities. **Locked by:** XHCC1.ACCTRL
23:19	0h RO	**Reserved**
18:8	008h RW/L	**Number of Interrupters (MAXINTRS):** Number of Interrupters (MaxInt) **Locked by:** XHCC1.ACCTRL
7:0	40h RW/L	**Number of Device Slots (MAXSLOTS):** Number of Device Slots (MaxSlots) **Locked by:** XHCC1.ACCTRL

8.3.5 Structural Parameters 2 (HCSPARAMS2) — Offset 8h

This register is modified and maintained by BIOS

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 8h	14200054h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:27	02h RW/L	**Max Scratchpad Buffers LO (MAXSCRATCHPADBUFS):** Max Scratchpad Buffers Lo (MaxScratchpadBufs) **Locked by:** XHCC1.ACCTRL
26	1h RW/L	**Scratchpad Restore (SPR):** Scratchpad Restore (SPR) **Locked by:** XHCC1.ACCTRL
25:21	01h RW/L	**Max Scratchpad Buffers HI (MAXSCRATCHPADBUFS_HI):** Max Scratchpad Buffers Hi (MaxScratchpadBufs) **Locked by:** XHCC1.ACCTRL
20:8	0h RO	**Reserved**
7:4	5h RW/L	**Event Ring Segment Table Max (ERSTMAX):** Event Ring Segment Table Max (ERSTMax) **Locked by:** XHCC1.ACCTRL
3:0	4h RW/L	**Isochronous Scheduling Threshold (IST):** Isochronous Scheduling Threshold (IST) **Locked by:** XHCC1.ACCTRL

8.3.6 Structural Parameters 3 (HCSPARAMS3) — Offset Ch

This register is modified and maintained by BIOS

Type	Size	Offset	Default
MMIO	32 bit	MBAR + Ch	00040001h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:16	0004h RW/L	**U2 Device Exit Latency (U2DEL):** U2 Device Exit Latency (U2DEL): **Locked by:** XHCC1.ACCTRL
15:8	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
7:0	01h RW/L	**U1 Device Exit Latency (U1DEL):** U1 Device Exit Latency (U1DEL): **Locked by:** XHCC1.ACCTRL

8.3.7 Capability Parameters (HCCPARAMS) — Offset 10h

This register is modified and maintained by BIOS

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 10h	200077C1h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:16	2000h RW/L	**xHCI Extended Capabilities Pointer (XECP):** xHCI Extended Capabilities Pointer (xECP): The Default value should be 2008h if NumUSB2 = 0 **Locked by:** XHCC1.ACCTRL
15:12	7h RW/L	**Maximum Primary Stream Array Size (MAXPSASIZE):** Maximum Primary Stream Array Size (MaxPSASize): **Locked by:** XHCC1.ACCTRL
11	0h RW/L	**Contiguous Frame ID Capability (CFC):** Contiguous Frame ID Capability (CFC) **Locked by:** XHCC1.ACCTRL
10	1h RW/L	**Stopped EDLTA Capability (SEC):** Stopped EDLTA Capability (SEC) **Locked by:** XHCC1.ACCTRL
9	1h RW/L	**Stopped - Short Packet Capability (SPC):** Stopped - Short Packet Capability (SPC) **Locked by:** XHCC1.ACCTRL
8	1h RW/L	**Parst All Event Data (PAE):** Parse All Event Data (PAE) **Locked by:** XHCC1.ACCTRL
7	1h RW/L	**No Secondary SID Support (NSS):** No Secondary SID Support (NSS) **Locked by:** XHCC1.ACCTRL
6	1h RW/L	**Latency Tolerance Messaging Capability (LTC):** Latency Tolerance Messaging Capability (LTC): **Locked by:** XHCC1.ACCTRL
5	0h RW/L	**Light HC Reset Capability (LHRC):** Light HC Reset Capability (LHRC) **Locked by:** XHCC1.ACCTRL
4	0h RW/L	**Port Indicators (PIND):** Port Indicators (PIND): **Locked by:** XHCC1.ACCTRL

Bit Range	Default & Access	Field Name (ID): Description
3	0h RW/L	**Port Power Control (PPC):** Port Power Control (PPC): **Locked by:** XHCC1.ACCTRL
2	0h RW/L	**Context Size (CSZ):** Context Size (CSZ): **Locked by:** XHCC1.ACCTRL
1	0h RW/L	**BW Negotiation Capability (BNC):** BW Negotiation Capability (BNC): **Locked by:** XHCC1.ACCTRL
0	1h RW/L	**64-bit Addressing Capability (AC64):** 64-bit Addressing Capability (AC64) **Locked by:** XHCC1.ACCTRL

8.3.8 Doorbell Offset (DBOFF) — Offset 14h

Doorbell Offset

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 14h	00003000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:2	00000C00h RO	**Doorbell Array Offset (DBAO):** Doorbell Array Offset (DBAO)
1:0	0h RO	**Reserved**

8.3.9 Runtime Register Space Offset (RTSOFF) — Offset 18h

Runtime Register Space Offset

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 18h	00002000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:5	0000100h RO	**Runtime Register Space Offset (RTRSO):** Runtime Register Space Offset (RTRSO):
4:0	0h RO	**Reserved**

8.3.10 USB Command (USBCMD) — Offset 80h

USB Command

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 80h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:15	0h RO	**Reserved**
14	0h RW	**Extended TCB Enable (ETE):** This flag indicates that the host controller implementation is enabled to support Transfer Burst Count values greater than 4 in Isoch TDs. This bit may be set only if ETC = 1.
13	0h RW	**CEM Enable (CEM):** Default = '0'. when set to '1', a Max Exit Latency Too Large Capability Error may be returned by a Configure Endpoint Command. When Cleared to '0', a Max Exit latency Too Large Capability Error shall not be returned by a Configure Endpoint Command. This bit is Reserved if CMC='0'.
12	0h RO	**Reserved**
11	0h RW	**Enable U3 MFINDEX Stop (EU3S):** Enable U3 MFINDEX Stop
10	0h RW	**Enable Wrap Event (EWE):** Enable Wrap Event
9	0h RW	**Controller Restore State (CRS):** Controller Restore State

Bit Range	Default & Access	Field Name (ID): Description
8	0h RW	**Controller Save State (CSS):** Controller Save State
7	0h RW	**Light Host Controller Reset (LHCRST):** Light Host Controller Reset
6:4	0h RO	**Reserved**
3	0h RW	**Host System Error Enable (HSEE):** Host System Error Enable
2	0h RW	**Interrupter Enable (INTE):** Interrupter Enable
1	0h RW	**Host Controller Reset (HCRST):** Host Controller Reset
0	0h RW	**RS:** Run or Stop

8.3.11 USB Status (USBSTS) — Offset 84h

USB Status

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 84h	00000001h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:13	0h RO	**Reserved**
12	0h RO	**Host Controller Error (HCE):** This bit is not preset in HC, this is deviation from XHCI 1.0 spec.
11	0h RO	**Controller Not Ready (CNR):** This is deviation from XHCI 1.0 spec.
10	0h RW/1C	**Save/Restore Error (SRE):** Save/Restore Error
9	0h RO	**Restore State Status (RSS):** Restore State Status
8	0h RO	**Save State Status (SSS):** Save State Status
7:5	0h RO	**Reserved**
4	0h RW/1C	**Port Change Detect (PCD):** Port Change Detect
3	0h RW/1C	**Event Interrupt (EINT):** Event Interrupt

Bit Range	Default & Access	Field Name (ID): Description
2	0h RW/1C	**Host System Error (HSE):** Host System Error
1	0h RO	**Reserved**
0	1h RO	**Host Controller Halted (HCH):** Host Controller Halted

8.3.12 Page Size (PAGESIZE) — Offset 88h

Page Size

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 88h	00000001h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:16	0h RO	**Reserved**
15:0	0001h RO	**Page Size (PAGESIZE):** Page Size

8.3.13 Device Notification Control (DNCTRL) — Offset 94h

Device Notification Control

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 94h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:16	0h RO	**Reserved**
15:0	0000h RW	**Notification Enable (N0_N15):** Notification Enable

8.3.14 Command Ring Low (CRCR_LO) — Offset 98h

Command Ring Low

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 98h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:6	0000000h WO	**Command Ring Pointer (CRP):** Command Ring Pointer
5:4	0h RO	**Reserved**
3	0h RO	**Command Ring Running (CRR):** Command Ring Running
2	0h WO	**Command Abort (CA):** Command Abort
1	0h WO	**Command Stop (CS):** Command Stop
0	0h WO	**Ring Cycle State (RCS):** Ring Cycle State

8.3.15 Command Ring High (CRCR_HI) — Offset 9Ch

Command Ring High

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 9Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h WO	**Command Ring Pointer (CRP):** Command Ring Pointer

8.3.16 Device Context Base Address Array Pointer Low (DCBAAP_LO) — Offset B0h

Device Context Base Address Array Pointer Low

Type	Size	Offset	Default
MMIO	32 bit	MBAR + B0h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:6	0000000h RW	**Device Context Base Address Array Pointer (DCBAAP):** Device Context Base Address Array Pointer
5:0	0h RO	**Reserved**

8.3.17 Device Context Base Address Array Pointer High (DCBAAP_HI) — Offset B4h

Device Context Base Address Array Pointer High

Type	Size	Offset	Default
MMIO	32 bit	MBAR + B4h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RW	**Device Context Base Address Array Pointer (DCBAAP):** Device Context Base Address Array Pointer High

8.3.18 Configure Reg (CONFIG) — Offset B8h

Configure Reg

Type	Size	Offset	Default
MMIO	32 bit	MBAR + B8h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:10	0h RO	**Reserved**
9	0h RW	**Configuration Information Enable (CIE):** Configuration Information Enable
8	0h RW	**U3 Entry Enable (U3E):** U3 Entry Enable
7:0	00h RW	**Max Device Slots Enabled (MAXSLOTSEN):** Max Device Slots Enabled

8.3.19 Port Status AndControl USB2 (PORTSC1) — Offset 480h

There are NumUSB2 USB2 PORTSC registers at offsets :

480h, 490h, ... (480h + (NumUSB2-1)*10h)

The USB PORTSC registers should be accessed via DW writes for any modification.

Byte Writes have unintended behavior.

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 480h	000002A0h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RW/1S	**Warm Port Reset (WPR):** Warm Port Reset
30	0h RW/L	**Device Removable (DR):** Device Removable **Locked by:** XHCC1.ACCTRL
29:28	0h RO	**Reserved**
27	0h RW/P	**Wake on Over-current Enable (WOE):** Note: This register is sticky.

Bit Range	Default & Access	Field Name (ID): Description
26	0h RW/P	**Wake on Disconnect Enable (WDE):** Note: This register is sticky.
25	0h RW/P	**Wake on Connect Enable (WCE):** Note: This register is sticky.
24	0h RO	**Cold Attach Status (CAS):** Cold Attach Status
23	0h RW/1C	**Port Config Error Change (CEC):** Note: This register is sticky.
22	0h RW/1C	**Port Link State Change (PLC):** Note: This register is sticky.
21	0h RW/1C	**Port Reset Change (PRC):** Note: This register is sticky.
20	0h RW/1C	**Over-current Change (OCC):** Note: This register is sticky.
19	0h RW/1C	**Warm Port Reset Change (WRC):** Note: This register is sticky.
18	0h RW/1C	**Port Enabled Disabled Change (PEC):** Note: This register is sticky.
17	0h RW/1C	**Connect Status Change (CSC):** Note: This register is sticky.
16	0h RW	**Port Link State Write Strobe (LWS):** Port Link State Write Strobe
15:14	0h RW/P	**Port Indicator Control (PIC):** Note: This register is sticky.
13:10	0h RW	**Port Speed (PORTSPEED):** Note: This register is sticky.
9	1h RW/P	**Port Power (PP):** Note: This register is sticky.
8:5	5h RW/P	**Port Link State (PLS):** Note: This register is sticky.
4	0h RW/1S	**Port Reset (PR):** Port Reset
3	0h RW	**Over-current Active (OCA):** Note: This register is sticky.
2	0h RO	**Reserved**
1	0h RW/1C	**Port Enabled Disabled (PED):** Note: This register is sticky.
0	0h RW	**Current Connect Status (CCS):** Note: This register is sticky.

8.3.20 Port Power Management Status Aand Control USB2 (PORTPMSC1) — Offset 484h

There are 6 USB2 PORTPMSC registers at offsets:

484h, 494h, ... (484h + (NumUSB2-1)*10h)

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 484h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:28	0h RW/P	**Port Test Control (PTC):** Note: This register is sticky.
27:17	0h RO	**Reserved**
16	0h RW	**Hardware LPM Enable (HLE):** Hardware LPM Enable
15:8	00h RW/P	**Device Address (DA):** Note: This register is sticky.
7:4	0h RW/P	**Host Initiated Resume Duration (HIRD):** Note: This register is sticky.
3	0h RW/P	**Remote Wake Enable (RWE):** Note: This register is sticky.
2:0	0h RW	**L1 Status (L1S):** Note: This register is sticky.

8.3.21 Port X Hardware LPM Control Register (PORTHLPMC1) — Offset 48Ch

There are 9 PORTHLPMC registers at offsets 48Ch, 49Ch, 4ACh, 4BCh, 4CCh, 4DCh, 4ECh, 4FCh, 50Ch

This register is reset only by platform hardware during cold reset or in response to a Host Controller Reset (HCRST).

The definition for the fields depend on the protocol supported. For USB3 this register is reserved and shall be treated by software as RsvdP. For USB2 the definition is given below. Fields contain parameters neccessary for xHC to automatically generate an LPM Token to the downstream device.

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 48Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:14	0h RO	**Reserved**
13:10	0h RW	**Host Initiated Resume Duration-Deep (HIRDD):** System software sets this field to indicate to the recipient device how long the xHC will drive resume if an exit from L1. The HIRDD value is is encoded as follows: 0h: 50 us (default) 1h: 125 us 2h: 200 us ... Fh: 1.175ms The value of 0h is interpreted as 50 us. Each incrementing value adds 75 us to the previous value.
9:2	00h RW/P	**L1 Timeout (L1_TO):** Timeout value for L1 inactivity timer. This field shall be set to 00h by assertion of PR to '1'. Following are permissible values: 00h: 128 us (default) 01h: 256 us. ... FFh: 65,280us Note: This register is sticky.
1:0	0h RW/P	**Host Initiated Resume Duration Mode (HIRDM):** Indicates which HIRD value should be used. Following are permissible values: 0: Initiate L1 using HIRD only time out (default) 1: Initiate HIRDDon timeout. If rejected by device, initiate L1 using HIRD 2,3: Reserved Note: This register is sticky.

8.3.22 Port Status And Control USB3 (PORTSC2) — Offset 490h

The USB3 PORTSC registers are at offsets:

First USB3 port: 480h+NumUSB2*10h

Next USB3 port: First USB3 Port + 10h

and so on...

Final USB3 Port: First USB3 Port + (NumUSB3-1)*10h)

The USB PORTSC registers should be accessed via DW writes for any modification.

Byte Writes have unintended behavior.

Note: Bit definitions are the same as PORTSC1, offset 480h.

8.3.23 Port Power Management Status And Control USB3 (PORTPMSC2) — Offset 494h

Port Power Management Status And Control USB3

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 494h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:17	0h RO	**Reserved**
16	0h RW	**Force Link PM Accept (FLA):** Force Link PM Accept
15:8	00h RW/P	**U2 Timeout (U2T):** U2 Timeout
7:0	00h RW/P	**U1 Timeout (U1T):** U1 Timeout

8.3.24 USB3 Port Link Info (PORTLI2) — Offset 498h

The USB3 PORTLI registers are at offsets:

First USB3 port: 488h+NumUSB2*10h

Next USB3 port: First USB3 Port + 10h

and so on...

Final USB3 Port: First USB3 Port + (NumUSB3-1)*10h)

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 498h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:16	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
15:0	0000h RW	**Link Error Count (LEC):** Link Error Count

8.3.25 Port Status And Control USB3 (PORTSC3) — Offset 4A0h

The USB3 PORTSC registers are at offsets:

First USB3 port: 480h+NumUSB2*10h

Next USB3 port: First USB3 Port + 10h

and so on...

Final USB3 Port: First USB3 Port + (NumUSB3-1)*10h)

The USB PORTSC registers should be accessed via DW writes for any modification.

Byte Writes have unintended behavior.

Note: Bit definitions are the same as PORTSC1, offset 480h.

8.3.26 Port Power Management Status And Control USB3 (PORTPMSC3) — Offset 4A4h

Port Power Management Status And Control USB3

Note: Bit definitions are the same as PORTPMSC2, offset 494h.

8.3.27 USB3 Port Link Info (PORTLI3) — Offset 4A8h

The USB3 PORTLI registers are at offsets:

First USB3 port: 488h+NumUSB2*10h

Next USB3 port: First USB3 Port + 10h

and so on...

Final USB3 Port: First USB3 Port + (NumUSB3-1)*10h)

Note: Bit definitions are the same as PORTLI2, offset 498h.

8.3.28 Port Status And Control USB3 (PORTSC4) — Offset 4B0h

The USB3 PORTSC registers are at offsets:

First USB3 port: 480h+NumUSB2*10h

Next USB3 port: First USB3 Port + 10h

and so on...

Final USB3 Port: First USB3 Port + (NumUSB3-1)*10h)

The USB PORTSC registers should be accessed via DW writes for any modification.

Byte Writes have unintended behavior.

Note: Bit definitions are the same as PORTSC1, offset 480h.

8.3.29 Port Power Management Status And Control USB3 (PORTPMSC4) — Offset 4B4h

Port Power Management Status And Control USB3

Note: Bit definitions are the same as PORTPMSC2, offset 494h.

8.3.30 USB3 Port Link Info (PORTLI4) — Offset 4B8h

The USB3 PORTLI registers are at offsets:

First USB3 port: 488h+NumUSB2*10h

Next USB3 port: First USB3 Port + 10h

and so on...

Final USB3 Port: First USB3 Port + (NumUSB3-1)*10h)

Note: Bit definitions are the same as PORTLI2, offset 498h.

8.3.31 Port Status And Control USB3 (PORTSC5) — Offset 4C0h

The USB3 PORTSC registers are at offsets:

First USB3 port: 480h+NumUSB2*10h

Next USB3 port: First USB3 Port + 10h

and so on...

Final USB3 Port: First USB3 Port + (NumUSB3-1)*10h)

The USB PORTSC registers should be accessed via DW writes for any modification.

Byte Writes have unintended behavior.

Note: Bit definitions are the same as PORTSC1, offset 480h.

8.3.32 Port Power Management Status And Control USB3 (PORTPMSC5) — Offset 4C4h

Port Power Management Status And Control USB3

Note: Bit definitions are the same as PORTPMSC2, offset 494h.

8.3.33 USB3 Port Link Info (PORTLI5) — Offset 4C8h

The USB3 PORTLI registers are at offsets:

First USB3 port: 488h+NumUSB2*10h

Next USB3 port: First USB3 Port + 10h

and so on...

Final USB3 Port: First USB3 Port + (NumUSB3-1)*10h)

Note: Bit definitions are the same as PORTLI2, offset 498h.

8.3.34 Microframe Index (RTMFINDEX) — Offset 2000h

Microframe Index

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 2000h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:14	0h RO	**Reserved**
13:0	0000h RO	**Microframe Index (IMAN0):** Microframe Index

8.3.35 Interrupter Management (IMAN0) — Offset 2020h

There are 8 IMAN registers.

x = 1, 2, ..., 8

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 2020h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:2	0h RO	**Reserved**
1	0h RW	**Interrupt Enable (IE):** Interrupt Enable

Bit Range	Default & Access	Field Name (ID): Description
0	0h RW/1C	**Interrupt Pending (IP):** Interrupt Pending

8.3.36 Interrupter Moderation (IMOD0) — Offset 2024h

There are 8 IMOD registers.

x = 1, 2, ..., 8

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 2024h	00000FA0h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:16	0000h RW	**Interrupt Moderation Counter (IMODC):** Interrupt Moderation Counter
15:0	0FA0h RW	**Interrupt Moderation Interval (IMODI):** Interrupt Moderation Interval

8.3.37 Event Ring Segment Table Size (ERSTSZ0) — Offset 2028h

There are 8 ERSTSZ register.

x = 1, 2, ..., 8

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 2028h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:16	0h RO	**Reserved**
15:0	0000h RW	**Event Ring Segment Table Size (ERSTS):** Event Ring Segment Table Size

8.3.38 Event Ring Segment Table Base Address Low (ERSTBA_LO0) — Offset 2030h

There are 8 ERSTBA_LO registers

x = 1, 2, ..., 8

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 2030h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:6	0000000h RW	**Event Ring Segment Table Base Address Register (ERSTBA):** Event Ring Segment Table Base Address Register
5:0	0h RO	**Reserved**

8.3.39 Event Ring Segment Table Base Address High (ERSTBA_HI0) — Offset 2034h

Event Ring Segment Table Base Address High

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 2034h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RW	**Event Ring Segment Table Base Address (ERSTBA):** Event Ring Segment Table Base Address

8.3.40 Event Ring Dequeue Pointer Low (ERDP_LO0) — Offset 2038h

There are 8 ERDP_LO registers.

x = 1, 2, ...,8

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 2038h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:4	0000000h RW	**Event Ring Dequeue Pointer (ERDP):** Event Ring Dequeue Pointer
3	0h RW/1C	**Event Handler Busy (EHB):** Event Handler Busy
2:0	0h RW	**Dequeue ERST Segment Index (DESI):** Dequeue ERST Segment Index

8.3.41 Event Ring Dequeue Pointer High (ERDP_HI0) — Offset 203Ch

There are 8 ERDP_HI registers.

x = 1, 2, ..., 8

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 203Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RW	**Event Ring Dequeue Pointer (ERDP):** Event Ring Dequeue Pointer

8.3.42 Interrupter Management (IMAN1) — Offset 2040h

There are 8 IMAN registers.

x = 1, 2, ..., 8

Note: Bit definitions are the same as IMAN0, offset 2020h.

8.3.43 Interrupter Moderation (IMOD1) — Offset 2044h

There are 8 IMOD registers.

x = 1, 2, ..., 8

Note: Bit definitions are the same as IMOD0, offset 2024h.

8.3.44 Event Ring Segment Table Size (ERSTSZ1) — Offset 2048h

There are 8 ERSTSZ register.

x = 1, 2, ..., 8

Note: Bit definitions are the same as ERSTSZ0, offset 2028h.

8.3.45 Event Ring Segment Table Base Address Low (ERSTBA_LO1) — Offset 2050h

There are 8 ERSTBA_LO registers

x = 1, 2, ..., 8

Note: Bit definitions are the same as ERSTBA_LO0, offset 2030h.

8.3.46 Event Ring Segment Table Base Address High (ERSTBA_HI1) — Offset 2054h

Event Ring Segment Table Base Address High

Note: Bit definitions are the same as ERSTBA_HI0, offset 2034h.

8.3.47 Event Ring Dequeue Pointer Low (ERDP_LO1) — Offset 2058h

There are 8 ERDP_LO registers.

x = 1, 2, ...,8

Note: Bit definitions are the same as ERDP_LO0, offset 2038h.

8.3.48 Event Ring Dequeue Pointer High (ERDP_HI1) — Offset 205Ch

There are 8 ERDP_HI registers.

x = 1, 2, ..., 8

Note: Bit definitions are the same as ERDP_HI0, offset 203Ch.

8.3.49 Interrupter Management (IMAN2) — Offset 2060h

There are 8 IMAN registers.

x = 1, 2, ..., 8

Note: Bit definitions are the same as IMAN0, offset 2020h.

8.3.50 Interrupter Moderation (IMOD2) — Offset 2064h

There are 8 IMOD registers.

x = 1, 2, ..., 8

Note: Bit definitions are the same as IMOD0, offset 2024h.

8.3.51 Event Ring Segment Table Size (ERSTSZ2) — Offset 2068h

There are 8 ERSTSZ register.

x = 1, 2, ..., 8

Note: Bit definitions are the same as ERSTSZ0, offset 2028h.

8.3.52 Event Ring Segment Table Base Address Low (ERSTBA_LO2) — Offset 2070h

There are 8 ERSTBA_LO registers

x = 1, 2, ..., 8

Note: Bit definitions are the same as ERSTBA_LO0, offset 2030h.

8.3.53 Event Ring Segment Table Base Address High (ERSTBA_HI2) — Offset 2074h

Event Ring Segment Table Base Address High

Note: Bit definitions are the same as ERSTBA_HI0, offset 2034h.

8.3.54 Event Ring Dequeue Pointer Low (ERDP_LO2) — Offset 2078h

There are 8 ERDP_LO registers.

x = 1, 2, ...,8

Note: Bit definitions are the same as ERDP_LO0, offset 2038h.

8.3.55 Event Ring Dequeue Pointer High (ERDP_HI2) — Offset 207Ch

There are 8 ERDP_HI registers.

x = 1, 2, ..., 8

Note: Bit definitions are the same as ERDP_HI0, offset 203Ch.

8.3.56 Interrupter Management (IMAN3) — Offset 2080h

There are 8 IMAN registers.

x = 1, 2, ..., 8

Note: Bit definitions are the same as IMAN0, offset 2020h.

8.3.57 Interrupter Moderation (IMOD3) — Offset 2084h

There are 8 IMOD registers.

x = 1, 2, ..., 8

Note: Bit definitions are the same as IMOD0, offset 2024h.

8.3.58 Event Ring Segment Table Size (ERSTSZ3) — Offset 2088h

There are 8 ERSTSZ register.

x = 1, 2, ..., 8

Note: Bit definitions are the same as ERSTSZ0, offset 2028h.

8.3.59 Event Ring Segment Table Base Address Low (ERSTBA_LO3) — Offset 2090h

There are 8 ERSTBA_LO registers

x = 1, 2, ..., 8

Note: Bit definitions are the same as ERSTBA_LO0, offset 2030h.

8.3.60 Event Ring Segment Table Base Address High (ERSTBA_HI3) — Offset 2094h

Event Ring Segment Table Base Address High

Note: Bit definitions are the same as ERSTBA_HI0, offset 2034h.

8.3.61 Event Ring Dequeue Pointer Low (ERDP_LO3) — Offset 2098h

There are 8 ERDP_LO registers.

x = 1, 2, ...,8

Note: Bit definitions are the same as ERDP_LO0, offset 2038h.

8.3.62 Event Ring Dequeue Pointer High (ERDP_HI3) — Offset 209Ch

There are 8 ERDP_HI registers.

x = 1, 2, ..., 8

Note: Bit definitions are the same as ERDP_HI0, offset 203Ch.

8.3.63 Interrupter Management (IMAN4) — Offset 20A0h

There are 8 IMAN registers.

x = 1, 2, ..., 8

Note: Bit definitions are the same as IMAN0, offset 2020h.

8.3.64 Interrupter Moderation (IMOD4) — Offset 20A4h

There are 8 IMOD registers.

x = 1, 2, ..., 8

Note: Bit definitions are the same as IMOD0, offset 2024h.

8.3.65 Event Ring Segment Table Size (ERSTSZ4) — Offset 20A8h

There are 8 ERSTSZ register.

x = 1, 2, ..., 8

Note: Bit definitions are the same as ERSTSZ0, offset 2028h.

8.3.66 Event Ring Segment Table Base Address Low (ERSTBA_LO4) — Offset 20B0h

There are 8 ERSTBA_LO registers

x = 1, 2, ..., 8

Note: Bit definitions are the same as ERSTBA_LO0, offset 2030h.

8.3.67 Event Ring Segment Table Base Address High (ERSTBA_HI4) — Offset 20B4h

Event Ring Segment Table Base Address High

Note: Bit definitions are the same as ERSTBA_HI0, offset 2034h.

8.3.68 Event Ring Dequeue Pointer Low (ERDP_LO4) — Offset 20B8h

There are 8 ERDP_LO registers.

x = 1, 2, ...,8

Note: Bit definitions are the same as ERDP_LO0, offset 2038h.

8.3.69 Event Ring Dequeue Pointer High (ERDP_HI4) — Offset 20BCh

There are 8 ERDP_HI registers.

x = 1, 2, ..., 8

Note: Bit definitions are the same as ERDP_HI0, offset 203Ch.

8.3.70 Interrupter Management (IMAN5) — Offset 20C0h

There are 8 IMAN registers.

x = 1, 2, ..., 8

Note: Bit definitions are the same as IMAN0, offset 2020h.

8.3.71 Interrupter Moderation (IMOD5) — Offset 20C4h

There are 8 IMOD registers.

x = 1, 2, ..., 8

Note: Bit definitions are the same as IMOD0, offset 2024h.

8.3.72 Event Ring Segment Table Size (ERSTSZ5) — Offset 20C8h

There are 8 ERSTSZ register.

x = 1, 2, ..., 8

Note: Bit definitions are the same as ERSTSZ0, offset 2028h.

8.3.73 Event Ring Segment Table Base Address Low (ERSTBA_LO5) — Offset 20D0h

There are 8 ERSTBA_LO registers

x = 1, 2, ..., 8

Note: Bit definitions are the same as ERSTBA_LO0, offset 2030h.

8.3.74 Event Ring Segment Table Base Address High (ERSTBA_HI5) — Offset 20D4h

Event Ring Segment Table Base Address High

Note: Bit definitions are the same as ERSTBA_HI0, offset 2034h.

8.3.75 Event Ring Dequeue Pointer Low (ERDP_LO5) — Offset 20D8h

There are 8 ERDP_LO registers.

x = 1, 2, ...,8

Note: Bit definitions are the same as ERDP_LO0, offset 2038h.

8.3.76 Event Ring Dequeue Pointer High (ERDP_HI5) — Offset 20DCh

There are 8 ERDP_HI registers.

x = 1, 2, ..., 8

Note: Bit definitions are the same as ERDP_HI0, offset 203Ch.

8.3.77 Interrupter Management (IMAN6) — Offset 20E0h

There are 8 IMAN registers.

x = 1, 2, ..., 8

Note: Bit definitions are the same as IMAN0, offset 2020h.

8.3.78 Interrupter Moderation (IMOD6) — Offset 20E4h

There are 8 IMOD registers.

x = 1, 2, ..., 8

Note: Bit definitions are the same as IMOD0, offset 2024h.

8.3.79 Event Ring Segment Table Size (ERSTSZ6) — Offset 20E8h

There are 8 ERSTSZ register.

x = 1, 2, ..., 8

Note: Bit definitions are the same as ERSTSZ0, offset 2028h.

8.3.80 Event Ring Segment Table Base Address Low (ERSTBA_LO6) — Offset 20F0h

There are 8 ERSTBA_LO registers

x = 1, 2, ..., 8

Note: Bit definitions are the same as ERSTBA_LO0, offset 2030h.

8.3.81 Event Ring Segment Table Base Address High (ERSTBA_HI6) — Offset 20F4h

Event Ring Segment Table Base Address High

Note: Bit definitions are the same as ERSTBA_HI0, offset 2034h.

8.3.82 Event Ring Dequeue Pointer Low (ERDP_LO6) — Offset 20F8h

There are 8 ERDP_LO registers.

x = 1, 2, ...,8

Note: Bit definitions are the same as ERDP_LO0, offset 2038h.

8.3.83 Event Ring Dequeue Pointer High (ERDP_HI6) — Offset 20FCh

There are 8 ERDP_HI registers.

x = 1, 2, ..., 8

Note: Bit definitions are the same as ERDP_HI0, offset 203Ch.

8.3.84 Interrupter Management (IMAN7) — Offset 2100h

There are 8 IMAN registers.

x = 1, 2, ..., 8

Note: Bit definitions are the same as IMAN0, offset 2020h.

8.3.85 Interrupter Moderation (IMOD7) — Offset 2104h

There are 8 IMOD registers.

x = 1, 2, ..., 8

Note: Bit definitions are the same as IMOD0, offset 2024h.

8.3.86 Event Ring Segment Table Size (ERSTSZ7) — Offset 2108h

There are 8 ERSTSZ register.

x = 1, 2, ..., 8

Note: Bit definitions are the same as ERSTSZ0, offset 2028h.

8.3.87 Event Ring Segment Table Base Address Low (ERSTBA_LO7) — Offset 2110h

There are 8 ERSTBA_LO registers

x = 1, 2, ..., 8

Note: Bit definitions are the same as ERSTBA_LO0, offset 2030h.

8.3.88 Event Ring Segment Table Base Address High (ERSTBA_HI7) — Offset 2114h

Event Ring Segment Table Base Address High

Note: Bit definitions are the same as ERSTBA_HI0, offset 2034h.

8.3.89 Event Ring Dequeue Pointer Low (ERDP_LO7) — Offset 2118h

There are 8 ERDP_LO registers.

x = 1, 2, ...,8

Note: Bit definitions are the same as ERDP_LO0, offset 2038h.

8.3.90 Event Ring Dequeue Pointer High (ERDP_HI7) — Offset 211Ch

There are 8 ERDP_HI registers.

x = 1, 2, ..., 8

Note: Bit definitions are the same as ERDP_HI0, offset 203Ch.

8.3.91 Door Bell (DB0) — Offset 3000h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 3000h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:16	0000h RW	**DB Stream ID (DSI):** DB Stream ID
15:8	0h RO	**Reserved**
7:0	00h RW	**DB Target (DT):** DB Target

8.3.92 Door Bell (DB1) — Offset 3004h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.93 Door Bell (DB2) — Offset 3008h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.94 Door Bell (DB3) — Offset 300Ch

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.95 Door Bell (DB4) — Offset 3010h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.96 Door Bell (DB5) — Offset 3014h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.97 Door Bell (DB6) — Offset 3018h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.98 Door Bell (DB7) — Offset 301Ch

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.99 Door Bell (DB8) — Offset 3020h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.100 Door Bell (DB9) — Offset 3024h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.101 Door Bell (DB10) — Offset 3028h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.102 Door Bell (DB11) — Offset 302Ch

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.103 Door Bell (DB12) — Offset 3030h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.104 Door Bell (DB13) — Offset 3034h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.105 Door Bell (DB14) — Offset 3038h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.106 Door Bell (DB15) — Offset 303Ch

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.107 Door Bell (DB16) — Offset 3040h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.108 Door Bell (DB17) — Offset 3044h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.109 Door Bell (DB18) — Offset 3048h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.110 Door Bell (DB19) — Offset 304Ch

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.111 Door Bell (DB20) — Offset 3050h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.112 Door Bell (DB21) — Offset 3054h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.113 Door Bell (DB22) — Offset 3058h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.114 Door Bell (DB23) — Offset 305Ch

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.115 Door Bell (DB24) — Offset 3060h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.116 Door Bell (DB25) — Offset 3064h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.117 Door Bell (DB26) — Offset 3068h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.118 Door Bell (DB27) — Offset 306Ch

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.119 Door Bell (DB28) — Offset 3070h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.120 Door Bell (DB29) — Offset 3074h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.121 Door Bell (DB30) — Offset 3078h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.122 Door Bell (DB31) — Offset 307Ch

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.123 Door Bell (DB32) — Offset 3080h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.124 Door Bell (DB33) — Offset 3084h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.125 Door Bell (DB34) — Offset 3088h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.126 Door Bell (DB35) — Offset 308Ch

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.127 Door Bell (DB36) — Offset 3090h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.128 Door Bell (DB37) — Offset 3094h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.129 Door Bell (DB38) — Offset 3098h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.130 Door Bell (DB39) — Offset 309Ch

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.131 Door Bell (DB40) — Offset 30A0h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.132 Door Bell (DB41) — Offset 30A4h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.133 Door Bell (DB42) — Offset 30A8h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.134 Door Bell (DB43) — Offset 30ACh

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.135 Door Bell (DB44) — Offset 30B0h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.136 Door Bell (DB45) — Offset 30B4h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.137 Door Bell (DB46) — Offset 30B8h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.138 Door Bell (DB47) — Offset 30BCh

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.139 Door Bell (DB48) — Offset 30C0h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.140 Door Bell (DB49) — Offset 30C4h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.141 Door Bell (DB50) — Offset 30C8h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.142 Door Bell (DB51) — Offset 30CCh

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.143 Door Bell (DB52) — Offset 30D0h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.144 Door Bell (DB53) — Offset 30D4h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.145 Door Bell (DB54) — Offset 30D8h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.146 Door Bell (DB55) — Offset 30DCh

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.147 Door Bell (DB56) — Offset 30E0h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.148 Door Bell (DB57) — Offset 30E4h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.149 Door Bell (DB58) — Offset 30E8h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.150 Door Bell (DB59) — Offset 30ECh

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.151 Door Bell (DB60) — Offset 30F0h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.152 Door Bell (DB61) — Offset 30F4h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.153 Door Bell (DB62) — Offset 30F8h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.154 Door Bell (DB63) — Offset 30FCh

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.155 Door Bell (DB64) — Offset 3100h

Door Bell registers are an array of 64 registers, with 0 to 32 being used by the XHC and the rest being reserved.

Note: Bit definitions are the same as DB0, offset 3000h.

8.3.156 XECP USB2 Support (XECP_SUPP_USB2_1) — Offset 8004h

XECP USB2 Support

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 8004h	20425355h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:0	20425355h RO	**XECP USB2 Support (XECP_SUPP_USB2_1):** Namestring USB

8.3.157 XECP SUPP USB3_3 (XECP_SUPP_USB2_3) — Offset 800Ch

XECP SUPP USB3_3

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 800Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:5	0h RO	**Reserved**
4:0	00h RO	**Protocol Slot Type (PROTOCOL_SLOT_TYPE):** Protocol Slot Type

8.3.158 XECP SUPP USB2_4 Full Speed (XECP_SUPP_USB2_4) — Offset 8010h

XECP SUPP USB2_4 Full Speed

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 8010h	000C0021h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:16	000Ch RO	**Protocol Speed ID Mantissa (PSIM):** Protocol Speed ID Mantissa
15:9	0h RO	**Reserved**
8	0h RO	**PSI Full Duplex (PFD):** PSI Full Duplex
7:6	0h RO	**PSI Type (PLT):** PSI Type
5:4	2h RO	**Protocol Speed ID Exponent (PSIE):** Protocol Speed ID Exponent
3:0	1h RO	**Protocol Speed ID Value (PSIV):** Protocol Speed ID Value

8.3.159 XECP_SUPP USB2_5 Low Speed (XECP_SUPP_USB2_5) — Offset 8014h

XECP_SUPP USB2_5 Low Speed

Note: Bit definitions are the same as XECP_SUPP_USB2_4, offset 8010h.

8.3.160 XECP SUPP USB2_6 High Speed (XECP_SUPP_USB2_6) — Offset 8018h

XECP SUPP USB2_6 High Speed

Note: Bit definitions are the same as XECP_SUPP_USB2_4, offset 8010h.

8.3.161 XECP SUPP USB3_0 (XECP_SUPP_USB3_0) — Offset 8020h

XECP SUPP USB3_0

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 8020h	03101402h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:24	03h RO	**USB Major Revision: 3.0 (USB3_MAJ_REV):** USB Major Revision: 3.0
23:16	10h RO	**USB Minor Revision (USB3_MIN_REV):** USB Minor Revision: 0.1
15:8	14h RO	**Next Capability Pointer (NCP):** Next Capability Pointer
7:0	02h RO	**Supported Protocol ID (SPID):** Supported Protocol ID

8.3.162 XECP USB3.1 Support (XECP_SUPP_USB3_1) — Offset 8024h

XECP USB3.1 Support

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 8024h	20425355h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:0	20425355h RO	**XECP USB3 Support (XECP_SUPP_USB3_1):** Namestring USB

8.3.163 XECP USB3.2 Support (XECP_SUPP_USB3_2) — Offset 8028h

XECP USB3.2 Support

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 8028h	80000402h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:28	8h RO	**Protocol Speed ID Count (PROT_SPD_ID_CNT):** 1 USB 3.0 Speed (Supper Speed)
27:16	0h RO	**Reserved**
15:8	04h RO	**Compatible Port Count (CPC):** The compatible port count varies based on SKU.
7:0	02h RO	**Compatible Port Offset (CPO):** Compatible Port Offset

8.3.164 XECP SUPP USB3_3 (XECP_SUPP_USB3_3) — Offset 802Ch

XECP SUPP USB3_3

Note: Bit definitions are the same as XECP_SUPP_USB2_3, offset 800Ch.

8.3.165 XECP SUPP USB3_4 (XECP_SUPP_USB3_4) — Offset 8030h

XECP SUPP USB3_4

Note: Bit definitions are the same as XECP_SUPP_USB2_4, offset 8010h.

8.3.166 XECP SUPP USB3_5 (XECP_SUPP_USB3_5) — Offset 8034h

XECP SUPP USB3_5

Note: Bit definitions are the same as XECP_SUPP_USB2_4, offset 8010h.

8.3.167 XECP SUPP USB3_6 (XECP_SUPP_USB3_6) — Offset 8038h

XECP SUPP USB3_6

Note: Bit definitions are the same as XECP_SUPP_USB2_4, offset 8010h.

8.3.168 XECP SUPP USB3_7 (XECP_SUPP_USB3_7) — Offset 803Ch

XECP SUPP USB3_7

Note: Bit definitions are the same as XECP_SUPP_USB2_4, offset 8010h.

8.3.169 XECP SUPP USB3_8 (XECP_SUPP_USB3_8) — Offset 8040h

XECP SUPP USB3_8

Note: Bit definitions are the same as XECP_SUPP_USB2_4, offset 8010h.

8.3.170 XECP SUPP USB3_9 (XECP_SUPP_USB3_9) — Offset 8044h

XECP SUPP USB3_9

Note: Bit definitions are the same as XECP_SUPP_USB2_4, offset 8010h.

8.3.171 XECP SUPP USB3_10 (XECP_SUPP_USB3_10) — Offset 8048h

XECP SUPP USB3_10

Note: Bit definitions are the same as XECP_SUPP_USB2_4, offset 8010h.

8.3.172 XECP SUPP USB3_11 (XECP_SUPP_USB3_11) — Offset 804Ch

XECP SUPP USB3_11

Note: Bit definitions are the same as XECP_SUPP_USB2_4, offset 8010h.

8.3.173 Host Control Scheduler (HOST_CTRL_SCH_REG) — Offset 8094h

Host Control Scheduler

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 8094h	00008100h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RW	**Disable repeat scheduler service of USB2 periodic (SCH_USB2_PRDC):** Disable repeat scheduler service of USB2 periodic
30:27	0h RW	**Enable scheduler limiter functions to block async. traffic types across ports while periodic pending (SCH_BLOCK_ASYNC):** Enable scheduler limiter functions to block async. traffic types across ports while periodic pending
26	0h RW	**Enable pkt pending notification to usb3 ports (EN_PP_NTFC_USB3):** Enable pkt pending notification to usb3 ports
25	0h RW	**disable async. burst limitation while periodic in progress (DIS_ASYNC_BURST):** disable async. burst limitation while periodic in progress
24	0h RW	**Disable marking overlap flag on all TT periodic INs. (DIS_OVERLAP_TT_PERIODIC):** Disable marking overlap flag on all TT periodic INs.
23	0h RW	**disable blocking of async. scheduling while periodic active to same port (DIS_BLOCK_ASYNC_PER_ACT):** disable blocking of async. scheduling while periodic active to same port
22	0h RW	**Setting this bit enables pipelining of multiple OUT EPs (EN_PIPELINE_MULTIPLE_OUT):** Setting this bit enables pipelining of multiple OUT EPs (across diff ports). This will help boost the performance for multiple ports OUT test case
21	0h RW	**Strobe Method Port Periodic Done Check (EN_STROBE_USB2_PRDC_DONE):** Enable strobe method of USB2 port periodic done check (off by default)
20:17	0h RW	**TTE Host Control (TTE_HOST_CTRL):** 0: disable interrupt complete split limit to 3 microframes 1: disable checking of missed microframes 2: disable split error request w/NULL pointer on speculative INs with data payload and no TRB. 3: disable deferred split error request on speculative IN with data payload and no TRB. Other values are reserved.

Bit Range	Default & Access	Field Name (ID): Description
16	0h RW	**disable deferred split error request on speculative IN with data payload and no TRB. (DIS_DEFFER_SPLIT_ERR):** disable deferred split error request on speculative IN with data payload and no TRB.
15	1h RW	**TTE: disable split error request w/NULL pointer on speculative INs with data payload and no TRB. (TTE_DIS_SPLIT_ERR_IN_DATA_NO_TRB):** TTE: disable split error request w/NULL pointer on speculative INs with data payload and no TRB.
14	0h RW	**TTE: Disable checking of missed microframes (DIS_MISSED_UFRAME_CHECK):** TTE: Disable checking of missed microframes
13	0h RW	**TTE: Disable interrupt complete split limit to 3 micro frames (DIS_INTER_SPLIT_LIMIT):** TTE: Disable interrupt complete split limit to 3 micro frames
12:11	0h RW	**Cache Size Control Reg (CACHE_SZ_CTRL):** 0: 64 1: 32 2,3: 16
10:9	0h RW	**Maximum EP Per Slot (MAX_EP_SLOT):** 0: 32 1: 16 2: 8 3: 4
8	1h RW	**Turn on scratch_pad_en (TO_SCRATCH_PAD_EN):** Cmd Mgr: Enables scratch pad function
7	0h RW	**Scheduler Host Control Reg (STOP_SCH_UNCON):** enable check to stop scheduling on port that are not connected
6	0h RW	**disable 1 pack scheduling limit when ISO pending in present microframe (DIS_SCH_LIMIT):** disable 1 pack scheduling limit when ISO pending in present microframe
5:4	0h RW	**scheduler sort pattern (SCH_SORT_PATTERN):** 00 (default) search ISO ahead of interrupt within each service interval 01 - search USB2-ISO, USB3-ISO, USB2-Interrupt, USB3-Interrupt within each service interval 10 - search strictly by interval 11 - search all ISO intervals ahead interrupt intervals and within each interval, USB2 ahead of USB3
3	0h RW	**enable TTE overlap prevention on interrupt OUT EPs (at cost of possible service interval slip (EN_TTE_OVERLAP_PREV_OUT):** enable TTE overlap prevention on interrupt OUT EPs (at cost of possible service interval slip
2	0h RW	**enable TTE overlap prevention on interrupt IN EPs (at cost of possible service interval slip (EN_TTE_OVERLAP_PREV_IN):** enable TTE overlap prevention on interrupt IN EPs (at cost of possible service interval slip
1	0h RW	**Disable TRM active IN EP valid check function (DIS_TRM_ACT_IN_VALID):** Disable TRM active IN EP valid check function
0	0h RW	**Disable poll delay function (DIS_POLL_DELAY):** Scheduler: Disable poll delay function

8.3.174 Power Management Control (PMCTRL_REG) — Offset 80A4h

Power Management Control

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 80A4h	012DFF94h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RW	**Async PME Source Enable (ASYNC_PME_SRC_EN):** This field allows the async PME source to be allowed to generate PME. This is specifically required for SOCs that do not allow for any clock other than RTC to be available during RTD3.
30	0h RW	**Legacy PME Source Enable (LEGACY_PME_SRC_EN):** This field allows the legacy PME source to be used in PME generation. The legacy source in in reference to the source prior to the RTD3 changes.
29	0h RW	**Reset Warn Power Gate Trigger Disable (RESET_WARN_PWR_GATE_TRIGGER_DISABLE):** This field controls the actions taken for due to reset warn. 0 - Reset Warn will trigger a HW autonomous Power Gate 1 - Reset Warn will not trigger a HW autonomous Power Gate
28	0h RW	**Clear PME Flag (CLR_PME_FLAG_PULSE_AUX_CCLK):** Internal PME flag Clear This Write-Only bit can be used to clear the internal PME flag. SW write to 1 will clear the PME flag. SW write to 0 will have no effect and be ignored by the controller. Read always return 0
27	0h RW	**Disable RTD3 power gating when in D3 (DIS_D3_PG):** Disable RTD3 power gating when in D3 and context save operation is not performed
26	0h RW	**XLFPSCOUNTSRC:** XLFPSCOUNTSRC (Source for LFPS OFF Counter) 0: Central RTC Counter for LFPS detection 1: Local Counter for LFPS detection
25	0h RW	**XELFPSRTC:** XELFPSRTC (Enable LFPS Filtering on RTC) 0: Use Oscillator clock for LFPS Filtering during P3 1: Use RTC Clock for LFPS Filtering during P3
24	1h RW	**XMPHYSPGDD0I2:** XMPHYSPGDD0I2 (ModPhy Sus Well Power Gate Disable for D0I2) 0: Modphy sus well power gating enabled 1: Modphy sus well power gating disabled
23	0h RW	**XMPHYSPGDD0I3:** XMPHYSPGDD0I3 (ModPhy Sus Well Power Gate Disable for D0I3) 0: Modphy sus well power gating enabled 1: Modphy sus well power gating disabled
22	0h RW	**XMPHYSPGDRTD3:** XMPHYSPGDRTD3 (ModPhy Sus Well Power Gate Disable for RTD3) 0: Modphy sus well power gating enabled 1: Modphy sus well power gating disabled

Bit Range	Default & Access	Field Name (ID): Description
21:18	Bh RW	**XD3RTCPTTM:** XD3RTCPTTM (D3 RTC Port Timer Tick Multiplier) This register will be the multiplication factor for determining USB3 Wake Detection Frequency and RXDET based on the XD3RTCPTTC value. If XD3RTCPTTC is 9h and this register is Bh, frequency for RXDET H8EXIT detection while MODPHY SUS Power gating is enabled would be 99ms.
17	0h RW	**U3 LFPS Periodic Sampling ON Time Control (U3_LFPS_PRDC_SAMPLING_ON_TIME_CTRL):** This field controls the ON time for the LFPS periodic sampling for USB3 ports. 0 ON time is 2 rtc clocks 1 ON time is 3 rtc clocks Note: This field is ignored if USB3 PHY SUS Well Power Gating is enabled.
16	1h RW	**AON LFPS Detector Enable Mode (AON_LFPS_DETECTOR_EN_MODE):** 1 - Allow the LFSP Detector in AON to own LFPS detection when the port is in PS3 for U2/U3 - not RxD regardless of port ownership. 0 - Allow the LFPS Detector in AON to own the LFPS detection only when the AON owns the port and in U2/U3 - not RxD
15:8	FFh RW	**SS U3 LFPS Detection Threshold (SS_U3_LFPS_DETECTION_THRESHOLD):** This field controls the threshold used to determine when a valid U3 Wake is detected through when using the unfiltered LFPS source. The value on this field will reflect the binary count required to have been detected on the counter being clocked by the unfiltered lfps source to result in a valid U3 wake detection.
7:4	9h RW	**U3 LFPS Periodic Sampling Off Time Control (SS_U3_LFPS_PRDC_SAMPLING_OFFTIME_CTRL):** This field controls the OFF time for the LFPS periodic sampling for USB3 Ports 0x0 periodic sampling is disabled. 0x1 OFF time is 1ms 0x2 OFF time is 2ms 0xF OFF time is 15ms The ON Time is determined by the amount of time required to reliably determine if there is a valid LFPS and is HW implementation specific. A speed up mode shall be implemented where this field is in units of us. i.e. 0x1 = 1 us OFF time, 0x2 = 2 us OFF time, etc.
3	0h RW	**PS3 LFPS Source Select (PS3_LFPS_SRC_SEL):** 0 LFPS Source is unfiltered 1 LFPS Source is filtered (Rx-Elec-Idle) LFPS Source is Rx-Elec-Idle for any non PS3 state.
2	1h RW	**XHCI Engine Autonomous Power Gate Exit Reset Policy (XHC_AUTO_PWRGATE_EXITRST_POLICY):** Controls when the xHCI engine is brought out of reset due to a power ungate. 0 Engine is brought out of reset when D3 to D0 is triggered. This allows for a quick power up sequence while leaving the virtual PCIe LTSSM in L23 is power ungate is not due to D3 to D0. 1 Engine is brought out of reset along with the rest of the IP. This is required for PMC save/restore flow.
1	0h RW	**USB2 Port Wake Unit Coupling Policy (USB2_PORT_WAKE_COUPLING_POLICY):** Controls the trigger for USB2 Port Wake Units to initiate Port Level Power Off Preparation. 0 RTD3 triggered 1 - Port Triggered when in L1, L2 or Disabled, Disconnected

Bit Range	Default & Access	Field Name (ID): Description
0	0h RW	**USB3 Port Wake Unit Coupling Policy (USB3_PORT_WAKE_COUPLING_POLICY):** Controls the trigger for USB3 Port Wake Units to initiate Port Level Power Off Preparation. 0 - RTD3 Triggered 1 - Port Triggered when in PS3 due to RxDetect, U3, U2 or Disabled

8.3.175 Host Controller Misc Reg (HOST_CTRL_MISC_REG) — Offset 80B0h

Host Controller Misc Reg

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 80B0h	0001037Fh

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RW	**USB2 LTR Update Disable (USB2_LTRUPDT_DIS):** This controls the inclusion of the USB2 LTR based on link state. Setting this bit will disable USB2 LTR and will expose a NO Requirement from USB2 thus not impacting the aggregated LTR vaule for the controller.
30	0h RW	**USB2 Line State Debounce During Port Reset Policy (USB2_LINE_STATE_DEBOUNCE_DURING_PORT_RESET_POLICY):** This register controls how the debounce is enforced during the Port Reset phase. 0 do not enable the line state debounce during port reset. 1 enable the line state debounce during port reset.
29	0h RW	**TTE PEXE Credit Fix Disable (TTE_PEXE_CREDIT_FIX_DISABLE):** When set, it disables a fix implemented to re-deem PEXE credits when a port is disconnected
28	0h RW	**TTE Scheduling policy (TTE_SCHEDULING_POLICY):** This register controls a fix made to prevent over-scheduling by not account for 188B in each uFrame. Setting this bit will disable the fix and allow for over-scheduling.
27	0h RW	**USB3 ITP Delta Timer Source Select (USB3_ITP_DELTA_TIMER_SOURCE_SELECT):** This register selects the source for the delta timer tracking used for ITP generation. 0 the source is a 16.666 ns tick generated from a crystal reference clock 1 - the source is a 16.666 ns tick generated from the aux_cclk. This field needs to remain in sync with Frame Timer Source Select to ensure the are both set or both cleared. There is no support for any other combination.
26	0h RW	**Frame Timer Source Select (FRAME_TIMER_SOURCE_SELECT):** This register controls the source for the frame timer. 0 the source for the frame timer is a crystal reference clock 1 the source for the frame timer is the aux_cclk.

Bit Range	Default & Access	Field Name (ID): Description
25	0h RW	**uFrame Masking Enable (UFRAME_MASKING_ENABLE):** If set, enables the uFrame tick to be masked due to ports being in U3/NC. This controls a fix made to disable the auto masking of uFrame tick due to port state without any pipeline idle condition. When cleared, the controller relies on gating of frame timer due to proper port state and idleness tracking from the pipeline.
24	0h RW	**Late FID Check Disable (LATE_FID_CHECK_DISABLE):** This register disables the Late FID Check performed when starting an ISOCH stream.
23	0h RW	**Late FID TTE count adjust Disable (DIS_LATE_FID_TTE_CNT_ADJ):** 0 the value of frame late skip count starts at 1 for TTE eps and 0 for non tte eps. this represents an adjustment for the number of SI missed 1 the value of frame late skip count starts at 0 for both TTE eps and non tte eps
22	0h RW	**Late FID difference calculation legacy (DIS_DIF_CAL_LEGACY):** 0 late uframeid uses the new difference calculation to compute how may SI the TD is late 1 late uframeid uses the legacy difference calculation to compute how may SI the TD is late
21	0h RW	**ERDY flag Disable (ERDY_FLAG_DIS):** 0 An ERDY received on any interrupt EP will force the backbone clock high untill the next uframe to allow that eps trm pending mask to be cleared 1 This feature is disabled
20	0h RW	**Enable LTR DB Device Clear (EN_LTR_DB_DEV_CLR):** 1 TDB 0 Enable bit operation
19	0h RW	**USB2 Resume Cx Inhibit Disable (USB2_RESUME_CX_INHIBIT_DISABLE):** Controls if USB2 L1 Resume is allowed to contribute to DMA Active which will inhibit Cx state. 0 USB2 L1 Resume is allowed to inhibit Cx via DMA Active 1 USB2 L1 Resume is NOT allowed to inhibit Cx via DMA Active When cleared, Cx will only be inhibited when the DMA traffic for the port begins.
18	0h RW	**Late FID TTE Disable (LATE_FID_TTE_DIS):** Late FID TTE Disable 0: Late Frame ID Check is enabled for TTE Endpoints 1: Late Frame ID Check is disabled for TTE Endpoints
17	0h RW	**Late FID uframe Check Disable (LATE_FID_UFRAME_CHK_DIS):** 0 Frame ID Match only asserts in uframe 7 for non-TTE Endpoints Frame before match 1 Frame ID Match can assert in any uframe
16	1h RW	**Late FID Extra Interval (LATE_FID_EXTRA_INTER):** This register controls the extra number of intervals added onto the advancing of late FID check escentially a bias used to correct for possible errors in implementation
15:0	037Fh RW	**Valid Isoch Scheduling Range (VALID_ISOCH_SCHEDULING_RANGE):** This register defines the window in miliseconds from the current Frame that will be considered for scheduling in an upcoming Frame. Anything scheduled outside of this window will be considered as late and will trigger the Missed Service Error.

8.3.176 Host Controller Misc Reg2 (HOST_CTRL_MISC_REG2) — Offset 80B4h

Host Controller Misc Reg2

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 80B4h	00000100h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:29	0h RW	**Max Short Packet Advance Counter (MAX_SHORT_PKT_ADV_CNT):** Short Packet Advance Throttling 0 - Limit SPA to 4 TRB's 1 - Limit SPA to 16 TRB's 2 - limit SPA to 64 TRB's 3 - limit SPA to 128 TRB's 4 - limit SPA to 512 TRB's 5 - limit SPA to 1024 TRB's 6 - limit SPA to 2048 TRB's 7 - Disabled
28	0h RW	**Disable Scheduler FrameID Check (DIS_SCH_FRAMEID_CHK):** Disable Scheduler FrameID check. 0: Scheduler FrameID check is enabled. 1: Scheduler FrameID check is disabled
27	0h RW	**Disable ISOC Buffer Overrun Detect (DISABLE_ISOC_BUF_OVERRUN_DETECT):** Enable bit to disable ISOC buff overrun error code reporting. 0: Enables the reporting of ISOC buffer Overrun Error code. 1: Disabled ISOC buffer Overrun Error Code and reports Babble instead
26	0h RW	**Disable CPL NODMA TRB Walk (DISABLE_CPL_NODMA_TRB_WALK):** Enable bit to walk NON-DMA TRB at the end of TD. 0-Enables the walk of NON-DMA TRB on encountering TRB Cache Invalidation scenario for TTE EP. 1-Disables the NON_DMA TRB walk on encountering TRB Cache Invalidation Scenario
25	0h RW	**LTM Belt Valid Clear (LTM_BELT_VALID_CLR):** LTM Belt Valid Clear
24	0h RW	**TRM Drop Scheduler Request Disable (CFG_TRM_DROP_SCH_REQ_DIS):** TRM Drop Scheduler Request Disable
23	0h RW	**TRM Drop TTE Request Disable (CFG_TRM_DROP_TTE_REQ_DIS):** TRM Drop TTE Request Disable
22	0h RW	**TRM EDTLA Clear Disable (CFG_TRM_EDTLA_CLR_DIS):** TRM EDTLA Clear Disable
21	0h RW	**XFER is_serve Check Enable (CFG_XFER_IS_SERVE_CHK_EN):** Enable checking is_serve condition in XFER, mainly for undoing fix if needed
20	0h RW	**Remote Flow Control Disable (CFG_CPL_NPKT0_FC_DIS):** Set low to allow receiving ACK with NUMP>0 to bring the TRM out of Remote Flow Control
19:18	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
17	0h RW	**Disable IDT credit leak fix (CFG_DIS_ODMA_IDT_CRD_LEAK_FIX):** Disable the IDT credit leak fix in odma. 0 Fix is enabled 1 Fix is disabled
16	0h RW	**IDMA Tranfer Type_Check Disable (CFG_IDMA_TTYPE_CHK_DIS):** Set to disable packet Transfer Type checking in IDMA
15	0h RW	**Host Controller Reset Controller Isolation Disable (HCRST_CTRL_ISOL_DISABLE):** Setting this bit to 1 will disable the Host Controller Reset based quiescing/isolation flow
14	0h RW	**Disable IDMA Performance Fix (DISABLE_IDMA_PERF_FIX):** Fix is enabled by default 0: Fix enabled 1: Fix disabled
13	0h RW	**Enable HH Frindex Not Run (EN_HH_FRINDEX_NOT_RUN):** Enable HH Frindex Not Run
12	0h RW	**Disable IDT Fix ODMA (DISABLE_IDT_FIX_ODMA):** Disable DMA_RD_WAIT_IDT arc fix. 0: Fix enabled 1: Fix disabled
11	0h RW	**Disable Ping Fix ODMA (DISABLE_PING_FIX_ODMA):** 0: Fix enabled 1: Fix disabled
10	0h RW	**Disable CERR Fix IDMA (DISABLE_CERR_FIX_IDMA):** 0: Fix enabled 1: Fix disabled
9	0h RW	**Enable 100ms Watch Dog Timer (EN_100MS_WATCH_DOG_TIMER):** 100ms Watch Dog Timer 0: 300ms Watch Dog Timer for PHY status assertion 1: 100ms Watch Dog Timer for PHY status assertion
8	1h RW	**Enable Watch Dog Timer (EN_WATCH_DOG_TIMER):** When set, it will enable 100/300ms watch dog timer for PHY status assertion
7	0h RW	**enable SSP ISOC Pipelining (EN_SSP_ISOC_PIPELINING):** Enable ISOC Pipelining feature for SSP devices. 0: disable the feature 1: enable the feature
6	0h RW	**Disable Trunk Clock Gating Un-gate on Flush (DISABLE_TCG_UNGATE_ON_FLUSH):** When set, it will ungate the trunk clock gating for PIPE clock when there is flush whe DBC/EXI HHH is not idle.
5	0h RW	**Disable VNN Frame Timer (DISABLE_VNN_FRAME_TIMER):** Frame Timer Select This register defines the frame timer used for all frame timer derived ticks. 0 - Frame timer in the VNN is the source for all frame timer related tracking. 1 - Frame timer in the Gated VNN is the source for all frame timer related tracking.
4	0h RW	**Disable Clear CCS on CAS Set (DISABLE_CLR_CCS_ON_CAS_SET):** Disables Clear CCS on CAS. When set, XHCI port will not clear the CAS when CCS is set.

Bit Range	Default & Access	Field Name (ID): Description
3	0h RW	**Disable Root Hub Park at DBC Disconnect (DISABLE_RHUB_PARK_AT_DBCDISC):** On Default Enables Root Hub s/m to arc to DBC_DISCONNECTED from ERROR and RESET states if the reason to enter into those state was a prior connection failure to exchange Link Capabilities Set 1 Keep the Root hub s/m in ERROR or RESET as the case may be, on a successful connection as a DBC if the first attempt was failed due to PortConfigTimeout
2	0h RW	**Disable WPR on Disconnected Ports (DISABLE_BLOCK_WPR_ON_DISPORTS):** Warm Port Reset on Disconnected Port Disable When set, disables the generation of a WPR on a disconnected port.
1:0	0h RO	**Reserved**

8.3.177 Super Speed Port Enable (SSPE_REG) — Offset 80B8h

Super Speed Port Enable

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 80B8h	80000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	1h RW	**Block Power Down for Active LFPS (SS_CFG_BLOCK_PWRDWN_4_ACT_LFPS):** Delay power down entry if Rx LFPS is active. Setting this bit will block the controllers power down entry seq (for Sx/D3/D0i2 etc) if Rx LFPS is active. The power down entry will happen once a device stops sending LFPS.
30	0h RW	**Enable Clear CCS for Host Controller Reset (DIS_CLR_CCS_4_HCRESET):** Enable Clearing of CCS for Host Controller Reset - Setting this bit clears the USB3 ports PORTSC.CCS bit upon Host Controller Reset.
29	0h RW	**Disable Raw LFPS Based Detection Wake (DISABLE_RAWLFPS_BASED_WAKE_FIX):** Disable Raw LFPS Detection Based Wake from P3 This bit is used to disable RTL fix provided to separate Raw LFPS and RxElecIDle detection 0: Transition port to RESUME based on raw LFPS detection 1: Transition port to RESUME based Filtered RxElecIdle detection
28	0h RW	**EXI Override Disable (EXI_OVERRIDE_DIS):** EXI Override Disable
27:4	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
3:0	0h RW	**USB3 Port Enable (SSPE_REG):** This field controls whether SuperSpeed capability is enabled for a given USB3 port. When set to 1, Enables SuperSpeed termination Enables PORTSC to see the connects on the ports. When set to 0, Disables SuperSpeed termination Blocks PORTSC from reporting attach/connect. Places port in the lowest power state.

8.3.178 AUX Power Management Control (AUX_CTRL_REG1) — Offset 80E0h

AUX Power Management Control

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 80E0h	8081BCE0h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	1h RW	**D3 Hot function enable register (D3_HOT_FXN_EN):** This bit is from pin input which is set 1. Software can alter it as needed. 0: D3 Hot Disabled 1: D3 Hot Enabled
30	0h RW	**Allow L1 Core Clock Gating (ALL_L1_CORE_CG):** When set to 1 allows core clock being gated during L1 state.
29	0h RW	**Allow Engine PHY Status Extension (AL_EP_SEXT):** When set to 1 allows the engine to extend PHY status of PCIe PIPE for one more cycle. This is due to the fact that our rate change function has a potential of not being able to sample the phystatus signal.
28	0h RW	**Allow Engine PCIe Rate Change Passing (ALL_EP_RCP):** When set to 1 allows the engine to pass PCIe rate change signal as it is from PCIe core to PCIe PHY.
27	0h RW	**Allow Engine PERST Fundamental Reset (AL_PERST_FRST):** When set to 1 allow engine to treat PERST# as a foundamental reset
26	0h RW	**Overwrite PCIe P2 to P1 (OVR_PCIE_P2_P1):** When set to 1 will overwrite a PCIe powerdown state of P2 to P1.
25	0h RW	**Set Internal SSV 1 (SET_ISSV_1):** When set to 1 set the internal SSV to 1.
24	0h RW	**Clear Internal SSV 0 (CLR_ISSV_0):** When set to 1 clear the internal SSV to 0.
23	1h RW	**Enable Save/Restore Software Loading (EN_SRE_SW_LD):** This is a bit that enables the save_restore_enable signal being loaded when a software command has set Save bit. This is a debug function.

Bit Range	Default & Access	Field Name (ID): Description
22	0h RO	**Reserved**
21	0h RW	**Force Save/Restore 1 (FORCE_SR1):** When set to 1, it will force the save_restore flag to 1. This flag is an bit to ensure that the controller has masked the update during low power state. If software write this bit to 1, it must write it to 0 in order to resume the normal save and restore function.
20	0h RW	**Disable Warm Reset Detect Speculative Upstream Ports (CFG_DIS_WRSTDET_SPECU):** 0: Speculative upstream for Debug and SS/SSP port will detect WPR 1: No speculative upstream till port configuration is completed
19	0h RW	**I/O Buffer Drive Strength (CIDS1):** Controls the drive strength of the IO buffer
18	0h RW	**I/O Buffer Drive Strength (CIDS0):** Controls the drive strength of the IO buffer
17	0h RW	**Disable Arc RXDP3 (CFG_DIS_ARC_RXDP3):** When set to '1' DIsables arc to RXDET_p3 on disc from U2P3/U3
16	1h RW	**cfg clk gate dis (CCGD):** 1: Disable USB3 port clock gating 0: Enable USB3 port clock gating
15	1h RW	**Enable CFG RXDET P3 (EN_CFG_RDP3):** When set to '1' enable cfg rxdet p3
14	0h RW	**Enable CFG PIPE Reset (EN_CFG_PIPE_RST):** When set to '1' enable cfg pipe rst
13	1h RW	**Enable Filter TX Idle (EN_FILT_TX_IDLE):** When set to 1 enables a filter function to TX electrical idle signal at PCIe PIPE. The controller has a filter that sets TXelecidle signal of PCIe PIPE to 1 when it is in isolation state or power down transition states.
12	1h RW	**Enable Host Engine Generate PME (EN_HE_GEN_PME):** This is a global switch to whether or not eable this host engine to generate PME message.
11	1h RW	**Enable Isolation (EN_ISOL):** When set to '1' enable isolation
10	1h RW	**Enable L1 Caused P2 Overwrite (EN_L1_P2_OVR):** Set 1 to enable a new feature. This new feature is designed to use L1 as a state to identify whether the controller should do P2 Overwrite or not. Legacy behavior: P1 state was used to identify whether or not to invoke P2 overwrite function.
9	0h RW	**Enable Core Clock Gating (EN_CORE_CG):** When set to '1' disable core clock gating based on low power state entered
8	0h RW	**Enable PHY Status Timeout (EN_PHY_STS_TO):** When set to '1' enable PHY status timeout function which is designed to cover the PCIePHY issue that the controller may have not able to detect the PHY status toggle.
7	1h RW	**Ignore aux_pm_en PCIe Core (IGN_APE_PC):** When set to '1' ignore the aux_pm_en reg from PCIe core to continue the remote wake/clock switching support
6	1h RW	**Enable P2 Overwrite P1 (EN_P2_OVR_P1):** When set to '1' enable P2 overwrite P1 when PCIe core has indicated the transition from P0 to P1. This is to enable entering the even lower power state.
5	1h RW	**Enable P2 Remote Wake (EN_P2_REM_WAKE):** When set 1 '1' enable the remote wake function by allowing P2 clock/switching and P2 entering
4:1	0h RW	**Forced PM State (FORCED_PM_STATE):** Forced PM state

Bit Range	Default & Access	Field Name (ID): Description
0	0h RW	**Initiate Force PM State (INIT_FPMS):** When set to '1' force PM state to go to the state indicated in bit 4:1

8.3.179 SuperSpeed Port Link Control (HOST_CTRL_PORT_LINK_REG) — Offset 80ECh

SuperSpeed Port Link Control

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 80ECh	18000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:27	03h RW	**Force LTSSM State (FORCE_LTSSM_ST):** LTSSM state to be forced This value is for test purpose only.
26	0h RW	**Direct Link LTSSM State (DL_LTSSM_ST):** 0: Normal operation mode 1: Direct link to a specific state specified by bit 31:27 This bit is for test purpose only. It shall be written 0 in normal operation mode.
25	0h RW	**Direct Link To U0 (DL_U0):** 0: Normal operation mode 1: Direct link to U0 This bit is for test purpose only. It shall be written 0 in normal operation mode.
24:21	0h RW	**Forced Compliance Pattern (FORCED_CMP_PAT):** Compliance pattern to be forced to enter compliance mode This value is for test purpose only.
20	0h RW	**Enable Link Error Slave Count (EN_LES_CNT):** 0: Disable link error slave count 1: Enable link error slave count
19	0h RW	**TS Receive to Complete U1/U2/U3 Exit LFPS Handshake (TS_RCV_UX_EXIT_LFPS_HS):** 1: enable TS receive to complete U1/U2/U3 exit LFPS handshake 0: disable TS receive to complete U1/U2/U3 exit LFPS handshake
18	0h RW	**Enable Logic Idle Receive to Exit Polling (EN_LOGIC_TO_EXIT_POLLCONF_AND_RECCONF):** 0: disable logic idle receive to exit Polling. Configuration and Recovery. 1: enable logic idle receive to exit Polling. Configuration and Recovery.
17	0h RW	**Port Initialization Timeout Value (PORT_INTIL_TIMEOUT_VAL):** This bit specifies the port initialization timeout value. 1: 20us - 21us 0: 19us - 20us

Bit Range	Default & Access	Field Name (ID): Description
16:15	0h RW	**PHY Low Power Latency (PHY_LP_LAT):** This field defines the latency to drive the PHY to enter low power mode 0: 4 cycles 1: 8 cycles 2: 16 cycles 3: 32 cycles
14:12	0h RW	**Link Recovery Minimum Time (LR_MIN_TM):** This value defines the minimum time for the link to stay in Recovery.Active other than from U3. The granuity is 128us.
11:9	0h RW	**Link Polling Minimum Time (LP_MIN_TM):** This value defines the minimum time for the link to stay in Polling.Active and Recovery.Active from U3. The granuity is 128us.
8	0h RW	**Force Link Accept PM Command (FORCE_LA_PMC):** 0: Normal operation mode 1: Force link to accept power management command
7	0h RW	**Direct Link Recovery U0 (DL_REC_U0):** 0: Normal operation mode 1: Direct link to Recovery from U0
6	0h RW	**Link Fast Training Mode (LINK_FTM):** 0: Normal operation mode 1: Link fast training mode This bit should be written 0 in normal operation.
5	0h RW	**Disable Link Scrambler (DIS_LINK_SCRAM):** 0: Enable link scrambler 1: Disable link scramber
4	0h RW	**Direct Link U3 From U0 (DL_U3_U0):** 0: Normal operation mode 1: Direct link to U3 from U0 This bit is for test purpose only. It shall be written 0 in normal operation mode.
3	0h RW	**Direct Link U3 From U0 (DL_U2_U0):** 0: Normal operation mode 1: Direct link to U2 from U0 This bit is for test purpose only. It shall be written 0 in normal operation mode.
2	0h RW	**Direct Link U3 From U0 (DL_U1_U0):** 0: Normal operation mode 1: Direct link to U1 from U0 This bit is for test purpose only. It shall be written 0 in normal operation mode.
1	0h RW	**Enable Link Loopback Master Mode (EN_LINK_LB_MAST):** 0: Disable link loopback master mode 1: Enable link loopback master mode
0	0h RW	**Disable Link Compliance Mode (DIS_LINK_CM):** 0: Enable link compliance mode 1: Disable link compliance mode

8.3.180 USB2 Port Link Control 1 (USB2_LINK_MGR_CTRL_REG1) — Offset 80F0h

These set of registers is used to control jey USB set of timers. They are spread over 4 registers each 32 bits wide.

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 80F0h	310803A0h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:24	31h RW	**FS/LS Mode SE0 Disconnect Delay (FSLS_SE0_DIS_DEL_7_0):** Number of microseconds of SE0 in FS/LS mode to register disconnect had occurred.
23:21	0h RO	**Reserved**
20	0h RW	**L1 Exit Recovery Mode (L1_EXIT_RECOVERY_MODE):** Mode for extended L1 Exit recovery delay: 0: 12us 1: 50us
19	1h RW	**L1 Timeout Increment MODE (L1_TO_INCR_MODE):** Mode select for L1 Timeout increments: 0: time out increments are in 125us 1: L1 Timeout increments are in 256us. Refer to USB2 PORTHLPMC.L1 Timeout in XHCI Spec for additional details
18	0h RO	**Reserved**
17	0h RW	**Detect Nominal Packet EOP (EN_DETECT_NOMINAL_PKT_EOP):** 0: Detect minimal packet EOP. 1: Detect nominal packet EOP.
16	0h RW	**Disable Chirp Response (DIS_CHIRP_RESPONSE):** 0: Normal 1: Force full speed on host ports (disable chirp response)
15	0h RW	**Disable 192 Byte Limit Check (DIS_192B_LIM):** 0: Enforce 192 byte limit on complete-split INs. Treat any packet) 192 as babble case. 1: Disable 192 byte limit check.
14	0h RW	**External Provided FS/LS Disconnect (EXT_FSLS_DIS):** 0: Internal FS/LS Disconnect from linestate(1:0) 1: External provided FS/LS Disconnect from hostdisconnect input
13:12	0h RW	**UTMI Reset Source Select (UTMI_RST_SEL):** Select UTMI Reset Source (FRD UTMI Reset Only) 00: HCReset or Force PHY Reset or internal reset after disconnect/suspend for restart (default) 01,11: UTMI reset = ~UTMI suspendm 10: UTMI reset = ~UTMI suspendm and synchronization to port clk.
11	0h RW	**Disable HS Disconnect Window (DIS_HS_DIS_WIN):** 0: Enable HS Disconnect Window Function 1: Disable HS Disconnect Window Function
10	0h RW	**Disable Port Error Detection (DIS_PERR_DET):** 0: Enable Port Error Detection (default) 1: Disable Port Error Detection

Bit Range	Default & Access	Field Name (ID): Description
9	1h RW	**Disable Peek Function for ISO-OUT (DIS_PF_IOUT):** 0: Enable Peek function for ISO-OUT (default) 1: Disable Peek function for ISO-OUT
8	1h RW	**Drive Resume-K FS/LS Serial Interface (DRV_RESK_FSLS_SER):** 0: Drive Resume-K on parallel Interface 1: Drive Resume-K directly on FS/LS Serial Interface (default)
7	1h RW	**Enable USB2 Drop-Ping (EN_U2_DROP_PING):** 0: Disable Drop-Ping Function in USB2 Protocol (default) 1: Enable Drop-Ping Function in USB2 Protocol
6	0h RW	**Enable USB2 Force-Ping (EN_U2_FORCE_PING):** 0: Disable Force-Ping Function in USB2 Protocol (default) 1: Enable Force-Ping Function in USB2 Protocol
5	1h RW	**Enable USB2 Auto-Ping (EN_U2_AUTO_PING):** 0: Disable Auto-Ping Function 1: Enable Auto-Ping Function in USB2 Protocol (default)
4	0h RW	**Disable PHY SuspendM (DIS_PHY_SUSM):** 0: PHY is suspend=U3,U2,disconnect (default) 1: Disable PHY SuspendM in All States
3	0h RW	**UTMI Internal Clock Gate Disable (UTMI_INT_CG_DIS):** 0: Normal operation (internal clock gated in U2,U3,disconnect) 1: UTMI Internal Clock Gate Disable
2	0h RW	**Disable PHY SuspendM in Disconnect State (DIS_PSUSM_DS):** 0: PHY is suspendM=0 in Disconnect State (default) 1: Disable PHY SuspendM in Disconnect State
1	0h RW	**Force PHY Reset (FORCE_PHY_RST):** 0: Normal Operation (default) 1: Force PHY Reset
0	0h RW	**USB2 Accelerated Simulation Timing (U2_ACC_SIM_TIM):** 0: Normal Operation (default - FPGA/ASIC) 1: USB2 Accelerated Simulation Timing (default - simulation)

8.3.181 USB2 Port Link Control 2 (USB2_LINK_MGR_CTRL_REG2) — Offset 80F4h

These set of registers is used to control jey USB set of timers. They are spread over 4 registers each 32 bits wide.

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 80F4h	80C40620h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	1h RW	**Total Reset Duration[0] (TOT_RST_DUR_0):** # of microseconds for total reset duration
30:18	0031h RW	**Chirp-K Duration (CHIRPK_DUR):** # of microseconds of Chirp-K to register that a device is chirping
17:5	0031h RW	**K/J Disconnect Connect Delay (KJ_DIS_CON_DEL):** # of microseconds of K/J in disconnected state to register connect has occurred.
4:0	00h RW	**FS/LS Mode SE0 Disconnect Delay[12:8] (FSLS_SE0_DIS_DEL_12_8):** # of microseconds of SE0 in FS/LS mode to register disconnect had occurred.

8.3.182 USB2 Port Link Control 3 (USB2_LINK_MGR_CTRL_REG3) — Offset 80F8h

These set of registers is used to control jey USB set of timers. They are spread over 4 registers each 32 bits wide.

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 80F8h	F865EB6Bh

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:28	Fh RW	**U2 Entry Ignore Linestate Changes Duration[3:0] (U2_IGN_LS_DUR_3_0):** # of microseconds after entering U2, linestate changes are ignored as bus settles
27:15	10CBh RW	**U3 Entry Ignore Linestate Changes Duration (U3_IGN_LS_DUR):** # of microseconds after entering U3, linestate changes are ignored as bus settles
14:0	6B6Bh RW	**Total Reset Duration[15:1] (TOT_RST_DUR_15_1):** # of microseconds for total reset duration

8.3.183 USB2 Port Link Control 4 (USB2_LINK_MGR_CTRL_REG4) — Offset 80FCh

These set of registers is used to control jey USB set of timers. They are spread over 4 registers each 32 bits wide.

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 80FCh	00008003h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:29	0h RO	**Reserved**
28:27	0h RW	**Additional Guardband for L1 Advance Prewake (ADD_GB_4_L1_PREWAKE):** additional guardband for L1 advance prewake. 00 = +0uF 01 = +1uF 10 = +2uF 11 = +4uF
26	0h RW	**select L1 min idle duration that will be driven to Scheduler. Either drive '0' or based on L1 Timeout value (SEL_L1_MIN_IDLE):** select L1 min idle duration that will be driven to Scheduler. Either drive '0' or based on L1 Timeout value
25	0h RW	**Enable periodic_prewake to prevent L1 entry if in U0, or wake from L1 if already in U2. (EN_PER_PREWAKE):** Enable periodic_prewake to prevent L1 entry if in U0, or wake from L1 if already in U2.
24:22	0h RO	**Reserved**
21:9	0040h RW	**U2 Detect Remote Wake Delay (U2D_RWAKE_DEL):** #of microseconds after detecting U2 remote wake condition to reflect K
8:0	003h RW	**U2 Entry Ignore Linestate Changes Duration[12:4] (U2_IGN_LS_DUR_12_4):** # of microseconds after entering U2, linestate changes are ignored as bus settles

8.3.184 Power Scheduler Control 0 (PWR_SCHED_CTRL0) — Offset 8140h

Power Scheduler Control 0.

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 8140h	0A019132h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:24	0Ah RW	**Engine Idle Hysteresis (EIH):** This register controls the min. idle span that has to be observed from the engine idle indicators before the power state flags (xhc_*_idle) will indicate a 1.
23:12	019h RW	**Backbone PLL Shutdown Advance Wake (BPSAW):** This register controls the time before the next scheduled transaction where the Backbone PLL request will assert. Register Format: Bits [11:7] # of 125us uframes Bits [6:0] # of microseconds (0-124)
11:0	132h RW	**Backbone PLL Shutdown Min. Idle Duration (BPSMID):** The sum of this register plus the Backbone PLL Shutdown Advance Wake form to a Total Idle time. When the next scheduled periodic transaction is after present time + Total Idle, the Backbone PLL request will de-assert, allowing the PLL to shutdwon. Register Format: Bits [11:7] # of 125us uframes Bits [6:0] # of microseconds (0-124)

8.3.185 Power Scheduler Control 1 (PWR_SCHED_CTRL2) — Offset 8144h

These bit enable by EP type those EPs classes that are considered for determining next periodic active interval for pre-wake of the periodic_active signal. EP classes that are disabled may never be observed in setting of the periodic_active signal.

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 8144h	0000033Fh

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:19	0h RO	**Reserved**
18	0h RW	**Flow-Controlled SS INTR 2SI Mode (FLOW_CTRL_2SI_MODE):** 0: The Power Scheduler will Schedule all Flow-Controlled SS INTR Endpoint's alarm to the SI determined by the Endpoint's Interval value. 1: The Power Scheduler will Schedule all Flow-Controlled SS INTR Endpoint's alarm to twice the SI determined by the Endpoint's Interval value.

Bit Range	Default & Access	Field Name (ID): Description
17	0h RW	**d0i2 Clear Alarm Fix Disable (D0I2_CLR_ALARM_FIX_DISAB):** d0i2 Clear Alarm Fix Disable
16	0h RW	**No Doorbell Clear Valid Disable (NO_DB_CLR_VAL_DISAB):** No Doorbell Clear Valid Disable
15	0h RW	**Disable BELT Latch (DISAB_BELT_LATCH):** 1: The Power Scheduler's interface to the LTR Manager signals BELT and No_Requirement are not latched with the Request signal and can change before Halt is deasserted. . 0: The Power Scheduler's interface to the LTR Manager signals BELT and No_Requirement are latched when the Request signal is asserted and will remain latched until Halt is deasserted.
14	0h RW	**LPM Prewake Interrupt NAK Disable (LPM_PREWAKE_INTR_NAK_DIS):** LPM Prewake Naked Interrupt Enable 0: Ignore the Naked INTR for LPM. 1: Do not ignore the Naked INTR for LPM.
13:12	0h RW	**LPM Prewake Interrupt Enable (LPM_PREWAKE_INTR_EN):** LPM Prewake Interrupt Enable 11: Disable interrupt prewake for LPM. 01: Enable interrupt OUT prewake for LPM. 10: Enable interrupt IN prewake for LPM. 00: Enable both interrupt IN/OUT prewake for LPM.
11:10	0h RW	**Idle Scale (IDLE_SCALE):** Engine Idle Hysteresis Scale Controls the Engine Idle Hysteresis scale. 0 - clock 1 - 1 us 2 - 125 us
9	1h RW	**HS Interrupt-OUT Alarm (HS_INT_OUT_ALRM):** HS Interrupt OUT Alarm
8	1h RW	**HS Interrupt-IN Alarm (HS_INT_IN_ALRM):** HS Interrupt IN Alarm (HSII): Note: This is required to be set to enable the functionality behind the PCICFG.HSCFG2.HSIIPAPC method of tracking HS Intr IN EPs for Periodic Active.
7	0h RW	**SS Interrupt-OUT FC Alarm (SS_INT_OUT_FC_ALRM):** SS Interrupt OUT Alarm
6	0h RW	**SS Interrupt-IN Alarm (SS_INT_IN_FC_ALRM):** SS Interrupt IN Alarm
5	1h RW	**SS Interrupt-OUT & not in FC Alarm (SS_INT_OUT_ALRM):** SS Interrupt OUT and not in FC Frame Alarm
4	1h RW	**SS Interrupt-IN & not in FC Alarm (SS_INT_IN_ALRM):** SS Interrupt IN and not in FC Frame Alarm
3	1h RW	**HS ISO-OUT Alarm (HS_ISO_OUT_ALRM):** HS ISO-OUT Alarm
2	1h RW	**HS ISO-IN Alarm (HS_ISO_IN_ALRM):** HS ISO-IN Alarm
1	1h RW	**SS ISO-OUT Alarm (SS_ISO_OUT_ALRM):** SS ISO-OUT Alarm
0	1h RW	**SS ISO-IN Alarm (SS_ISO_IN_ALRM):** SS ISO-IN Alarm

8.3.186 AUX Power Management Control (AUX_CTRL_REG2) — Offset 8154h

AUX Power Management Control Register2

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 8154h	81390206h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	1h RW	**Disable L1P2 Exit on Wake (DIS_L1P2_EXIT_ON_WAKE_EN):** This bit disables the dependency on Wake Enables defined in PORTSC for L1P2 exit when in D0
30	0h RW	**Fast Training (CFG_FAST_TRAINING):** 0: Normal operation mode 1: Link fast training mode This bit should be written 0 in normal operation
29	0h RW	**SNPS PHY Status Done L1 Disable (SNPS_PHYSTATUS_DONE_L1_DIS):** SNPS PHY Status Done L1 Disable
28	0h RW	**Shadow Decode Disable (SHADOW_DECODE_DIS):** Shadow Decode Disable
27	0h RW	**Battery Charge D3 Enable (BATT_CHARGE_D3_EN):** Battery Charge D3 Enable
26	0h RW	**Debounce Enable (CFG_DEBOUNCE_EN):** Debounce Enable
25	0h RW	**PCIe P0 Exit L1 Enable (PCIE_P0_EXIT_L1_EN):** PCIe P0 Exit L1 Enable
24	1h RW	**Enable L1 exit notification to SNPS PCIe core (EN_L1_EXIT_NOTIF_PCIE):** This bit enables a L1 exit notification to SNPS PCIe core. There is a case where USB ports have waked up and AUX PM module has started the wakeup process. The AUX PM control state got into a wait for P0 state because it needs to wait until PCIe core to signal powerdown state change. Due to the fact that the core is in D3Hot, there is no run_stop bit set such that no internal interrupt will be fired. This causes the LTSSM of PCIe stayed in L1 even though AUX PM has known that it needs an L1 exit. This bit works together with bit21 of this register. 1: enables this feature 0: disables this feature.
23	0h RW	**Disable PLC on Disconnect (DIS_PLC_ON_DISCONNECT):** 1: do not assert PLC for disconnection 0: assert PLC for disconnection
22	0h RW	**Treat Idle as TS2 in LTSSM Wait for TS2 (TREAT_IDLE_AS_TS2_IN_LTSSM_WAIT_4_TS2):** This bit enables a feature in PCIe core LTSSM to treat IDLE received as TS2 when LTSSM is in wait for TS2 receive state. This is a function requested from PHY where it is possible to not able to receive TS2 without error. 1: treat Logic IDLE as TS2 received when in some PCIe LTSSM state. 0: disable this feature.

Bit Range	Default & Access	Field Name (ID): Description
21	1h RW	**Disable p2 overwrite due to the D3HOT where PCIe core enters the L1 (DIS_P2_OVERWRITE_DUE2_D3HOT):** This feature applies when if PCIe core LTSSM enters L1 due to the D3hot, the aux PM control will not start a P2 overwrite function in anticipating for the next L23 enter. 1: disables p2 overwrite due to the D3HOT where PCIe core enters the L1. 0: enables P2 overwrite even when in D3Hot state.
20	1h RW	**Enable the Port to Enter U3 Automatically When in U1/U2 (ENABLE_AUTO_U3_ENTRY_FROM_U2_U3):** 1: enables the port to enter U3 automatically when in U1/U2 0: disables the port to enter U3 automatically when in U1/U2
19	1h RW	**No Linkdown Reset is Issue During Low Power State (DIS_LINKDOWN_RST_DURING_LOW_POWER):** No linkdown reset is issue during low power state
18	0h RW	**Exit Deep Sleep If PCIe In P0 (EN_EXIT_DEEP_SLEEP_IF_PCIE_IN_P0):** This bit enables a feature in AUX PM module where if PCIe core LTSSM is in P0 for a duration of time, the controller will exit the deep sleep state. This is for failure control in case. 0: disable this feature 1: enables this feature
17	0h RW	**U2 Exit LFPS Timer Value (U2_EXIT_LFPS_TIMER_VALUE):** This bit selects U2 exit LFPS timer value 0: 320ns 400ns in 25MHz domain 1: 240ns 320ns in 25MHz domain
16	1h RW	**Exit Deep Sleep On USB Port Wakeup (EN_EXIT_DEEP_SLEEP_ON_USB_PORT_WAKEUP):** This bit enables a function that AUX PM module exits from the deep sleep state due to the USB ports wakeup level signal. 0: disables this function which means that a wakeup pulse generated from each USB PortSC event will wake up the AUX PM module from deep sleep if the D3 state is programmed. 1: enables this function
15:14	0h RW	**P3 Entry Timeout (P3_ENTRY_TIMEOUT):** This field defines the timeout value to enter P3 mode in U2. 00: 7us 8us 01: 511us 512us 10: disables the timer (0us) 11: disables the timer (0us)
13	0h RW	**Enable U2 P3 Mode (EN_U2_P3):** 0: Disable U2 P3 mode 1: Enable U2 P3 mode
12:11	0h RW	**Fine Debug Mode Select (FINE_DM_SEL):** Fine Debug Mode Select
10	0h RW	**Enable Low Power State Based Core Clock Gating (EN_LP_CORE_CG):** When set to '1' enable core clock gating based on low power state entered
9	1h RW	**Disable USB3 Port Status Changed Event (DIS_U3_PORT_SCE):** 0: Enable USB3 port status change event generation if any change bit is not cleared 1: Disable USB3 port status change event generation if any change bit is not cleared Bit 12 default 0
8:4	00h RW	**Debug Mode Select Register (DEB_MODE_SEL):** Debug Mode Select Register
3	0h RW	**Enable Auto Wakeup Non-IDLE (EN_AWAK_NIDLE):** When set to 1 enables the auto wakeup function when engine has identified non IDLE condition.

Bit Range	Default & Access	Field Name (ID): Description
2	1h RW	**Enable PM Control P1 Exit P2 (EN_PMC_P1_EXIT_P2):** When set 1 enables the PM control module to transition to P1 instead of P0 when exit P2.
1	1h RW	**Enable PCIe PIPE CLK Isolation (EN_PP_CLK_ISOL):** When set to 1 enables the PCIe PIPE CLK to be isolated when main power is removed.
0	0h RW	**Enable P2 Overwrite P1 Allowed Detect (EN_P2OVRP1_ADET):** When set to 1 enables a function that can detect whether or not enable P2 overwrite P1 function. The condition to get to P2 overwrite is when engine is in idle conditions. This means that there is no ISO EP pending.

8.3.187 USB2 PHY Power Management Control (USB2_PHY_PMC) — Offset 8164h

USB2 PHY Power Management Control

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 8164h	000000FCh

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RW	**125us Sync Select (FRAMETICK_SYNC_SEL):** 0: Selects 125us tick synched from Frame Clock. 1: Selects 125us tick synched from aux_clk.
30:8	0h RO	**Reserved**
7	1h RW	**Enable Command Manager Active Indication for Tx/Rx Bias (EN_CMDM_TXRXB):** Enable Command Manager Active indication for Tx/Rx Bias circuit HS Phy PM Policy
6	1h RW	**Enable TTE Active Indication for Tx/Rx Bias (EN_TTE_TXRXB):** Enable TTE Active indication for Tx/Rx Bias circuit HS Phy PM Policy
5	1h RW	**Enable IDMA Active Indication for Tx/Rx Bias (EN_IDMA_TXRXB):** Enable IDMA Active indication for Tx/Rx Bias circuit HS Phy PM Policy
4	1h RW	**Enable ODMA Active Indication for Tx/Rx Bias (EN_ODMA_TXRXB):** Enable ODMA Active indication for Tx/Rx Bias circuit HS Phy PM Policy
3	1h RW	**Enable Transfer Active Indication for Tx/Rx Bias (EN_TRM_TXRXB):** Enable Transfer Manager Active indication for Tx/Rx Bias circuit HS Phy PM Policy
2	1h RW	**Enable Scheduler Active Indication for Tx/Rx Bias (EN_SCH_TXRXB):** Enable Scheduler Active indication for Tx/Rx Bias circuit HS Phy PM Policy
1	0h RW	**Enable Rx Bias ckt disable (EN_RXB_CD):** When set enables the Rx bias ckt to be disabled when conditions met (as described by the HS phy PM policy bits)

Bit Range	Default & Access	Field Name (ID): Description
0	0h RW	**Enable Tx Bias ckt disable (EN_TXB_CD):** When set enables the Tx bias ckt to be disabled when conditions met (as described by the HS phy PM policy bits)

8.3.188 XHCI Aux Clock Control Register (XHCI_AUX_CCR) — Offset 816Ch

XHCI Aux Clock Control Register

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 816Ch	00000400h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:20	0h RO	**Reserved**
19	0h RW	**USB3 Partition Engine/Link trunk gating Enable (PARUSB3_ENG_GEN):** When set to 1 enables gating of the SOSC trunk to the XHCI engine and link in the PARUSB3 partition.
18	0h RW	**USB3 Partition Frame Timer trunk gating Enable (PARUSB3_LINK_GEN):** When set to 1 enables gating of the SOSC trunk to the Frame timer in the PARUSB3 partition.
17	0h RW	**USB2 link partition clock gating enable (PARUSB2_CLK_GEN):** When set to 1 enables gating of the SOSC trunk to the USB2 link and Phy logic in the PARUSB2 partition.
16	0h RW	**USB2/USHIP 12.5 MHz partition clock gating enable (USHIP_PCGEN):** When set to 1 enables gating of the 12.5 MHz SOSC trunk to the USB2 and USHIP logic in the PARUSB2 partition.
15	0h RO	**Reserved**
14	0h RW	**USB3 Port Aux/Core clock gating enable (USB3_AC_CGE):** When set, allows the aux_cclk clock into the USB3 port to be gated when conditions are met.
13:12	0h RW	**Rx Detect Timer when port Aux Clock is Gated (RX_DT_ACG):** This field defines the value of the timer used to perform Rx Detect when port Aux Clock has been gated. 0x0: 100ms 0x1: 12ms Others: Reserved Note: This timer shall use the Fast Training Timer Tick (about 1us tick) for simulation purposes. For Fast Training mode, the above timeouts will become about 11us and about 100us, +/- implementation uncertainty, respectively.

Bit Range	Default & Access	Field Name (ID): Description
11:8	4h RW	**U2 Residency Before ModPHY Clock Gating (U2R_BM_CG):** Before gating ModPHY Aux clock, Host Controller shall wait for this time in U2. This time is meant to ensure that the attached device has entered U2 as well. 0x0: 1us 0x1: 128us 0x2: 256us 0x3: 512us 0x4: 640us 0x5: 768us 0x6: 896us 0x7: 1024us Others: Reserved Note: This counter shall start counting once pipe has entered PS3 state in response to link in U2.
7	0h RW	**Frame Timer Clock Gating Ports in U2 Enable (FTCGPU2E):** This bit, when set, allows Host Controller to gate the clock to the Frame Timer when ports are in U2.
6	0h RW	**USB2 port clock throttle enable (USB2_PC_TE):** When set, allows the Aux clock into the USB2 ports to be throttled when conditions allow.
5	0h RW	**XHCI Engine Aux clock gating enable (XHCI_AC_GE):** When set, allows the aux clock into the XHCI engine to be gated when idle.
4	0h RW	**XHCI Aux PM block clock gating enable (XHCI_APMB_CGE):** When set, allows the aux clock into the Aux PM block to be gated when idle.
3	0h RW	**USB3 Aux Clock Trunk Gating Enable (USB3_AC_TGE):** When set, allows Aux Clock Trunk feeding to USB3.0 ports to be gated when port Aux clock is gated at all USB3.0 ports and all USB3.0 modPHY instances.
2	0h RW	**USB3 Port Aux/Port clock gating enable (USB3_AP_CGE):** When set, allows the aux_pclk clock into the USB3 port to be gated when conditions are met.
1	0h RW	**ModPHY port Aux clock gating enable in U2 (MPP_AC_GEU2):** When set, allows the aux clock into the ModPhy to be gated when Link is in U2 and pipe has been in PS3 for at least the time defined by U2 Residency Before ModPHY Clock Gating field.
0	0h RW	**ModPHY port Aux clock gating enable in Disconnected, U3 or Disabled (MPP_AC_GE_DDU3):** When set, allows the aux clock into the ModPHY to be gated when Link is in Disconnected, U3 or Disabled state.

8.3.189 XHC Latency Tolerance Parameters LTV Control (XLTP_LTV1) — Offset 8174h

XHC Latency Tolerance Parameters LTV Control

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 8174h	0040047Dh

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RW	**Disable scheduler direct transition from IDLE to NO requirement (DIS_SDT_IDL_NR):** 0: (default) allow scheduler direct transition from IDLE to NO requirement 1: Disable scheduler direct transition from IDLE to NO requirement
30:26	0h RO	**Reserved**
25	0h RW	**XHCI LTR Transition Policy (XLTRTP):** When '0', LTR messaging state machine transitions from High, Medium, or Low LTR states to Active state upon the Alarm Timer timout and stays in Active until the next service boundary. When '1', the LTR messaging state machine transitions through High Med Low Active states assuming enough latency is available for each transition.
24	0h RW	**XHCI LTR Enable (XLTRE):** This bit must be set to enable LTV messaging from XHCI to the PMC.
23:12	400h RW	**Periodic Active LTV (PA_LTV):** 23:22 Latency Scale 00b: Reserved 01b: Latency Value to be multiplied by 1024 10b: Latency Value to be multiplied by 32,768 11b: Latency Value to be multiplied by 1,048,576 21:12 Latency Value (ns) Defaults to 0 micro seconds
11:0	47Dh RW	**USB2 Port L0 LTV (USB2_PL0_LTV):** 11:10 Latency Scale 00b: Reserved 01b: Latency Value to be multiplied by 1024 10b: Latency Value to be multiplied by 32,768 11b: Latency Value to be multiplied by 1,048,576 9:0 Latency Value (ns) Defaults to 128 Micro Seconds

8.3.190 XHC Latency Tolerance Parameters LTV Control 2 (XLTP_LTV2) — Offset 8178h

XHC Latency Tolerance Parameters LTV Control 2

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 8178h	000017FFh

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:13	0h RO	**Reserved**
12:0	17FFh RW	**LTV Limit (LTV_LMT):** This register defines a maximum LTR value that is allowed to be advertised to the PMC. This is meant to be used as a workaround or mitigation if issues are discovered with the LTR values generated by the XHC using the defined algorithms. If the LTR value of the XHC is larger than the value in this register field, the value in this field is sent to the PMC instead. Default value is the highest possible - 101b 12:10: Latency Multiplier Field 000b - Value times 1 ns 001b - Value times 32 ns 010b - Value times 1,024 ns 011b - Value times 32,768 ns 100b - Value times 1,048,576 ns 101b - Value times 33,554,432 ns 110b-111b - Not Permitted 9:0: Latency Value Default = 3FFh

8.3.191 XHC Latency Tolerance Parameters High Idle Time Control (XLTP_HITC) — Offset 817Ch

XHC Latency Tolerance Parameters High Idle Time Control

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 817Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:29	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
28:16	0000h RW	**Minimum High Idle Time (MHIT):** This is the minimum schedule idle time that must be available before a "High" LTR value can be indicated. This value must be larger than HIWL 12:7 - Time value in # of 125 Micro Seconds Bus Intervals (0 - 8ms) 6:0 - Fractional BI Time value in Micro Seconds (0 - 124 Micro Seconds)
15:13	0h RO	**Reserved**
12:0	0000h RW	**High Idle Wake Latency (HIWL):** This is the latency to access memory from the High Idle Latency state. This value must be larger than MIWL and LIWL 12:7 - Time value in # of 125 Micro Seconds Bus Intervals (0 - 8ms) 6:0 - Fractional BI Time value in Micro Seconds (0 - 124 Micro Seconds)

8.3.192 XHC Latency Tolerance Parameters Medium Idle Time Control (XLTP_MITC) — Offset 8180h

XHC Latency Tolerance Parameters Medium Idle Time Control

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 8180h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:29	0h RO	**Reserved**
28:16	0000h RW	**Minimum Medium Idle Time (MMIT):** This is the minimum schedule idle time that must be available before a "Medium" LTR value can be indicated. This value must be larger than MIWL 12:7 - Time value in # of 125 Micro Seconds Bus Intervals (0 - 8ms) 6:0 - Fractional BI Time value in Micro Seconds (0 - 124 Micro Seconds)
15:13	0h RO	**Reserved**
12:0	0000h RW	**Medium Idle Wake Latency (MIWL):** This is the latency to access memory from the Medium Idle Latency state. This value must be larger than LIWL 12:7 - Time value in # of 125 Micro Seconds Bus Intervals (0 - 8ms) 6:0 - Fractional BI Time value in Micro Seconds (0 - 124 Micro Seconds)

8.3.193 XHC Latency Tolerance Parameters Low Idle Time Control (XLTP_LITC) — Offset 8184h

XHC Latency Tolerance Parameters Low Idle Time Control

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 8184h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:29	0h RO	**Reserved**
28:16	0000h RW	**Minimum Low Idle Time (MLIT):** This is the minimum schedule idle time that must be available before a "Low" LTR value can be indicated. This value must be larger than LIWL 12:7 - Time value in # of 125 Micro Seconds Bus Intervals (0 - 8ms) 6:0 - Fractional BI Time value in Micro Seconds (0 - 124 Micro Seconds)
15:13	0h RO	**Reserved**
12:0	0000h RW	**Low Idle Wake Latency (LIWL):** This is the latency to access memory from the Medium Idle Latency state. 12:7 - Time value in # of 125 Micro Seconds Bus Intervals (0 - 8ms) 6:0 - Fractional BI Time value in Micro Seconds (0 - 124 Micro Seconds)

8.3.194 LFPS On Count (LFPSONCOUNT_REG) — Offset 81B8h

LFPS On Count

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 81B8h	000400C8h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:22	0h RO	**Reserved**
21	0h RW	**RTC Clock Generation Override (RTCCLKGENOVERRIDE):** when set it will Disable the RTC tick generation unconditionally.This will be used by software to disable the tick and CRO if WDE/WCE is disabled during D3
20	0h RW	**Disable U3 Wait for Ownership (DISABLE_U3_WAIT_FOROWNERSHIP):** Debug bit when set will allow Gated SS Link to send the LFPS even though AON owns the LFPS detection
19	0h RW	**RXLFPS Detection Filter Time (RXLFPSFILT_8US_EN):** 0: RXLFPS detection filter for U3 Exit is 4 ticks of 128ns 1: RXLFPS Filter will remain at 8us

Bit Range	Default & Access	Field Name (ID): Description
18	1h RW	**XDISRTCPOLLING:** 1: Disable the RTC tick generation which is consumed for the RxDet Polling, LFPS Polling and Aux Clock PCG Wakup to enable this. 0: RTC tick generation based on the defined interval
17:16	0h RW	**U2P3 LFPS Periodic Sampling Control (XU2P3LPSC):** This field controls the OFF time for the LFPS periodic sampling for USB3 ports in U2P3. If LFPSPM for a port is 1, it will override the OFF time and LFPS receiver will remain OFF permanently. For Fast Sim mode, 500us will be equivalent to 5us. 0x0 Polling Disable. (RXDET Polling will become 100ms.) 0x1 500us OFF Time 0x2 1ms OFF Time 0x3 1.5ms OFF Time
15:10	0h RO	**Reserved**
9:0	0C8h RW	**XLFPSONCNTSS:** This time would describe the number of clocks LFPS will remain ON. LFPS detection operation may be carried out on using RTC clock or Oscillator clock. The value of this register should be adjusted accordingly. For RTC recommended value is 2. For Oscillator clock, recommended value is 200.

8.3.195 USB2 Power Management Control (USB2PMCTRL_REG) — Offset 81C4h

USB2 Power Management Control

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 81C4h	00000900h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:13	0h RO	**Reserved**
12	0h RW	**USB2 HOST PHY UTMI Clock Gate Disable Policy (U2HPUCGDP):** This controls the policy for Host PHY UTMI Clock Gating. When Set HOST PHY UTMI Clock Gating is disabled else Host PHY UTMI Clock Gating is enable
11	1h RW	**USB2 PHY SUS Power Gate PORTSC Block Policy (U2PSPGPSCBP):** This controls the policy for blocking PORTSC Updates while the USB2 PHY SUS Well is power gated. When set, the controller will block any updates to the PORTSC caused by port status change if the USB2 PHY SUS is power gated. 0 Do not

Bit Range	Default & Access	Field Name (ID): Description
10:8	1h RW	**USB2 PHY SUS Well Power Gate Entry Hysteresis Count (U2PSPGEHC):** This controls the amount of hysteresis time the controller will enforce after detecting the USB2 PHY SUS Power Gate entry condition. 0h 0 clocks 1h 32 clocks 2h 64 clocks 3h 128 clocks 4h 256 clocks 5h 512 clocks 6h 1024 clocks 7h 2048 clocks
7:4	0h RW	**USB2 PHY SUS Power Gate PORTSC Block Policy (U2CLPGLAT):** This field represents the worst case latency for the USB2 Common Lane to enter and exit its power gate state. This fields is required to be compared to a ports HIRD/HIRD value for the ports that have allowed L1 to L2 mapping to determine if the Common Lane can be allowed to power off. If the power gate entry/exit latency is greater than the HIRD/HIRDD then the common lane should not be allowed to power gate as this will result in a L1 exit violation. 0h 100 us 1h 200 us 2h 300 us Eh 1500us Fh 1600 us
3:2	0h RW	**USB2 PHY SUS Well Power Gate Policy (U2PSUSPGP):** This field controls when to enable the USB2 PHY SUS Well Power Gating when the proper conditions are met. 00 USB2 PHY SUS Power Gating is Disabled. 01 USB2 PHY SUS Power Gating is Enabled in Only D0 and D0i2 (Excludes D0i3 and D3) 10 USB2 PHY SUS Power Gating is Eanabled in only in D0, D0i2 and D0i3 (Excludes D3) 11 USB2 PHY SUS Power Gating is Eanabled in D0/D0i2/D0i3/D3
1:0	0h RO	**Reserved**

8.3.196 USB Legacy Support Capability (USBLEGSUP) — Offset 846Ch

This register is modified and maintained by BIOS

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 846Ch	00002201h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:25	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
24	0h RW	**HC OS Owned Semaphore (HCOSOS):** HC OS Owned Semaphore
23:17	0h RO	**Reserved**
16	0h RW	**HC BIOS Owned Semaphore (HCBIOSOS):** HC BIOS Owned Semaphore
15:8	22h RW/L	**Next Capability Pointer (NEXTCP):** Next Capability Pointer **Locked by:** XHCC1.ACCTRL
7:0	01h RW/L	**Capability ID (CID):** Capability ID **Locked by:** XHCC1.ACCTRL

8.3.197 USB Legacy Support Control Status (USBLEGCTLSTS) — Offset 8470h

USB Legacy Support Control Status

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 8470h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RW/1C	**SMI on BAR (SMIBAR):** SMI on BAR
30	0h RW/1C	**SMI on PCI Command (SMIPCIC):** SMI on PCI Command
29	0h RW/1C	**SMI on OS Ownership Change (SMIOSOC):** SMI on OS Ownership Change
28:21	0h RO	**Reserved**
20	0h RO	**SMI on Host System Error (SMIHSE):** SMI on Host System Error
19:17	0h RO	**Reserved**
16	0h RO	**SMI on Event Interrupt (SMIEI):** SMI on Event Interrupt
15	0h RW	**SMI on BAR Enable (SMIBARE):** SMI on BAR Enable
14	0h RW	**SMI on PCI Command Enable (SMIPCICE):** SMI on PCI Command Enable

Bit Range	Default & Access	Field Name (ID): Description
13	0h RW	**SMI on OS Ownership Enable (SMIOSOE):** SMI on OS Ownership Enable
12:5	0h RO	**Reserved**
4	0h RW	**SMI on Host System Error Enable (SMIHSEE):** SMI on Host System Error Enable
3:1	0h RO	**Reserved**
0	0h RW	**USB SMI Enable (USBSMIE):** USB SMI Enable

8.3.198 Port Disable Override Capability Register (PDO_CAPABILITY) — Offset 84F4h

Port Disable Override Capability Register

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 84F4h	000003C6h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:16	0h RO	**Reserved**
15:8	03h RO	**Next Capability Pointer (NCP):** Next Capability Pointer
7:0	C6h RO	**Capability ID (CID):** Capability ID

8.3.199 Command Reg (CMD_MMIO) — Offset 8604h

Mirror of physical register as CMD

Type	Size	Offset	Default
MMIO	16 bit	MBAR + 8604h	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:11	0h RO	**Reserved**
10	0h RW	**Interrupt Disable (INTR_DIS):** When cleared to 0, the function is capable of generating interrupts. When 1, the function can not generate its interrupt to the interrupt controller. Note that the corresponding Interrupt Status bit is not affected by the interrupt enable.
9	0h RO	**Fast Back to Back Enable (FBE):** Fast Back to Back Enable
8	0h RW	**SERR# Enable (SERR):** When set to 1, the XHC is capable of generating (internally) SERR#.
7	0h RO	**Wait Cycle Control (WCC):** Wait Cycle Control
6	0h RW	**Parity Error Response (PER):** When set to 1, the XHCI Host Controller will check for correct parity (on its internal interface) and halt operation when bad parity is detected during the data phase as recommended by the XHCI specification. Note that this applies to both requests and completions from the system interface. This bit must be set in order for the parity errors to generate SERR#.
5	0h RO	**VGA Palette Snoop (VPS):** VGA Palette Snoop
4	0h RO	**Memory Write Invalidate (MWI):** Memory Write Invalidate
3	0h RO	**Special Cycle Enable (SCE):** Special Cycle Enable
2	0h RW	**Bus Master Enable (BME):** When set, it allows XHC to act as a bus master. When cleared, it disable XHC from initiating transactions on the system bus.
1	0h RW	**Memory Space Enable (MSE):** This bit controls access to the XHC Memory Space registers. If this bit is set, accesses to the XHC registers are enabled. The Base Address register for the XHC should be programmed before this bit is set.
0	0h RO	**I/O Space Enable (IOSE):** Reserved

8.3.200 Device Status (STS_MMIO) — Offset 8606h

Device Status

Type	Size	Offset	Default
MMIO	16 bit	MBAR + 8606h	0290h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15	0h RW/1C	**Detected Parity Error (DPE):** This bit is set by the Intel PCH whenever a parity error is seen on the internal interface to the XHC host controller, regardless of the setting of bit 6 or bit 8 in the Command register or any other conditions. Software clears this bit by writing a 1 to this bit location.
14	0h RW/1C	**Signaled System Error (SSE):** This bit is set by the Intel PCH whenever it signals SERR# (internally). The SERR_EN bit (bit 8 in the Command Register) must be 1 for this bit to be set. Software clears this bit by writing a 1 to this bit location.
13	0h RW/1C	**Received Master-Abort Status (RMA):** This bit is set when XHC, as a master, receives a master-abort status on a memory access. This is treated as a Host Error and halts the DMA engines. Software clears this bit by writing a 1 to this bit location.
12	0h RW/1C	**Received Target Abort Status (RTA):** This bit is set when XHC, as a master, receives a target abort status on a memory access. This is treated as a Host Error and halts the DMA engines. Software clears this bit by writing a 1 to this bit location.
11	0h RW/1C	**Signaled Target-Abort Status (STA):** This bit is used to indicate when the XHC function responds to a cycle with a target abort.
10:9	1h RO	**DEVSEL# Timing Status (DEVT):** This 2-bit field defines the timing for DEVSEL# assertion. Read-Only.
8	0h RW/1C	**Master Data Parity Error Detected (MDPED):** This bit is set by the Intel PCH whenever a data parity error is detected on a XHC read completion packet on the internal interface to the XHC host controller and bit 6 of the Command register is set to 1. Software clears this bit by writing a 1 to this bit location.
7	1h RO	**Fast Back-to-Back Capable (FBBC):** Reserved
6	0h RO	**User Definable Features (UDF):** Reserved
5	0h RO	**66 MHz Capable (MC):** Reserved
4	1h RO	**Capabilities List (CL):** Hardwired to 1 indicating that offset 34h contains a valid capabilities pointer.
3	0h RO/V	**Interrupt Status (INTR_STS):** This read-only bit reflects the state of this function's interrupt at the input of the enable/disable logic. This bit is a 1 when the interrupt is asserted. This bit will be 0 when the interrupt is deasserted. The value reported in this bit is independent of the value in the Interrupt Enable bit.
2:0	0h RO	**Reserved**

8.3.201 Revision ID (RID_MMIO) — Offset 8608h

Revision ID

Type	Size	Offset	Default
MMIO	8 bit	MBAR + 8608h	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:0	00h RO/V	**Revision ID (RID):** See Chap 6 for value.

8.3.202 Programming Interface (PI_MMIO) — Offset 8609h

Programming Interface

Type	Size	Offset	Default
MMIO	8 bit	MBAR + 8609h	30h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:0	30h RO	**Programming Interface (PI):** A value of 30h indicates that this USB Host Controller conforms to the XHCI specification.

8.3.203 Sub Class Code (SCC_MMIO) — Offset 860Ah

Sub Class Code

Type	Size	Offset	Default
MMIO	8 bit	MBAR + 860Ah	03h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:0	03h RO	**Sub Class Code (SCC):** A value of 03h indicates that this is a Universal Serial Bus Host Controller.

8.3.204 Base Class Code (BCC_MMIO) — Offset 860Bh

Base Class Code

Type	Size	Offset	Default
MMIO	8 bit	MBAR + 860Bh	0Ch

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:0	0Ch RO	**Base Class Code (BCC):** A value of 0Ch indicates that this is a Serial Bus controller.

8.3.205 Master Latency Timer (MLT_MMIO) — Offset 860Dh

Master Latency Timer

Type	Size	Offset	Default
MMIO	8 bit	MBAR + 860Dh	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:0	00h RO	**Master Latency Timer (MLT):** Because the XHC controller is internally implemented with arbitration on an internal interface, it does not need a master latency timer. The bits will be fixed at 0.

8.3.206 Header Type (HT_MMIO) — Offset 860Eh

Header Type

Type	Size	Offset	Default
MMIO	8 bit	MBAR + 860Eh	80h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7	1h RO	**Multi-Function Bit (MFB):** Read only indicating single function device.
6:0	00h RO	**Configuration layout (CL):** Hardwired to 0 to indicate a standard PCI configuration layout.

8.3.207 Memory Base Address (MBAR_MMIO) — Offset 8610h

Mirror of physical register as MBAR. Value in this register will be different after the enumeration process.

Type	Size	Offset	Default
MMIO	64 bit	MBAR + 8610h	0000000000000004h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
63:16	0000000000000h RW	**Base Address (BA):** Bits (63:16) correspond to memory address signals (63:16), respectively. This gives 64 KB of relocatable memory space aligned to 64 KB boundaries.
15:4	0h RO	**Reserved**
3	0h RO	**PREFETCHABLE:** This bit is hardwired to 0 indicating that this range should not be prefetched.
2:1	2h RO	**Memory BAR Type (MBAR_TYPE):** If this field is hardwired to 00 it indicates that this range can be mapped anywhere within 32-bit address space. If this field is hardwired to 10 it indicates that this range can be mapped anywhere within 64-bit address space.
0	0h RO	**Resource Type Indicator (RTE):** This bit is hardwired to 0 indicating that the base address field in this register maps to memory space

8.3.208 USB Subsystem Vendor ID (SSVID_MMIO) — Offset 862Ch

Mirror of physical register as SSVID. This register is modified and maintained by BIOS.

Type	Size	Offset	Default
MMIO	16 bit	MBAR + 862Ch	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:0	0000h RW/L	**USB Subsystem Vendor ID (SSVID):** This register, in combination with the USB Subsystem ID register, enables the operating system to distinguish each subsystem from the others. **Locked by:** XHCC1.ACCTRL

8.3.209 USB Subsystem ID (SSID_MMIO) — Offset 862Eh

Mirror of physical register as SSID. This register is modified and maintained by BIOS

Type	Size	Offset	Default
MMIO	16 bit	MBAR + 862Eh	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:0	0000h RW/L	**USB Subsystem ID (SSID):** BIOS sets the value in this register to identify the Subsystem ID. This register, in combination with the Subsystem Vendor ID register, enables the operating system to distinguish each subsystem from other(s). **Locked by:** XHCC1.ACCTRL

8.3.210 Capabilities Pointer (CAP_PTR_MMIO) — Offset 8634h

Capabilities Pointer

Type	Size	Offset	Default
MMIO	8 bit	MBAR + 8634h	70h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:0	70h RO	**Capabilities Pointer (CAP_PTR):** This register points to the starting offset of the capabilities ranges.

8.3.211 Interrupt Line (ILINE_MMIO) — Offset 863Ch

Mirror of physical register as ILINE.

Type	Size	Offset	Default
MMIO	8 bit	MBAR + 863Ch	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
7:0	00h RW	**Interrupt Line (ILINE):** This data is not used by the Intel PCH. It is used as a scratchpad register to communicate to software the interrupt line that the interrupt pin is connected to.

8.3.212 Interrupt Pin (IPIN_MMIO) — Offset 863Dh

Mirror of physical register as IPIN.

Type	Size	Offset	Default
MMIO	8 bit	MBAR + 863Dh	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
7:0	00h RW/L	**Interrupt pin (IPIN):** Bits 7:0 reflect the Interrupt Pin assigned to the host controller by the platform (and are hardwired). **Locked by:** XHCC1.ACCTRL

8.3.213 Serial Bus Release Number (SBRN_MMIO) — Offset 8660h

Serial Bus Release Number

Type	Size	Offset	Default
MMIO	8 bit	MBAR + 8660h	31h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:0	31h RO	**Serial Bus Release Number (SBRN):** A value of 30h indicates that this controller follows USB release 3.0.

8.3.214 Frame Length Adjustment (FLADJ_MMIO) — Offset 8661h

This feature is used to adjust any offset from the clock source that generates the clock that drives the SOF counter. When a new value is written into these six bits, the length of the frame is adjusted. Its initial programmed value is system dependent based on the accuracy of hardware USB clock and is initialized by system BIOS. This register should only be modified when the HChalted bit in the USBSTS register is a one. Changing value of this register while the host controller is operating yields undefined results.

Type	Size	Offset	Default
MMIO	8 bit	MBAR + 8661h	60h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7	0h RO	**Reserved**
6	1h RO	**No Frame Length Timing Capability (NO_FRAME_LENGTH_TIMING_CAP):** This flag is set to 1 to indicate that the host controller does not support a programmable Frame Length Timing Value field.
5:0	20h RO	**Frame Length Timing Value (FLTV):** SOF micro-frame length) is equal to 59488 + value in this field. The default value is decimal 32 (20h), which gives a SOF cycle time of 60000. Frame Length (number of High Speed bit times) FLADJ Value (decimal) (decimal) 59488 0 (00h) 59504 1 (01h) 59520 2 (02h) ... 59984 31 (1Fh) 60000 32 (20h) ... 60480 62 (3Eh) 60496 63 (3Fh) Each decimal value change to this register corresponds to 16 high-speed bit times. The SOF cycle time (number of SOF counter clock periods to generate a SOF micro-frame length) is equal to 59488 + value in this field. The default value is decimal 32 (20h), which gives a SOF cycle time of 60000. Frame Length (# High Speed bit times) FLADJ Value

8.3.215 Best Effort Service Latency (BESL_MMIO) — Offset 8662h

Mirror of physical register as BESL. Best Effort Service Latency.

Type	Size	Offset	Default
MMIO	8 bit	MBAR + 8662h	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
7:4	0h RW/L	**Default Best Effort Service Latency Deep (DBESLD):** Default Best Effort Service Latency (DBESLD) If the value of this field is non-zero, it defines the recommended value for programming the PORTPMSC register BESLD field. This is programmed by BIOS based on platform parameters. **Locked by:** XHCC1.ACCTRL
3:0	0h RW/L	**Default Best Effort Service Latency (DBESL):** If the value of this field is non-zero, it defines the recommended value for programming the PORTPMSC register BESL field. This is programmed by BIOS based on platform parameters. **Locked by:** XHCC1.ACCTRL

8.3.216 PCI Power Management Capability ID (PM_CID_MMIO) — Offset 8670h

PCI Power Management Capability ID

Type	Size	Offset	Default
MMIO	8 bit	MBAR + 8670h	01h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:0	01h RO	**PCI Power Management Capability ID (PM_CID):** A value of 01h indicates that this is a PCI Power Management capabilities field.

8.3.217 Next Item Pointer 1 (PM_NEXT_MMIO) — Offset 8671h

Mirror of physical register as PM_NEXT. This register is modified and maintained by BIOS

Type	Size	Offset	Default
MMIO	8 bit	MBAR + 8671h	80h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
7:0	80h RW/L	**Next Item Pointer 1 (PM_NEXT):** This register defaults to 80h, which indicates that the next capability registers begin at configuration offset 80h. This register is writable when the Access Control bit is set to '0'. This allows BIOS to effectively hide the next capability registers, if necessary. This register should only be written during system initialization before the plug-and-play software has enabled any master-initiated traffic. Values of: 80h implies next capability is MSI 00h implies that MSI capability is hidden. Note: This value is never expected to be programmed. **Locked by:** XHCC1.ACCTRL

8.3.218 Power Management Capabilities (PM_CAP_MMIO) — Offset 8672h

Mirror of physical register as PM_CAP. Normally, this register is read-only to report capabilities to the power management software. In order to report different power management capabilities depending on the system in which the Intel PCH is used, the write access to this register is controlled by the Access Control bit (ACCTRL). The value written to this register does not affect the hardware other than changing the value returned during a read.

This register is modified and maintained by BIOS

Type	Size	Offset	Default
MMIO	16 bit	MBAR + 8672h	C1C2h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:11	18h RW/L	**PME Support (PME_SUPPORT):** This 5-bit field indicates the power states in which the function may assert PME#. The Intel PCH XHC does not support the D1 or D2 states. For all other states, the Intel PCH XHC is capable of generating PME#. Software should never need to modify this field. **Locked by:** XHCC1.ACCTRL

Bit Range	Default & Access	Field Name (ID): Description
10	0h RW/L	**D2 Support (D2_SUPPORT):** The D2 state is not supported. **Locked by:** XHCC1.ACCTRL
9	0h RW/L	**D1 Support (D1_SUPPORT):** The D1 state is not supported. **Locked by:** XHCC1.ACCTRL
8:6	7h RW/L	**Auxiliary Current (AUX_CURRENT):** The Intel PCH XHC reports 375mA maximum Suspend well current required when in the D3cold state. This value can be written by BIOS when a more accurate value is known. **Locked by:** XHCC1.ACCTRL
5	0h RW/L	**DSI:** The Intel PCH reports 0, indicating that no device-specific initialization is required. **Locked by:** XHCC1.ACCTRL
4	0h RO	**Reserved**
3	0h RW/L	**PME Clock (PMECLOCK):** The Intel PCH reports 0, indicating that no PCI clock is required to generate PME#. **Locked by:** XHCC1.ACCTRL
2:0	2h RW/L	**VERSION:** The Intel PCH reports 010, indicating that it complies with Revision 1.1 of the PCI Power Management Specification. **Locked by:** XHCC1.ACCTRL

8.3.219 Power Management Control/Status (PM_CS_MMIO) — Offset 8674h

Mirror of physical register as PM_CS

Type	Size	Offset	Default
MMIO	16 bit	MBAR + 8674h	0008h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15	0h RW/1C	**PME Status (PME_STATUS):** This bit is set when the Intel PCH XHC would normally assert the PME# signal independent of the state of the PME_En bit. Writing a 1 to this bit will clear it and cause the internal PME to deassert (if enabled). Writing a 0 has no effect. This bit must be explicitly cleared by the operating system each time the operating system is loaded.
14:13	0h RO	**Data Scale (DATA_SCALE):** The Intel PCH hardwires these bits to 00 because it does not support the associated Data register.

Bit Range	Default & Access	Field Name (ID): Description
12:9	0h RO	**Data Select (DATA_SELECT):** The Intel PCH hardwires these bits to 0000 because it does not support the associated Data register.
8	0h RW	**PME Enable (PME_EN):** A 1 enables the Intel PCH XHC to generate an internal PME signal when PME_Status is 1. This bit must be explicitly cleared by the operating system each time it is initially loaded.
7:4	0h RO	**Reserved**
3	1h RO	**No Soft Reset (NSR):** No_Soft_Reset - When set ("1"), this bit indicates that devices transitioning from D3hot to D0 because of PowerState commands do not perform an internal reset. Configuration Context is preserved. Upon transition from the D3hot to the D0 Initialized state, no additional operating system intervention is required to preserve Configuration Context beyond writing the PowerState bits. Transition from D3hot to D0 by a system or bus segment reset will return to the device state D0 Uninitialized with only PME context preserved if PME is supported and enabled.
2	0h RO	**Reserved**
1:0	0h RW	**POWERSTATE:** This 2-bit field is used both to determine the current power state of XHC function and to set a new power state. The definition of the field values are: 00b - D0 state 11b - D3hot state If software attempts to write a value of 10b or 01b in to this field, the write operation must complete normally, however, the data is discarded and no state change occurs. When in the D3hot state, the Intel PCH must not accept accesses to the XHC memory range, but the configuration space must still be accessible.

8.3.220 Message Signaled Interrupt CID (MSI_CID_MMIO) — Offset 8680h

Message Signaled Interrupt CID

Type	Size	Offset	Default
MMIO	8 bit	MBAR + 8680h	05h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:0	05h RO	**Capability ID (CID):** Indicates that this is an MSI capability

8.3.221 Next Item Pointer (MSI_NEXT_MMIO) — Offset 8681h

Mirror of physical register as MSI_NEXT

Type	Size	Offset	Default
MMIO	8 bit	MBAR + 8681h	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
7:0	00h RW/L	**Next Pointer (NEXT_POINTER):** Indicates that this is the last item on the capability list **Locked by:** XHCC1.ACCTRL

8.3.222 Message Signaled Interrupt Message Control (MSI_MCTL_MMIO) — Offset 8682h

Mirror of physical register as MSI_MCTL

Type	Size	Offset	Default
MMIO	16 bit	MBAR + 8682h	0086h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:9	0h RO	**Reserved**
8	0h RO	**Per-Vector Masking Capable (PVM):** Specifies whether controller supports MSI per vector masking. Not supported
7	1h RO	**64 Bit Address Capable (C64):** Specifies whether capable of generating 64-bit messages. This device is 64-bit capable.
6:4	0h RW	**Multiple Message Enable (MME):** Indicates the number of messages the controller should assert. This device supports multiple message MSI.
3:1	3h RO	**Multiple Message Capable (MMC):** Indicates the number of messages the controller wishes to assert. This field must be set by HW to reflect the number of Interrupters supported. Encoding number of Vectors requested (number of Interrupters) 000 1 001 2 010 4 011 8 100 16 101 32 110-111 Reserved

Bit Range	Default & Access	Field Name (ID): Description
0	0h RW	**MSI Enable (MSIE):** If set to 1, MSI is enabled and the traditional interrupt pins are not used to generate interrupts. If cleared to 0, MSI operation is disabled and the traditional interrupt pins are used.

8.3.223 Message Signaled Interrupt Message Address (MSI_MAD_MMIO) — Offset 8684h

Mirror of physical register as MSI_MAD

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 8684h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:2	00000000h RW	**ADDR:** Lower DW of system specified message address, always DWORD aligned
1:0	0h RO	**Reserved**

8.3.224 Message Signaled Interrupt Upper Address (MSI_MUAD_MMIO) — Offset 8688h

Mirror of physical register as MSI_MUAD

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 8688h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RW	**Upper Addr (UPPERADDR):** Upper DW of system specified message address.

8.3.225 Message Signaled Interrupt Message Data (MSI_MD_MMIO) — Offset 868Ch

Mirror of physical register as MSI_MD

Type	Size	Offset	Default
MMIO	16 bit	MBAR + 868Ch	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:0	0000h RW	**DATA:** This 16-bit field is programmed by system software if MSI is enabled. Its content is driven onto the lower word (PCI AD(15:0)) during the data phase of the MSI memory write transaction. The Multiple Message Enable field (bits 6-4 of the Message Control register) defines the number of low order message data bits the function is permitted to modify to generate its system software allocated vectors. For example, a Multiple Message Enable encoding of 010 indicates the function has been allocated four vectors and is permitted to modify message data bits 1 and 0 (a function modifies the lower message data bits to generate the allocated number of vectors). If the Multiple Message Enable field is 000, the function is not permitted to modify the message data.

8.3.226 High Speed Configuration 2 (HSCFG2_MMIO) — Offset 86A4h

Mirror of physical register as HSCFG2

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 86A4h	00002000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:19	0h RO	**Reserved**
18	0h RW	**Port1 Host Mode Override (PORT1_HOST_MODE_OVERRIDE):** When set, this bit causes the Host_Device mux on port 1 to be forced into the Host mode.

Bit Range	Default & Access	Field Name (ID): Description
17:16	0h RW	**EUSB2SEL:** The two bits are associate with USB2 ports 1 - bit 16 and 2 - bit 2 0: Port is mapped to USB2 1: Port is mapped to eUSB2
15	0h RW	**HS ASYNC Active IN Mask (HSAAIM):** Determines if the Async Active will mask/ignore IN EP s. 0 HS ASYNC Active will include IN EP s. 1 HS ASYNC Active will mask/ignore IN EP s.
14	0h RW	**HS OUT ASYNC Active Polling EP Mask (HSOAAPEPM):** Determines if the Async Active for OUT HS/FS/LS masks/ignores EP s that are polling/PINGing (HS) due to NAK. 0 HS OUT ASYNC Active will include EP s that are polling. 1 HS OUT ASYNC Active will mask/ignore EP s that are polling.
13	1h RW	**HS IN ASYNC Active Polling EP Mask (HSIAAPEPM):** Determines if the Async Active for IN HS/FS/LS masks/ignores EP s that are polling due to NAK. 0 HS IN ASYNC Active will include EP s that are polling. 1 HS IN ASYNC Active will mask/ignore EP s that are polling.
12:11	0h RW	**HS INTR IN Periodic Active Policy Control (HSIIPAPC):** Controls how the HS INTR IN periodic active is used to generate the global periodic active. This will determine how the smallest service interval among active EP s and number of active EP s are used. 0 HS INTR IN periodic active will be used to generate periodic active if Service Interval Threshold OR Numb of EP Threshold values meet the requirement. 1 HS INTR IN periodic active will be used to generate periodic active if Service Interval Threshold AND Numb of EP Threshold values meet the requirement. 2 Always allow HS INTR EP s to be used in the generation of the global Periodic Active indication. 3 Never allow HS INTR EP s to be used in the generation of the global Periodic Active indication
10:4	00h RW	**HS INTR IN Periodic Active Num of EP Threshold (HSIIPANEPT):** Defines the threshold used to determine if Periodic active may include HS/FS/LS INTR IN EP active indication. If there are more than NumEPThreshold active HS/FS/LS INTR EP s then they may be included as part of the periodic active generation.
3:0	0h RW	**HS INTR IN Periodic Active Service Interval Threshold (HSIIPASIT):** Defines the Service Interval threshold used to determine if Periodic active will include HS/FS/LS INTR IN EP active indication. If there are any active HS/FS/LS INTR EP s with a service interval less than or equal to this threshold then they may be included as part of the periodic active generation.

8.3.227 XHCI USB2 Overcurrent Pin Mapping (U2OCM1_MMIO) — Offset 86B0h

The RW/L property of this register is controlled by OCCFDONE bit.

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 86B0h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:1	0h RO	**Reserved**
0	0h RW/L	**OC Mapping (OCM):** USB2 Port assignment When Set to 1, Bit 0 maps the OC pin N to USB2 std. port 1 Bit 1 maps the OC pin N to USB2 std port 2 ... Bit (NumUSB2std-1) maps the OC pin N to USB2 Std port NumUSB2std Note: The USB-R port which is the most significant USB2 port does not have an OC pin. Thus the OC assignment for the USB-R port is ignored. **Locked by:** XHCC2.OCCFGDONE

8.3.228 XHCI USB2 Overcurrent Pin Mapping (U2OCM2_MMIO) — Offset 86B4h

The RW/L property of this register is controlled by OCCFDONE bit.

Note: Bit definitions are the same as U2OCM1_MMIO, offset 86B0h.

8.3.229 XHCI USB2 Overcurrent Pin Mapping (U2OCM3_MMIO) — Offset 86B8h

The RW/L property of this register is controlled by OCCFDONE bit.

Note: Bit definitions are the same as U2OCM1_MMIO, offset 86B0h.

8.3.230 XHCI USB2 Overcurrent Pin Mapping (U2OCM4_MMIO) — Offset 86BCh

The RW/L property of this register is controlled by OCCFDONE bit.

Note: Bit definitions are the same as U2OCM1_MMIO, offset 86B0h.

8.3.231 XHCI USB3 Overcurrent Pin Mapping (U3OCM1_MMIO) — Offset 86D0h

The RW/L property of this register is controlled by OCCFDONE bit.

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 86D0h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:4	0h RO	**Reserved**
3:0	0h RW/L	**OC Mapping (OCM):** USB3 Port assignment When Set to 1, Bit 0 maps the OC pin N to USB3 std. port 1 Bit 1 maps the OC pin N to USB3 std port 2 ... Bit (NumUSB3std-1) maps the OC pin N to USB3 Std port NumUSB3std **Locked by:** XHCC2.OCCFGDONE

8.3.232 XHCI USB3 Overcurrent Pin Mapping (U3OCM2_MMIO) — Offset 86D4h

The RW/L property of this register is controlled by OCCFDONE bit.

Note: Bit definitions are the same as U3OCM1_MMIO, offset 86D0h.

8.3.233 XHCI USB3 Overcurrent Pin Mapping (U3OCM3_MMIO) — Offset 86D8h

The RW/L property of this register is controlled by OCCFDONE bit.

Note: Bit definitions are the same as U3OCM1_MMIO, offset 86D0h.

8.3.234 XHCI USB3 Overcurrent Pin Mapping (U3OCM4_MMIO) — Offset 86DCh

The RW/L property of this register is controlled by OCCFDONE bit.

Note: Bit definitions are the same as U3OCM1_MMIO, offset 86D0h.

8.3.235 Debug Capability ID Register (DCID) — Offset 8700h

This register is modified and maintained by BIOS

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 8700h	0005100Ah

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:21	0h RO	**Reserved**
20:16	05h RW/L	**Debug Capability Event Ring Segment Table Max (DCERSTM):** Note: This register is sticky. **Locked by:** XHCC1.ACCTRL
15:8	10h RW/L	**Next Capability Pointer (NCP):** Note: This register is sticky. **Locked by:** XHCC1.ACCTRL
7:0	0Ah RW/L	**Capability ID (CID):** Note: This register is sticky. **Locked by:** XHCC1.ACCTRL

8.3.236 Debug Capability Doorbell Register (DCDB) — Offset 8704h

Debug Capability Doorbell Register

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 8704h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:16	0h RO	**Reserved**
15:8	00h RW	**Doorbell Target (DBTGT):** This field defines the target of the doorbell reference. The table below defines the Debug Capability notification that is generated by ringing the doorbell. Value Definition 0 Data EP 1 OUT Enqueue Pointer Update 1 Data EP 1 IN Enqueue Pointer Update 2:255 Reserved This field returns '0' when read and the value should be treated as undefined by software.

Bit Range	Default & Access	Field Name (ID): Description
7:0	0h RO	**Reserved**

8.3.237 Debug Capability Event Ring Segment Table Size Register (DCERSTSZ) — Offset 8708h

Debug Capability Event Ring Segment Table Size Register

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 8708h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:16	0h RO	**Reserved**
15:0	0000h RW	**Event Ring Segment Table Size (ERSTS):** This field identifies the number of valid Event Ring Segment Table entries in the Event Ring Segment Table pointed to by the Debug Capability Event Ring Segment Table Base Address register. The maximum value supported by an xHC implementation for this register is defined by the DCERST Max field in the DCID register Software shall initialize this register before setting the Debug Capability Enable field in the DCCTRL register to '1'.

8.3.238 Debug Capability Event Ring Segment Table Base Address Register (DCERSTBA) — Offset 8710h

Debug Capability Event Ring Segment Table Base Address Register

Type	Size	Offset	Default
MMIO	64 bit	MBAR + 8710h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
63:4	00000000 0000000h RW	**Event Ring Segment Table Base Address Register (ERSTBAR):** This field defines the high order bits of the start address of the Debug Capability Event Ring Segment Table. Software shall initialize this register before setting the Debug Capability Enable field in the DCCTRL register to '1'.
3:0	0h RO	**Reserved**

8.3.239 Debug Capability Event Ring Dequeue Pointer Register (DCERDP) — Offset 8718h

Debug Capability Event Ring Dequeue Pointer Register

Type	Size	Offset	Default
MMIO	64 bit	MBAR + 8718h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
63:4	00000000 0000000h RW	**Dequeue Pointer (DQP):** This field defines the high order bits of the 64-bit address of the current Debug Capability Event Ring Dequeue Pointer. Software shall initialize this register before setting the Debug Capability Enable field in the DCCTRL register to '1'.
3	0h RO	**Reserved**
2:0	0h RW	**Dequeue ERST Segment Index (DESI):** This field may be used by the xHC to accelerate checking the Event Ring full condition. This field is written with the low order 3 bits of the offset of the ERST entry which defines the Event Ring segment that the Event Ring Dequeue Pointer resides in.

8.3.240 Debug Capability Control Register (DCCTRL) — Offset 8720h

Debug Capability Event Ring Dequeue Pointer Register

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 8720h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RW	**Debug Capability Enable (DCE):** Debug Capability Enable
30:24	00h RO	**Device Address (DADDR):** Device Address
23:16	00h RO	**Debug Max Burst Size (DMBS):** LPT-LP USB Debug Device does not support bursting.
15:5	0h RO	**Reserved**
4	0h RW/1C	**DbC Run Change (DRC):** DbC Run Change
3	0h RW/1S	**Halt IN TR (HIT):** Halt IN TR
2	0h RW/1S	**Halt OUT TR (HOT):** Halt OUT TR
1	0h RW	**Link Status Event Enable (LSE):** Link Status Event Enable
0	0h RO	**DbC Run (DCR):** DbC Run

8.3.241 Debug Capability Status Register (DCST) — Offset 8724h

Debug Capability Status Register

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 8724h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:24	00h RO	**Debug Port Number (DPNUM):** This field provides the ID of the Root Hub port that the Debug Capability has been automatically attached to. The value is '0' when the Debug Capability is not attached to a Root Hub port.
23:1	0h RO	**Reserved**
0	0h RO	**Event Ring Not Empty (ERNE):** When '1', this field indicates that the Debug Capability Event Ring has a Transfer Event on it. It is automatically cleared to '0' by the xHC when the Debug Capability Event Ring is empty, i.e. the Debug Capability Enqueue Pointer is equal to the Debug Capability Event Ring Dequeue Pointer register.

8.3.242 Debug Capability Port Status And Control Register (DCPORTSC) — Offset 8728h

Debug Capability Port Status And Control Register

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 8728h	00000080h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:24	0h RO	**Reserved**
23	0h RW/1C	**Port Config Error Change (CEC):** This flag indicates that the port failed to configure its link partner. 0 = No change. 1 = Port Config Error detected. Software shall clear this bit by writing a '1' to it.

Bit Range	Default & Access	Field Name (ID): Description
22	0h RW/1C	**Port Link Status Change (PLC):** This flag is set to '1' due to the following PLS transitions: U0 -) U3 Suspend signaling detected from Debug Host U3 -) U0 Resume complete Polling -) Disabled Training Error Ux or Recovery -) Inactive Error Software shall clear this bit by writing a '1' to it. This field is '0' if DCE is '0'
21	0h RW/1C	**Port Reset Change (PRC):** This bit is set when reset processing on this port is complete (i.e. a '1' to '0' transition of PR). '0' = No change. '1' = Reset complete.Software shall clear this bit by writing a '1' to it. This field is '0' if DCE is '0'.
20:18	0h RO	**Reserved**
17	0h RW/1C	**Connect Status Change (CSC):** '1' = Change in Current Connect Status. '0' = No change. Indicates a change has occurred in the port's Current Connect Status. The xHC sets this bit to '1' for all changes to the Debug Device connect status, even if system software has not cleared an existing DbC Connect Status Change. For example, the insertion status changes twice before system software has cleared the changed condition, hardware will be \"setting\" an already-set bit (i.e., the bit will remain '1'). Software shall clear this bit by writing a '1' to it. This field is '0' if DCE is '0'.
16:14	0h RO	**Reserved**
13:10	0h RO	**Port Speed (PSPD):** This field identifies the speed of the port. This field is only relevant when a Debug Host is attached (CCS = '1') in all other cases this field shall indicate Undefined Speed. 0 Undefined Speed 1-15 Protocol Speed ID (PSI) Note: The Debug Capability onlydoes not supports LS, FS, or HS operation.
9	0h RO	**Reserved**
8:5	4h RO	**Port Link State (PLS):** This field reflects its current link state. This field is only relevant when a Debug Host is attached (Debug Port Number) '0'). Value Meaning 0 Link is in the U0 State 1 Link is in the U1 State 2 Link is in the U2 State 3 Link is in the U3 State (Device Suspended) 4 Link is in the Disabled State 5 Link is in the RxDetect State 6 Link is in the Inactive State 7 Link is in the Polling State 8 Link is in the Recovery State 9 Link is in the Hot Reset State 15:10 Reserved Note: Transitions between different states are not reflected until the transition is complete.
4	0h RO	**Port Reset (PR):** '1' = Port is in Reset. '0' = Port is not in Reset. This bit is set to '1' when the bus reset sequence as defined in the USB Specification is detected on the Root Hub port assigned to the Debug capability. It is cleared when the bus reset sequence is completed by the Debug Host, and the DbC shall transition to the USB Default state. A '0' to '1' transition of this bit shall clear DCPORTSC PED ('0'). This field is '0' if DCE or CCS are '0'.

Bit Range	Default & Access	Field Name (ID): Description
3:2	0h RO	**Reserved**
1	0h RW	**Port Enabled/Disabled (PED):** Default = '0'. '1' = Enabled. '0' = Disabled. This flag shall be set to '1' by a '0' to '1' transition of CCS or a '1' to '0' transition of the PR. When PED transitions from '1' to '0' due to the assertion of PR, the port's link shall transition to the Rx.Detect state. This flag may be used by software to enable or disable the operation of the Root Hub port assigned to the Debug Capability. The Debug Capability Root Hub port operation may be disabled by a fault condition (disconnect event or other fault condition, e.g. a LTSSM Polling substate timeout, tPortConfiguration timeout error, etc.), the assertion of DCPORTSC PR, or by software. 0 = Debug Capability Root Hub port is disabled. 1 = Debug Capability Root Hub port is enabled. When the port is disabled (PED = '0') the port's link shall enter the SS.Disabled state and remain there until PED is reasserted ('1') or DCE is negated ('0'). Note that the Root Hub port is remains mapped to Debug Capability while PED = '0'. While PED = '0' the Debug Capability will appear to be disconnected to the Debug Host. Note, this bit is not affected by PORTSC PR bit transitions. This field is '0' if DCE or CCS are '0'.
0	0h RO	**Current Connect Status (CCS):** '1' = A Root Hub port is connected to a Debug Host and assigned to the Debug Capability. '0' = No Debug Host is present. This value reflects the current state of the port, and may not correspond to the value reported by the Connect Status Change (CSC) field in the Port Status Change Event that was generated by a '0' to '1' transition of this bit. This flag is '0' if Debug Capability Enable (DCE) is '0'.

8.3.243 Debug Capability Context Pointer Register (DCCP) — Offset 8730h

Debug Capability Context Pointer Register

Type	Size	Offset	Default
MMIO	64 bit	MBAR + 8730h	0000000000000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
63:4	00000000 0000000h RW	**Debug Capability Context Pointer Register (DCCPR):** This field defines the high order bits of the start address of the Debug Capability Context data structure associated with the Debug Capability. Software shall initialize this register before setting the Debug Capability Enable bit in the Debug Capability Control Register to '1'.
3:0	0h RO	**Reserved**

8.3.244 GLOBAL TIME SYNC CAP REG (GLOBAL_TIME_SYNC_CAP_REG) — Offset 8E10h

GLOBAL TIME SYNC CAP REG

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 8E10h	000012C9h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:16	0h RO	**Reserved**
15:8	12h RO	**Next Capability pointer (NCP):** Next Capability pointer
7:0	C9h RO	**Capability ID (CID):** Capability ID

8.3.245 GLOBAL TIME SYNC CTRL REG (GLOBAL_TIME_SYNC_CTRL_REG) — Offset 8E14h

GLOBAL TIME SYNC CTRL REG

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 8E14h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:1	0h RO	**Reserved**
0	0h RW/1S	**Time Stamp Counter Capture Initiate (TIME_STAMP_CNTR_CAPTURE_INITIATE):** SW sets this bit to initiate a time capture. Once the time capture is complete and the time values are valid in the Local and Global time capture registers, HW clears the bit.

8.3.246 MICROFRAME TIME REG (MICROFRAME_TIME_REG) — Offset 8E18h

MICROFRAME TIME REG

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 8E18h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:30	0h RO	**Reserved**
29:16	0000h RO	**Captured Frame List Current Index/Frame Number (CMFI):** The value in this register is updated in response to sample_now signal. Bits [29:16] reflect state of bits [13:0] of FRINDEX
15:13	0h RO	**Reserved**
12:0	0000h RO	**Captured Micro-frame BLIF (CMFB):** The value is updated in response to sample_now signal and provides information about offset within micro-frame. Captured value represents number of 8 high-speed bit time units from start of micro-frame. At the beginning of micro-frame captured value will be 0 and increase to maximum value at the end. Default maximum value is 7499 but it may be changed as result of adjustment done via Bus Interval Adjust (BIA).

8.3.247 Global Time Low (GLOBAL_TIME_LOW_REG) — Offset 8E20h

Global Time Value (Low).

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 8E20h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RO	**Global Time Low (GLOBAL_TIME_LOW):** Global Time Value (Low):

8.3.248 Global Time High (GLOBAL_TIME_HI_REG) — Offset 8E24h

Global Time Value (High):

Type	Size	Offset	Default
MMIO	32 bit	MBAR + 8E24h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RO	**Global Time High (GLOBAL_TIME_HI):** Global Time Value (High):

8.4 USB Device Controller (xDCI) Configuration Registers (D13:F1)

This chapter documents the registers in Bus: 0, Device 13, Function 1.

Note: These registers do not apply to S/H processors.

8.4.1 Summary of Registers

Table 8-5. Summary of Bus: 0, Device: 13, Function: 1 Registers

Offset	Size (Bytes)	Register Name (Register Symbol)	Default Value
0h	4	Device ID And Vendor ID Register (DEVVENDID)	0AAA8086h
4h	4	Command and Status (STATUSCOMMAND)	00100000h
8h	4	Revision Id And Class Code (REVCLASSCODE)	0C03FE00h
Ch	4	Cache Line Latency Header And Bist (CLLATHEADERBIST)	00000000h
10h	4	Base Address Register (BAR)	00000004h
14h	4	Base Address Register High (BAR_HIGH)	00000000h
18h	4	Base Address Register1 (BAR1)	00000004h
1Ch	4	Base Address Register1 High (BAR1_HIGH)	00000000h
2Ch	4	Subsystem Vendor And Subsystem ID (SUBSYSTEMID)	00000000h
30h	4	EXPANSION ROM Base Address (EXPANSION_ROM_BASEADDR)	00000000h
34h	4	Capabilities Pointer Register (CAPABILITYPTR)	00000080h
3Ch	4	Interrupt Register (INTERRUPTREG)	00000100h
80h	4	Power Management Capability Id (POWERCAPID)	48039001h
84h	4	Power Management Control And Status Register (PMECTRLSTATUS)	00000008h
90h	4	Pci Device Idle Vendor Capability Register (PCIDEVIDLE_CAP_RECORD)	F0140009h
94h	4	Vendor Specific Extended Capability Register (DEVID_VEND_SPECIFIC_REG)	01400010h
98h	4	Software Ltr Update Mmio Location Register (D0I3_CONTROL_SW_LTR_MMIO_REG)	00000000h
9Ch	4	Device Idle Pointer Register (DEVICE_IDLE_POINTER_REG)	010F8301h
A0h	4	D0i3 And Power Control Enable Register (D0I3_MAX_POW_LAT_PG_CONFIG)	00080800h
F8h	4	Manufacturers ID (MANID)	04000F1Ch

8.4.2 Device ID And Vendor ID Register (DEVVENDID) — Offset 0h

Device ID and Vendor ID provided by this register uniquely identifies the Device

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:1] + 0h	0AAA8086h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:16	0AAAh RO/P	**Device ID (DEVICEID):** Device ID identifies the particular PCI device
15:0	8086h RO	**Vendor ID (VENDORID):** Vendor ID is a unique ID provided by the PCI SIG which identifies the manufacturer of the device

8.4.3 Command and Status (STATUSCOMMAND) — Offset 4h

Command register to program interrupt disable, bus master enable and Memory space enable.

Status register to read the errors and aborts

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:1] + 4h	00100000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:30	0h RO	**Reserved**
29	0h RW/1C	**Received Master Abort (RMA):** Received Master Abort
28	0h RW/1C	**Received Target Abort (RTA):** Received Target Abort
27:21	0h RO	**Reserved**
20	1h RO	**Capabilities List (CAPLIST):** Indicates that the controller contains a capabilities pointer list.
19	0h RO	**Interrupt Status (INTR_STATUS):** Interrupt Status: This bit reflects state of interrupt in the device
18:11	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
10	0h RW	**Interrupt Disable (INTR_DISABLE):** Interrupt Disable
9	0h RO	**Reserved**
8	0h RW	**SERR Reporting Enable (SERR_ENABLE):** SERR Enable Not implemented
7:3	0h RO	**Reserved**
2	0h RW	**Bus Master Enable (BME):** Bus Master Enable
1	0h RW	**Memory Space Enable (MSE):** Memory Space Enable
0	0h RO	**Reserved**

8.4.4 Revision Id And Class Code (REVCLASSCODE) — Offset 8h

Revision ID register identifies revision of particular device and Class Code register is used to identify generic function of the device

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:1] + 8h	0C03FE00h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:8	0C03FEh RO	**Revision ID (CLASS_CODES):** Class Code register is read-only and is used to identify the generic function of the device and in some cases a specific register-level programming interface
7:0	00h RO/P	**Class Code (RID):** Revision ID identifies the revision of particular PCI device.

8.4.5 Cache Line Latency Header And Bist (CLLATHEADERBIST) — Offset Ch

Cache Line size as RW with def 0 Latency timer RW with def 0 Header type with Type 0 configuration header and Reserved BIST register

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:1] + Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:24	0h RO	**Reserved**
23	0h RO	**Multi-Function Device (MULFNDEV):** Multi-Function Device
22:16	00h RO	**Header Type (HEADERTYPE):** Header Type: Implements Type 0 Configuration header
15:8	00h RO	**Latency Timer (LATTIMER):** Latency Timer.
7:0	00h RW/P	**Cache Line Size (CACHELINE_SIZE):** Cacheline Size

8.4.6 Base Address Register (BAR) — Offset 10h

Base Address Register low [31:2] type[2:1] in 32bit or 64bit addr range and memory space indicator [0]

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:1] + 10h	00000004h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:21	000h RW	**Base Address (BASEADDR):** Base Address Register Low Base address of the OCP fabric memory space. Taken from Strap values as ones
20:12	0h RO	**Reserved**
11:4	00h RO	**Size Indicator (SIZEINDICATOR):** Size Indicator RO Always returns 0 The size of this register depends on the size of the memory space
3	0h RO	**Prefetchable Memory (PREFETCHABLE):** 0: BAR memory is not prefetchable 1: BAR memory is prefetchable

Bit Range	Default & Access	Field Name (ID): Description
2:1	2h RO	**Memory Type (TYPE0):** 00b: 32 bit base address 01b: reserved 10b: 64-bit base address 11b: reserved
0	0h RO	**Message Space (MESSAGE_SPACE):** Memory Space Indicator: 0 indicates this BAR is present in the memory space.

8.4.7 Base Address Register High (BAR_HIGH) — Offset 14h

Base Address Register High enabled if [2:1] of BAR_type_LOW is 10

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:1] + 14h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RW	**Base Address High (BASEADDR_HIGH):** Base Address high - MSB

8.4.8 Base Address Register1 (BAR1) — Offset 18h

Base Address Register1 accesses to PCI configuration space and is always 4K type in [2:1] and memory space indicator in [0]

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:1] + 18h	00000004h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:12	00000h RW	**Base Address (BASEADDR1):** Base Address1 This field is present if BAR1 is enabled through private configuration space.
11:4	00h RO	**Size Indicator (SIZEINDICATOR1):** Always is 0 as minimum size is 4K

Bit Range	Default & Access	Field Name (ID): Description
3	0h RO	**Prefetchable Memory (PREFETCHABLE1):** 0: BAR memory is not prefetchable 1: BAR memory is prefetchable
2:1	2h RO	**Memory Type (TYPE1):** 00b: 32 bit base address 01b: reserved 10b: 64-bit base address 11b: reserved
0	0h RO	**Message Space (MESSAGE_SPACE1):** Memory Space Indicator: 0 Indicates this BAR is present in the memory space

8.4.9 Base Address Register1 High (BAR1_HIGH) — Offset 1Ch

Base Address Register1 High enabled only if [2:1] of BAR1 register is 10

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:1] + 1Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RW	**Base Address High (BASEADDR1_HIGH):** Base Address: Base address of the OCP fabric memory space. Taken from Strap values as ones

8.4.10 Subsystem Vendor And Subsystem ID (SUBSYSTEMID) — Offset 2Ch

SVID register along with SID register is to distinguish subsystem from another

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:1] + 2Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:16	0000h RW/O/P	**Subsystem ID (SUBSYSTEMID):** Subsystem ID: This register is implemented for any function that can be instantiated more than once in a given system.

Bit Range	Default & Access	Field Name (ID): Description
15:0	0000h RW/O/P	**Subsystem Vendor (SUBSYSTEMVENDORID):** Subsystem Vendor ID: This register must be implemented for any function that can be instantiated more than once in a given system

8.4.11 EXPANSION ROM Base Address (EXPANSION_ROM_BASEADDR) — Offset 30h

EXPANSION ROM base address register is a RO indicates support for expansion ROMs

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:1] + 30h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RO	**Expansion ROM Base Address (EXPANSION_ROM_BASE):** Value of all zeros indicates no support for Expansion ROM

8.4.12 Capabilities Pointer Register (CAPABILITYPTR) — Offset 34h

Capabilities Pointer register indicates what the next capability is

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:1] + 34h	00000080h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:8	0h RO	**Reserved**
7:0	80h RO	**Capabilities Pointer (CAPPTR_POWER):** Capabilities Pointer: Indicates what the next capability is.

8.4.13 Interrupt Register (INTERRUPTREG) — Offset 3Ch

Interrupt line Register isn't used in Bridge directly Interrupt Pin register reflects the IPIN value in private config space.

Min_gnt register indicating the req of latency timers and max_lat register max latency.

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:1] + 3Ch	00000100h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:24	00h RO	**Maximum Latency (MAX_LAT):** Value of 0 indicates device has no major requirements for the settings of latency timers
23:16	00h RO	**Minimum Latency (MIN_GNT):** Value of 0 indicates device has no major requirements for the settings of latency timers.
15:12	0h RO	**Reserved**
11:8	1h RO	**Interrupt Pin (INTPIN):** Interrupt Pin: Value in this register is reflected from the IPIN value in the private configuration space.
7:0	00h RW/P	**Interrupt Line (INTLINE):** Used to communicate to software the interrupt line to which the interrupt pin is connected.

8.4.14 Power Management Capability Id (POWERCAPID) — Offset 80h

Power Management Capability ID register points to next capability structure and power management capability with Power management capabilities register for PME support and version

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:1] + 80h	48039001h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:27	09h RO	**PME Support (PMESUPPORT):** This 5-bit field indicates the power states in which the function can assert the PME#
26:19	0h RO	**Reserved**
18:16	3h RO	**VERSION:** Indicates support for Revision 1.2 of the PCI Power Management Specification
15:8	90h RO	**Next Capability (NXTCAP):** Points to the next capability structure.
7:0	01h RO	**Power Capability ID (POWER_CAP):** Power Management Capability: Indicates this is power management capability

8.4.15 Power Management Control And Status Register (PMECTRLSTATUS) — Offset 84h

power management control and status register to set and read PME status PME enable No Soft reset and power state

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:1] + 84h	00000008h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:16	0h RO	**Reserved**
15	0h RW/1C/P	**PME Status (PMESTATUS):** PME Status
14:9	0h RO	**Reserved**
8	0h RW/P	**PME Enable (PMEENABLE):** PME Enable
7:4	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
3	1h RO	**No Soft Reset (NO_SOFT_RESET):** This bit indicates that devices transitioning from D3hot to D0 because of Powerstate commands do not perform an internal reset
2	0h RO	**Reserved**
1:0	0h RW	**Power State (POWERSTATE):** Power State: This field is used both to determine the current power state and to set a new power state

8.4.16 Pci Device Idle Vendor Capability Register (PCIDEVIDLE_CAP_RECORD) — Offset 90h

PCI Device Vendor Specific Capability register defines Vendor specific Capability ID revision length next capability and CAPID

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:1] + 90h	F0140009h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:28	Fh RO	**Vendor Cap (VEND_CAP):** Vendor Specific Capability ID
27:24	0h RO	**Revision ID (REVID):** Revision ID of capability structure
23:16	14h RO	**Cap Length (CAP_LENGTH):** Vendor Specific Capability Length
15:8	00h RO	**Next Capability (NEXT_CAP):** Next Capability
7:0	09h RO	**Capability ID (CAPID):** Capability ID

8.4.17 Vendor Specific Extended Capability Register (DEVID_VEND_SPECIFIC_REG) — Offset 94h

Extended Vendor capability register for VSEC Length revision and ID

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:1] + 94h	01400010h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:20	014h RO	**Vendor Specific ID (VSEC_LENGTH):** Vendor Specific Extended Capability Length
19:16	0h RO	**Vendor Specific Revision (VSEC_REV):** Vendor specific Extended Capability revision
15:0	0010h RO	**Vendor Specific Length (VSECID):** Vendor Specific Extended Capability ID

8.4.18 Software Ltr Update Mmio Location Register (D0I3_CONTROL_SW_LTR_MMIO_REG) — Offset 98h

Software location pointer in MMIO space as an offset specified by BAR

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:1] + 98h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:4	0000000h RO	**SW LTR Dword Offset (SW_LAT_DWORD_OFFSET):** SW LTR Update MMIO Offset Location (SWLTRLOC)
3:1	0h RO	**SW LTR BAR Number (SW_LAT_BAR_NUM):** Indicates that the SW LTR update MMIO location is always at BAR0
0	0h RO	**SW LTR Valid (SW_LAT_VALID):** This value is reflected from the SW LTR valid strap at the top level

8.4.19 Device Idle Pointer Register (DEVICE_IDLE_POINTER_REG) — Offset 9Ch

Device IDLE pointer register giving details on Device MMIO offset location BAR NUM and D0i3 Valid Strap

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:1] + 9Ch	010F8301h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:4	010F830h RO	**D0i3 Dword Offset (DWORD_OFFSET):** contains the location pointer to the SW LTR register in MMIO space as an offset from the specified BAR
3:1	0h RO	**BAR Number (BAR_NUM):** Indicates that the D0i3 MMIO location is always at BAR0
0	1h RO	**D0i3 Valid (VALID):** Valid: This value is reflected from the D0i3 valid strap at the top level.

8.4.20 D0i3 And Power Control Enable Register (D0I3_MAX_POW_LAT_PG_CONFIG) — Offset A0h

D0idle_Max_Power_On_Latency register set at boot and Power control enable register to enable communication with the PGCB block below the Bridge

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:1] + A0h	00080800h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:22	0h RO	**Reserved**
21	0h RW/P	**Hardware Autonomous Enable (HAE):** Hardware Autonomous Enable.
20	0h RO	**Reserved**
19	1h RW/P	**Sleep Enable (SLEEP_EN):** Sleep Enable
18	0h RW/P	**D3-Hot Enable (D3HEN):** If 1b then function will power gate when idle and the PMCSR[1:0] register in the function = 11b (D3).
17	0h RW/P	**Device Idle Enable (DEVIDLEN):** If 1b then the function will power gate when idle and the DevIdle register (DevIdleC[2] = 1) is set.

Bit Range	Default & Access	Field Name (ID): Description
16	0h RW/P	**D3 Enable (D3_ENABLE):** D3 Enable.
15:13	0h RO	**Reserved**
12:10	2h RW/O/P	**Power Latency Scale (POW_LAT_SCALE):** Power On Latency Scale
9:0	000h RW/O/P	**Power Latency Value (POW_LAT_VALUE):** Power On Latency value

8.4.21 Manufacturers ID (MANID) — Offset F8h

Manufacturers ID register

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:13, F:1] + F8h	04000F1Ch

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:0	04000F1Ch RO/P	**Manufacturers ID (MANID):** Manufacturer ID: Default value comes from straps.

8.5 Thunderbolt PCI Express* Controller Registers (D7:F0-3)

This chapter documents the registers of the Thunderbolt PCIe devices. The Thunderbolt device contains multiple PCIe controller devices:

- Bus: 0, Device: 7, Function: 0 (TBT_PCIe0)
- Bus: 0, Device: 7, Function: 1 (TBT_PCIe1)
- Bus: 0, Device: 7, Function: 2 (TBT_PCIe2)
- Bus: 0, Device: 7, Function: 3 (TBT_PCIe3)

The specified function number assignment is applicable under a single segment PCIe configuration space programming. Please refer to the Ice Lake EDS Vol1 for other programming options.

Note: Register default values are taken from device PCIe0 only. Consult the Ice Lake EDS Vol1 for Device IDs

8.5.1 Summary of Registers

Table 8-6. Summary of Bus: 0, Device: 7, Function: 0 Registers

Offset	Size (Bytes)	Register Name (Register Symbol)	Default Value
0h	4	Device Identifiers (ID)	00008086h
4h	2	Device Command (CMD)	0000h
6h	2	Primary Status (PSTS)	0010h
8h	4	Revision ID (RID_CC)	060400F0h
Ch	1	Cache Line Size (CLS)	00h
Dh	1	Primary Latency Timer (PLT)	00h
Eh	1	Header Type (HTYPE)	81h
18h	4	Bus Numbers (BNUM_SLT)	00000000h
1Ch	2	I/O Base And Limit (IOBL)	0000h
1Eh	2	Secondary Status (SSTS)	0000h
20h	4	Memory Base And Limit (MBL)	00000000h
24h	4	Prefetchable Memory Base And Limit (PMBL)	00010001h
28h	4	Prefetchable Memory Base Upper 32 Bits (PMBU32)	00000000h
2Ch	4	Prefetchable Memory Limit Upper 32 Bits (PMLU32)	00000000h
34h	1	Capabilities List Pointer (CAPP)	40h
3Ch	2	Interrupt Information (INTR)	0100h
3Eh	2	Bridge Control (BCTRL)	0000h
40h	2	Capabilities List (CLIST)	8010h
42h	2	PCI Express Capabilities (XCAP)	0042h
44h	4	Device Capabilities (DCAP)	00008001h
48h	2	Device Control (DCTL)	0020h
4Ah	2	Device Status (DSTS)	0010h
4Ch	4	Link Capabilities (LCAP)	01714C10h

Offset	Size (Bytes)	Register Name (Register Symbol)	Default Value
50h	2	Link Control (LCTL)	0000h
52h	2	Link Status (LSTS)	1011h
54h	4	Slot Capabilities (SLCAP)	00040060h
58h	2	Slot Control (SLCTL)	0000h
5Ah	2	Slot Status (SLSTS)	0000h
5Ch	2	Root Control (RCTL)	0000h
60h	4	Root Status (RSTS)	00000000h
64h	4	Device Capabilities 2 (DCAP2)	00080837h
68h	2	Device Control 2 (DCTL2)	0000h
6Ah	2	Device Status 2 (DSTS2)	0000h
6Ch	4	Link Capabilities 2 (LCAP2)	0000000Eh
70h	2	Link Control 2 (LCTL2)	0001h
72h	2	Link Status 2 (LSTS2)	0000h
74h	4	Slot Capabilities 2 (SLCAP2)	00000000h
78h	2	Slot Control 2 (SLCTL2)	0000h
7Ah	2	Slot Status 2 (SLSTS2)	0000h
80h	2	Message Signaled Interrupt Identifiers (MID)	9005h
82h	2	Message Signaled Interrupt Message (MC)	0000h
84h	4	Message Signaled Interrupt Message Address (MA)	00000000h
88h	2	Message Signaled Interrupt Message Data (MD)	0000h
90h	2	Subsystem Vendor Capability (SVCAP)	A00Dh
94h	4	Subsystem Vendor IDs (SVID)	00000000h
A0h	2	Power Management Capability (PMCAP)	0001h
A2h	2	PCI Power Management Capabilities (PMC)	C803h
A4h	4	PCI Power Management Control (PMCS)	00000008h
100h	4	Advanced Error Extended (AECH)	00000000h
104h	4	Uncorrectable Error Status (UES)	00000000h
108h	4	Uncorrectable Error Mask (UEM)	00000000h
10Ch	4	Uncorrectable Error Severity (UEV)	00060010h
110h	4	Correctable Error Status (CES)	00000000h
114h	4	Correctable Error Mask (CEM)	00002000h
118h	4	Advanced Error Capabilities And Control (AECC)	00000000h
11Ch	4	Header Log (HL_DW1)	00000000h
120h	4	Header Log (HL_DW2)	00000000h
124h	4	Header Log (HL_DW3)	00000000h
128h	4	Header Log (HL_DW4)	00000000h
12Ch	4	Root Error Command (REC)	00000000h
130h	4	Root Error Status (RES)	00000000h
134h	4	Error Source Identification (ESID)	00000000h
150h	4	PTM Extended Capability Header (PTMECH)	00000000h
154h	4	PTM Capability Register (PTMCAPR)	00000400h

Offset	Size (Bytes)	Register Name (Register Symbol)	Default Value
158h	4	PTM Control Register (PTMCTLR)	00000000h
220h	4	ACS Extended Capability Header (ACSECH)	00000000h
224h	2	ACS Capability Register (ACSCAPR)	000Fh
226h	2	ACS Control Register (ACSCTLR)	0000h
A00h	4	DPC Extended Capability Header (DPCECH)	00000000h
A04h	2	DPC Capability Register (DPCCAPR)	14E0h
A06h	2	DPC Control Register (DPCCTLR)	0000h
A08h	2	DPC Status Register (DPCSR)	1F00h
A0Ah	2	DPC Error Source ID Register (DPCESIDR)	0000h
A0Ch	4	RP PIO Status Register (RPPIOSR)	00000000h
A10h	4	RP PIO Mask Register (RPPIOMR)	00070707h
A14h	4	RP PIO Severity Register (RPPIOVR)	00000000h
A18h	4	RP PIO SysError Register (RPPIOSER)	00000000h
A1Ch	4	RP PIO Exception Register (RPPIOER)	00000000h
A20h	4	RP PIO Header Log DW1 Register (RPPIOHLR_DW1)	00000000h
A24h	4	RP PIO Header Log DW2 Register (RPPIOHLR_DW2)	00000000h
A28h	4	RP PIO Header Log DW3 Register (RPPIOHLR_DW3)	00000000h
A2Ch	4	RP PIO Header Log DW4 Register (RPPIOHLR_DW4)	00000000h
A30h	4	Secondary PCI Express Extended Capability Header (SPEECH)	00000000h
A34h	4	Link Control 3 (LCTL3)	00000000h
A38h	4	Lane Error Status (LES)	00000000h
A3Ch	4	Lane 0 And Lane 1 Equalization Control (L01EC)	7F7F7F7Fh
A40h	4	Lane 2 And Lane 3 Equalization Control (L23EC)	7F7F7F7Fh
A44h	4	Lane 4 And Lane 5 Equalization Control (L45EC)	7F7F7F7Fh
A48h	4	Lane 6 And Lane 7 Equalization Control (L67EC)	7F7F7F7Fh
A4Ch	4	Lane 8 And Lane 9 Equalization Control (L89EC)	7F7F7F7Fh
A50h	4	Lane 10 And Lane 11 Equalization Control (L1011EC)	7F7F7F7Fh
A54h	4	Lane 12 And Lane 13 Equalization Control (L1213EC)	7F7F7F7Fh
A58h	4	Lane 14 And Lane 15 Equalization Control (L1415EC)	7F7F7F7Fh

8.5.2 Device Identifiers (ID) — Offset 0h

Device ID and Vendor ID

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + 0h	00008086h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:16	0000h RO/V	**Device Identification (DID):** See the Device ID table in the first volume of this document.
15:0	8086h RO	**Vendor Identification (VID):** Indicates Intel.

8.5.3 Device Command (CMD) — Offset 4h

Device Command

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:7, F:0] + 4h	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:11	0h RO	**Reserved**
10	0h RW/V2	**Interrupt Disable (ID):** This disables pin-based INTx# interrupts on enabled hot plug and power management events. This bit has no effect on MSI operation. When set, internal INTx# messages will not be generated. When cleared, internal INTx# messages are generated if there is an interrupt for hot plug or power management and MSI is not enabled. This bit does not affect interrupt forwarding from devices connected to the root port. Assert_INTx and Deassert_INTx messages will still be forwarded to the internal interrupt controllers if this bit is set. For PCI Bus Emulation Mode compatibility, if the PCIBEM register is set, this register is RO and returns a value of 0 when read, else it is RW with the functionality described above.
9	0h RO	**Fast Back to Back Enable (FBE):** This field is reserved per PCI-Express spec.
8	0h RW	**SERR# Enable (SEE):** When set, enables the root port to generate an SERR# message when PSTS.SSE is set.
7	0h RO	**Wait Cycle Control (WCC):** This field is reserved per PCI-Express spec.

Bit Range	Default & Access	Field Name (ID): Description
6	0h RW	**Parity Error Response Enable (PERE):** Indicates that the device is capable of reporting parity errors as a master on the backbone.
5	0h RO	**VGA Palette Snoop (VGA_PSE):** This field is reserved per PCI-Express spec.
4	0h RO	**Memory Write and Invalidate Enable (MWIE):** This field is reserved per PCI-Express spec.
3	0h RO	**Special Cycle Enable (SCE):** This field is reserved per PCI-Express and PCI bridge spec.
2	0h RW	**Bus Master Enable (BME):** When set, allows the root port to forward Memory and I/O Read/Write cycles onto the backbone from a PCI-Express device. When this bit is 0b, Memory and I/O requests received at a Root Port must be handled as Unsupported Requests (UR). This bit does not affect forwarding of Completions in either the Upstream or Downstream direction. The forwarding of Requests other than Memory or I/O requests is not controlled by this bit.
1	0h RW	**Memory Space Enable (MSE):** When set, memory cycles within the range specified by the memory base and limit registers can be forwarded to the PCI-Express device. When cleared, these memory cycles are master aborted on the backbone.
0	0h RW	**I/O Space Enable (IOSE):** When set, I/O cycles within the range specified by the I/O base and limit registers can be forwarded to the PCI-Express device. When cleared, these cycles are master aborted on the backbone.

8.5.4 Primary Status (PSTS) — Offset 6h

Primary Status

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:7, F:0] + 6h	0010h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15	0h RW/1C/V	**Detected Parity Error (DPE):** Set when the root port receives a command or data from the backbone with a parity error. This is set even if PCMD.PERE is not set.
14	0h RW/1C/V	**Signaled System Error (SSE):** Set when the root port signals a system error to the internal SERR# logic.
13	0h RW/1C/V	**Received Master Abort (RMA):** Set when the root port receives a completion with unsupported request status from the backbone.
12	0h RW/1C/V	**Received Target Abort (RTA):** Set when the root port receives a completion with completer abort from the backbone.

Bit Range	Default & Access	Field Name (ID): Description
11	0h RW/1C/V	**Signaled Target Abort (STA):** Set whenever the root port forwards a target abort received from the downstream device onto the backbone.
10:9	0h RO	**Primary DEVSEL# Timing Status (PDTS):** This field is reserved per PCI-Express spec
8	0h RW/1C/V	**Master Data Parity Error Detected (DPD):** Set when the root port receives a completion with a data parity error on the backbone and PCMD.PERE is set.
7	0h RO	**Primary Fast Back to Back Capable (PFBC):** This field is reserved per PCI-Express spec.
6	0h RO	**Reserved**
5	0h RO	**Primary 66 MHz Capable (PC66):** This field is reserved per PCI-Express spec.
4	1h RO	**Capabilities List (CLIST):** Indicates the presence of a capabilities list.
3	0h RO/V	**Interrupt Status (IS):** Indicates status of hot plug and power management interrupts on the root port that result in INTx# message generation. This bit is not set if MSI is enabled. If MSI is not enabled, this bit is set regardless of the state of CMD.ID.
2:0	0h RO	**Reserved**

8.5.5 Revision ID (RID_CC) — Offset 8h

Revision ID

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + 8h	060400F0h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:24	06h RO	**Base Class Code (BCC):** Indicates the device is a bridge device.
23:16	04h RO/V	**Sub-Class Code (SCC):** The default indicates the device is a PCI-to-PCI bridge. If the MPC.Bridge Type register is set to a '1' for a Host Bridge, this register reads 00h.
15:8	00h RO/V	**Programming Interface (PI):** PCI-to-PCI bridge.
7:0	F0h RO/V	**Revision ID (RID):** Indicates the revision of the bridge.

8.5.6 Cache Line Size (CLS) — Offset Ch

Cache Line Size

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:7, F:0] + Ch	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
7:0	00h RW	**Line Size (LS):** This is read/write but contains no functionality, per PCI-Express spec

8.5.7 Primary Latency Timer (PLT) — Offset Dh

Primary Latency Timer

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:7, F:0] + Dh	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:3	00h RO	**Latency Count (CT):** This field is reserved per PCI-Express spec
2:0	0h RO	**Reserved**

8.5.8 Header Type (HTYPE) — Offset Eh

Header Type

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:7, F:0] + Eh	81h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7	1h RO	**Multi-function Device (MFD):** This bit is '1' to indicate a multi-function device.
6:0	01h RO/V	**Header Type (HTYPE):** The default mode identifies the header layout of the configuration space, which is a PCI-to-PCI bridge. If the MPC.Bridge Type register is set to a '1' for a Host Bridge, this register reads 00h.

8.5.9 Bus Numbers (BNUM_SLT) — Offset 18h

Bus Numbers

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + 18h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:24	00h RW/V2	**Secondary Latency Timer (SLT):** For PCI Bus Emulation Mode compatibility, if the PCIBEM register is set, this register is a RW register - else this register is RO and returns 0. This register does not affect the behavior of any HW logic.
23:16	00h RW	**Subordinate Bus Number (SBBN):** Indicates the highest PCI bus number below the bridge.
15:8	00h RW	**Secondary Bus Number (SCBN):** Indicates the bus number the port.
7:0	00h RW	**Primary Bus Number (PBN):** Indicates the bus number of the backbone.

8.5.10 I/O Base And Limit (IOBL) — Offset 1Ch

I/O Base And Limit

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:7, F:0] + 1Ch	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:12	0h RW	**I/O Address Limit (IOLA):** I/O Base bits corresponding to address lines 15:12 for 4KB alignment. Bits 11:0 are assumed to be padded to FFFh.
11:8	0h RO	**I/O Limit Address Capability (IOLC):** Indicates that the bridge does not support 32-bit I/O addressing.
7:4	0h RW	**I/O Base Address (IOBA):** I/O Base bits corresponding to address lines 15:12 for 4KB alignment. Bits 11:0 are assumed to be padded to 000h.
3:0	0h RO	**I/O Base Address Capability (IOBC):** Indicates that the bridge does not support 32-bit I/O addressing.

8.5.11 Secondary Status (SSTS) — Offset 1Eh

Secondary Status

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:7, F:0] + 1Eh	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15	0h RW/1C/V	**Detected Parity Error (DPE):** Set when the port receives a poisoned TLP.
14	0h RW/1C/V	**Received System Error (RSE):** Set when the port receives an ERR_FATAL or ERR_NONFATAL message from the device.
13	0h RW/1C/V	**Received Master Abort (RMA):** Set when the port receives a completion with 'Unsupported Request' status from the device.
12	0h RW/1C/V	**Received Target Abort (RTA):** Set when the port receives a completion with 'Completion Abort' status from the device.
11	0h RW/1C/V	**Signaled Target Abort (STA):** Set when the port generates a completion with 'Completion Abort' status to the device.

Bit Range	Default & Access	Field Name (ID): Description
10:9	0h RO/V	**Secondary DEVSEL# Timing Status (SDTS):** This field is reserved per PCI-Express spec For PCI Bus Emulation Mode compatibility, if the PCIBEM register is set, this register returns a value of 01b when read, else this register returns a value of 00b.
8	0h RW/1C/V	**Data Parity Error Detected (DPD):** Set when the BCTRL.PERE, and either of the following two conditions occurs: Port receives completion marked poisoned. Port poisons a write request to the secondary side.
7	0h RO/V	**Secondary Fast Back to Back Capable (SFBC):** This field is reserved per PCI Express spec For PCI Bus Emulation Mode compatibility, if the PCIBEM register is set, this register returns a value of 1b when read, else this register returns a value of 0b.
6	0h RO	**Reserved**
5	0h RO	**Secondary 66 MHz Capable (SC66):** This field is reserved per PCI Express spec
4:0	0h RO	**Reserved**

8.5.12 Memory Base And Limit (MBL) — Offset 20h

Memory Base And Limit

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + 20h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:20	000h RW	**Memory Limit (ML):** These bits are compared with bits 31:20 of the incoming address to determine the upper 1MB aligned value of the range.
19:16	0h RO	**Reserved**
15:4	000h RW	**Memory Base (MB):** These bits are compared with bits 31:20 of the incoming address to determine the lower 1MB aligned value of the range.
3:0	0h RO	**Reserved**

8.5.13 Prefetchable Memory Base And Limit (PMBL) — Offset 24h

Prefetchable Memory Base And Limit

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + 24h	00010001h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:20	000h RW	**Prefetchable Memory Limit (PML):** These bits are compared with bits 31:20 of the incoming address to determine the upper 1MB aligned value of the range.
19:16	1h RO	**64-bit Indicator (I64L):** Indicates support for 64-bit addressing.
15:4	000h RW	**Prefetchable Memory Base (PMB):** These bits are compared with bits 31:20 of the incoming address to determine the lower 1MB aligned value of the range.
3:0	1h RO	**64-bit Indicator (I64B):** Indicates support for 64-bit addressing.

8.5.14 Prefetchable Memory Base Upper 32 Bits (PMBU32) — Offset 28h

Prefetchable Memory Base Upper 32 Bits

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + 28h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RW	**Prefetchable Memory Base Upper Portion (PMBU):** Upper 32-bits of the prefetchable address base.

8.5.15 Prefetchable Memory Limit Upper 32 Bits (PMLU32) — Offset 2Ch

Prefetchable Memory Limit Upper 32 Bits

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + 2Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RW	**Prefetchable Memory Limit Upper Portion (PMLU):** Upper 32-bits of the prefetchable address limit.

8.5.16 Capabilities List Pointer (CAPP) — Offset 34h

Capabilities List Pointer

Type	Size	Offset	Default
PCI	8 bit	[B:0, D:7, F:0] + 34h	40h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
7:0	40h RW/O	**Capabilities Pointer (PTR):** Indicates that the pointer for the first entry in the capabilities list. BIOS can determine which capabilities will be exposed by including or removing them from the capability linked list. As this register is RWO, BIOS must write a value to this register, even if it is to re-write the default value. **Capability Linked List (Default Settings)** Offset | Capability | Next Pointer 40h | PCI Express | 80h 80h | Message Signaled Interrupt (MSI) | 90h 90h | Subsystem Vendor | A0h A0h | PCI Power Management | 00h **Extended PCIe Capability Linked List** Offset | Capability | Next Pointer 100h | Advanced Error Reporting | 000h 140h | Access Control Services | 000h 200h | L1 Sub-states | 000h 220h | Secondary PCI Express Capability | 000h

8.5.17 Interrupt Information (INTR) — Offset 3Ch

Interrupt Information

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:7, F:0] + 3Ch	0100h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:8	01h RO/V	**Interrupt Pin (IPIN):** Indicates the interrupt pin driven by the root port. At reset, this register takes on the following values, which reflect the reset state of the STRPFUSECFG.PxIP field: Port Bits[15:12] Bits[11:08] 1 0h STRPFUSECFG.P1IP 2 0h STRPFUSECFG.P2IP 3 0h STRPFUSECFG.P3IP ... X 0h STRPFUSECFG.PxIP The value that is programmed into STRPFUSECFG.PxIP is always reflected in this register. For PCI Bus Emulation Mode compatibility, if the PCIBEM register is set, this register returns a value of 00h when read, else this register returns the value from the table above. Note: Depending on the platform, the number of Root Ports supported may vary. In this case, the encodings defined in this register will be scaled accordingly.
7:0	00h RW	**Interrupt Line (ILINE):** Software written value to indicate which interrupt line (vector) the interrupt is connected to. No hardware action is taken on this register.

8.5.18 Bridge Control (BCTRL) — Offset 3Eh

Bridge Control

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:7, F:0] + 3Eh	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:12	0h RO	**Reserved**
11	0h RW/V2	**Discard Timer SERR# Enable (DTSE):** This field is reserved per PCI-Express spec. For PCI Bus Emulation Mode compatibility, if the PCIBEM register is set, this register is RW else it is RO. This register is only maintained for SW compatibility and has no functionality within the port.

Bit Range	Default & Access	Field Name (ID): Description
10	0h RO	**Discard Timer Status (DTS):** This field is reserved per PCI-Express spec. For PCI Bus Emulation Mode compatibility, this register can remain RO as no secondary discard timer exists that will ever cause it to be set.
9	0h RW/V2	**Secondary Discard Timer (SDT):** This field is reserved per PCI-Express spec. For PCI Bus Emulation Mode compatibility, if the PCIBEM register is set, this register is RW else it is RO. This register is only maintained for SW compatibility and has no functionality within the port.
8	0h RW/V2	**Primary Discard Timer (PDT):** This field is reserved per PCI-Express spec. For PCI Bus Emulation Mode compatibility, if the PCIBEM register is set, this register is RW else it is RO. This register is only maintained for SW compatibility and has no functionality within the port.
7	0h RO	**Fast Back to Back Enable (FBE):** This field is reserved per PCI-Express spec.
6	0h RW	**Secondary Bus Reset (SBR):** Triggers a Hot Reset on the PCI-Express port.
5	0h RW/V2	**Master Abort Mode (MAM):** This field is reserved per PCI-Express spec. For PCI Bus Emulation Mode compatibility, if the PCIBEM register is set, this register is RW else it is RO. This register is only maintained for SW compatibility and has no functionality within the port.
4	0h RW	**VGA 16-Bit Decode (V16):** When set, indicates that the I/O aliases of the VGA range (see BCTRL:VE definition below), are not enabled. 0: Execute 10-bit address decode on VGA I/O accesses. 1: Execute 16-bit address decode on VGA I/O accesses.
3	0h RW	**VGA Enable (VE):** When set, the following ranges will be claimed off the backbone by the root port: Memory ranges A0000h-BFFFFh I/O ranges 3B0h - 3BBh and 3C0h - 3DFh, and all aliases of bits 15:10 in any combination of 1's
2	0h RW	**ISA Enable (IE):** This bit only applies to I/O addresses that are enabled by the I/O Base and I/O Limit registers and are in the first 64KB of PCI I/O space. If this bit is set, the root port will block any forwarding from the backbone to the device of I/O transactions addressing the last 768 bytes in each 1KB block (offsets 100h to 3FFh).
1	0h RW	**SERR# Enable (SE):** When set, ERR_COR, ERR_NONFATAL, and ERR_FATAL messages received are forwarded to the backbone. When cleared, they are not.
0	0h RW	**Parity Error Response Enable (PERE):** When set, poisoned write TLPs and completions indicating poisoned TLPs will set the SSTS.DPD.

8.5.19 Capabilities List (CLIST) — Offset 40h

Capabilities List

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:7, F:0] + 40h	8010h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:8	80h RW/O	**Next Capability (NEXT):** Indicates the location of the next capability. The default value of this register is 80h which points to the MSI Capability structure. BIOS can determine which capabilities will be exposed by including or removing them from the capability linked list. As this register is RWO, BIOS must write a value to this register, even if it is to re-write the default value.
7:0	10h RO	**Capability ID (CID):** Indicates this is a PCI Express capability

8.5.20 PCI Express Capabilities (XCAP) — Offset 42h

PCI Express Capabilities

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:7, F:0] + 42h	0042h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:14	0h RO	**Reserved**
13:9	00h RO	**Interrupt Message Number (IMN):** The Root Port does not have multiple MSI interrupt numbers.
8	0h RW/O	**Slot Implemented (SI):** Indicates whether the root port is connected to a slot. Slot support is platform specific. BIOS programs this field, and it is maintained until a platform reset.
7:4	4h RO	**Device / Port Type (DT):** Indicates this is a PCI-Express root port
3:0	2h RO	**Capability Version (CV):** Version 2.0 indicates devices compliant to the PCI Express 2.0 and 3.0 specification which incorporates the Register Expansion ECN.

8.5.21 Device Capabilities (DCAP) — Offset 44h

Device Capabilities

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + 44h	00008001h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:29	0h RO	**Reserved**
28	0h RO	**Function Level Reset Capable (FLRC):** Not supported in Root Ports
27:26	0h RO	**Captured Slot Power Limit Scale (CSPS):** Not supported.
25:18	00h RO	**Captured Slot Power Limit Value (CSPV):** Not supported.
17:16	0h RO	**Reserved**
15	1h RO	**Role Based Error Reporting (RBER):** Indicates that this device implements the functionality defined in the Error Reporting ECN as required by the PCI Express 1.1 spec.
14:12	0h RO	**Reserved**
11:9	0h RO	**Endpoint L1 Acceptable Latency (E1AL):** This field is reserved for root ports.
8:6	0h RO	**Endpoint L0s Acceptable Latency (E0AL):** This field is reserved for Root port.
5	0h RO	**Extended Tag Field Supported (ETFS):** The Root Port never needs to initiate a transaction as a Requester with the Extended Tag bits being set. This bit does not affect the root port's ability to forward requests as a bridge as the root port always supports forwarding requests with extended tags.
4:3	0h RO	**Phantom Functions Supported (PFS):** No phantom functions supported

Bit Range	Default & Access	Field Name (ID): Description
2:0	1h RW/O	**Max Payload Size Supported (MPS):** BIOS should write to this field during system initialization. Max Payload Size of up to 256B is supported. Programming this field to any values other than 128B or 256B max payload size will result in aliasing to 128B max payload size. 000b: 128 bytes max payload size. 001b: 256 bytes max payload size. 010b: 512 bytes max payload size. 011b: 1024 bytes max payload size. 100b: 2048 bytes max payload size. 101b: 4096 bytes max payload size. 110b: Reserved. 111b: Reserved. This field applies only to the PCIe link interface.

8.5.22 Device Control (DCTL) — Offset 48h

Device Control

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:7, F:0] + 48h	0020h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15	0h RO	**Reserved**
14:12	0h RO	**Max Read Request Size (MRRS):** Hardwired to 0. This field applies only to the PCIe link interface.
11	0h RO	**Enable No Snoop (ENS):** Not supported. The root port will never issue non-snoop requests.
10	0h RW/P	**Aux Power PM Enable (APME):** Must be RW for OS testing. The OS will set this bit to '1' if the device connected has detected aux power. It has no effect on the root port otherwise.
9	0h RO	**Phantom Functions Enable (PFE):** Not supported
8	0h RO	**Extended Tag Field Enable (ETFE):** Not supported

Bit Range	Default & Access	Field Name (ID): Description
7:5	1h RW	**Max Payload Size (MPS):** The root port supports up to 256B max payload. Programming this field to any values greater than DCAP.MPS will result in aliasing to 128B max payload size. 000b: 128 bytes max payload size. 001b: 256 bytes max payload size. 010b: 512 bytes max payload size. 011b: 1024 bytes max payload size. 100b: 2048 bytes max payload size. 101b: 4096 bytes max payload size. 110b: Reserved. 111b: Reserved. This field applies only to the PCIe link interface. Note: Software should ensure that the system is quiescent and no TLP is in progress prior to changing this field. BIOS should program this field prior to enabling BME.
4	0h RO	**Enable Relaxed Ordering (ERO):** Not supported
3	0h RW	**Unsupported Request Reporting Enable (URE):** When set, allows signaling ERR_NONFATAL, ERR_FATAL, or ERR_COR to the Root Control register when detecting an unmasked Unsupported Request (UR). An ERR_COR is signaled when a unmasked Advisory Non-Fatal UR is received. An ERR_FATAL, ERR_or NONFATAL, is sent to the Root Control Register when an uncorrectable non-advisory UR is received with the severity set by the Uncorrectable Error Severity register.
2	0h RW	**Fatal Error Reporting Enable (FEE):** Enables signaling of ERR_FATAL to the Root Control register due to internally detected errors or error messages received across the link. Other bits also control the full scope of related error reporting.
1	0h RW	**Non-Fatal Error Reporting Enable (NFE):** When set, enables signaling of ERR_NONFATAL to the Root Control register due to internally detected errors or error messages received across the link. Other bits also control the full scope of related error reporting.
0	0h RW	**Correctable Error Reporting Enable (CEE):** When set, enables signaling of ERR_CORR to the Root Control register due to internally detected errors or error messages received across the link. Other bits also control the full scope of related error reporting.

8.5.23 Device Status (DSTS) — Offset 4Ah

Device Status

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:7, F:0] + 4Ah	0010h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:6	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
5	0h RO	**Transactions Pending (TDP):** This bit has no meaning for the root port since it never initiates a non-posted request with its own RequesterID.
4	1h RO	**AUX Power Detected (APD):** The root port contains AUX power for wakeup
3	0h RW/1C/V	**Unsupported Request Detected (URD):** Indicates an unsupported request was detected.
2	0h RW/1C/V	**Fatal Error Detected (FED):** Indicates a fatal error was detected. Set when a fatal error occurred on from a data link protocol error, buffer overflow, or malformed tlp
1	0h RW/1C/V	**Non-Fatal Error Detected (NFED):** Indicates a non-fatal error was detected. Set when an received a non-fatal error occurred from a poisoned tlp, unexpected completions, unsupported requests, completor abort, or completer timeout
0	0h RW/1C/V	**Correctable Error Detected (CED):** Indicates a correctable error was detected. Set when received an internal correctable error from receiver errors / framing errors, tlp crc error, dllp crc error, replay num rollover, replay timeout.

8.5.24 Link Capabilities (LCAP) — Offset 4Ch

Link Capabilities

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + 4Ch	01714C10h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:24	01h RO/V	**Port Number (PN):** Indicates the port number for the root port. This value is different for each implemented port: Port # Value of PN field 1 01h 2 02h 3 03h : : X 0Xh Note: Depending on the platform, the number of Root Ports supported may vary. In this case, the encodings defined in this register will be scaled accordingly.
23	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
22	1h RW/O	**ASPM Optionality Compliance (ASPMOC):** This bit must be set to 1b for PCIe 3.0 compliant port. Components implemented against certain earlier versions of this specification will have this bit set to 0b. Software is permitted to use the value of this bit to help determine whether to enable ASPM or whether to run ASPM compliance tests.
21	1h RO	**Link Bandwidth Notification Capability (LBNC):** This port supports Link Bandwidth Notification status and interrupt mechanisms.
20	1h RO	**Link Active Reporting Capable (LARC):** This port supports the optional capability of reporting the DL_Active state of the Data Link Control and Management State Machine.
19	0h RO	**Surprise Down Error Reporting Capable (SDERC):** Set to '0' to indicate the Root Port does not support Surprise Down Error Reporting
18	0h RO	**Clock Power Management (CPM):** 0' Indicates that root ports do not support the CLKREQ# mechanism.
17:15	2h RW/O	**L1 Exit Latency (EL1):** Indicates an exit latency of 2us to 4us. 000b: Less than 1 us 001b: 1 us to less than 2 us 010b: 2 us to less than 4 us 011b: 4 us to less than 8 us 100b: 8 us to less than 16 us 101b: 16 us to less than 32 us 110b: 32 us to 64 us 111b: More than 64 us Note: If power management (e.g PLL shutdown) is enabled, BIOS should program this latency to comprehend PLL lock latency.
14:12	4h RO/V	**L0s Exit Latency (EL0):** Indicates an exit latency based upon common-clock configuration: LCTL.CCC Value 0 MPC.UCEL 1 MPC.CCEL
11:10	3h RW/O	**Active State Link PM Support (APMS):** Indicates the level of active state power management on this link Bits Definition 00b: No ASPM Support 01b: L0s Supported 10b: L1 Supported 11b: L0s and L1 Supported
9:4	01h RO/V	**Maximum Link Width (MLW):** Indicates the maximum link width of the link 0x1: x1 Link Width 0x2: x2 Link Width 0x4: x4 Link Width 0x8: x8 Link Width

Bit Range	Default & Access	Field Name (ID): Description
3:0	0h RO/V	**Max Link Speed (MLS):** This field indicates the maximum Link speed of the associated Port. The encoded value specifies a bit location in the Supported Link Speeds Vector (in the Link Capabilities 2 register) that corresponds to the maximum Link speed. Defined encodings are: '0001b': Supported Link Speeds Vector field bit 0. '0010b': Supported Link Speeds Vector field bit 1. '0011b': Supported Link Speeds Vector field bit 2. '0100b': Supported Link Speeds Vector field bit 3. '0101b': Supported Link Speeds Vector field bit 4. '0110b': Supported Link Speeds Vector field bit 5. '0111b': Supported Link Speeds Vector field bit 6. All other encodings are reserved. This field reports a value of 0001b if GEN1 data rate is supported but both GEN2 and GEN3 data rate support are disabled through PCI Express Speed Limit setting or MPC.PCIESD register. This field reports a value of 0010b if both GEN1 and GEN2 data rate are supported but GEN3 data rate support is disabled through PCI Express Speed Limit setting or MPC.PCIESD register. Otherwise, this field reports a value of 0011b.

8.5.25 Link Control (LCTL) — Offset 50h

Link Control

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:7, F:0] + 50h	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:12	0h RO	**Reserved**
11	0h RW	**Link Autonomous Bandwidth Interrupt Enable (LABIE):** Link Autonomous Bandwidth Interrupt Enable - When Set, this bit enables the generation of an interrupt to indicate that the Link Autonomous Bandwidth Status bit has been Set.
10	0h RW	**Link Bandwidth Management Interrupt Enable (LBMIE):** When Set, this bit enables the generation of an interrupt to indicate that the Link Bandwidth Management Status bit has been Set. This bit is not applicable and is reserved for Endpoints, PCI Express-to-PCI/PCI-X bridges, and Upstream Ports of Switches. Functions that do not implement the Link Bandwidth Notification Capability must hardwire this bit to 0b. Default value of this bit is 0b.

Bit Range	Default & Access	Field Name (ID): Description
9	0h RW	**Hardware Autonomous Width Disable (HAWD):** When Set, this bit disables hardware from changing the Link width for reasons other than attempting to correct unreliable Link operation by reducing Link width. Note: When operating as PCI Express, this bit defines the value of the Link Upconfigure Capability in TS2 Ordered Sets. Default value of this bit is 0b.
8	0h RO	**Enable Clock Power Management (ECPM):** Not supported on Root Ports.
7	0h RW	**Extended Synch (ES):** When set, forces extended transmission of FTS ordered sets in FTS and extra TS2 at exit from L1 prior to entering L0.
6	0h RW	**Common Clock Configuration (CCC):** When set, indicates that the Root Port and device are operating with a distributed common reference clock.
5	0h WO	**Retrain Link (RL):** When set, the root port will train its downstream link. This bit always returns '0' when read. Software uses LSTS.LT and LSTS.LTE to check the status of training. It is permitted to write 1b to this bit while simultaneously writing modified values to other fields in this register. If the LTSSM is not already in Recovery or Configuration, the resulting Link training must use the modified values. If the LTSSM is already in Recovery or Configuration, the modified values are not required to affect the Link training that's already in progress.
4	0h RW	**Link Disable (LD):** When set, the root port will disable the link by directing the LTSSM to the Disabled state.
3	0h RW/O	**Read Completion Boundary Control (RCBC):** Indicates the read completion boundary is 64 bytes.
2	0h RO	**Reserved**
1:0	0h RW	**Active State Link PM Control (ASPM):** Indicates whether the root port should enter L0s or L1 or both. Bits Definition 00 Disabled 01 L0s Entry Enabled 10 L1 Entry Enabled 11 L0s and L1 Entry Enabled The value of this register is used unless the Root Port ASPM Control Override Enable register is set, in which case the Root Port ASPM Control Override value is used. Note: If STRPFUSECFG.ASPMDIS is '1', hardware will always see '00' as an output from this register. BIOS reading this register should always return the correct value.

8.5.26 Link Status (LSTS) — Offset 52h

Link Status

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:7, F:0] + 52h	1011h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15	0h RW/1C/V	**Link Autonomous Bandwidth Status (LABS):** This bit is Set by hardware to indicate that hardware has autonomously changed Link speed or width, without the Port transitioning through DL_Down status, for reasons other than to attempt to correct unreliable Link operation. This bit must be set if the Physical Layer reports a speed or width change was initiated by the Downstream component that was indicated as an autonomous change. The default value of this bit is 0b.
14	0h RW/1C/V	**Link Bandwidth Management Status (LBMS):** This bit is Set by hardware to indicate that either of the following has occurred without the Port transitioning through DL_Down status: A Link retraining has completed following a write of 1b to the Retrain Link bit Note: This bit is Set following any write of 1b to the Retrain Link bit, including when the Link is in the process of retraining for some other reason. Hardware has changed Link speed or width to attempt to correct unreliable Link operation, either through an LTSSM timeout or a higher level process This bit must be set if the Physical Layer reports a speed or width change was initiated by the Downstream component that was not indicated as an autonomous change. The default value of this bit is 0b.
13	0h RO/V	**Link Active (LA):** Set to 1b when the Data Link Control and Management State Machine is in the DL_Active state, 0b otherwise.
12	1h RO/V	**Slot Clock Configuration (SCC):** In normal mode, Root Port uses the same reference clock as on the platform and does not generate its own clock. Note: When operating in PCI Express mode, the default of this register bit is dependent on the 'PCIe Non-Common Clock With SSC Mode Enable Strap'. If the strap enables non-common clock with SSC support, this bit shall default to '0'. Otherwise, this bit shall default to '1'.
11	0h RO/V	**Link Training (LT):** The root port sets this bit whenever link training is occurring, or that 1b was written to the Retrain Link bit but Link training has not yet begun. It clears the bit upon completion of link training.
10	0h RO	**Reserved**
9:4	01h RO/V	**Negotiated Link Width (NLW):** Negotiated link width. 0x1: x1 Link Width 0x2: x2 Link Width 0x4: x4 Link Width 0x8: x8 Link Width 0x10: x16 Link Width The value of this register is undefined if the link has not successfully trained.

Bit Range	Default & Access	Field Name (ID): Description
3:0	1h RO/V	**Current Link Speed (CLS):** This field indicates the negotiated Link speed of the given link. The encoded value specifies a bit location in the Supported Link Speeds Vector (in the Link Capabilities 2 register) that corresponds to the current Link speed. Defined encodings are: '0001b': Supported Link Speeds Vector field bit 0. '0010b': Supported Link Speeds Vector field bit 1. '0011b': Supported Link Speeds Vector field bit 2. '0100b': Supported Link Speeds Vector field bit 3. '0101b': Supported Link Speeds Vector field bit 4. '0110b': Supported Link Speeds Vector field bit 5. '0111b': Supported Link Speeds Vector field bit 6. All other encodings are reserved. The value of this field is undefined if the link is not up.

8.5.27 Slot Capabilities (SLCAP) — Offset 54h

Slot Capabilities

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + 54h	00040060h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:19	0000h RW/O	**Physical Slot Number (PSN):** This is a value that is unique to the slot number. BIOS sets this field and it remains set until a platform reset.
18	1h RO	**No Command Completed Support (NCCS):** Set to '1' as this port does not implement a Hot Plug controller and can handle back-2-back writes to all fields of the slot control register without delay between successive writes.
17	0h RO	**Electromechanical Interlock Present (EMIP):** Set to 0 to indicate that no electro-mechanical interlock is implemented.
16:15	0h RW/O	**Slot Power Limit Scale (SLS):** specifies the scale used for the slot power limit value. BIOS sets this field and it remains set until a platform reset.
14:7	00h RW/O	**Slot Power Limit Value (SLV):** Specifies the upper limit (in conjunction with SLS value), on the upper limit on power supplied by the slot. The two values together indicate the amount of power in watts allowed for the slot. BIOS sets this field and it remains set until a platform reset.
6	1h RW/O	**Hot Plug Capable (HPC):** When set, Indicates that hot plug is supported.
5	1h RW/O	**Hot Plug Surprise (HPS):** When set, indicates the device may be removed from the slot without prior notification.

Bit Range	Default & Access	Field Name (ID): Description
4	0h RO	**Power Indicator Present (PIP):** Indicates that a power indicator LED is not present for this slot.
3	0h RO	**Attention Indicator Present (AIP):** Indicates that an attention indicator LED is not present for this slot.
2	0h RO	**MRL Sensor Present (MSP):** Indicates that an MRL sensor is not present
1	0h RO	**Power Controller Present (PCP):** Indicates that a power controller is not implemented for this slot
0	0h RO	**Attention Button Present (ABP):** Indicates that an attention button is not implemented for this slot.

8.5.28 Slot Control (SLCTL) — Offset 58h

Slot Control

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:7, F:0] + 58h	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:14	0h RO	**Reserved**
13	0h RW	**Auto Slot Power Limit Disable (ASPLD):** When set, this bit disables automatic sending of Set_Slot_Power_Limit message when the link transitions from non-DL_Up status to DL_Up status.
12	0h RW	**Data Link Layer State Changed Enable (DLLSCE):** When set, this field enables generation of a hot plug interrupt when the Data Link Layer Link Active field is changed.
11	0h RO	**Electromechanical Interlock Control (EMIC):** This port does not support an Electromechanical Interlock.
10	0h RO	**Power Controller Control (PCC):** This bit has no meaning for module based hot plug.
9:8	0h RO	**Power Indicator Control (PIC):** This register is RO as this port does not implement a Hot Plug Controller.
7:6	0h RO	**Attention Indicator Control (AIC):** This register is RO as this port does not implement a Hot Plug Controller.
5	0h RW	**Hot Plug Interrupt Enable (HPE):** When set, enables generation of a hot plug interrupt on enabled hot plug events.
4	0h RO	**Command Completed Interrupt Enable (CCE):** This register is RO as this port does not implement a Hot Plug Controller.
3	0h RW	**Presence Detect Changed Enable (PDE):** When set, enables the generation of a hot plug interrupt or wake message when the presence detect logic changes state.

Bit Range	Default & Access	Field Name (ID): Description
2	0h RO	**MRL Sensor Changed Enable (MSE):** This register is RO as this port does not implement a Hot Plug Controller.
1	0h RO	**Power Fault Detected Enable (PFE):** This register is RO as this port does not implement a Hot Plug Controller.
0	0h RO	**Attention Button Pressed Enable (ABE):** This register is RO as this port does not implement a Hot Plug Controller.

8.5.29 Slot Status (SLSTS) — Offset 5Ah

Slot Status

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:7, F:0] + 5Ah	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:9	0h RO	**Reserved**
8	0h RW/1C/V	**Data Link Layer State Changed (DLLSC):** This bit is set when the value reported in Data Link Layer Link Active field of the Link Status register is changed. In response to a Data Link Layer State Changed event, software must read Data Link Layer Link Active field of the Link Status register to determine if the link is active before initiating configuration cycles to the hot plugged device.
7	0h RO	**Electromechanical Interlock Status (EMIS):** This port does not support and electromechanical interlock.
6	0h RO/V	**Presence Detect State (PDS):** If XCAP.SI is set (indicating that this root port spawns a slot), then this bit indicates whether a device is connected ('1') or empty ('0'). If XCAP.SI is cleared, this bit is a '1'.
5	0h RO	**MRL Sensor State (MS):** Reserved
4	0h RO	**Command Completed (CC):** This register is RO as this port does not implement a Hot Plug Controller.
3	0h RW/1C/V	**Presence Detect Changed (PDC):** This bit is set by the root port when the PD bit changes state.
2	0h RO	**MRL Sensor Changed (MSC):** MRL sensor is not implemented.
1	0h RO	**Power Fault Detected (PFD):** Power controller is not implemented.
0	0h RO	**Attention Button Pressed (ABP):** This register is RO as this port does not implement an attention button.

8.5.30 Root Control (RCTL) — Offset 5Ch

Root Control

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:7, F:0] + 5Ch	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:4	0h RO	**Reserved**
3	0h RW	**PME Interrupt Enable (PIE):** When set, enables interrupt generation when RSTS.PS is in a set state (either due to a '0' to '1' transition, or due to this bit being set with RSTS.PS already set).
2	0h RW	**System Error on Fatal Error Enable (SFE):** When set, an SERR# will be generated if a fatal error is reported by any of the devices in the hierarchy of this root port, including fatal errors in this root port. This register is not dependent on CMD.SEE being set.
1	0h RW	**System Error on Non-Fatal Error Enable (SNE):** When set, an SERR# will be generated if a non-fatal error is reported by any of the devices in the hierarchy of this root port, including non-fatal errors in this root port. This register is not dependent on CMD.SEE being set.
0	0h RW	**System Error on Correctable Error Enable (SCE):** When set, an SERR# will be generated if a correctable error is reported by any of the devices in the hierarchy of this root port, including correctable errors in this root port. This register is not dependent on CMD.SEE being set.

8.5.31 Root Status (RSTS) — Offset 60h

Root Status

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + 60h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:18	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
17	0h RO/V	**PME Pending (PP):** Indicates another PME is pending when the PME status bit is set. When the original PME is cleared by software, it will be set again, the requestor ID will be updated, and this bit will be cleared. Root Ports have a one deep PME pending queue.
16	0h RW/1C/V	**PME Status (PS):** Indicates that PME was asserted by the requestor ID in RID. Subsequent PMEs are kept pending until this bit is cleared.
15:0	0000h RO/V	**PME Requestor ID (RID):** Indicates the PCI requestor ID of the last PME requestor. Valid only when PS is set. Root ports are capable of storing the requester ID for two PM_PME messages, with one active (this register) and a one deep pending queue. Subsequent PM_PME messages will be dropped.

8.5.32 Device Capabilities 2 (DCAP2) — Offset 64h

Device Capabilities 2

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + 64h	00080837h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:20	0h RO	**Reserved**
19:18	2h RW/O	**Optimized Buffer Flush/Fill Supported (OBFFS):** 00b: OBFF is not supported. 01b: OBFF is supported using Message signaling only. 10b: OBFF is supported using WAKE# signaling only. 11b: OBFF is supported using WAKE# and Message signaling. BIOS should program this field to 00b or 10b during system initialization to advertise the level of hardware OBFF support to software. BIOS should never program this field to 01b or 11b since OBFF messaging is not supported. Note: OBFF is not supported. BIOS should program this field to '00b'.
17:12	0h RO	**Reserved**
11	1h RW/O	**LTR Mechanism Supported (LTRMS):** A value of 1b indicates support for the optional Latency Tolerance Reporting (LTR) mechanism capability. BIOS must write to this register with either a '1' or a '0' to enable/disable the root port from declaring support for the LTR capability.
10	0h RO	**Reserved**
9	0h RW/O	**CAS Completer 128-bit Supported (AC128BS):** Applicable to Functions with Memory Space BARs as well as all Root Ports - must be 0b otherwise. This bit must be set to 1b if the Function supports this optional capability.

Bit Range	Default & Access	Field Name (ID): Description
8	0h RW/O	**AtomicOp Completer 64-bit Supported (AC64BS):** Applicable to Functions with Memory Space BARs as well as all Root Ports - must be 0b otherwise. Includes FetchAdd, Swap, and CAS AtomicOps. This bit must be set to 1b if the Function supports this optional capability
7	0h RW/O	**AtomicOp Completer 32-bit Supported (AC32BS):** Applicable to Functions with Memory Space BARs as well as all Root Ports - must be 0b otherwise. Includes FetchAdd, Swap, and CAS AtomicOps. This bit must be set to 1b if the Function supports this optional capability
6	0h RW/O	**Atomic Routing Supported (ARS):** This bit must be set to 1b if the Port supports this optional capability
5	1h RO	**ARI Forwarding Supported (AFS):** Applicable only to Switch Downstream Ports and Root Ports - must be 0b for other Function types. This bit must be set to 1b if a Switch Downstream Port or Root Port supports this optional capability. Note: This bit is not made RWO to simplify implementation, since there is a requirement that the ARI Forwarding Enable bit must be hardwired to '0b' if ARI Forwarding Supported bit is '0b'. It is low risk to keep this bit '1b'.
4	1h RO	**Completion Timeout Disable Supported (CTDS):** A value of 1b indicates support for the Completion Timeout Disable mechanism.
3:0	7h RO	**Completion Timeout Ranges Supported (CTRS):** This field indicates device support for the optional Completion Timeout programmability mechanism. This mechanism allows system software to modify the Completion Timeout value. This field is applicable only to Root Ports, Endpoints that issue requests on their own behalf, and PCI Express to PCI/PCI-X Bridges that take ownership of requests issued on PCI Express. For all other devices this field is reserved and must be hardwired to 0000b. Four time value ranges are defined: Range A: 50us to 10ms Range B: 10ms to 250ms Range C: 250ms to 4s Range D: 4s to 64s Bits are set according to the table below to show timeout value ranges supported. 0000b Completion Timeout programming not supported. 0001b Range A 0010b Range B 0011b Ranges A & B 0110b Ranges B & C 0111b Ranges A, B & C <-- This is what Root Port supports 1110b Ranges B, C & D 1111b Ranges A, B, C & D All other values are reserved.

8.5.33 Device Control 2 (DCTL2) — Offset 68h

Device Control 2

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:7, F:0] + 68h	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15	0h RO	**Reserved**
14:13	0h RW	**Optimized Buffer Flush/Fill Enable (OBFFEN):** Optimized Buffer Flush/Fill Enable (OBFFEN): 00b Disable OBFF mechanism. 01b Enable OBFF mechanism using Message signaling (Variation A). 10b Enable OBFF mechanism using Message signaling (Variation B). 11b Enable OBFF using WAKE# signaling. Note: Only encoding 00b and 11b are supported. The encoding of 01b or 10b would be aliased to 00b. If DCAP2.OBFFS is clear, programming this field to any non-zero values will have no effect.
12:11	0h RO	**Reserved**
10	0h RW	**LTR Mechanism Enable (LTREN):** When Set to 1b, this bit enables the Latency Tolerance Reporting (LTR) mechanism. For Downstream Ports, this bit must be reset to the default value if the Port goes to DL_Down status. If DCAP2.LTRMS is clear, programming this field to any non-zero values will have no effect.
9:8	0h RO	**Reserved**
7	0h RW	**AtomicOp Egress Blocking (AEB):** Applicable and mandatory for Switch Upstream Ports, Switch Downstream Ports, and Root Ports that implement AtomicOp routing capability - otherwise must be hardwired to 0b. When this bit is Set, AtomicOp Requests that target going out this Egress Port must be blocked.
6	0h RW	**AtomicOp Requester Enable (ARE):** Applicable only to Endpoints and Root Ports - must be hardwired to 0b for other Function types. The Function is allowed to initiate AtomicOp Requests only if this bit and the Bus Master Enable bit in the Command register are both Set. This bit is required to be RW if the Endpoint or Root Port is capable of initiating AtomicOp Requests, but otherwise is permitted to be hardwired to 0b. This bit does not serve as a capability bit. This bit is permitted to be RW even if no AtomicOp Requester capabilities are supported by the Endpoint or Root Port.
5	0h RW	**ARI Forwarding Enable (AFE):** When set, the Downstream Port disables its traditional Device Number field being '0b' enforcement when turning a Type 1 Configuration Request into a Type 0 Configuration Request, permitting access to Extended Functions in an ARI Device immediately below the Port.

Bit Range	Default & Access	Field Name (ID): Description
4	0h RW	**Completion Timeout Disable (CTD):** When set to 1b, this bit disables the Completion Timeout mechanism. This field is required for all devices that support the Completion Timeout Disable Capability. Software is permitted to set or clear this bit at any time. When set, the Completion Timeout detection mechanism is disabled. If there are outstanding requests when the bit is cleared, it is permitted but not required for hardware to apply the completion timeout mechanism to the outstanding requests. If this is done, it is permitted to base the start time for each request on either the time this bit was cleared or the time each request was issued.
3:0	0h RW	**Completion Timeout Value (CTV):** In Devices that support Completion Timeout programmability, this field allows system software to modify the Completion Timeout value. This field is applicable to Root Ports, Endpoints that issue requests on their own behalf, and PCI Express to PCI/PCI-X Bridges that take ownership of requests issued on PCI Express. For all other devices this field is reserved and must be hardwired to 0000b. A Device that does not support this optional capability must hardwire this field to 0000b and is required to implement a timeout value in the range 50us to 50ms. Devices that support Completion Timeout programmability must support the values given below corresponding to the programmability ranges indicated in the Completion Timeout Values Supported field. The Root Port targeted configurable ranges are listed below, along with the range allowed by the PCI Express 2.0 specification. Defined encodings: 0000b Default range: 40-50ms (spec range 50us to 50ms) Values available if Range A (50us to 10 ms) programmability range is supported: 0001b 90-100us (spec range is 50us to 100us) 0010b 9-10ms (spec range is 1ms to 10 ms) Values available if Range B (10ms to 250ms) programmability range is supported: 0101b 40-50ms (spec range is 16ms to 55ms) 0110b 160-170ms (spec range is 65ms to 210ms) Values available if Range C (250ms to 4s) programmability range is supported: 1001b 400-500ms (spec range is 260ms to 900ms) 1010b 1.6-1.7s (spec range is 1s to 3.5s) Values not defined above are Reserved. Software is permitted to change the value in this field at any time. For requests already pending when the Completion Timeout Value is changed, hardware is permitted to use either the new or the old value for the outstanding requests, and is permitted to base the start time for each request either on when this value was changed or on when each request was issued.

8.5.34 Device Status 2 (DSTS2) — Offset 6Ah

Device Status 2

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:7, F:0] + 6Ah	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
15:0	0h RO	**Reserved**

8.5.35 Link Capabilities 2 (LCAP2) — Offset 6Ch

Link Capabilities 2

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + 6Ch	0000000Eh

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:23	0h RO	**Reserved**
22:16	00h RO	**Lower SKP OS Reception Supported Speeds Vector (LSOSRSS):** If this field is non-zero, it indicates that the Port, when operating at the indicated speed(s) supports SRIS and also supports receiving SKP OS at the rate defined for SRNS while running in SRIS. Bit definitions within this field are: Bit 0 2.5 GT/s Bit 1 5.0 GT/s Bit 2 8.0 GT/s Bits 6:3 RsvdP Behavior is undefined if a bit is set in this field and the corresponding bit is not set in the Supported Link Speeds Vector.
15:9	00h RO	**Lower SKP OS Generation Supported Speeds Vector (LSOSGSSV):** If this field is non-zero, it indicates that the Port, when operating at the indicated speed(s) supports SRIS and also supports software control of the SKP Ordered Set transmission scheduling rate. Bit definitions within this field are: Bit 0 2.5 GT/s Bit 1 5.0 GT/s Bit 2 8.0 GT/s Bits 6:3 RsvdP Behavior is undefined if a bit is set in this field and the corresponding bit is not set in the Supported Link Speeds Vector.

Bit Range	Default & Access	Field Name (ID): Description
8	0h RO	**Crosslink Supported (CS):** No support for Crosslink.
7:1	07h RO/V	**Supported Link Speeds Vector (SLSV):** This field indicates the supported Link speed of the associated Port. For each bit, a value of 1b indicates that the corresponding Link speed is supported - otherwise, the Link speed is not supported. Bit definitions within this field for PCI Express are: Bit 0: 2.5 GT/s. Bit 1: 5.0 GT/s. Bit 2: 8.0 GT/s. Bits 6:3: Reserved.
0	0h RO	**Reserved**

8.5.36 Link Control 2 (LCTL2) — Offset 70h

Link Control 2

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:7, F:0] + 70h	0001h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:12	0h RW/P	**Compliance Preset/De-emphasis (CD):** For 8.0 GT/s Data Rate: This field sets the Transmitter Preset in Polling.Compliance state if the entry occurred due to the Enter Compliance bit being 1b. Results are undefined if a reserved preset encoding is used when entering Polling.Compliance in this way. For 5.0 GT/s Data Rate: This bit sets the de-emphasis level in Polling.Compliance state if the entry occurred due to the Enter Compliance bit being 1b. Encodings: 0001b -3.5 dB 0000b -6 dB When the Link is operating at 2.5 GT/s, the setting of this field has no effect. The default value of this field is 0000b. This bit is intended for debug, compliance testing purposes. System firmware and software is allowed to modify this bit only during debug or compliance testing. In all other cases, the system must ensure that this field is set to the default value.
11	0h RW/P	**Compliance SOS (CSOS):** When set to 1b, the LTSSM is required to send SKP Ordered Sets periodically in between the (modified) compliance patterns. The default value of this bit is 0b. This bit is applicable when the Link is operating at 2.5 GT/s or 5.0 GT/s data rates only.

Bit Range	Default & Access	Field Name (ID): Description
10	0h RW/P	**Enter Modified Compliance (EMC):** When this bit is set to 1b, the device transmits Modified Compliance Pattern if the LTSSM enters Polling.Compliance substate. Default value of this bit is 0b. This register is intended for debug, compliance testing purposes only. System firmware and software is allowed to modify this register only during debug or compliance testing. In all other cases, the system must ensure that this register is set to the default value.
9:7	0h RW/P	**Transmit Margin (TM):** This field controls the value of the nondeemphasized voltage level at the Transmitter pins. This field is reset to 000b on entry to the LTSSM Polling.Configuration substate (see PCI Express Chapter 4 for details of how the Transmitter voltage level is determined in various states). Encodings: 000b Normal operating range 001b 800-1200 mV for full swing and 400-700 mV for half-swing 010b - (n-1) Values must be monotonic with a non-zero slope. The value of n must be greater than 3 and less than 7. At least two of these must be below the normal operating range of n: 200-400 mV for full-swing and 100-200 mV for half-swing n - 111b reserved For a Multi-Function device associated with an Upstream Port, the field in Function 0 is of type RWS, and only Function 0 controls the component's Link behavior. In all other Functions of that device, this field is of type RsvdP. Default value of this field is 000b. Components that support only the 2.5 GT/s speed are permitted to hardwire this bit to 000b. This register is intended for debug, compliance testing purposes only. System firmware and software is allowed to modify this register only during debug or compliance testing. In all other cases, the system must ensure that this register is set to the default value.
6	0h RW/P	**Selectable De-emphasis (SD):** When the Link is operating at 5.0 GT/s speed, this bit selects the level of de-emphasis for an Upstream component. Encodings: 1b -3.5 dB 0b -6 dB When the Link is not operating at 5.0 GT/s speed, the setting of this bit has no effect.
5	0h RO	**Reserved**
4	0h RW/P	**Enter Compliance (EC):** Software is permitted to force a Link to enter Compliance mode at the speed indicated in the Target Link Speed field by setting this bit to 1b in both components on a Link and then initiating a hot reset on the Link. Default value of this bit following Fundamental Reset is 0b. This bit is intended for debug, compliance testing purposes only. System firmware and software is allowed to modify this bit only during debug or compliance testing. In all other cases, the system must ensure that this bit is set to the default value.

Bit Range	Default & Access	Field Name (ID): Description
3:0	1h RW/V/P	**Target Link Speed (TLS):** This field sets an upper limit on Link operational speed by restricting the values advertised by the upstream component in its training sequences. The encoded value specifies a bit location in the Supported Link Speeds Vector (in the Link Capabilities 2 register) that corresponds to the current Link speed. Defined encodings are: '0001b': Supported Link Speeds Vector field bit 0. '0010b': Supported Link Speeds Vector field bit 1. '0011b': Supported Link Speeds Vector field bit 2. '0100b': Supported Link Speeds Vector field bit 3. '0101b': Supported Link Speeds Vector field bit 4. '0110b': Supported Link Speeds Vector field bit 5. '0111b': Supported Link Speeds Vector field bit 6. All other encodings are reserved. If a value is written to this field that does not correspond to a supported speed, as indicated by the Supported Link Speeds Vector, the result is undefined. The default value of this field is GEN1. Note: This register field could be used by REUT software to limit the link speed to 2.5 GT/s or 5 GT/s data rate.

8.5.37 Link Status 2 (LSTS2) — Offset 72h

Link Status 2

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:7, F:0] + 72h	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:6	0h RO	**Reserved**
5	0h RW/1C/V/P	**Link Equalization Request (LER):** This bit is set by hardware to request the Link equalization process to be performed on the Link.
4	0h RO/V/P	**Equalization Phase 3 Successful (EQP3S):** When set to 1, this bit indicates that Phase 3 of the Transmitter Equalization procedure has successfully completed.
3	0h RO/V/P	**Equalization Phase 2 Successful (EQP2S):** When set to 1, this bit indicates that Phase 2 of the Transmitter Equalization procedure has successfully completed.
2	0h RO/V/P	**Equalization Phase 1 Successful (EQP1S):** When set to 1, this bit indicates that Phase 1 of the Transmitter Equalization procedure has successfully completed.
1	0h RO/V/P	**Equalization Complete (EQC):** When set to 1, this bit indicates that the Transmitter Equalization procedure has completed.

Bit Range	Default & Access	Field Name (ID): Description
0	0h RO/V	**Current De-emphasis Level (CDL):** When the Link is operating at 5.0 GT/s speed, this bit reflects the level of de-emphasis. Encodings: 1b -3.5 dB 0b -6 dB The value in this bit is undefined when the Link is not operating at 5.0 GT/s speed.

8.5.38 Slot Capabilities 2 (SLCAP2) — Offset 74h

Slot Capabilities 2

Note: Bit definitions are the same as DSTS2, offset 6Ah.

8.5.39 Slot Control 2 (SLCTL2) — Offset 78h

Slot Control 2

Note: Bit definitions are the same as DSTS2, offset 6Ah.

8.5.40 Slot Status 2 (SLSTS2) — Offset 7Ah

Slot Status 2

Note: Bit definitions are the same as DSTS2, offset 6Ah.

8.5.41 Message Signaled Interrupt Identifiers (MID) — Offset 80h

Message Signaled Interrupt Identifiers

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:7, F:0] + 80h	9005h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:8	90h RW/O	**Next Pointer (NEXT):** Indicates the location of the next capability in the list. The default value of this register is 90h which points to the Subsystem Vendor capability structure. BIOS can determine which capabilities will be exposed by including or removing them from the capability linked list. As this register is RWO, BIOS must write a value to this register, even if it is to re-write the default value.

Bit Range	Default & Access	Field Name (ID): Description
7:0	05h RO	**Capability ID (CID):** Capabilities ID indicates MSI.

8.5.42 Message Signaled Interrupt Message (MC) — Offset 82h

Message Signaled Interrupt Message

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:7, F:0] + 82h	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:8	0h RO	**Reserved**
7	0h RO	**64 Bit Address Capable (C64):** Capable of generating a 32-bit message only.
6:4	0h RW	**Multiple Message Enable (MME):** These bits are RW for software compatibility, but only one message is ever sent by the root port.
3:1	0h RO	**Multiple Message Capable (MMC):** Only one message is required.
0	0h RW	**MSI Enable (MSIE):** If set, MSI is enabled and traditional interrupt pins are not used to generate interrupts. CMD.BME must be set for an MSI to be generated. If CMD.BME is cleared, and this bit is set, no interrupts (not even pin based) are generated.

8.5.43 Message Signaled Interrupt Message Address (MA) — Offset 84h

Message Signaled Interrupt Message Address

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + 84h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:2	00000000h RW	**ADDR:** Lower 32 bits of the system specified message address, always DW aligned.
1:0	0h RO	**Reserved**

8.5.44 Message Signaled Interrupt Message Data (MD) — Offset 88h

Message Signaled Interrupt Message Data

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:7, F:0] + 88h	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:0	0000h RW	**DATA:** This 16-bit field is programmed by system software if MSI is enabled. Its content is driven onto the lower word (PCI AD[15:0]) during the data phase of the MSI memory write transaction.

8.5.45 Subsystem Vendor Capability (SVCAP) — Offset 90h

Subsystem Vendor Capability

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:7, F:0] + 90h	A00Dh

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:8	A0h RW/O	**Next Capability (NEXT):** Indicates the location of the next capability in the list. The default value of this register is A0h which points to the PCI Power Management capability structure. BIOS can determine which capabilities will be exposed by including or removing them from the capability linked list. As this register is RWO, BIOS must write a value to this register, even if it is to re-write the default value.
7:0	0Dh RO	**Capability Identifier (CID):** Value of 0Dh indicates this is a PCI bridge subsystem vendor capability.

8.5.46 Subsystem Vendor IDs (SVID) — Offset 94h

Subsystem Vendor IDs

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + 94h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:16	0000h RW/O	**Subsystem Identifier (SID):** Indicates the subsystem as identified by the vendor. This field is write once and is locked down until a bridge reset occurs (not the PCI bus reset).
15:0	0000h RW/O	**Subsystem Vendor Identifier (SVID):** Indicates the manufacturer of the subsystem. This field is write once and is locked down until a bridge reset occurs (not the PCI bus reset).

8.5.47 Power Management Capability (PMCAP) — Offset A0h

Power Management Capability

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:7, F:0] + A0h	0001h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
15:8	00h RO	**Next Capability (NEXT):** Indicates this is the last item in the list.
7:0	01h RO	**Capability Identifier (CID):** Value of 01h indicates this is a PCI power management capability.

8.5.48 PCI Power Management Capabilities (PMC) — Offset A2h

PCI Power Management Capabilities

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:7, F:0] + A2h	C803h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
15:11	19h RO	**PMES:** Indicates PME# is supported for states D0, D3HOT and D3COLD. The root port does not generate PME#, but reporting that it does is necessary for legacy Windows operating systems to enable PME# in devices connected behind this root port.
10	0h RO	**D2S:** The D2 state is not supported.
9	0h RO	**D1S:** The D1 state is not supported.
8:6	0h RO	**AC:** Reports 375mA maximum suspend well current required when in the D3COLD state.
5	0h RO	**Device Specific Initialization (DSI):** Indicates that no device-specific initialization is required.
4	0h RO	**Reserved**
3	0h RO	**PME Clock (PMEC):** Indicates that PCI clock is not required to generate PME#.
2:0	3h RO	**VS:** Indicates support for Revision 1.2 of the PCI Power Management Specification.

8.5.49 PCI Power Management Control (PMCS) — Offset A4h

PCI Power Management Control

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + A4h	00000008h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:24	00h RO	**DTA:** Reserved
23	0h RO	**Bus Power / Clock Control Enable (BPCE):** This field is reserved per PCI Express specification
22	0h RO	**B2/B3 Support (B23S):** This field is reserved per PCI Express specification.
21:16	0h RO	**Reserved**
15	0h RO	**PME Status (PMES):** Indicates a PME was received on the downstream link.
14:13	0h RO	**Data Scale (DSC):** Reserved
12:9	0h RO	**Data Select (DSEL):** Reserved
8	0h RW/P	**PME Enable (PMEE):** Indicates PME is enabled. The root port takes no action on this bit, but it must be RW for legacy Windows operating systems to enable PME# on devices connected to this root port.
7:4	0h RO	**Reserved**
3	1h RW/O	**No Soft Reset (NSR):** When set to 1 this bit indicates that devices transitioning from D3hot to D0 because of Power State commands do not perform an internal reset. Configuration context is preserved. Upon transition from D3hot to D0 Initialized state, no additional operating system intervention is required to preserve Configuration Context beyond writing the Power State bits. When clear, devices do perform an internal reset upon transitioning from D3hot to D0 via software control of the Power State bits. Configuration Context is lost when performing the soft reset. Upon transition from D3hot to D0 state, full reinitialization sequence is needed to return the device to D0 Initialized. Regardless of this bit, devices that transition from D3hot to D0 by a system or bus segment reset will return to the device state D0 Uninitialized with only PME context preserved if PME is supported and enabled.
2	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
1:0	0h RW	**Power State (PS):** This field is used both to determine the current power state of the root port and to set a new power state. The values are: 00: D0 state 11: D3HOT state When in the D3HOT state, the controller's configuration space is available, but the I/O and memory spaces are not. Type 1 configuration cycles are also not accepted. Interrupts are not required to be blocked as software will disable interrupts prior to placing the port into D3HOT. If software attempts to write a '10' or '01' to these bits, the write will be ignored.

8.5.50 Advanced Error Extended (AECH) — Offset 100h

Advanced Error Extended

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + 100h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:20	000h RW/O	**Next Capability Offset (NCO):** Points to the next capability.
19:16	0h RW/O	**Capability Version (CV):** For systems that support AER, BIOS should write a 1h to this register else it should write 0
15:0	0000h RW/O	**Capability ID (CID):** For systems that support AER, BIOS should write a 0001h to this register else it should write 0

8.5.51 Uncorrectable Error Status (UES) — Offset 104h

Uncorrectable Error Status

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + 104h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:27	0h RO	**Reserved**
26	0h RW/1C/V/P	**Poisoned TLP Egress Blocked Status (PTLPEBS):** Indicates that poisoned TLP Egress Blocked error has occurred. Note: This bit can only be set if DPCCAPR.PTLPEBS = '1' and DPCCTLR.PTLPEBE = '1'.
25	0h RO	**Reserved**
24	0h RW/1C/V/P	**AtomicOp Egress Blocked Status (AEBS):** AtomicOp Egress Blocked Status
23:22	0h RO	**Reserved**
21	0h RW/1C/V/P	**ACS Violation Status (AVS):** Indicates an ACS Violation is logged.
20	0h RW/1C/V/P	**Unsupported Request Error Status (URE):** Indicates an unsupported request was received.
19	0h RO	**ECRC Error Status (EE):** ECRC is not supported.
18	0h RW/1C/V/P	**Malformed TLP Status (MT):** Indicates a malformed TLP was received.
17	0h RW/1C/V/P	**Receiver Overflow Status (RO):** Indicates a receiver overflow occurred.
16	0h RW/1C/V/P	**Unexpected Completion Status (UC):** Indicates an unexpected completion was received.
15	0h RW/1C/V/P	**Completer Abort Status (CA):** Indicates a completer abort was received
14	0h RW/1C/V/P	**Completion Timeout Status (CT):** Indicates a completion timed out. This is signaled if Completion Timeout is enabled and a completion fails to return within the amount of time specified by the Completion Timeout Value
13	0h RO	**Flow Control Protocol Error Status (FCPE):** Not supported.
12	0h RW/1C/V/P	**Poisoned TLP Status (PT):** Indicates a poisoned TLP was received.

Bit Range	Default & Access	Field Name (ID): Description
11:6	0h RO	**Reserved**
5	0h RO	**Surprise Down Error Status (SDE):** Surprise Down is not supported.
4	0h RW/1C/V/P	**Data Link Protocol Error Status (DLPE):** Indicates a data link protocol error occurred.
3:1	0h RO	**Reserved**
0	0h RO	**Training Error Status (TE):** Not supported.

8.5.52 Uncorrectable Error Mask (UEM) — Offset 108h

Uncorrectable Error Mask

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + 108h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:27	0h RO	**Reserved**
26	0h RW/P	**Poisoned TLP Egress Blocked Mask (PTLPEBM):** Mask for Poisoned TLP Egress Blocked error.
25	0h RO	**Reserved**
24	0h RW/P	**AtomicOp Egress Blocked Mask (AEBM):** Mask for AtomicOp Egress Blocked
23:22	0h RO	**Reserved**
21	0h RW/P	**ACS Violation Mask (AVM):** Mask for ACS Violation errors.
20	0h RW/P	**Unsupported Request Error Mask (URE):** Mask for uncorrectable errors.
19	0h RO	**ECRC Error Mask (EE):** ECRC is not supported.
18	0h RW/P	**Malformed TLP Mask (MT):** Mask for malformed TLPs
17	0h RW/P	**Receiver Overflow Mask (RO):** Mask for receiver overflows.

Bit Range	Default & Access	Field Name (ID): Description
16	0h RW/P	**Unexpected Completion Mask (UC):** Mask for unexpected completions.
15	0h RW/P	**Completer Abort Mask (CM):** Mask for completer abort.
14	0h RW/P	**Completion Timeout Mask (CT):** Mask for completion timeouts.
13	0h RO	**Flow Control Protocol Error Mask (FCPE):** Not supported.
12	0h RW/P	**Poisoned TLP Mask (PT):** Mask for poisoned TLPs.
11:6	0h RO	**Reserved**
5	0h RO	**Surprise Down Error Mask (SDE):** Surprise Down is not supported.
4	0h RW/P	**Data Link Protocol Error Mask (DLPE):** Mask for data link protocol errors.
3:1	0h RO	**Reserved**
0	0h RO	**Training Error Mask (TE):** Not supported.

8.5.53 Uncorrectable Error Severity (UEV) — Offset 10Ch

Uncorrectable Error Severity

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + 10Ch	00060010h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:27	0h RO	**Reserved**
26	0h RW/P	**Poisoned TLP Egress Blocked Severity (PTLPEBS):** Severity for Poisoned TLP Egress Blocked error.
25	0h RO	**Reserved**
24	0h RW/P	**AtomicOp Egress Blocked Severity (AEBS):** AtomicOp Egress Blocked Severity
23:22	0h RO	**Reserved**
21	0h RW/P	**ACS Violation Severity (AVS):** Severity for ACS Violation.

Bit Range	Default & Access	Field Name (ID): Description
20	0h RW/P	**Unsupported Request Error Severity (URE):** Severity for unsupported request reception.
19	0h RO	**ECRC Error Severity (EE):** ECRC is not supported.
18	1h RW/P	**Malformed TLP Severity (MT):** Severity for malformed TLP reception.
17	1h RW/P	**Receiver Overflow Severity (RO):** Severity for receiver overflow occurrences.
16	0h RW/P	**Unexpected Completion Severity (UC):** Severity for unexpected completion reception.
15	0h RW/P	**Completer Abort Severity (CA):** Severity for completer abort.
14	0h RW/P	**Completion Timeout Severity (CT):** Severity for completion timeout.
13	0h RO	**Flow Control Protocol Error Severity (FCPE):** Not supported.
12	0h RW/P	**Poisoned TLP Severity (PT):** Severity for poisoned TLP reception.
11:6	0h RO	**Reserved**
5	0h RO	**Surprise Down Error Severity (SDE):** Surprise Down is not supported.
4	1h RW/P	**Data Link Protocol Error Severity (DLPE):** Severity for data link protocol errors.
3:1	0h RO	**Reserved**
0	0h RO	**Training Error Severity (TE):** TE not supported.

8.5.54 Correctable Error Status (CES) — Offset 110h

Correctable Error Status

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + 110h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:14	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
13	0h RW/1C/V/P	**Advisory Non-Fatal Error Status (ANFES):** When set, indicates that an Advisory Non-Fatal Error occurred.
12	0h RW/1C/V/P	**Replay Timer Timeout Status (RTT):** Indicates the replay timer timed out.
11:9	0h RO	**Reserved**
8	0h RW/1C/V/P	**Replay Number Rollover Status (RNR):** Indicates the replay number rolled over.
7	0h RW/1C/V/P	**Bad DLLP Status (BD):** Indicates a bad DLLP was received.
6	0h RW/1C/V/P	**Bad TLP Status (BT):** Indicates a bad TLP was received.
5:1	0h RO	**Reserved**
0	0h RW/1C/V/P	**Receiver Error Status (RE):** Indicates a receiver error occurred.

8.5.55 Correctable Error Mask (CEM) — Offset 114h

Correctable Error Mask

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + 114h	00002000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:14	0h RO	**Reserved**
13	1h RW/P	**Advisory Non-Fatal Error Mask (ANFEM):** When set, masks Advisory Non-Fatal errors from (a) signaling ERR_COR to the device control register and (b) updating the Uncorrectable Error Status register. This register is set by default to enable compatibility with software that does not comprehend Role-Based Error Reporting.
12	0h RW/P	**Replay Timer Timeout Mask (RTT):** Mask for replay timer timeout.
11:9	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
8	0h RW/P	**Replay Number Rollover Mask (RNR):** Mask for replay number rollover.
7	0h RW/P	**Bad DLLP Mask (BD):** Mask for bad DLLP reception.
6	0h RW/P	**Bad TLP Mask (BT):** Mask for bad TLP reception.
5:1	0h RO	**Reserved**
0	0h RW/P	**Receiver Error Mask (RE):** Mask for receiver errors.

8.5.56 Advanced Error Capabilities And Control (AECC) — Offset 118h

Advanced Error Capabilities And Control

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + 118h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:13	0h RO	**Reserved**
12	0h RO	**Completion Timeout Prefix/Header Log Capable (CTPHLC):** If set, this bit indicates that port records the prefix/header of Request TLPs that experience a Completion Timeout error. Note: BIOS should program this bit before enable the Completion Timeout mechanism.
11:9	0h RO	**Reserved**
8	0h RO	**ECRC Check Enable (ECE):** ECRC is not supported.
7	0h RO	**ECRC Check Capable (ECC):** ECRC is not supported.
6	0h RO	**ECRC Generation Enable (EGE):** ECRC is not supported.
5	0h RO	**ECRC Generation Capable (EGC):** ECRC is not supported.
4:0	00h RO/V/P	**First Error Pointer (FEP):** Identifies the bit position of the first error reported in the Uncorrectable Error Status Register.

8.5.57 Header Log (HL_DW1) — Offset 11Ch

Header Log

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + 11Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RO/V/P	**1st dWord of TLP (DW1):** Byte0 && Byte1 && Byte2 && Byte3

8.5.58 Header Log (HL_DW2) — Offset 120h

Header Log

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + 120h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RO/V/P	**2nd dWord of TLP (DW2):** Byte4 && Byte5 && Byte6 && Byte7

8.5.59 Header Log (HL_DW3) — Offset 124h

Header Log

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + 124h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RO/V/P	**3rd dWord of TLP (DW3):** Byte8 && Byte9 && Byte10 && Byte11

8.5.60 Header Log (HL_DW4) — Offset 128h

Header Log

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + 128h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RO/V/P	**4th dWord of TLP (DW4):** Byte12 && Byte13 && Byte14 && Byte15

8.5.61 Root Error Command (REC) — Offset 12Ch

Root Error Command

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + 12Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:3	0h RO	**Reserved**
2	0h RW	**Fatal Error Reporting Enable (FERE):** When set, the root port will generate an interrupt when a fatal error is reported by the attached device.
1	0h RW	**Non-fatal Error Reporting Enable (NERE):** When set, the root port will generate an interrupt when a non-fatal error is reported by the attached device.
0	0h RW	**Correctable Error Reporting Enable (CERE):** When set, the root port will generate an interrupt when a correctable error is reported by the attached device.

8.5.62 Root Error Status (RES) — Offset 130h

Root Error Status

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + 130h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:27	00h RO	**Advanced Error Interrupt Message Number (AEMN):** Reserved
26:7	0h RO	**Reserved**
6	0h RW/1C/V/P	**Fatal Error Messages Received (FEMR):** Set when one or more Fatal Uncorrectable Error Messages have been received.
5	0h RW/1C/V/P	**Non-Fatal Error Messages Received (NFEMR):** Set when one or more Non-Fatal Uncorrectable error messages have been received
4	0h RW/1C/V/P	**First Uncorrectable Fatal (FUF):** Set when the first Uncorrectable Error message received is for a fatal error.

Bit Range	Default & Access	Field Name (ID): Description
3	0h RW/1C/V/P	**Multiple ERR_FATAL/NONFATAL Received (MENR):** Set when either a fatal or a non-fatal error is received and the ENR bit is already set.
2	0h RW/1C/V/P	**ERR_FATAL/NONFATAL Received (ENR):** Set when either a fatal or a non-fatal error message is received.
1	0h RW/1C/V/P	**Multiple ERR_COR Received (MCR):** Set when a correctable error message is received and the ERR_COR bit is already set.
0	0h RW/1C/V/P	**ERR_COR Received (CR):** Set when a correctable error message is received.

8.5.63 Error Source Identification (ESID) — Offset 134h

Error Source Identification

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + 134h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:16	0000h RO/V/P	**ERR_FATAL/NONFATAL Source Identification (EFNFSID):** Loaded with the requester ID indicated in the received ERR_FATAL or ERR_NONFATAL message when RES.ENR is first set, or the internal requestor ID if an internally detected error.
15:0	0000h RO/V/P	**ERR_COR Source Identification (ECSID):** Loaded with the requester ID indicated in the received ERR_COR message when RES.CR is first set, or the internal requester ID if an internally detected error.

8.5.64 PTM Extended Capability Header (PTMECH) — Offset 150h

PTM Extended Capability Header

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + 150h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:20	000h RW/O	**Next Capability Offset (NCO):** Points to the next capability.
19:16	0h RW/O	**Capability Version (CV):** For systems that support PTM Extended Capability, BIOS should write a 1h to this register else it should write 0.
15:0	0000h RW/O	**Capability ID (CID):** For systems that support PTM Extended Capability, BIOS should write a 001Fh to this register else it should write 0.

8.5.65 PTM Capability Register (PTMCAPR) — Offset 154h

PTM Capability Register

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + 154h	00000400h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:16	0h RO	**Reserved**
15:8	04h RW/O	**Local Clock Granularity (LCG):** 0000 0000b: Time Source does not implement a local clock. It simply propagates timing information obtained from further Upstream in the PTM Hierarchy when responding to PTM Request messages. 0000 0001b - 1111 1110b: Indicates the period of this Time Source's local clock in ns. 1111 1111b: Indicates the period of this Time Source's local clock is greater than 254 ns. If the PTM Root Select bit is Set, this local clock is used to provide PTM Master Time. Otherwise, the Time Source uses this local clock to locally track PTM Master Time received from further Upstream within a PTM Hierarchy.
7:3	0h RO	**Reserved**
2	0h RW/O	**PTM Root Capable (PTMRC):** Root Ports must set this bit to 1b.

Bit Range	Default & Access	Field Name (ID): Description
1	0h RW/O	**PTM Responder Capable (PTMRSPC):** Root Ports are permitted to set this bit to 1b to indicate that they implement the PTM Responder role.
0	0h RO	**PTM Requester Capable (PTMREQC):** PTM Requester Role is not supported by Root Port.

8.5.66 PTM Control Register (PTMCTLR) — Offset 158h

PTM Control Register

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + 158h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:16	0h RO	**Reserved**
15:8	00h RO	**Effective Granularity (EG):** Root Port does not support PTM Requester role.
7:2	0h RO	**Reserved**
1	0h RW	**Root Select (RS):** When Set, if the PTM Enable bit is also Set, this Time Source is the PTM Root. Within each PTM Hierarchy, it is recommended that system software select only the furthest Upstream Time Source to be the PTM Root.
0	0h RW	**PTM Enable (PTME):** When Set, this Function is permitted to participate in the PTM mechanism according to its selected role. Software must not have the PTM Enable bit Set in the PTM Control register on a Function associated with an Upstream Port unless the associated Downstream Port on the Link already has the PTM Enable bit Set in its associated PTM Control register.

8.5.67 ACS Extended Capability Header (ACSECH) — Offset 220h

ACS Extended Capability Header

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + 220h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:20	000h RW/O	**Next Capability Offset (NCO):** Points to the next capability.
19:16	0h RW/O	**Capability Version (CV):** For systems that support ACS Extended Capability, BIOS should write a 1h to this register else it should write 0.
15:0	0000h RW/O	**Capability ID (CID):** For systems that support ACS Extended Capability, BIOS should write a 000Dh to this register else it should write 0.

8.5.68 ACS Capability Register (ACSCAPR) — Offset 224h

ACS Capability Register

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:7, F:0] + 224h	000Fh

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:7	0h RO	**Reserved**
6	0h RO	**ACS Direct Translated P2P (T):** ACS Direct Translated P2P is not supported.
5	0h RO	**ACS P2P Egress Control (E):** ACS P2P Egress Control is not supported.
4	0h RW/O	**ACS Upstream Forwarding (U):** ACS Upstream Forwarding.
3	1h RW/O	**ACS P2P Completion Redirect (C):** Required for all Functions that support ACS P2P Request Redirect - must be hardwired to 0b otherwise. If 1b, indicates that the component implements ACS P2P Completion Redirect.

Bit Range	Default & Access	Field Name (ID): Description
2	1h RW/O	**ACS P2P Request Redirect (R):** Required for Root Ports that support peer-to-peer traffic with other Root Ports - required for Switch Downstream Ports - required for multi-function device Functions that support peer-to-peer traffic with other Functions - must be hardwired to 0b otherwise. If 1b, indicates that the component implements ACS P2P Request Redirect.
1	1h RW/O	**ACS Translation Blocking (B):** Required for Root Ports and Switch Downstream Ports - must be hardwired to 0b otherwise. If 1b, indicates that the component implements ACS Translation Blocking.
0	1h RW/O	**ACS Source Validation (V):** Required for Root Ports and Switch Downstream Ports - must be hardwired to 0b otherwise. If 1b, indicates that the component implements ACS Source Validation.

8.5.69 ACS Control Register (ACSCTLR) — Offset 226h

ACS Control Register

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:7, F:0] + 226h	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:7	0h RO	**Reserved**
6	0h RO	**ACS Direct Translated P2P Enable (TE):** ACS Direct Translated P2P is not supported.
5	0h RO	**ACS P2P Egress Control Enable (EE):** ACS P2P Egress Control is not supported.
4	0h RW	**ACS Upstream Forwarding Enable (UE):** ACS Upstream Forwarding.
3	0h RW	**ACS P2P Completion Redirect Enable (CE):** Determines when the component redirects peer-to-peer Completions upstream - applicable only to Read Completions whose Relaxed Ordering Attribute is clear. Requests are never affected by ACS P2P Completion Redirect. Default value of this field is 0b.
2	0h RW	**ACS P2P Request Redirect Enable (RE):** Determines when the component redirects peer-to-peer memory Requests targeting another peer port upstream. I/O, Configuration, VDM Messages and Completions are never affected by ACS P2P Request Redirect. Default value of this field is 0b.

Bit Range	Default & Access	Field Name (ID): Description
1	0h RW	**ACS Translation Blocking Enable (BE):** When set, the component blocks all upstream Memory Requests whose Address Translation (AT) field is not set to the default value. I/O, Configuration, Completions and Messages are never affected by ACS Translation Blocking. Default value of this field is 0b.
0	0h RW	**ACS Source Validation Enable (VE):** When set, the component validates the Bus Number from the Requester ID of upstream Requests against the secondary / subordinate Bus Numbers. I/O, Configuration and Completions are never affected by ACS Source Validation. Default value of this field is 0b.

8.5.70 DPC Extended Capability Header (DPCECH) — Offset A00h

DPC Extended Capability Header

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + A00h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:20	000h RW/O	**Next Capability Offset (NCO):** Points to the next capability.
19:16	0h RW/O	**Capability Version (CV):** For systems that support DPC Extended Capability, BIOS should write a 1h to this register else it should write 0.
15:0	0000h RW/O	**Capability ID (CID):** For systems that support DPC Extended Capability, BIOS should write a 001Dh to this register else it should write 0.

8.5.71 DPC Capability Register (DPCCAPR) — Offset A04h

DPC Capability Register

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:7, F:0] + A04h	14E0h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:13	0h RO	**Reserved**
12	1h RW/O	**DL_Active ERR_COR Signaling Supported (DLAECSS):** This field when set, indicates that the Root Port supports the ability to signal with ERR_COR when the link transitions to the DL_Active state. Root Port that supports RP Extensions for DPC must set this bit.
11:8	4h RW/O	**RP PIO Log Size (RPPIOLS):** This field indicates how many DWORDs are allocated for the RP PIO log registers, comprised by the RP PIO Header Log, RP PIO ImpSpec Log and RP PIO TLP Prefix Log. If the Root Port supports RP Extensions for DPC, the value of this field must be 4 or greater - otherwise the value of this field must be 0.
7	1h RW/O	**DPC Software Triggering Supported (DPCSTS):** This field when set, indicates that the Root Port supports the ability for software to trigger DPC. Root Ports that support RP Extensions for DPC must set this bit.
6	1h RW/O	**Poisoned TLP Egress Blocking Supported (PTLPEBS):** This field when set, indicates that the Root Port supports the ability to block the transmission of a poisoned TLP from its Egress port. Root Ports that support RP Extensions for DPC must set this bit.
5	1h RW/O	**RP Extensions For DPC (RPEFDPC):** This field when set, indicates that a Root Port supports a defined set of DPC Extensions that are specific to Root Ports.
4:0	00h RW/O	**DPC Interrupt Message Number (DPCIMN):** This field indicates which MSI/MSI-X vector is used for the interrupt message generated in association with the DPC Capability structure. For MSI, the value in this field indicates the offset between the base Message Data and the interrupt message that is generated. Hardware is required to update this field so that it is correct if the number of MSI Messages assigned to the Function changes when software writes to the Multiple Message Enable field in the MSI Message Control register. For MSI-X, the value in this field indicates which MSI-X Table entry is used to generate the interrupt message. The entry must be one of the first 32 entries even if the Function implements more than 32 entries. For a given MSI-X implementation, the entry must remain constant. If both MSI and MSI-X are implemented, they are permitted to use different vectors, though software is permitted to enable only one mechanism at a time. If MSI-X is enabled, the value in this field must indicate the vector for MSI-X. If MSI is enabled or neither is enabled, the value in this field must indicate the vector for MSI. If software enables both MSI and MSI-X at the same time, the value in this field is undefined. Note: BIOS is expected to update this field with the right value before enabling DPC interrupt.

8.5.72 DPC Control Register (DPCCTLR) — Offset A06h

DPC Control Register

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:7, F:0] + A06h	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:8	0h RO	**Reserved**
7	0h RW	**DL_Active ERR_COR Enable (DLAECE):** This bit when set, enables the downstream port to signal ERR_COR when the link transitions to the DL_Active state.
6	0h RW/1S/V	**DPC Software Trigger (DPCST):** If DPC Trigger is enabled and the DPC Trigger Status bit is clear, software writing a 1b to this bit will cause DPC to be triggered. If DPC Trigger is not enabled or DPC Trigger Status is set, software writing a 1b to this bit has no effect. Note: It is permitted to write 1b to this bit while simultaneously writing updated values to other fields in this register, notably the DPC Trigger Enable field. For this case, the DPC Software Trigger semantics are based on the updated value of the DPC Trigger Enable field. *Note: This bit always return 0b when read.
5	0h RW	**Poisoned TLP Egress Blocking Enable (PTLPEBE):** This bit, when set, enables the associated Egress Port to block the transmission of poisoned TLP.
4	0h RW	**DPC ERR_COR Enable (DPCECE):** When set, this bit enables the generation of an interrupt to indicate that DPC has been triggered.
3	0h RW	**DPC Interrupt Enable (DPCIE):** When set, this bit enables the generation of an interrupt to indicate that DPC has been triggered.
2	0h RW	**DPC Completion Control (DPCCC):** This bit controls the Completion Status for completions formed during DPC. '0b': Completer Abort(CA) Completion Status. '1b': Unsupported Request(UR) Completion Status.
1:0	0h RW	**DPC Trigger Enable (DPCTE):** This field enables DPC and controls the conditions that cause DPC to be triggered. '00b': DPC is disabled. '01b': DPC is enabled and is triggered when the Downstream Port detects an unmasked uncorrectable error or when the Downstream Port receives an ERR_FATAL message. '10b': DPC is enabled and is triggered when the Downstream Port detects an unmasked uncorrectable error or when the Downstream Port receives an ERR_NONFATAL or ERR_FATAL message. '11b': Reserved.

8.5.73 DPC Status Register (DPCSR) — Offset A08h

DPC Status Register

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:7, F:0] + A08h	1F00h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
15:13	0h RO	**Reserved**
12:8	1Fh RO/V/P	**RP PIO First Error Pointer (RPPIOFEP):** The value of this field identifies a bit position in the RP PIO Status register, and this field is considered valid when that bit is set. When this field is valid, and software writes a 1b to the indicated RP PIO Status bit(thus clearing it), this field must revert to its default value. This field is applicable only for Root Ports that support RP Extensions for DPC, and is otherwise reserved. If this field is not reserved, the default value is 11111b.
7	0h RO	**Reserved**
6:5	0h RO/V/P	**DPC Trigger Extension (DPCTE):** This field serves as an extension to the DPC Trigger Reason field. When that field is valid and has a value of 11b, this field indicates why DPC has been triggered. '00b': DPC was triggered due to RP PIO error. '01b': DPC was triggered due to DPC Software Trigger bit. '10b': Reserved. '11b': Reserved. This field is valid only when the DPC Trigger Status bit is set and the value of the DPC Trigger Reason field is 11b. Otherwise the value of this field is undefined.
4	0h RO	**DPC RP Busy (DPCRPB):** When the DPC Trigger Status bit is Set and this bit is Set, the Root Port is busy with internal activity that must complete before software is permitted to clear the DPC Trigger Status bit. If software Clears the DPC Trigger Status bit while this bit is set, the behavior is undefined. This field is valid only when the DPC Trigger Status bit is Set - otherwise the value of this field is undefined. This bit is applicable only for Root Ports that support RP Extensions for DPC, and is Reserved otherwise.
3	0h RW/1C/V/P	**DPC Interrupt Status (DPCIS):** This bit is set if DPC is triggered while the DPC Interrupt Enable bit is set.
2:1	0h RO/V/P	**DPC Trigger Reason (DPCTR):** This field indicates why DPC has been triggered. '00b': DPC was triggered due to an unmasked uncorrectable error. '01b': DPC was triggered due to receiving an ERR_NONFATAL. '10b': DPC was triggered due to receiving an ERR_FATAL. '11b': DPC was triggered due to a reason that is indicated by the DPC Trigger Reason Extension field. Note: This field is only valid when DPC Trigger Status bit is set - otherwise the value of this field is undefined.

Bit Range	Default & Access	Field Name (ID): Description
0	0h RW/1C/V/P	**DPC Trigger Status (DPCTS):** When set, indicates that DPC has been triggered. DPC is event triggered. While this bit is set, hardware must direct the LTSSM to the Disabled state. This bit must be cleared before the LTSSM can be released from Disabled state. Once the requirements for how long software must leave the downstream port in DPC is met, software is permitted to clear this bit regardless of the state of other status bits associated with the triggering event. Refer to PCIe Base specification 3.0 for more timing requirements pertaining to this bit.

8.5.74 DPC Error Source ID Register (DPCESIDR) — Offset A0Ah

DPC Error Source ID Register

Type	Size	Offset	Default
PCI	16 bit	[B:0, D:7, F:0] + A0Ah	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
15:0	0000h RO/V/P	**DPC Error Source ID (DPCESID):** When the DPC Trigger Reason field indicates that DPC was triggered due to the reception of an ERR_NONFATAL or ERR_FATAL message, this register field contains the Requester ID of the received messages. Otherwise, the value of this register is undefined.

8.5.75 RP PIO Status Register (RPPIOSR) — Offset A0Ch

RP PIO Status Register

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + A0Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:19	0h RO	**Reserved**
18	0h RW/1C/V/P	**Memory Completion Timeout Status (MCTS):** Non-posted memory request completion times out.

Bit Range	Default & Access	Field Name (ID): Description
17	0h RW/1C/V/P	**Memory Completer Abort Completion Status (MCACS):** Non-posted memory request received CA completion.
16	0h RW/1C/V/P	**Memory Unsupported Request Completion Status (MURCS):** Non-posted Memory request received UR completion.
15:11	0h RO	**Reserved**
10	0h RW/1C/V/P	**I/O Completion Timeout Status (IOCTS):** I/O request completion times out.
9	0h RW/1C/V/P	**I/O Completer Abort Completion Status (IOCACS):** I/O request received CA completion.
8	0h RW/1C/V/P	**I/O Unsupported Request Completion Status (IOURCS):** I/O request received UR completion.
7:3	0h RO	**Reserved**
2	0h RW/1C/V/P	**Configuration Completion Timeout Status (CCTS):** Configuration request completion times out.
1	0h RW/1C/V/P	**Configuration Completer Abort Completion Status (CCACS):** Configuration request received CA completion.
0	0h RW/1C/V/P	**Configuration Unsupported Request Completion Status (CURCS):** Configuration request received UR completion.

8.5.76 RP PIO Mask Register (RPPIOMR) — Offset A10h

RP PIO Mask Register

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + A10h	00070707h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:19	0h RO	**Reserved**
18	1h RW/P	**Memory Completion Timeout Mask (MCTM):** Mask bit for Memory Completion Timeout Status.
17	1h RW/P	**Memory Completer Abort Completion Mask (MCACM):** Mask bit for Memory Completer Abort Completion Status.

Bit Range	Default & Access	Field Name (ID): Description
16	1h RW/P	**Memory Unsupported Request Completion Mask (MURCM):** Mask bit for Memory Unsupported Request Completion Status.
15:11	0h RO	**Reserved**
10	1h RW/P	**I/O Completion Timeout Mask (IOCTM):** Mask bit for I/O Completion Timeout Status.
9	1h RW/P	**I/O Completer Abort Completion Mask (IOCACM):** Mask bit for I/O Completer Abort Completion Status.
8	1h RW/P	**I/O Unsupported Request Completion Mask (IOURCM):** Mask bit for I/O Unsupported Request Completion Status.
7:3	0h RO	**Reserved**
2	1h RW/P	**Configuration Completion Timeout Mask (CCTM):** Mask bit for Configuration Completion Timeout Status.
1	1h RW/P	**Configuration Completer Abort Completion Mask (CCACM):** Mask bit for Configuration Completer Abort Status.
0	1h RW/P	**Configuration Unsupported Request Completion Mask (CURCM):** Mask bit for Configuration Unsupported Request Completion Status.

8.5.77 RP PIO Severity Register (RPPIOVR) — Offset A14h

RP PIO Severity Register

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + A14h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:19	0h RO	**Reserved**
18	0h RW/P	**Memory Completion Timeout Severity (MCTSV):** Severity bit for Memory Completion Timeout Status.
17	0h RW/P	**Memory Completer Abort Completion Severity (MCACSV):** Severity bit for Memory Completer Abort Completion Status.
16	0h RW/P	**Memory Unsupported Request Completion Severity (MURCSV):** Severity bit for Memory Unsupported Request Completion Status.
15:11	0h RO	**Reserved**
10	0h RW/P	**I/O Completion Timeout Severity (IOCTSV):** Severity bit for I/O Completion Timeout Status.
9	0h RW/P	**I/O Completer Abort Completion Severity (IOCACSV):** Severity bit for I/O Completer Abort Completion Status.

Bit Range	Default & Access	Field Name (ID): Description
8	0h RW/P	**I/O Unsupported Request Completion Severity (IOURCSV):** Severity bit for I/O Unsupported Request Completion Status.
7:3	0h RO	**Reserved**
2	0h RW/P	**Configuration Completion Timeout Severity (CCTSV):** Severity bit for Configuration Completion Timeout Status.
1	0h RW/P	**Configuration Completer Abort Completion Severity (CCACSV):** Severity bit for Configuration Completer Abort Status.
0	0h RW/P	**Configuration Unsupported Request Completion Severity (CURCSV):** Severity bit for Configuration Unsupported Request Completion Status.

8.5.78 RP PIO SysError Register (RPPIOSER) — Offset A18h

RP PIO SysError Register

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + A18h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:19	0h RO	**Reserved**
18	0h RW/P	**Memory Completion Timeout SysErr (MCTSE):** SysErr bit for Memory Completion Timeout Status.
17	0h RW/P	**Memory Completer Abort Completion SysErr (MCACSE):** SysErr bit for Memory Completer Abort Completion Status.
16	0h RW/P	**Memory Unsupported Request Completion SysErr (MURCSE):** SysErr bit for Memory Unsupported Request Completion Status.
15:11	0h RO	**Reserved**
10	0h RW/P	**I/O Completion Timeout SysErr (IOCTSE):** SysErr bit for I/O Completion Timeout Status.
9	0h RW/P	**I/O Completer Abort Completion SysErr (IOCACSE):** SysErr bit for I/O Completer Abort Completion Status.
8	0h RW/P	**I/O Unsupported Request Completion SysErr (IOURCSE):** SysErr bit for I/O Unsupported Request Completion Status.
7:3	0h RO	**Reserved**
2	0h RW/P	**Configuration Completion Timeout SysErr (CCTSE):** SysErr bit for Configuration Completion Timeout Status.
1	0h RW/P	**Configuration Completer Abort Completion SysErr (CCACSE):** SysErr bit for Configuration Completer Abort Status.

Bit Range	Default & Access	Field Name (ID): Description
0	0h RW/P	**Configuration Unsupported Request Completion SysErr (CURCSE):** SysErr bit for Configuration Unsupported Request Completion Status.

8.5.79 RP PIO Exception Register (RPPIOER) — Offset A1Ch

RP PIO Exception Register

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + A1Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:19	0h RO	**Reserved**
18	0h RW/P	**Memory Completion Timeout Exception (MCTE):** Exception bit for Memory Completion Timeout Status.
17	0h RW/P	**Memory Completer Abort Completion Exception (MCACE):** Exception bit for Memory Completer Abort Completion Status.
16	0h RW/P	**Memory Unsupported Request Completion Exception (MURCE):** Exception bit for Memory Unsupported Request Completion Status.
15:11	0h RO	**Reserved**
10	0h RW/P	**I/O Completion Timeout Exception (IOCTE):** Exception bit for I/O Completion Timeout Status.
9	0h RW/P	**I/O Completer Abort Completion Exception (IOCACE):** Exception bit for I/O Completer Abort Completion Status.
8	0h RW/P	**I/O Unsupported Request Completion Exception (IOURCE):** Exception bit for I/O Unsupported Request Completion Status.
7:3	0h RO	**Reserved**
2	0h RW/P	**Configuration Completion Timeout Exception (CCTE):** Exception bit for Configuration Completion Timeout Status.
1	0h RW/P	**Configuration Completer Abort Completion Exception (CCACE):** Exception bit for Configuration Completer Abort Status.
0	0h RW/P	**Configuration Unsupported Request Completion Exception (CURCE):** Exception bit for Configuration Unsupported Request Completion Status.

8.5.80 RP PIO Header Log DW1 Register (RPPIOHLR_DW1) — Offset A20h

RP PIO Header Log DW1 Register

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + A20h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RO/V/P	**1st dWord of TLP (DW1):** Byte0 AND Byte1 AND Byte2 AND Byte3.

8.5.81 RP PIO Header Log DW2 Register (RPPIOHLR_DW2) — Offset A24h

RP PIO Header Log DW2 Register

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + A24h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RO/V/P	**2nd dWord of TLP (DW2):** Byte4 AND Byte5 AND Byte6 AND Byte7.

8.5.82 RP PIO Header Log DW3 Register (RPPIOHLR_DW3) — Offset A28h

RP PIO Header Log DW3 Register

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + A28h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RO/V/P	**3rd dWord of TLP (DW3):** Byte8 AND Byte9 AND Byte10 AND Byte11.

8.5.83 RP PIO Header Log DW4 Register (RPPIOHLR_DW4) — Offset A2Ch

RP PIO Header Log DW4 Register

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + A2Ch	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000h RO/V/P	**4th dWord of TLP (DW4):** Byte12 AND Byte13 AND Byte14 AND Byte15.

8.5.84 Secondary PCI Express Extended Capability Header (SPEECH) — Offset A30h

Secondary PCI Express Extended Capability Header

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + A30h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:20	000h RW/O	**Next Capability Offset (NCO):** This field contains the offset to the next PCI Express Capability structure or 000h if no other items exist in the linked list of Capabilities. For Extended Capabilities implemented in Configuration Space, this offset is relative to the beginning of PCI compatible Configuration Space and thus must always be either 000h (for terminating list of Capabilities) or greater than 0FFh. The bottom 2 bits of this offset are Reserved and must be implemented as 00b and software must mask them to allow for future uses of these bits.
19:16	0h RW/O	**Capability Version (CV):** This field is a PCI-SIG defined version number that indicates the version of the Capability structure present. For systems that support Secondary PCI Express Extended Capability, BIOS should write a 1h to this register else it should write 0.
15:0	0000h RW/O	**PCI Express Extended Capability ID (PCIEECID):** This field is a PCI-SIG defined ID number that indicates the nature and format of the Extended Capability. PCI Express Extended Capability ID for the Secondary PCI Express Extended Capability is 0019h. For systems that support Secondary PCI Express Extended Capability, BIOS should write a 0019h to this register else it should write 0.

8.5.85 Link Control 3 (LCTL3) — Offset A34h

Link Control 3

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + A34h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:16	0h RO	**Reserved**

Bit Range	Default & Access	Field Name (ID): Description
15:9	00h RO	**Enable Lower SKP OS Generation Vector (ELSOSGV):** When the Link is in L0 and the bit in this field corresponding to the current Link speed is Set, SKP Ordered Sets are scheduled at the rate defined for SRNS, overriding the rate required based on the clock tolerance architecture. Bit definitions within this field are: Bit 0 2.5 GT/s Bit 1 5.0 GT/s Bit 2 8.0 GT/s Bits 6:3 Rsvd Behavior is undefined if a bit is Set in this field and the corresponding bit in the Lower SKP OS Generation Supported Speeds Vector is not set.
8:2	0h RO	**Reserved**
1	0h RW	**Link Equalization Request Interrupt Enable (LERIE):** When set, this bit enables the generation of an interrupt to indicate that the Link Equalization Request bit has been set.
0	0h RW/1S/V	**Perform Equalization (PE):** When this bit is 1b and Link Retrain bit is set with the Target Link Speed field set to 8 GT/s, the Downstream Port must perform Link Equalization. This bit is cleared by Root Port upon entry to Link Equalization Phase 1.

8.5.86 Lane Error Status (LES) — Offset A38h

Lane Error Status

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + A38h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:16	0h RO	**Reserved**
15	0h RW/1C/V/P	**Lane 15 Error Status (L15ES):** Lane 15 detected a Lane-based error.
14	0h RW/1C/V/P	**Lane 14 Error Status (L14ES):** Lane 14 detected a Lane-based error.
13	0h RW/1C/V/P	**Lane 13 Error Status (L13ES):** Lane 13 detected a Lane-based error.
12	0h RW/1C/V/P	**Lane 12 Error Status (L12ES):** Lane 12 detected a Lane-based error.

Bit Range	Default & Access	Field Name (ID): Description
11	0h RW/1C/V/P	**Lane 11 Error Status (L11ES):** Lane 11 detected a Lane-based error.
10	0h RW/1C/V/P	**Lane 10 Error Status (L10ES):** Lane 10 detected a Lane-based error.
9	0h RW/1C/V/P	**Lane 9 Error Status (L9ES):** Lane 9 detected a Lane-based error.
8	0h RW/1C/V/P	**Lane 8 Error Status (L8ES):** Lane 8 detected a Lane-based error.
7	0h RW/1C/V/P	**Lane 7 Error Status (L7ES):** Lane 7 detected a Lane-based error.
6	0h RW/1C/V/P	**Lane 6 Error Status (L6ES):** Lane 6 detected a Lane-based error.
5	0h RW/1C/V/P	**Lane 5 Error Status (L5ES):** Lane 5 detected a Lane-based error.
4	0h RW/1C/V/P	**Lane 4 Error Status (L4ES):** Lane 4 detected a Lane-based error.
3	0h RW/1C/V/P	**Lane 3 Error Status (L3ES):** Lane 3 detected a Lane-based error.
2	0h RW/1C/V/P	**Lane 2 Error Status (L2ES):** Lane 2 detected a Lane-based error.
1	0h RW/1C/V/P	**Lane 1 Error Status (L1ES):** Lane 1 detected a Lane-based error.
0	0h RW/1C/V/P	**Lane 0 Error Status (L0ES):** Lane 0 detected a Lane-based error.

8.5.87 Lane 0 And Lane 1 Equalization Control (L01EC) — Offset A3Ch

Lane 0 And Lane 1 Equalization Control

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + A3Ch	7F7F7F7Fh

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RO	**Reserved**
30:28	7h RW	**Upstream Port Lane 1 Receiver Preset Hint (UPL1RPH):** Field contains the Receiver Preset Hint value sent or received during Link Equalization. Port Direction: Downstream Port Crosslink Supported: Any Usage: Contains value sent on the associated Lane during Link EQ.
27:24	Fh RW	**Upstream Port Lane 1 Transmitter Preset (UPL1TP):** Field contains the Transmitter Preset value sent or received during Link Equalization. Port Direction: Downstream Port Crosslink Supported: Any Usage: Contains value sent on the associated Lane during Link EQ.
23	0h RO	**Reserved**
22:20	7h RW	**Downstream Port Lane 1 Receiver Preset Hint (DPL1RPH):** Receiver Preset Hint may be used as a hint for receiver equalization by this Port when the Port is operating as a Downstream Port.
19:16	Fh RW	**Downstream Port Lane 1 Transmitter Preset (DPL1TP):** Transmitter Preset used for equalization by this Port when the Port is operating as a Downstream Port. This field is ignored when the Port is operating as an Upstream Port.
15	0h RO	**Reserved**
14:12	7h RW	**Upstream Port Lane 0 Receiver Preset Hint (UPL0RPH):** Field contains the Receiver Preset Hint value sent or received during Link Equalization. Port Direction: Downstream Port Crosslink Supported: Any Usage: Contains value sent on the associated Lane during Link EQ.
11:8	Fh RW	**Upstream Port Lane 0 Transmitter Preset (UPL0TP):** Field contains the Transmitter Preset value sent or received during Link Equalization. Port Direction: Downstream Port Crosslink Supported: Any Usage: Contains value sent on the associated Lane during Link EQ.
7	0h RO	**Reserved**
6:4	7h RW	**Downstream Port Lane 0 Receiver Preset Hint (DPL0RPH):** Receiver Preset Hint may be used as a hint for receiver equalization by this Port when the Port is operating as a Downstream Port.

Bit Range	Default & Access	Field Name (ID): Description
3:0	Fh RW	**Downstream Port Lane 0 Transmitter Preset (DPL0TP):** Transmitter Preset used for equalization by this Port when the Port is operating as a Downstream Port. This field is ignored when the Port is operating as an Upstream Port.

8.5.88 Lane 2 And Lane 3 Equalization Control (L23EC) — Offset A40h

Lane 2 And Lane 3 Equalization Control

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + A40h	7F7F7F7Fh

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RO	**Reserved**
30:28	7h RW	**Upstream Port Lane 3 Receiver Preset Hint (UPL3RPH):** Field contains the Receiver Preset Hint value sent or received during Link Equalization. Port Direction: Downstream Port Crosslink Supported: Any Usage: Contains value sent on the associated Lane during Link EQ.
27:24	Fh RW	**Upstream Port Lane 3 Transmitter Preset Hint (UPL3TP):** Field contains the Transmitter Preset Hint value sent or received during Link Equalization. Port Direction: Downstream Port Crosslink Supported: Any Usage: Contains value sent on the associated Lane during Link EQ.
23	0h RO	**Reserved**
22:20	7h RW	**Downstream Port Lane 3 Receiver Preset Hint (DPL3RPH):** Receiver Preset Hint may be used as a hint for receiver equalization by this Port when the Port is operating as a Downstream Port.
19:16	Fh RW	**Downstream Port Lane 3 Transmitter Preset (DPL3TP):** Transmitter Preset used for equalization by this Port when the Port is operating as a Downstream Port. This field is ignored when the Port is operating as an Upstream Port.
15	0h RO	**Reserved**
14:12	7h RW	**Upstream Port Lane 2 Receiver Preset Hint (UPL2RPH):** Field contains the Receiver Preset Hint value sent or received during Link Equalization. Port Direction: Downstream Port Crosslink Supported: Any Usage: Contains value sent on the associated Lane during Link EQ.

Bit Range	Default & Access	Field Name (ID): Description
11:8	Fh RW	**Upstream Port Lane 2 Transmitter Preset (UPL2TP):** Field contains the Transmitter Preset Hint value sent or received during Link Equalization. Port Direction: Downstream Port Crosslink Supported: Any Usage: Contains value sent on the associated Lane during Link EQ.
7	0h RO	**Reserved**
6:4	7h RW	**Downstream Port Lane 2 Receiver Preset Hint (DPL2RPH):** Receiver Preset Hint may be used as a hint for receiver equalization by this Port when the Port is operating as a Downstream Port.
3:0	Fh RW	**Downstream Port Lane 2 Transmitter Preset (DPL2TP):** Transmitter Preset used for equalization by this Port when the Port is operating as a Downstream Port. This field is ignored when the Port is operating as an Upstream Port.

8.5.89 Lane 4 And Lane 5 Equalization Control (L45EC) — Offset A44h

Lane 4 And Lane 5 Equalization Control

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + A44h	7F7F7F7Fh

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RO	**Reserved**
30:28	7h RW	**Upstream Port Lane 5 Receiver Preset Hint (UPL5RPH):** Field contains the Receiver Preset Hint value sent or received during Link Equalization. Port Direction: Downstream Port Crosslink Supported: Any Usage: Contains value sent on the associated Lane during Link EQ.
27:24	Fh RW	**Upstream Port Lane 5 Transmitter Preset (UPL5TP):** Field contains the Transmitter Preset value sent or received during Link Equalization. Port Direction: Downstream Port Crosslink Supported: Any Usage: Contains value sent on the associated Lane during Link EQ.
23	0h RO	**Reserved**
22:20	7h RW	**Downstream Port Lane 5 Receiver Preset Hint (DPL5RPH):** Receiver Preset Hint may be used as a hint for receiver equalization by this Port when the Port is operating as a Downstream Port.

Bit Range	Default & Access	Field Name (ID): Description
19:16	Fh RW	**Downstream Port Lane 5 Transmitter Preset (DPL5TP):** Transmitter Preset used for equalization by this Port when the Port is operating as a Downstream Port. This field is ignored when the Port is operating as an Upstream Port.
15	0h RO	**Reserved**
14:12	7h RW	**Upstream Port Lane 4 Receiver Preset Hint (UPL4RPH):** Field contains the Receiver Preset Hint value sent or received during Link Equalization. Port Direction: Downstream Port Crosslink Supported: Any Usage: Contains value sent on the associated Lane during Link EQ.
11:8	Fh RW	**Upstream Port Lane 4 Transmitter Preset (UPL4TP):** Field contains the Transmitter Preset value sent or received during Link Equalization. Port Direction: Downstream Port Crosslink Supported: Any Usage: Contains value sent on the associated Lane during Link EQ.
7	0h RO	**Reserved**
6:4	7h RW	**Downstream Port Lane 4 Receiver Preset Hint (DPL4RPH):** Receiver Preset Hint may be used as a hint for receiver equalization by this Port when the Port is operating as a Downstream Port.
3:0	Fh RW	**Downstream Port Lane 4 Transmitter Preset (DPL4TP):** Transmitter Preset used for equalization by this Port when the Port is operating as a Downstream Port. This field is ignored when the Port is operating as an Upstream Port.

8.5.90 Lane 6 And Lane 7 Equalization Control (L67EC) — Offset A48h

Lane 6 And Lane 7 Equalization Control

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + A48h	7F7F7F7Fh

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RO	**Reserved**
30:28	7h RW	**Upstream Port Lane 7 Receiver Preset Hint (UPL7RPH):** Field contains the Receiver Preset Hint value sent or received during Link Equalization. Port Direction: Downstream Port Crosslink Supported: Any Usage: Contains value sent on the associated Lane during Link EQ.

Bit Range	Default & Access	Field Name (ID): Description
27:24	Fh RW	**Upstream Port Lane 7 Transmitter Preset (UPL7TP):** Field contains the Transmitter Preset Hint value sent or received during Link Equalization. Port Direction: Downstream Port Crosslink Supported: Any Usage: Contains value sent on the associated Lane during Link EQ.
23	0h RO	**Reserved**
22:20	7h RW	**Downstream Port Lane 7 Receiver Preset Hint (DPL7RPH):** Receiver Preset Hint may be used as a hint for receiver equalization by this Port when the Port is operating as a Downstream Port.
19:16	Fh RW	**Downstream Port Lane 7 Transmitter Preset (DPL7TP):** Transmitter Preset used for equalization by this Port when the Port is operating as a Downstream Port. This field is ignored when the Port is operating as an Upstream Port.
15	0h RO	**Reserved**
14:12	7h RW	**Upstream Port Lane 6 Receiver Preset Hint (UPL6RPH):** Field contains the Receiver Preset Hint value sent or received during Link Equalization. Port Direction: Downstream Port Crosslink Supported: Any Usage: Contains value sent on the associated Lane during Link EQ.
11:8	Fh RW	**Upstream Port Lane 6 Transmitter Preset (UPL6TP):** Field contains the Transmitter Preset Hint value sent or received during Link Equalization. Port Direction: Downstream Port Crosslink Supported: Any Usage: Contains value sent on the associated Lane during Link EQ.
7	0h RO	**Reserved**
6:4	7h RW	**Downstream Port Lane 6 Receiver Preset Hint (DPL6RPH):** Receiver Preset Hint may be used as a hint for receiver equalization by this Port when the Port is operating as a Downstream Port.
3:0	Fh RW	**Downstream Port Lane 6 Transmitter Preset (DPL6TP):** Transmitter Preset used for equalization by this Port when the Port is operating as a Downstream Port. This field is ignored when the Port is operating as an Upstream Port.

8.5.91 Lane 8 And Lane 9 Equalization Control (L89EC) — Offset A4Ch

Lane 8 And Lane 9 Equalization Control

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + A4Ch	7F7F7F7Fh

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RO	**Reserved**
30:28	7h RW	**Upstream Port Lane 9 Receiver Preset Hint (UPL9RPH):** Field contains the Receiver Preset Hint value sent or received during Link Equalization. Port Direction: Downstream Port Crosslink Supported: Any Usage: Contains value sent on the associated Lane during Link EQ.
27:24	Fh RW	**Upstream Port Lane 9 Transmitter Preset (UPL9TP):** Field contains the Transmitter Preset Hint value sent or received during Link Equalization. Port Direction: Downstream Port Crosslink Supported: Any Usage: Contains value sent on the associated Lane during Link EQ.
23	0h RO	**Reserved**
22:20	7h RW	**Downstream Port Lane 9 Receiver Preset Hint (DPL9RPH):** Receiver Preset Hint may be used as a hint for receiver equalization by this Port when the Port is operating as a Downstream Port.
19:16	Fh RW	**Downstream Port Lane 9 Transmitter Preset (DPL9TP):** Transmitter Preset used for equalization by this Port when the Port is operating as a Downstream Port. This field is ignored when the Port is operating as an Upstream Port.
15	0h RO	**Reserved**
14:12	7h RW	**Upstream Port Lane 8 Receiver Preset Hint (UPL8RPH):** Field contains the Receiver Preset Hint value sent or received during Link Equalization. Port Direction: Downstream Port Crosslink Supported: Any Usage: Contains value sent on the associated Lane during Link EQ.
11:8	Fh RW	**Upstream Port Lane 8 Transmitter Preset (UPL8TP):** Field contains the Transmitter Preset Hint value sent or received during Link Equalization. Port Direction: Downstream Port Crosslink Supported: Any Usage: Contains value sent on the associated Lane during Link EQ.
7	0h RO	**Reserved**
6:4	7h RW	**Downstream Port Lane 8 Receiver Preset Hint (DPL8RPH):** Receiver Preset Hint may be used as a hint for receiver equalization by this Port when the Port is operating as a Downstream Port.

Bit Range	Default & Access	Field Name (ID): Description
3:0	Fh RW	**Downstream Port Lane 8 Transmitter Preset (DPL8TP):** Transmitter Preset used for equalization by this Port when the Port is operating as a Downstream Port. This field is ignored when the Port is operating as an Upstream Port.

8.5.92 Lane 10 And Lane 11 Equalization Control (L1011EC) — Offset A50h

Lane 10 And Lane 11 Equalization Control

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + A50h	7F7F7F7Fh

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RO	**Reserved**
30:28	7h RW	**Upstream Port Lane 11 Receiver Preset Hint (UPL11RPH):** Field contains the Receiver Preset Hint value sent or received during Link Equalization. Port Direction: Downstream Port Crosslink Supported: Any Usage: Contains value sent on the associated Lane during Link EQ.
27:24	Fh RW	**Upstream Port Lane 11 Transmitter Preset (UPL11TP):** Field contains the Transmitter Preset Hint value sent or received during Link Equalization. Port Direction: Downstream Port Crosslink Supported: Any Usage: Contains value sent on the associated Lane during Link EQ.
23	0h RO	**Reserved**
22:20	7h RW	**Downstream Port Lane 11 Receiver Preset Hint (DPL11RPH):** Receiver Preset Hint may be used as a hint for receiver equalization by this Port when the Port is operating as a Downstream Port.
19:16	Fh RW	**Downstream Port Lane 11 Transmitter Preset (DPL11TP):** Transmitter Preset used for equalization by this Port when the Port is operating as a Downstream Port. This field is ignored when the Port is operating as an Upstream Port.
15	0h RO	**Reserved**
14:12	7h RW	**Upstream Port Lane 10 Receiver Preset Hint (UPL10RPH):** Field contains the Receiver Preset Hint value sent or received during Link Equalization. Port Direction: Downstream Port Crosslink Supported: Any Usage: Contains value sent on the associated Lane during Link EQ.

Bit Range	Default & Access	Field Name (ID): Description
11:8	Fh RW	**Upstream Port Lane 10 Transmitter Preset (UPL10TP):** Field contains the Transmitter Preset Hint value sent or received during Link Equalization. Port Direction: Downstream Port Crosslink Supported: Any Usage: Contains value sent on the associated Lane during Link EQ.
7	0h RO	**Reserved**
6:4	7h RW	**Downstream Port Lane 10 Receiver Preset Hint (DPL10RPH):** Receiver Preset Hint may be used as a hint for receiver equalization by this Port when the Port is operating as a Downstream Port.
3:0	Fh RW	**Downstream Port Lane 10 Transmitter Preset (DPL10TP):** Transmitter Preset used for equalization by this Port when the Port is operating as a Downstream Port. This field is ignored when the Port is operating as an Upstream Port.

8.5.93 Lane 12 And Lane 13 Equalization Control (L1213EC) — Offset A54h

Lane 12 And Lane 13 Equalization Control

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + A54h	7F7F7F7Fh

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RO	**Reserved**
30:28	7h RW	**Upstream Port Lane 13 Receiver Preset Hint (UPL13RPH):** Field contains the Receiver Preset Hint value sent or received during Link Equalization. Port Direction: Downstream Port Crosslink Supported: Any Usage: Contains value sent on the associated Lane during Link EQ.
27:24	Fh RW	**Upstream Port Lane 13 Transmitter Preset (UPL13TP):** Field contains the Transmitter Preset Hint value sent or received during Link Equalization. Port Direction: Downstream Port Crosslink Supported: Any Usage: Contains value sent on the associated Lane during Link EQ.
23	0h RO	**Reserved**
22:20	7h RW	**Downstream Port Lane 13 Receiver Preset Hint (DPL13RPH):** Receiver Preset Hint may be used as a hint for receiver equalization by this Port when the Port is operating as a Downstream Port.

Bit Range	Default & Access	Field Name (ID): Description
19:16	Fh RW	**Downstream Port Lane 13 Transmitter Preset (DPL13TP):** Transmitter Preset used for equalization by this Port when the Port is operating as a Downstream Port. This field is ignored when the Port is operating as an Upstream Port.
15	0h RO	**Reserved**
14:12	7h RW	**Upstream Port Lane 12 Receiver Preset Hint (UPL12RPH):** Field contains the Receiver Preset Hint value sent or received during Link Equalization. Port Direction: Downstream Port Crosslink Supported: Any Usage: Contains value sent on the associated Lane during Link EQ.
11:8	Fh RW	**Upstream Port Lane 12 Transmitter Preset (UPL12TP):** Field contains the Transmitter Preset Hint value sent or received during Link Equalization. Port Direction: Downstream Port Crosslink Supported: Any Usage: Contains value sent on the associated Lane during Link EQ.
7	0h RO	**Reserved**
6:4	7h RW	**Downstream Port Lane 12 Receiver Preset Hint (DPL12RPH):** Receiver Preset Hint may be used as a hint for receiver equalization by this Port when the Port is operating as a Downstream Port.
3:0	Fh RW	**Downstream Port Lane 12 Transmitter Preset (DPL12TP):** Transmitter Preset used for equalization by this Port when the Port is operating as a Downstream Port. This field is ignored when the Port is operating as an Upstream Port.

8.5.94 Lane 14 And Lane 15 Equalization Control (L1415EC) — Offset A58h

Lane 14 And Lane 15 Equalization Control

Type	Size	Offset	Default
PCI	32 bit	[B:0, D:7, F:0] + A58h	7F7F7F7Fh

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RO	**Reserved**
30:28	7h RW	**Upstream Port Lane 15 Receiver Preset Hint (UPL15RPH):** Field contains the Receiver Preset Hint value sent or received during Link Equalization. Port Direction: Downstream Port Crosslink Supported: Any Usage: Contains value sent on the associated Lane during Link EQ.

Bit Range	Default & Access	Field Name (ID): Description
27:24	Fh RW	**Upstream Port Lane 15 Transmitter Preset (UPL15TP):** Field contains the Transmitter Preset Hint value sent or received during Link Equalization. Port Direction: Downstream Port Crosslink Supported: Any Usage: Contains value sent on the associated Lane during Link EQ.
23	0h RO	**Reserved**
22:20	7h RW	**Downstream Port Lane 15 Receiver Preset Hint (DPL15RPH):** Receiver Preset Hint may be used as a hint for receiver equalization by this Port when the Port is operating as a Downstream Port.
19:16	Fh RW	**Downstream Port Lane 15 Transmitter Preset (DPL15TP):** Transmitter Preset used for equalization by this Port when the Port is operating as a Downstream Port. This field is ignored when the Port is operating as an Upstream Port.
15	0h RO	**Reserved**
14:12	7h RW	**Upstream Port Lane 14 Receiver Preset Hint (UPL14RPH):** Field contains the Receiver Preset Hint value sent or received during Link Equalization. Port Direction: Downstream Port Crosslink Supported: Any Usage: Contains value sent on the associated Lane during Link EQ.
11:8	Fh RW	**Upstream Port Lane 14 Transmitter Preset (UPL14TP):** Field contains the Transmitter Preset Hint value sent or received during Link Equalization. Port Direction: Downstream Port Crosslink Supported: Any Usage: Contains value sent on the associated Lane during Link EQ.
7	0h RO	**Reserved**
6:4	7h RW	**Downstream Port Lane 14 Receiver Preset Hint (DPL14RPH):** Receiver Preset Hint may be used as a hint for receiver equalization by this Port when the Port is operating as a Downstream Port.
3:0	Fh RW	**Downstream Port Lane 14 Transmitter Preset (DPL14TP):** Transmitter Preset used for equalization by this Port when the Port is operating as a Downstream Port. This field is ignored when the Port is operating as an Upstream Port.