



# **11<sup>th</sup> Generation Intel<sup>®</sup> Core<sup>™</sup> Processor**

**Datasheet, Volume 2 of 2**

---

***Supporting 11th Generation Intel<sup>®</sup> Core<sup>™</sup> Processor Families,  
Intel<sup>®</sup> Work Station Processors for Desktop Platform, formerly  
known as Rocket Lake***

**May 2021**

***Revision 002***



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

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at [intel.com](http://intel.com).

Intel technologies may require enabled hardware, specific software, or services activation. Check with your system manufacturer or retailer.

The products described may contain design defects or errors known as errata which may cause the product to deviate from published specifications.

Current characterized errata are available on request.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or visit [www.intel.com/design/literature.htm](http://www.intel.com/design/literature.htm).

Intel and the Intel logo are trademarks of Intel Corporation in the U.S. and/or other countries.

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

Copyright © 2021 Intel Corporation. All rights reserved.

# Contents

---

|          |  |           |
|----------|--|-----------|
| <b>1</b> | <b>Introduction</b> .....  | <b>22</b> |
| <b>2</b> | <b>Processor Configuration Register Definitions and Address Ranges</b> ..... | <b>23</b> |
| 2.1      | Register Terminology .....   | 23        |
| 2.2      | PCI Devices and Functions .....  | 24        |
| 2.3      | System Address Map .....   | 25        |
| 2.4      | DOS Legacy Address Range .....   | 27        |
| 2.4.1    | DOS Range (0h – 9_FFFFh) .....   | 28        |
| 2.4.2    | Legacy Video Area (A_0000h – B_FFFFh).....                                   | 28        |
| 2.4.3    | Programmable Attribute Map (PAM) (C_0000h – F_FFFFh) .....                   | 29        |
| 2.5      | Lower Main Memory Address Range (1 MB – TOLUD) .....                         | 30        |
| 2.5.1    | ISA Hole (15 MB –16 MB).....   | 31        |
| 2.5.2    | 1 MB to TSEGMB .....   | 31        |
| 2.5.3    | TSEG .....   | 31        |
| 2.5.4    | Protected Memory Range (PMR) - (Programmable) .....                          | 31        |
| 2.5.5    | DRAM Protected Range (DPR) .....   | 32        |
| 2.5.6    | Pre-allocated Memory .....   | 32        |
| 2.6      | PCI Memory Address Range (TOLUD – 4 GB).....                                 | 32        |
| 2.6.1    | APIC Configuration Space (FEC0_0000h – FECF_FFFFh).....                      | 35        |
| 2.6.2    | HSEG (FEDA_0000h – FEDB_FFFFh) .....   | 35        |
| 2.6.3    | MSI Interrupt Memory Space (FEE0_0000h – FEEF_FFFFh) .....                   | 35        |
| 2.6.4    | High BIOS Area.....  | 35        |
| 2.7      | Upper Main Memory Address Space (4 GB to TOUUD).....                         | 36        |
| 2.7.1    | Top of Memory (TOM) .....  | 36        |
| 2.7.2    | Top of Upper Usable DRAM (TOUUD).....  | 36        |
| 2.7.3    | Top of Low Usable DRAM (TOLUD) .....   | 36        |
| 2.7.4    | TSEG_BASE.....   | 36        |
| 2.7.5    | Memory Re-claim Background .....   | 37        |
| 2.7.6    | Indirect Accesses to MCHBAR Registers .....                                  | 37        |
| 2.7.7    | Memory Remapping .....   | 38        |
| 2.7.8    | Hardware Remap Algorithm .....   | 38        |
| 2.8      | PCI Express* Configuration Address Space .....                               | 38        |
| 2.9      | Graphics Memory Address Ranges .....   | 38        |
| 2.9.1    | IOBAR Mapped Access to Device 2 MMIO Space.....                              | 39        |
| 2.9.2    | Trusted Graphics Ranges.....   | 39        |
| 2.10     | System Management Mode (SMM) .....   | 39        |
| 2.11     | SMM and VGA Access Through GTT TLB.....                                      | 39        |
| 2.12     | Intel® Management Engine (Intel® ME) Stolen Memory Accesses.....             | 40        |
| 2.13     | I/O Address Space.....   | 40        |
| 2.13.1   | PCI Express* I/O Address Mapping .....                                       | 41        |
| 2.14     | Direct Media Interface (DMI) Interface Decode Rules.....                     | 42        |
| 2.14.1   | DMI Accesses to the Processor that Cross Device Boundaries .....             | 42        |
| 2.14.2   | Traffic Class (TC) / Virtual Channel (VC) Mapping Details .....              | 43        |
| 2.15     | PCI Express* Interface Decode Rules .....                                    | 45        |
| 2.15.1   | TC/VC Mapping Details.....   | 45        |
| 2.16     | Legacy VGA and I/O Range Decode Rules .....                                  | 46        |
| 2.17     | I/O Mapped Registers .....   | 50        |
| <b>3</b> | <b>Host Bridge and DRAM Controller (D0:F0)</b> .....                         | <b>51</b> |
| 3.1      | Host Bridge/DRAM Registers (D0:F0) .....                                     | 51        |
| 3.1.1    | Summary of Registers.....  | 51        |

|        |  |     |
|--------|--|-----|
| 3.1.2  | Device Identifiers (ID) — Offset 0h .....                                      | 52  |
| 3.1.3  | Device Command (CMD) — Offset 4h .....   | 53  |
| 3.1.4  | Primary Status (PSTS) — Offset 6h .....  | 54  |
| 3.1.5  | Revision ID (RID_CC) — Offset 8h .....   | 55  |
| 3.1.6  | Header Type (HTYPE) — Offset Eh.....   | 55  |
| 3.1.7  | Secondary Status (SSTS) — Offset 1Eh .....                                     | 56  |
| 3.1.8  | Subsystem Vendor IDs (SVD) — Offset 2Ch .....                                  | 57  |
| 3.1.9  | Capabilities List Pointer (CAPP) — Offset 34h.....                             | 57  |
| 3.1.10 | Bridge Control (BCTRL) — Offset 3Eh .....                                      | 58  |
| 3.1.11 | PCI Express Egress Port Base Address (PXPEPBAR_0_0_0_PCI) — Offset 40h ..      | 59  |
| 3.1.12 | MCHBAR Base Address Register (MCHBAR_0_0_0_PCI) — Offset 48h .....             | 59  |
| 3.1.13 | Graphics Control (GGC_0_0_0_PCI) — Offset 50h .....                            | 60  |
| 3.1.14 | Device Enable (DEVEN_0_0_0_PCI) — Offset 54h .....                             | 61  |
| 3.1.15 | Protected Audio Video Path Control (PAVPC_0_0_0_PCI) — Offset 58h.....         | 63  |
| 3.1.16 | DMA Protected Range (DPR_0_0_0_PCI) — Offset 5Ch .....                         | 65  |
| 3.1.17 | PCIEXBAR Base Address Register (PCIEXBAR_0_0_0_PCI) — Offset 60h .....         | 66  |
| 3.1.18 | DMIBAR Base Address Register (DMIBAR_0_0_0_PCI) — Offset 68h.....              | 68  |
| 3.1.19 | Programmable Attribute Map 0 (PAM0_0_0_0_PCI) — Offset 80h .....               | 69  |
| 3.1.20 | Programmable Attribute Map 1 (PAM1_0_0_0_PCI) — Offset 81h .....               | 70  |
| 3.1.21 | Programmable Attribute Map 2 (PAM2_0_0_0_PCI) — Offset 82h .....               | 71  |
| 3.1.22 | Programmable Attribute Map 3 (PAM3_0_0_0_PCI) — Offset 83h .....               | 72  |
| 3.1.23 | Programmable Attribute Map 4 (PAM4_0_0_0_PCI) — Offset 84h .....               | 73  |
| 3.1.24 | Programmable Attribute Map 5 (PAM5_0_0_0_PCI) — Offset 85h .....               | 74  |
| 3.1.25 | Programmable Attribute Map 6 (PAM6_0_0_0_PCI) — Offset 86h .....               | 75  |
| 3.1.26 | Legacy Access Control (LAC_0_0_0_PCI) — Offset 87h .....                       | 76  |
| 3.1.27 | Top of Memory (TOM_0_0_0_PCI) — Offset A0h .....                               | 79  |
| 3.1.28 | Top of Upper Usable DRAM (TOUUD_0_0_0_PCI) — Offset A8h .....                  | 80  |
| 3.1.29 | Base Data of Stolen Memory (BDSM_0_0_0_PCI) — Offset B0h .....                 | 81  |
| 3.1.30 | Base of GTT Stolen Memory (BGSM_0_0_0_PCI) — Offset B4h .....                  | 81  |
| 3.1.31 | TSEG Memory Base (TSEGMB_0_0_0_PCI) — Offset B8h .....                         | 82  |
| 3.1.32 | Top of Low Usable DRAM (TOLUD_0_0_0_PCI) — Offset BCh .....                    | 83  |
| 3.1.33 | Error Status (ERRSTS_0_0_0_PCI) — Offset C8h .....                             | 84  |
| 3.1.34 | Error Command (ERRCMD_0_0_0_PCI) — Offset CAh .....                            | 86  |
| 3.1.35 | SMI DMI Special Cycle (SMICMD_0_0_0_PCI) — Offset CCh .....                    | 87  |
| 3.1.36 | SMI DMI Special Cycle (SCICMD_0_0_0_PCI) — Offset CEh.....                     | 88  |
| 3.1.37 | Scratchpad Data (SKPD_0_0_0_PCI) — Offset DCh .....                            | 89  |
| 3.1.38 | Capabilities A (CAPID0_A_0_0_0_PCI) — Offset E4h .....                         | 90  |
| 3.1.39 | Capabilities B (CAPID0_B_0_0_0_PCI) — Offset E8h .....                         | 92  |
| 3.1.40 | Capabilities C (CAPID0_C_0_0_0_PCI) — Offset ECh .....                         | 94  |
| 3.2    | Memory Controller (MCHBAR) Registers .....                                     | 96  |
| 3.2.1  | Summary of Registers .....   | 96  |
| 3.2.2  | PRE Command Timing (TC_PRE_0_0_0_MCHBAR) — Offset 4000h .....                  | 98  |
| 3.2.3  | ACT Command Timing (TC_ACT_0_0_0_MCHBAR) — Offset 4004h.....                   | 99  |
| 3.2.4  | RD to RD Timings (TC_RDRD_0_0_0_MCHBAR) — Offset 400Ch .....                   | 100 |
| 3.2.5  | RD to WR Timings (TC_RDWR_0_0_0_MCHBAR) — Offset 4010h .....                   | 101 |
| 3.2.6  | WR to RD Timings (TC_WRRD_0_0_0_MCHBAR) — Offset 4014h .....                   | 102 |
| 3.2.7  | WR to WR Timings (TC_WRWR_0_0_0_MCHBAR) — Offset 4018h .....                   | 102 |
| 3.2.8  | Round-Trip Latency (SC_ROUNDTRIP_LATENCY_0_0_0_MCHBAR) — Offset<br>4020h ..... | 103 |
| 3.2.9  | ECC Debug Control (ECC_DEBUG_0_0_0_MCHBAR) — Offset 4034h.....                 | 105 |
| 3.2.10 | ECC Error Log 0 (ECCERRLOG0_0_0_0_MCHBAR) — Offset 4048h.....                  | 106 |
| 3.2.11 | ECC Error Log 0 (ECCERRLOG1_0_0_0_MCHBAR) — Offset 404Ch.....                  | 106 |
| 3.2.12 | Power Down Timing (TC_PWRDN_0_0_0_MCHBAR) — Offset 4050h .....                 | 107 |
| 3.2.13 | ODT Command Timing (TC_ODT_0_0_0_MCHBAR) — Offset 4070h.....                   | 108 |
| 3.2.14 | ODT Matrix (SC_ODT_MATRIX_0_0_0_MCHBAR) — Offset 4080h.....                    | 109 |

|        |   |     |
|--------|---|-----|
| 3.2.15 | Scheduler Configuration (SC_GS_CFG_0_0_0_MCHBAR) — Offset 4088h.....                  | 110 |
| 3.2.16 | DDRIO Power Mode Timing (SPID_LOW_POWER_CTL_0_0_0_MCHBAR) — Offset 4198h.....         | 112 |
| 3.2.17 | MR4 Rank Temperature (LPDDR_MR4_RANK_TEMPERATURE_0_0_0_MCHBAR) — Offset 4224h .....   | 113 |
| 3.2.18 | DDR4 Temperature (DDR4_MPR_RANK_TEMPERATURE_0_0_0_MCHBAR) — Offset 4228h .....        | 114 |
| 3.2.19 | Refresh Parameters (TC_RFP_0_0_0_MCHBAR) — Offset 4238h .....                         | 114 |
| 3.2.20 | Refresh Timing Parameters (TC_RFTP_0_0_0_MCHBAR) — Offset 423Ch .....                 | 115 |
| 3.2.21 | Self-Refresh Timing Parameters (TC_SRFTP_0_0_0_MCHBAR) — Offset 4240h ...             | 116 |
| 3.2.22 | Refresh Stagger Control (MC_REFRESH_STAGGER_0_0_0_MCHBAR) — Offset 4244h.....         | 116 |
| 3.2.23 | ZQCAL Control (TC_ZQCAL_0_0_0_MCHBAR) — Offset 4248h .....                            | 117 |
| 3.2.24 | Memory Controller Initial State (MC_INIT_STATE_0_0_0_MCHBAR) — Offset 4254h.....      | 117 |
| 3.2.25 | DIMM Idle Energy (PM_DIMM_IDLE_ENERGY_0_0_0_MCHBAR) — Offset 4260h .                  | 118 |
| 3.2.26 | DIMM Power-Down Energy (PM_DIMM_PD_ENERGY_0_0_0_MCHBAR) — Offset 4264h.....           | 119 |
| 3.2.27 | DIMM ACT Energy (PM_DIMM_ACT_ENERGY_0_0_0_MCHBAR) — Offset 4268h ..                   | 120 |
| 3.2.28 | DIMM RD Energy (PM_DIMM_RD_ENERGY_0_0_0_MCHBAR) — Offset 426Ch                        | 120 |
| 3.2.29 | DIMM WR Energy (PM_DIMM_WR_ENERGY_0_0_0_MCHBAR) — Offset 4270h....                    | 121 |
| 3.2.30 | ECC Inject Count (ECC_INJECT_COUNT_0_0_0_MCHBAR) — Offset 4274h...                    | 122 |
| 3.2.31 | WR Delay (SC_WR_DELAY_0_0_0_MCHBAR) — Offset 4278h.....                               | 122 |
| 3.2.32 | Per Bank Refresh (SC_PBR_0_0_0_MCHBAR) — Offset 4288h .....                           | 123 |
| 3.2.33 | TC LPDDR4x MISC 0 0 0 MCHBAR (TC_LPDDR4_MISC_0_0_0_MCHBAR) — Offset 4294h.....        | 123 |
| 3.2.34 | TC SREXITTP 0 0 0 MCHBAR (TC_SREXITTP_0_0_0_MCHBAR) — Offset 42C4h...                 | 124 |
| 3.2.35 | MCMNTS SPARE 0 0 0 MCHBAR (MCMNTS_SPARE_0_0_0_MCHBAR) — Offset 43FCh.....             | 124 |
| 3.2.36 | Inter-Channel Decode Parameters (MAD_INTER_CHANNEL_0_0_0_MCHBAR) — Offset 5000h ..... | 125 |
| 3.2.37 | Intra-Channel 0 Decode Parameters (MAD_INTRA_CH0_0_0_0_MCHBAR) — Offset 5004h .....   | 126 |
| 3.2.38 | Intra-Channel 1 Decode Parameters (MAD_INTRA_CH1_0_0_0_MCHBAR) — Offset 5008h .....   | 127 |
| 3.2.39 | Channel 0 DIMM Characteristics (MAD_DIMM_CH0_0_0_0_MCHBAR) — Offset 500Ch .....       | 128 |
| 3.2.40 | Channel 1 DIMM Characteristics (MAD_DIMM_CH1_0_0_0_MCHBAR) — Offset 5010h.....        | 129 |
| 3.2.41 | Channel Hash (CHANNEL_HASH_0_0_0_MCHBAR) — Offset 5024h .....                         | 129 |
| 3.2.42 | Channel Enhanced Hash (CHANNEL_EHASH_0_0_0_MCHBAR) — Offset 5028h ...                 | 130 |
| 3.2.43 | GT Memory Request Counter (PWM_GT_REQCOUNT_0_0_0_MCHBAR) — Offset 5040h.....          | 131 |
| 3.2.44 | IA Memory Request Counter (PWM_IA_REQCOUNT_0_0_0_MCHBAR) — Offset 5044h.....          | 132 |
| 3.2.45 | IO Memory Request Counter (PWM_IO_REQCOUNT_0_0_0_MCHBAR) — Offset 5048h.....          | 132 |
| 3.2.46 | RdCAS Counter (PWM_RDDATA_COUNT_0_0_0_MCHBAR) — Offset 5050h ..                       | 133 |
| 3.2.47 | WrCAS Counter (PWM_WRDATA_COUNT_0_0_0_MCHBAR) — Offset 5054h .                        | 133 |
| 3.2.48 | Command Counter (PWM_COMMAND_COUNT_0_0_0_MCHBAR) — Offset 5058h                       | 133 |

|        |  |     |
|--------|--|-----|
| 3.2.49 | Self Refresh Mode Control (PM_SREF_CONFIG_0_0_0_MCHBAR) — Offset 5060h<br>133                            |     |
| 3.2.50 | Address Compare for ECC Error Inject (ECC_INJ_ADDR_COMPARE_0_0_0_MCHBAR) — Offset 5088h                  | 134 |
| 3.2.51 | Remap Base (REMAPBASE_0_0_0_MCHBAR) — Offset 5090h   | 134 |
| 3.2.52 | Remap Limit (REMAPLIMIT_0_0_0_MCHBAR) — Offset 5098h   | 135 |
| 3.2.53 | Address Mask for ECC Error Inject (ECC_INJ_ADDR_MASK_0_0_0_MCHBAR) —<br>Offset 5158h                     | 136 |
| 3.2.54 | Graphics VT Base Address Register (GFXVTBAR_0_0_0_MCHBAR_NCU) — Offset<br>5400h                          | 136 |
| 3.2.55 | VTDPVC0BAR Base Address Register (VTDPVC0BAR_0_0_0_MCHBAR_NCU) —<br>Offset 5410h                         | 137 |
| 3.2.56 | IA Exclusion IMR Base Address (IMRIAEXCBASE_MCHBAR_CBO_INGRESS) — Off-<br>set 6A40h                      | 138 |
| 3.2.57 | IA Exclusion IMR Limit Address (IMRIAEXCLIMIT_MCHBAR_CBO_INGRESS) —<br>Offset 6A48h                      | 139 |
| 3.2.58 | GT Exclusion IMR Base Address (IMRGTEXCBASE_MCHBAR_CBO_INGRESS) —<br>Offset 6A50h                        | 139 |
| 3.2.59 | GT Exclusion IMR Limit Address (IMRGTEXCLIMIT_MCHBAR_CBO_INGRESS) —<br>Offset 6A58h                      | 140 |
| 3.3    | Power Management (MCHBAR) Registers  | 141 |
| 3.3.1  | Summary of Registers   | 141 |
| 3.3.2  | BIOS POST Code (BIOS_POST_CODE_0_0_0_MCHBAR_PCU) — Offset 5824h  | 143 |
| 3.3.3  | Cycle Sum of All Active Cores (PKG_IA_C0_ANY_SUM_0_0_0_MCHBAR_PCU) —<br>Offset 5828h                     | 143 |
| 3.3.4  | Cycle Sum of Any Active Core (PKG_IA_C0_ANY_0_0_0_MCHBAR_PCU) — Offset<br>5830h                          | 144 |
| 3.3.5  | Cycle Sum of Active Graphics (PKG_GT_C0_ANY_0_0_0_MCHBAR_PCU) — Offset<br>5838h                          | 144 |
| 3.3.6  | Cycle Sum of Overlapping Active GT and Core (PKG_GT_AND_IA_OVER-<br>LAP_0_0_0_MCHBAR_PCU) — Offset 5840h | 145 |
| 3.3.7  | Cycle Sum of Any Active GT Slice (PKG_GT_C0_ANY_SLICE_0_0_0_MCHBAR_P-<br>CU) — Offset 5848h              | 145 |
| 3.3.8  | Cycle Sum of All Active GT Slice (PKG_GT_C0_SLICES_SUM_0_0_0_MCHBAR_P-<br>CU) — Offset 5850h             | 146 |
| 3.3.9  | Cycle Sum of Any GT Media Engine (PKG_GT_C0_ANY_MEDIA_0_0_0_MCH-<br>BAR_PCU) — Offset 5858h              | 146 |
| 3.3.10 | Ratio Sum of Any Active Core (PKG_IA_C0_ANY_RATIO_0_0_0_MCHBAR_PCU) —<br>Offset 5860h                    | 147 |
| 3.3.11 | Ratio Sum of Active GT (PKG_GT_C0_ANY_RATIO_0_0_0_MCHBAR_PCU) — Off-<br>set 5868h                        | 147 |
| 3.3.12 | Ratio Sum of Active GT Slice (PKG_GT_C0_ANY_SLICE_RATIO_0_0_0_MCH-<br>BAR_PCU) — Offset 5870h            | 148 |
| 3.3.13 | DDR Power Limit (DDR_RAPL_LIMIT_0_0_0_MCHBAR_PCU) — Offset 58E0h   | 148 |
| 3.3.14 | Package RAPL Performance Status (PACKAGE_RAPL_PERF_STATUS_0_0_0_MCH-<br>BAR_PCU) — Offset 58F0h          | 149 |
| 3.3.15 | IA Performance Limit Reasons (IA_PERF_LIMIT_REASONS_0_0_0_MCHBAR_P-<br>CU) — Offset 58FCh                | 150 |
| 3.3.16 | GT Performance Limit Reasons (GT_PERF_LIMIT_REASONS_0_0_0_MCHBAR_P-<br>CU) — Offset 5900h                | 152 |
| 3.3.17 | System Agent Performance Status (SA_PERF_STATUS_0_0_0_MCHBAR_PCU) —<br>Offset 5918h                      | 154 |
| 3.3.18 | Primary Plane Turbo Policy (PRIP_TURBO_PLCY_0_0_0_MCHBAR_PCU) — Offset<br>5920h                          | 155 |
| 3.3.19 | Secondary Plane Turbo Policy (SECP_TURBO_PLCY_0_0_0_MCHBAR_PCU) — Off-<br>set 5924h                      | 156 |

|        |   |     |
|--------|---|-----|
| 3.3.20 | Primary Plane Energy Status (PRIP_NRG_STTS_0_0_0_MCHBAR_PCU) — Offset 5928h.....                    | 156 |
| 3.3.21 | Secondary Plane Energy Status (SECP_NRG_STTS_0_0_0_MCHBAR_PCU) — Offset 592Ch .....                 | 157 |
| 3.3.22 | Package Power SKU Unit (PACKAGE_POWER_SKU_UNIT_0_0_0_MCHBAR_PCU) — Offset 5938h.....                | 157 |
| 3.3.23 | Package Energy Status (PACKAGE_ENERGY_STATUS_0_0_0_MCHBAR_PCU) — Offset 593Ch .....                 | 158 |
| 3.3.24 | GT Performance Status (GT_PERF_STATUS_0_0_0_MCHBAR_PCU) — Offset 5948h.....                         | 158 |
| 3.3.25 | Power Plane 0 Efficient Cycles (PPO_EFFICIENT_CYCLES_0_0_0_MCHBAR_PCU) — Offset 5968h.....          | 159 |
| 3.3.26 | Power Plane 0 Thread Activity (PPO_THREAD_ACTIVITY_0_0_0_MCHBAR_PCU) — Offset 596Ch .....           | 160 |
| 3.3.27 | Primary Plane 0 Temperature (PPO_TEMPERATURE_0_0_0_MCHBAR_PCU) — Offset 597Ch .....                 | 160 |
| 3.3.28 | RP-State Limits (RP_STATE_LIMITS_0_0_0_MCHBAR_PCU) — Offset 5994h.....                              | 161 |
| 3.3.29 | RP-State Capability (RP_STATE_CAP_0_0_0_MCHBAR_PCU) — Offset 5998h.....                             | 161 |
| 3.3.30 | Temperature Target (TEMPERATURE_TARGET_0_0_0_MCHBAR_PCU) — Offset 599Ch .....                       | 162 |
| 3.3.31 | Package Power Limit (PACKAGE_RAPL_LIMIT_0_0_0_MCHBAR_PCU) — Offset 59A0h .....                      | 163 |
| 3.3.32 | Thermal Status GT (THERM_STATUS_GT_0_0_0_MCHBAR_PCU) — Offset 59C0h .....                           | 164 |
| 3.3.33 | Thermal Interrupt GT (THERM_INTERRUPT_GT_0_0_0_MCHBAR_PCU) — Offset 59C4h .....                     | 166 |
| 3.3.34 | Device Idle Duration Override (DEVICE_IDLE_DURATION_OVERRIDE_0_0_0_MCHBAR_PCU) — Offset 59C8h ..... | 167 |
| 3.3.35 | Package GT C0 EUs SUM (PKG_GT_C0_EUS_SUM) — Offset 59F0h .....                                      | 167 |
| 3.3.36 | Package GT C0 Media Sum (PKG_GT_C0_MEDIA_SUM) — Offset 59F8h.....                                   | 168 |
| 3.3.37 | FIVR FFFC EMI Control (FFFC_EMI_CONTROL_0_0_0_MCHBAR_PCU) — Offset 5A08h .....                      | 168 |
| 3.3.38 | FIVR FFFC RFI Control (FFFC_RFI_CONTROL_0_0_0_MCHBAR_PCU) — Offset 5A0Ch .....                      | 169 |
| 3.3.39 | FIVR FFFC RFI Control 2 (FFFC_RFI_CONTROL2_0_0_0_MCHBAR_PCU) — Offset 5A18h .....                   | 169 |
| 3.3.40 | BIOS 2 Level Memory Configuration (BIOS_2LM_CONFIG) — Offset 5A20h ..                               | 169 |
| 3.3.41 | Scratchpad Register (SSKPD_0_0_0_MCHBAR_PCU) — Offset 5D10h .....                                   | 170 |
| 3.3.42 | BIOS Mailbox Data (BIOS_MAILBOX_DATA_0_0_0_MCHBAR_PCU) — Offset 5DA0h .....                         | 170 |
| 3.3.43 | BIOS Mailbox Interface (BIOS_MAILBOX_INTERFACE_0_0_0_MCHBAR_PCU) — Offset 5DA4h.....                | 171 |
| 3.3.44 | BIOS Reset Complete (BIOS_RESET_CPL_0_0_0_MCHBAR_PCU) — Offset 5DA8h .....                          | 172 |
| 3.3.45 | Memory Controller BIOS Request (MC_BIOS_REQ_0_0_0_MCHBAR_PCU) — Offset 5E00h .....                  | 172 |
| 3.3.46 | Memory Controller BIOS Data (MC_BIOS_DATA_0_0_0_MCHBAR_PCU) — Offset 5E04h.....                     | 173 |
| 3.3.47 | System Agent Power Management Control (SAPMCTL_0_0_0_MCHBAR_PCU) — Offset 5F00h.....                | 174 |
| 3.3.48 | Configurable TDP Nominal (CONFIG_TDP_NOMINAL_0_0_0_MCHBAR_PCU) — Offset 5F3Ch .....                 | 176 |
| 3.3.49 | Configurable TDP Level 1 (CONFIG_TDP_LEVEL1_0_0_0_MCHBAR_PCU) — Offset 5F40h.....                   | 177 |
| 3.3.50 | Configurable TDP Level 1 (CONFIG_TDP_LEVEL2_0_0_0_MCHBAR_PCU) — Offset 5F48h.....                   | 177 |
| 3.3.51 | Configurable TDP Control (CONFIG_TDP_CONTROL_0_0_0_MCHBAR_PCU) —                                    |     |

|        |   |     |
|--------|---|-----|
|        | Offset 5F50h .....  | 178 |
| 3.3.52 | Turbo Activation Ratio (TURBO_ACTIVATION_RATIO_0_0_0_MCHBAR_PCU) — Offset 5F54h ..... | 178 |
| 3.3.53 | Overclocking Status (OC_STATUS_0_0_0_MCHBAR_PCU) — Offset 5F58h ....                  | 179 |
| 3.3.54 | Base Clock (BCLK) Frequency (BCLK_FREQ_0_0_0_MCHBAR) — Offset 5F60h ...               | 180 |
| 3.4    | Host Controller (MCHBAR) Registers .....  | 181 |
| 3.4.1  | Summary of Registers .....  | 181 |
| 3.4.2  | Type-C Sub-system Device Enable (TCSS_DEVEN_0_0_0_MCHBAR_IMPH) — Offset 7090h .....   | 181 |
| 3.4.3  | Capabilities D (CAPID0_D_0_0_0_MCHBAR) — Offset 7094h .....                           | 182 |
| 3.5    | Direct Media Interface BAR (DMIBAR) Registers .....                                   | 184 |
| 3.5.1  | Summary of Registers .....  | 184 |
| 3.5.2  | Device Identifiers (ID) — Offset 0h .....   | 187 |
| 3.5.3  | Device Command (CMD) — Offset 4h .....  | 187 |
| 3.5.4  | Primary Status (PSTS) — Offset 6h .....   | 188 |
| 3.5.5  | Revision ID (RID_CC) — Offset 8h .....  | 189 |
| 3.5.6  | Header Type (HTYPE) — Offset Eh .....   | 190 |
| 3.5.7  | Secondary Status (SSTS) — Offset 1Eh .....  | 190 |
| 3.5.8  | Subsystem Vendor IDs (SVD) — Offset 2Ch .....   | 191 |
| 3.5.9  | Capabilities List Pointer (CAPP) — Offset 34h .....                                   | 192 |
| 3.5.10 | Bridge Control (BCTRL) — Offset 3Eh .....   | 193 |
| 3.5.11 | Device Capabilities (DCAP) — Offset 44h .....   | 194 |
| 3.5.12 | Device Control (DCTL) — Offset 48h .....  | 194 |
| 3.5.13 | Device Status (DSTS) — Offset 4Ah .....   | 195 |
| 3.5.14 | Link Capabilities (LCAP) — Offset 4Ch .....   | 196 |
| 3.5.15 | Link Control (LCTL) — Offset 50h .....  | 198 |
| 3.5.16 | Link Status (LSTS) — Offset 52h .....   | 200 |
| 3.5.17 | Root Control (RCTL) — Offset 5Ch .....  | 201 |
| 3.5.18 | Root Status (RSTS) — Offset 60h .....   | 202 |
| 3.5.19 | Device Capabilities 2 (DCAP2) — Offset 64h .....                                      | 202 |
| 3.5.20 | Device Control 2 (DCTL2) — Offset 68h .....   | 204 |
| 3.5.21 | Device Status 2 (DSTS2) — Offset 6Ah .....  | 206 |
| 3.5.22 | Link Capabilities 2 (LCAP2) — Offset 6Ch .....  | 206 |
| 3.5.23 | Link Control 2 (LCTL2) — Offset 70h .....   | 208 |
| 3.5.24 | Link Status 2 (LSTS2) — Offset 72h .....  | 210 |
| 3.5.25 | Slot Capabilities 2 (SLCAP2) — Offset 74h .....                                       | 211 |
| 3.5.26 | Slot Control 2 (SLCTL2) — Offset 78h .....  | 211 |
| 3.5.27 | Slot Status 2 (SLSTS2) — Offset 7Ah .....   | 211 |
| 3.5.28 | Message Signaled Interrupt Identifiers (MID) — Offset 80h .....                       | 211 |
| 3.5.29 | Message Signaled Interrupt Message (MC) — Offset 82h .....                            | 212 |
| 3.5.30 | Message Signaled Interrupt Message Address (MA) — Offset 84h .....                    | 213 |
| 3.5.31 | Message Signaled Interrupt Message Data (MD) — Offset 88h .....                       | 213 |
| 3.5.32 | Subsystem Vendor Capability (SVCAP) — Offset 90h .....                                | 213 |
| 3.5.33 | Subsystem Vendor IDs (SVID) — Offset 94h .....  | 214 |
| 3.5.34 | Power Management Capability (PMCAP) — Offset A0h .....                                | 214 |
| 3.5.35 | PCI Power Management Capabilities (PMC) — Offset A2h .....                            | 215 |
| 3.5.36 | PCI Power Management Control (PMCS) — Offset A4h .....                                | 216 |
| 3.5.37 | Advanced Error Extended (AECH) — Offset 100h .....                                    | 217 |
| 3.5.38 | Uncorrectable Error Status (UES) — Offset 104h .....                                  | 217 |
| 3.5.39 | Uncorrectable Error Mask (UEM) — Offset 108h .....                                    | 219 |
| 3.5.40 | Correctable Error Severity (UEV) — Offset 10Ch .....                                  | 220 |
| 3.5.41 | Correctable Error Status (CES) — Offset 110h .....                                    | 221 |
| 3.5.42 | Correctable Error Mask (CEM) — Offset 114h .....                                      | 222 |
| 3.5.43 | Advanced Error Capabilities And Control (AECC) — Offset 118h .....                    | 223 |



|        |  |     |
|--------|--|-----|
| 3.5.44 | Header Log (HL_DW1) — Offset 11Ch .....  | 224 |
| 3.5.45 | Header Log (HL_DW2) — Offset 120h .....  | 224 |
| 3.5.46 | Header Log (HL_DW3) — Offset 124h .....  | 224 |
| 3.5.47 | Header Log (HL_DW4) — Offset 128h .....  | 225 |
| 3.5.48 | Root Error Command (REC) — Offset 12Ch .....   | 225 |
| 3.5.49 | Root Error Status (RES) — Offset 130h .....  | 226 |
| 3.5.50 | Error Source Identification (ESID) — Offset 134h.....  | 227 |
| 3.5.51 | PTM Extended Capability Header (PTMECH) — Offset 150h.....   | 227 |
| 3.5.52 | Port VC Capability Register 1 (PVCCR1) — Offset 284h .....   | 228 |
| 3.5.53 | Port VC Capability 2 (PVCC2) — Offset 288h .....   | 229 |
| 3.5.54 | Port VC Control (PVCC) — Offset 28Ch .....   | 229 |
| 3.5.55 | Port VC Status (PVCS) — Offset 28Eh .....  | 230 |
| 3.5.56 | Virtual Channel 0 Resource Capability (V0VCRC) — Offset 290h.....  | 231 |
| 3.5.57 | Virtual Channel 0 Resource Control (V0CTL) — Offset 294h.....  | 232 |
| 3.5.58 | Virtual Channel 0 Resource Status (V0STS) — Offset 29Ah .....  | 234 |
| 3.5.59 | Virtual Channel 1 Resource Capability (V1VCRC) — Offset 29Ch.....  | 235 |
| 3.5.60 | Virtual Channel 1 Resource Control (V1CTL) — Offset 2A0h.....  | 235 |
| 3.5.61 | Virtual Channel 1 Resource Status (V1STS) — Offset 2A6h .....  | 236 |
| 3.5.62 | Secondary PCI Express Extended Capability Header (SPEECH) — Offset A30h.....                                     | 236 |
| 3.5.63 | Link Control 3 (LCTL3) — Offset A34h .....   | 237 |
| 3.5.64 | Lane Error Status (LES) — Offset A38h .....  | 238 |
| 3.5.65 | Lane 0 And Lane 1 Equalization Control (L01EC) — Offset A3Ch.....  | 239 |
| 3.5.66 | Lane 2 And Lane 3 Equalization Control (L23EC) — Offset A40h.....  | 241 |
| 3.5.67 | Lane 4 And Lane 5 Equalization Control (L45EC) — Offset A44h.....  | 242 |
| 3.5.68 | Lane 6 And Lane 7 Equalization Control (L67EC) — Offset A48h.....  | 243 |
| 3.5.69 | Lane 8 And Lane 9 Equalization Control (L89EC) — Offset A4Ch.....  | 244 |
| 3.5.70 | Lane 10 And Lane 11 Equalization Control (L1011EC) — Offset A50h.....  | 246 |
| 3.5.71 | Lane 12 And Lane 13 Equalization Control (L1213EC) — Offset A54h.....  | 247 |
| 3.5.72 | Lane 14 And Lane 15 Equalization Control (L1415EC) — Offset A58h.....  | 248 |
| 3.5.73 | Data Link Feature Extended Capability Header (DLFECH) — Offset A90h .....  | 249 |
| 3.5.74 | Data Link Feature Capabilities Register (DLFCAP) — Offset A94h.....  | 250 |
| 3.5.75 | Data Link Feature Status Register (DLFSTS) — Offset A98h .....   | 251 |
| 3.5.76 | Physical Layer 16.0 GT/s Extended Capability Header (PL16GECH) — Offset A9Ch                                     | 251 |
| 3.5.77 | Physical Layer 16.0 GT/s Capability Register (PL16CAP) — Offset AA0h .....                                       | 252 |
| 3.5.78 | Physical Layer 16.0 GT/s Control Register (PL16CTL) — Offset AA4h .....  | 252 |
| 3.5.79 | Physical Layer 16.0 GT/s Status Register (PL16S) — Offset AA8h.....  | 252 |
| 3.5.80 | Physical Layer 16.0 GT/s Local Data Parity Mismatch Status Register (PL16LD-<br>PMS) — Offset AACH .....         | 253 |
| 3.5.81 | Physical Layer 16.0 GT/s First Retimer Data Parity Mismatch Status Register<br>(PL16FRDPMS) — Offset AB0h.....   | 253 |
| 3.5.82 | Physical Layer 16.0 GT/s Second Retimer Data Parity Mismatch Status Register<br>(PL16SRDPMS) — Offset AB4h ..... | 254 |
| 3.5.83 | Physical Layer 16.0 GT/s Extra Status Register (PL16ES) — Offset AB8h.....                                       | 254 |
| 3.5.84 | Physical Layer 16.0 GT/s Lane 01 Equalization Control Register (PL16L01EC) —<br>Offset ABCh.....                 | 255 |
| 3.5.85 | Physical Layer 16.0 GT/s Lane 23 Equalization Control Register (PL16L23EC) —<br>Offset ABEh .....                | 255 |
| 3.5.86 | Physical Layer 16.0 GT/s Lane 45 Equalization Control Register (PL16L45EC) —<br>Offset AC0h.....                 | 256 |
| 3.5.87 | Physical Layer 16.0 GT/s Lane 67 Equalization Control Register (PL16L67EC) —<br>Offset AC2h.....                 | 257 |
| 3.5.88 | Physical Layer 16.0 GT/s Lane 89 Equalization Control Register (PL16L89EC) —<br>Offset AC4h.....                 | 258 |
| 3.5.89 | Physical Layer 16.0 GT/s Lane 1011 Equalization Control Register (PL16L1011EC)                                   |     |



|         |  |     |
|---------|--|-----|
|         | — Offset AC6h.....   | 259 |
| 3.5.90  | Physical Layer 16.0 GT/s Lane 1213 Equalization Control Register (PL16L1213EC)<br>— Offset AC8h.....   | 260 |
| 3.5.91  | Physical Layer 16.0 GT/s Lane 1415 Equalization Control Register (PL16L1415EC)<br>— Offset ACAh .....  | 261 |
| 3.5.92  | Device ID Override (DIDOVR) — Offset D00h .....  | 262 |
| 3.5.93  | Physical Layer 16.0 GT/s Margining Extended Capability Header (PL16MECH) —<br>Offset EDCh .....        | 263 |
| 3.5.94  | Physical Layer 16.0 GT/s Margining Port Capabilities and Port Status (PL16MPCPS)<br>— Offset EE0h..... | 263 |
| 3.5.95  | Physical Layer 16.0 GT/s Lane0 Margin Control and Status Register (PL16L0MCS)<br>— Offset EE4h.....    | 264 |
| 3.5.96  | Physical Layer 16.0 GT/s Lane1 Margin Control and Status Register (PL16L1MCS)<br>— Offset EE8h.....    | 265 |
| 3.5.97  | Physical Layer 16.0 GT/s Lane2 Margin Control and Status Register (PL16L2MCS)<br>— Offset EECh.....    | 265 |
| 3.5.98  | Physical Layer 16.0 GT/s Lane3 Margin Control and Status Register (PL16L3MCS)<br>— Offset EF0h.....    | 265 |
| 3.5.99  | Physical Layer 16.0 GT/s Lane4 Margin Control and Status Register (PL16L4MCS)<br>— Offset EF4h.....    | 265 |
| 3.5.100 | Physical Layer 16.0 GT/s Lane5 Margin Control and Status Register (PL16L5MCS)<br>— Offset EF8h.....    | 266 |
| 3.5.101 | Physical Layer 16.0 GT/s Lane6 Margin Control and Status Register (PL16L6MCS)<br>— Offset EFCh.....    | 266 |
| 3.5.102 | Physical Layer 16.0 GT/s Lane7 Margin Control and Status Register (PL16L7MCS)<br>— Offset F00h.....    | 266 |
| 3.5.103 | Physical Layer 16.0 GT/s Lane8 Margin Control and Status Register (PL16L8MCS)<br>— Offset F04h.....    | 266 |
| 3.5.104 | Physical Layer 16.0 GT/s Lane9 Margin Control and Status Register (PL16L9MCS)<br>— Offset F08h.....    | 266 |
| 3.5.105 | Physical Layer 16.0 GT/s Lane10 Margin Control and Status Register<br>(PL16L10MCS) — Offset F0Ch.....  | 266 |
| 3.5.106 | Physical Layer 16.0 GT/s Lane11 Margin Control and Status Register<br>(PL16L11MCS) — Offset F10h.....  | 266 |
| 3.5.107 | Physical Layer 16.0 GT/s Lane12 Margin Control and Status Register<br>(PL16L12MCS) — Offset F14h.....  | 267 |
| 3.5.108 | Physical Layer 16.0 GT/s Lane13 Margin Control and Status Register<br>(PL16L13MCS) — Offset F18h.....  | 267 |
| 3.5.109 | Physical Layer 16.0 GT/s Lane14 Margin Control and Status Register<br>(PL16L14MCS) — Offset F1Ch.....  | 267 |
| 3.5.110 | Physical Layer 16.0 GT/s Lane15 Margin Control and Status Register<br>(PL16L15MCS) — Offset F20h.....  | 267 |
| 3.6     | PCI Express Egress Port BAR (PXPEPBAR) Registers.....  | 268 |
| 3.6.1   | Summary of Registers .....   | 268 |
| 3.6.2   | Egress Port Virtual Channel Capabilities (EPVCECH_0_0_0_PXPEPBAR) — Offset<br>0h .....                 | 269 |
| 3.6.3   | Egress Port Virtual Channel Capability Register 1 (EPPVCCAP1_0_0_0_PXPEPBAR)<br>— Offset 4h .....      | 269 |
| 3.6.4   | Egress Port Virtual Channel Capability Register 2 (EPPVCCAP2_0_0_0_PXPEPBAR)<br>— Offset 8h .....      | 270 |
| 3.6.5   | Egress Port Virtual Channel Control (EPPVCCTL_0_0_0_PXPEPBAR) — Offset Ch.<br>271                      |     |
| 3.6.6   | Egress Port Virtual Channel 0 Resource Capability (EPVCORCAP_0_0_0_PXPEP-<br>BAR) — Offset 10h.....    | 271 |
| 3.6.7   | Egress Port Virtual Channel 0 Resource Control (EPVCORCTL_0_0_0_PXPEPBAR)<br>— Offset 14h.....         | 272 |
| 3.6.8   | Egress Port Virtual Channel 0 Resource Status (EPVCORSTS_0_0_0_PXPEPBAR)                               |     |

|        |   |     |
|--------|---|-----|
|        | — Offset 1Ah .....  | 273 |
| 3.6.9  | Egress Port Virtual Channel 1 Resource Capability (EPVC1RCAP_0_0_0_PXPEPBAR) — Offset 1Ch ..... | 273 |
| 3.6.10 | Egress Port Virtual Channel 1 Resource Control (EPVC1RCTL_0_0_0_PXPEPBAR) — Offset 20h .....    | 274 |
| 3.6.11 | Egress Port Virtual Channel 1 Resource Status (EPVC1RSTS_0_0_0_PXPEPBAR) — Offset 26h .....     | 276 |
| 3.6.12 | Egress Port Capability Declaration (EPRCLDECH_0_0_0_PXPEPBAR) — Offset 40h .....                | 276 |
| 3.6.13 | Egress Port Element Declaration Capability (EPESD_0_0_0_PXPEPBAR) — Offset 44h .....            | 277 |
| 3.6.14 | Egress Port Link Element Declaration 1 (EPL1D_0_0_0_PXPEPBAR) — Offset 50h .....                | 277 |
| 3.6.15 | Egress Port Link Another Root Complex Declaration 1 (EPL1A_0_0_0_PXPEPBAR) — Offset 58h .....   | 278 |
| 3.6.16 | Egress Port Second Link Declaration 1 (EPL2A_0_0_0_PXPEPBAR) — Offset 5Ch .....                 | 279 |
| 3.6.17 | Egress Port Link Element Declaration 2 (EPL2D_0_0_0_PXPEPBAR) — Offset 60h .....                | 279 |
| 3.6.18 | Egress Port Link Another Root Complex Declaration 2 (EPL2A_0_0_0_PXPEPBAR) — Offset 68h .....   | 280 |
| 3.6.19 | Egress Port Second Link Declaration 2 (EPL2A_0_0_0_PXPEPBAR) — Offset 6Ch .....                 | 280 |
| 3.6.20 | Egress Port Link Element Declaration 3 (EPL3D_0_0_0_PXPEPBAR) — Offset 70h .....                | 280 |
| 3.6.21 | Egress Port Link Another Root Complex Declaration 3 (EPL3A_0_0_0_PXPEPBAR) — Offset 78h .....   | 281 |
| 3.6.22 | Egress Port Second Link Declaration 3 (EPL3A_0_0_0_PXPEPBAR) — Offset 7Ch .....                 | 281 |
| 3.6.23 | Egress Port Link Element Declaration 4 (EPL4D_0_0_0_PXPEPBAR) — Offset 80h .....                | 282 |
| 3.6.24 | Egress Port Link Another Root Complex Declaration 4 (EPL4A_0_0_0_PXPEPBAR) — Offset 88h .....   | 283 |
| 3.6.25 | Egress Port Second Link Declaration 4 (EPL4A_0_0_0_PXPEPBAR) — Offset 8Ch .....                 | 283 |
| 3.6.26 | Egress Port Link Element Declaration 5 (EPL5D_0_0_0_PXPEPBAR) — Offset 90h .....                | 283 |
| 3.6.27 | Egress Port Link Another Root Complex Declaration 5 (EPL5A_0_0_0_PXPEPBAR) — Offset 98h .....   | 284 |
| 3.6.28 | Egress Port Second Link Declaration 5 (EPL5A_0_0_0_PXPEPBAR) — Offset 9Ch .....                 | 284 |
| 3.6.29 | Miscellaneous Port Configuration PXPEPBAR (MPCP) — Offset A0h .....                             | 285 |
| 3.7    | VTDPVC0BAR Registers .....  | 286 |
| 3.7.1  | Summary of Registers .....  | 286 |
| 3.7.2  | Version Register (VER_REG_0_0_0_VTDDBAR) — Offset 0h .....                                      | 287 |
| 3.7.3  | Capability Register (CAP_REG_0_0_0_VTDDBAR) — Offset 8h .....                                   | 287 |
| 3.7.4  | Extended Capability Register (ECAP_REG_0_0_0_VTDDBAR) — Offset 10h .....                        | 291 |
| 3.7.5  | Global Command Register (GCMD_REG_0_0_0_VTDDBAR) — Offset 18h .....                             | 293 |
| 3.7.6  | Global Status Register (GSTS_REG_0_0_0_VTDDBAR) — Offset 1Ch .....                              | 296 |
| 3.7.7  | Root Table Address Register (RTADDR_REG_0_0_0_VTDDBAR) — Offset 20h .....                       | 298 |
| 3.7.8  | Context Command Register (CCMD_REG_0_0_0_VTDDBAR) — Offset 28h .....                            | 299 |
| 3.7.9  | Fault Status Register (FSTS_REG_0_0_0_VTDDBAR) — Offset 34h .....                               | 300 |
| 3.7.10 | Fault Event Control Register (FECTL_REG_0_0_0_VTDDBAR) — Offset 38h .....                       | 302 |
| 3.7.11 | Fault Event Data Register (FEDATA_REG_0_0_0_VTDDBAR) — Offset 3Ch .....                         | 303 |
| 3.7.12 | Fault Event Address Register (FEADDR_REG_0_0_0_VTDDBAR) — Offset 40h .....                      | 304 |
| 3.7.13 | Fault Event Upper Address Register (FEUADDR_REG_0_0_0_VTDDBAR) — Offset 44h .....               | 304 |



|          |  |            |
|----------|--|------------|
| 3.7.14   | Advanced Fault Log Register (AFLOG_REG_0_0_0_VTDBAR) — Offset 58h ...                    | 305        |
| 3.7.15   | Protected Memory Enable Register (PMEN_REG_0_0_0_VTDBAR) — Offset 64h..                  | 306        |
| 3.7.16   | Protected Low Memory Base Register (PLMBASE_REG_0_0_0_VTDBAR) — Offset 68h.....          | 307        |
| 3.7.17   | Protected Low-Memory Limit Register (PLMLIMIT_REG_0_0_0_VTDBAR) — Offset 6Ch .....       | 307        |
| 3.7.18   | Protected High-Memory Base Register (PHMBASE_REG_0_0_0_VTDBAR) — Offset 70h .....        | 308        |
| 3.7.19   | Protected High-Memory Limit Register (PHMLIMIT_REG_0_0_0_VTDBAR) — Offset 78h .....      | 309        |
| 3.7.20   | Invalidation Queue Head Register (IQH_REG_0_0_0_VTDBAR) — Offset 80h                     | 310        |
| 3.7.21   | Invalidation Queue Tail Register (IQT_REG_0_0_0_VTDBAR) — Offset 88h...                  | 311        |
| 3.7.22   | Invalidation Queue Address Register (IQA_REG_0_0_0_VTDBAR) — Offset 90h .                | 311        |
| 3.7.23   | Invalidation Completion Status Register (ICS_REG_0_0_0_VTDBAR) — Offset 9Ch .....        | 312        |
| 3.7.24   | Invalidation Event Control Register (IECTL_REG_0_0_0_VTDBAR) — Offset A0h.               | 312        |
| 3.7.25   | Invalidation Event Data Register (IEDATA_REG_0_0_0_VTDBAR) — Offset A4h..                | 313        |
| 3.7.26   | Invalidation Event Address Register (IEADDR_REG_0_0_0_VTDBAR) — Offset A8h .....         | 314        |
| 3.7.27   | Invalidation Event Upper Address Register (IEUADDR_REG_0_0_0_VTDBAR) — Offset ACh .....  | 314        |
| 3.7.28   | Interrupt Remapping Table Address Register (IRTA_REG_0_0_0_VTDBAR) — Offset B8h .....    | 315        |
| 3.7.29   | Page Request Status Register (PRESTS_REG_0_0_0_VTDBAR) — Offset DCh                      | 315        |
| 3.7.30   | Page Request Event Control Register (PRECTL_REG_0_0_0_VTDBAR) — Offset E0h.....          | 316        |
| 3.7.31   | Page Request Event Data Register (PREDATA_REG_0_0_0_VTDBAR) — Offset E4h.....            | 317        |
| 3.7.32   | Page Request Event Address Register (PREADDR_REG_0_0_0_VTDBAR) — Offset E8h.....         | 317        |
| 3.7.33   | Page Request Event Upper Address Register (PREUADDR_REG_0_0_0_VTDBAR) — Offset ECh ..... | 318        |
| 3.7.34   | Fault Recording Register Low [0] (FRCDL_REG_0_0_0_VTDBAR) — Offset 400h.                 | 318        |
| 3.7.35   | Fault Recording Register High [0] (FRCDH_REG_0_0_0_VTDBAR) — Offset 408h                 | 319        |
| 3.7.36   | Invalidate Address Register (IVA_REG_0_0_0_VTDBAR) — Offset 500h .....                   | 320        |
| 3.7.37   | IOTLB Invalidate Register (IOTLB_REG_0_0_0_VTDBAR) — Offset 508h .....                   | 321        |
| <b>4</b> | <b>Processor Graphics (D2:F0).....</b>   | <b>324</b> |
| 4.1      | Processor Graphics Registers (D2:F0).....  | 324        |
| 4.1.1    | Summary of Registers .....   | 324        |
| 4.1.2    | Vendor ID (VID2_0_2_0_PCI) — Offset 0h .....   | 326        |
| 4.1.3    | Device ID (DID2_0_2_0_PCI) — Offset 2h .....   | 326        |
| 4.1.4    | PCI Command (PCICMD_0_2_0_PCI) — Offset 4h .....   | 327        |
| 4.1.5    | PCI Status (PCISTS2_0_2_0_PCI) — Offset 6h .....   | 328        |
| 4.1.6    | Revision Identification and Class Code register (RID2_CC_0_2_0_PCI) — Offset 8h .....    | 329        |
| 4.1.7    | Cache Line Size (CLS_0_2_0_PCI) — Offset Ch.....   | 330        |
| 4.1.8    | Master Latency Timer (MLT2_0_2_0_PCI) — Offset Dh .....                                  | 330        |
| 4.1.9    | Header Type (HDR2_0_2_0_PCI) — Offset Eh.....  | 331        |
| 4.1.10   | Built In Self Test (BIST_0_2_0_PCI) — Offset Fh .....                                    | 331        |
| 4.1.11   | Graphics Translation Table Memory Mapped Range Address (GTTM-                            |            |

|   |     |
|---|-----|
| MADR0_0_2_0_PCI) — Offset 10h .....   | 331 |
| 4.1.12 Graphics Translation Table Memory Mapped Range Address (GTTM-<br>MADR1_0_2_0_PCI) — Offset 14h ..... | 332 |
| 4.1.13 Graphics Memory Range Address (GMADR0_0_2_0_PCI) — Offset 18h .....                                  | 333 |
| 4.1.14 Graphics Memory Range Address (GMADR1_0_2_0_PCI) — Offset 1Ch .....                                  | 334 |
| 4.1.15 I/O Base Address (IOBAR_0_2_0_PCI) — Offset 20h .....  | 334 |
| 4.1.16 Subsystem Vendor Identification (SVID2_0_2_0_PCI) — Offset 2Ch .....                                 | 335 |
| 4.1.17 Subsystem Identification (SID2_0_2_0_PCI) — Offset 2Eh .....   | 335 |
| 4.1.18 Video BIOS ROM Base Address (ROMADR_0_2_0_PCI) — Offset 30h .....                                    | 336 |
| 4.1.19 Capabilities Pointer (CAPPOINT_0_2_0_PCI) — Offset 34h .....   | 336 |
| 4.1.20 Interrupt Line (INTRLINE_0_2_0_PCI) — Offset 3Ch .....   | 337 |
| 4.1.21 Interrupt Pin (INTRPIN_0_2_0_PCI) — Offset 3Dh .....   | 337 |
| 4.1.22 Minimum Grant (MINGNT_0_2_0_PCI) — Offset 3Eh .....  | 338 |
| 4.1.23 Maximum Latency (MAXLAT_0_2_0_PCI) — Offset 3Fh .....  | 338 |
| 4.1.24 Capability Identifier (CAPID0_0_2_0_PCI) — Offset 40h .....  | 339 |
| 4.1.25 Capabilities Control (CAPCTRL0_0_2_0_PCI) — Offset 42h .....   | 339 |
| 4.1.26 Capabilities A (CAPID0_A_0_2_0_PCI) — Offset 44h .....   | 340 |
| 4.1.27 Capabilities B (CAPID0_B_0_2_0_PCI) — Offset 48h .....   | 341 |
| 4.1.28 PCI Mirror of GMCH Graphics Control (MGGC0_0_2_0_PCI) — Offset 50h .....                             | 341 |
| 4.1.29 Mirror of Device Enable (DEVEN0_0_2_0_PCI) — Offset 54h .....  | 343 |
| 4.1.30 Device 2 Control (DEV2CTL_0_2_0_PCI) — Offset 58h .....  | 344 |
| 4.1.31 Multi Size Aperture Control (MSAC_0_2_0_PCI) — Offset 60h .....                                      | 344 |
| 4.1.32 Push Aperture (PUSHAP_0_2_0_PCI) — Offset 68h .....  | 345 |
| 4.1.33 VTd Status (VTD_STATUS_0_2_0_PCI) — Offset 6Ch .....   | 345 |
| 4.1.34 PCI Express Capability Header (PCIECAPHDR_0_2_0_PCI) — Offset 70h .....                              | 346 |
| 4.1.35 PCI Express Capability (PCIECAP_0_2_0_PCI) — Offset 72h .....  | 346 |
| 4.1.36 Device Capabilities (DEVICECAP_0_2_0_PCI) — Offset 74h .....   | 347 |
| 4.1.37 PCI Express Device Control (DEVICECTL_0_2_0_PCI) — Offset 78h .....                                  | 348 |
| 4.1.38 PCI Express Capability Structure (DEVICESTS_0_2_0_PCI) — Offset 7Ah .....                            | 349 |
| 4.1.39 Message Signaled Interrupts Capability ID (MSI_CAPID_0_2_0_PCI) — Offset<br>ACh .....                | 350 |
| 4.1.40 Message Control (MC_0_2_0_PCI) — Offset AEh .....  | 351 |
| 4.1.41 Message Address (MA_0_2_0_PCI) — Offset B0h .....  | 351 |
| 4.1.42 Message Data (MD_0_2_0_PCI) — Offset B4h .....   | 352 |
| 4.1.43 MSI Mask Bits (MSI_MASK_0_2_0_PCI) — Offset B8h .....  | 352 |
| 4.1.44 MSI Pending Bits (MSI_PEND_0_2_0_PCI) — Offset BCh .....   | 353 |
| 4.1.45 Mirror of Base Data of Stolen Memory (BDSM0_0_2_0_PCI) — Offset C0h ...                              | 353 |
| 4.1.46 Mirror of Base Data of Stolen Memory (BDSM1_0_2_0_PCI) — Offset C4h ...                              | 354 |
| 4.1.47 Graphics VTd Base Address LSB (GFXVTDBAR_LSB_0_2_0_PCI) — Offset C8h ...<br>354                      |     |
| 4.1.48 Graphics VTd Base Address MSB (GFXVTDBAR_MSB_0_2_0_PCI) — Offset CCh .<br>355                        |     |
| 4.1.49 Power Management Capabilities ID (PMCAPID_0_2_0_PCI) — Offset D0h .....                              | 356 |
| 4.1.50 Power Management Capabilities (PMCAP_0_2_0_PCI) — Offset D2h .....                                   | 356 |
| 4.1.51 Power Management Control and Status (PMCS_0_2_0_PCI) — Offset D4h .....                              | 357 |
| 4.1.52 Software SMI (SWSMI_0_2_0_PCI) — Offset E0h .....  | 358 |
| 4.1.53 Graphics System Event (GSE_0_2_0_PCI) — Offset E4h .....   | 358 |
| 4.1.54 Software SCI (SWSCI_0_2_0_PCI) — Offset E8h .....  | 359 |
| 4.1.55 Device 2 Mirror of Protected Audio Video Path Control (PAVPC0_0_2_0_PCI) —<br>Offset F0h .....       | 360 |
| 4.1.56 Device 2 Mirror of Protected Audio Video Path Control (PAVPC1_0_2_0_PCI) —<br>Offset F4h .....       | 361 |
| 4.1.57 Stepping Revision ID (SRID_0_2_0_PCI) — Offset F8h .....   | 361 |
| 4.1.58 ASL Storage (ASLS_0_2_0_PCI) — Offset FCh .....  | 362 |
| 4.1.59 PASID Extended Capability Header (PASID_EXTCAP_0_2_0_PCI) — Offset 100h .                            |     |

|        |   |     |
|--------|---|-----|
|        | 362   |     |
| 4.1.60 | PASID Capability (PASID_CAP_0_2_0_PCI) — Offset 104h .....                          | 363 |
| 4.1.61 | PASID Control (PASID_CTRL_0_2_0_PCI) — Offset 106h .....                            | 363 |
| 4.1.62 | ATS Extended Capability Header (ATS_EXTCAP_0_2_0_PCI) — Offset 200h..               | 364 |
| 4.1.63 | ATS Capability (ATS_CAP_0_2_0_PCI) — Offset 204h.....                               | 364 |
| 4.1.64 | ATS Control (ATS_CTRL_0_2_0_PCI) — Offset 206h.....                                 | 365 |
| 4.1.65 | Page Request Extended Capability Header (PR_EXTCAP_0_2_0_PCI) — Offset 300h.....    | 366 |
| 4.1.66 | Page Request Control (PR_CTRL_0_2_0_PCI) — Offset 304h .....                        | 366 |
| 4.1.67 | Page Request Status (PR_STATUS_0_2_0_PCI) — Offset 306h.....                        | 367 |
| 4.1.68 | Outstanding Page Request Capacity (OPRC_0_2_0_PCI) — Offset 308h .....              | 368 |
| 4.1.69 | Outstanding Page Request Allocation (OPRA_0_2_0_PCI) — Offset 30Ch.....             | 369 |
| 4.1.70 | SRIOV Extended Capability Header (SRIOV_ECAPHDR_0_2_0_PCI) — Offset 320h 369        |     |
| 4.1.71 | SRIOV Capabilities (SRIOV_CAP_0_2_0_PCI) — Offset 324h.....                         | 370 |
| 4.1.72 | SRIOV Status (SRIOV_STS_0_2_0_PCI) — Offset 32Ah .....                              | 370 |
| 4.1.73 | SRIOV Initial VFs (SRIOV_INITVFS_0_2_0_PCI) — Offset 32Ch .....                     | 371 |
| 4.1.74 | SRIOV Total VFs (SRIOV_TOTVFS_0_2_0_PCI) — Offset 32Eh .....                        | 371 |
| 4.1.75 | First VF Offset (FIRST_VF_OFFSET_0_2_0_PCI) — Offset 334h .....                     | 372 |
| 4.1.76 | VF Stride (VF_STRIDE_0_2_0_PCI) — Offset 336h .....                                 | 372 |
| 4.1.77 | VF Device ID (VF_DEVICEID_0_2_0_PCI) — Offset 33Ah .....                            | 373 |
| 4.1.78 | Supported Page Sizes (SUPPORTED_PAGE_SIZES_0_2_0_PCI) — Offset 33Ch... 373          |     |
| 4.1.79 | System Page Sizes (SYSTEM_PAGE_SIZES_0_2_0_PCI) — Offset 340h.....                  | 374 |
| 4.1.80 | VF BAR0 Lower DWORD (VF_BAR0_LDW_0_2_0_PCI) — Offset 344h.....                      | 375 |
| 4.1.81 | VF BAR0 Upper DWORD (VF_BAR0_UDW_0_2_0_PCI) — Offset 348h .....                     | 376 |
| 4.1.82 | VF BAR1 LDW (VF_BAR1_LDW_0_2_0_PCI) — Offset 34Ch .....                             | 376 |
| 4.1.83 | VF BAR1 UDW (VF_BAR1_UDW_0_2_0_PCI) — Offset 350h.....                              | 377 |
| 4.1.84 | VF Migration State Array Offset (VF_MIGST_OFFSET_0_2_0_PCI) — Offset 35Ch 377       |     |
| 4.2    | Graphics VT BAR (GFXVTBAR) Registers.....   | 378 |
| 4.2.1  | Summary of Registers .....  | 378 |
| 4.2.2  | Version Register (VER_REG_0_0_0_VTDBAR) — Offset 0h.....                            | 380 |
| 4.2.3  | Capability Register (CAP_REG_0_0_0_VTDBAR) — Offset 8h .....                        | 381 |
| 4.2.4  | Extended Capability Register (ECAP_REG_0_0_0_VTDBAR) — Offset 10h .....             | 384 |
| 4.2.5  | Global Command Register (GCMD_REG_0_0_0_VTDBAR) — Offset 18h.....                   | 387 |
| 4.2.6  | Global Status Register (GSTS_REG_0_0_0_VTDBAR) — Offset 1Ch.....                    | 390 |
| 4.2.7  | Root Table Address Register (RTADDR_REG_0_0_0_VTDBAR) — Offset 20h .....            | 392 |
| 4.2.8  | Context Command Register (CCMD_REG_0_0_0_VTDBAR) — Offset 28h.....                  | 393 |
| 4.2.9  | Fault Status Register (FSTS_REG_0_0_0_VTDBAR) — Offset 34h .....                    | 394 |
| 4.2.10 | Fault Event Control Register (FECTL_REG_0_0_0_VTDBAR) — Offset 38h.....             | 396 |
| 4.2.11 | Fault Event Data Register (FEDATA_REG_0_0_0_VTDBAR) — Offset 3Ch.....               | 397 |
| 4.2.12 | Fault Event Address Register (FEADDR_REG_0_0_0_VTDBAR) — Offset 40h .....           | 398 |
| 4.2.13 | Fault Event Upper Address Register (FEUADDR_REG_0_0_0_VTDBAR) — Offset 44h.....     | 398 |
| 4.2.14 | Advanced Fault Log Register (AFLOG_REG_0_0_0_VTDBAR) — Offset 58h ...               | 399 |
| 4.2.15 | Protected Memory Enable Register (PMEN_REG_0_0_0_VTDBAR) — Offset 64h.. 400         |     |
| 4.2.16 | Protected Low Memory Base Register (PLMBASE_REG_0_0_0_VTDBAR) — Offset 68h.....     | 401 |
| 4.2.17 | Protected Low-Memory Limit Register (PLMLIMIT_REG_0_0_0_VTDBAR) — Offset 6Ch .....  | 401 |
| 4.2.18 | Protected High-Memory Base Register (PHMBASE_REG_0_0_0_VTDBAR) — Offset 70h .....   | 402 |
| 4.2.19 | Protected High-Memory Limit Register (PHMLIMIT_REG_0_0_0_VTDBAR) — Offset 78h ..... | 403 |

|        |   |     |
|--------|---|-----|
| 4.2.20 | Invalidation Queue Head Register (IQH_REG_0_0_0_VTDBAR) — Offset 80h                              | 404 |
| 4.2.21 | Invalidation Queue Tail Register (IQT_REG_0_0_0_VTDBAR) — Offset 88h ..                           | 405 |
| 4.2.22 | Invalidation Queue Address Register (IQA_REG_0_0_0_VTDBAR) — Offset 90h ..                        | 405 |
| 4.2.23 | Invalidation Completion Status Register (ICS_REG_0_0_0_VTDBAR) — Offset 9Ch .....                 | 406 |
| 4.2.24 | Invalidation Event Control Register (IECTL_REG_0_0_0_VTDBAR) — Offset A0h .                       | 406 |
| 4.2.25 | Invalidation Event Data Register (IEDATA_REG_0_0_0_VTDBAR) — Offset A4h ..                        | 407 |
| 4.2.26 | Invalidation Event Address Register (IEADDR_REG_0_0_0_VTDBAR) — Offset A8h .....                  | 408 |
| 4.2.27 | Invalidation Event Upper Address Register (IEUADDR_REG_0_0_0_VTDBAR) — Offset ACh.....            | 408 |
| 4.2.28 | Interrupt Remapping Table Address Register (IRTA_REG_0_0_0_VTDBAR) — Offset B8h .....             | 409 |
| 4.2.29 | Page Request Queue Head Register (PQH_REG_0_0_0_VTDBAR) — Offset C0h...                           | 409 |
| 4.2.30 | Page Request Queue Tail Register (PQT_REG_0_0_0_VTDBAR) — Offset C8h                              | 410 |
| 4.2.31 | Page Request Queue Address Register (PQA_REG_0_0_0_VTDBAR) — Offset D0h                           | 411 |
| 4.2.32 | Page Request Status Register (PRS_REG_0_0_0_VTDBAR) — Offset DCh.....                             | 411 |
| 4.2.33 | Page Request Event Control Register (PECTL_REG_0_0_0_VTDBAR) — Offset E0h                         | 412 |
| 4.2.34 | Page Request Event Data Register (PEDATA_REG_0_0_0_VTDBAR) — Offset E4h                           | 413 |
| 4.2.35 | Page Request Event Address Register (PEADDR_REG_0_0_0_VTDBAR) — Offset E8h .....                  | 413 |
| 4.2.36 | Page Request Event Upper Address Register (PEUADDR_REG_0_0_0_VTDBAR) — Offset ECh.....            | 414 |
| 4.2.37 | MTRR Capability Register (MTRRCAP_0_0_0_VTDBAR) — Offset 100h .....                               | 414 |
| 4.2.38 | MTRR Default Type Register (MTRRDEFAULT_0_0_0_VTDBAR) — Offset 108h ....                          | 415 |
| 4.2.39 | Fixed-Range MTRR Format 64K-00000 (MTRR_FIX64K_00000_REG_0_0_0_VTDBAR) — Offset 120h.....         | 416 |
| 4.2.40 | Fixed-Range MTRR Format 16K-80000 (MTRR_FIX16K_80000_REG_0_0_0_VTDBAR) — Offset 128h.....         | 416 |
| 4.2.41 | Fixed-Range MTRR Format 16K-A0000 (MTRR_FIX16K_A0000_REG_0_0_0_VTDBAR) — Offset 130h.....         | 416 |
| 4.2.42 | Fixed-Range MTRR Format 4K-C0000 (MTRR_FIX4K_C0000_REG_0_0_0_VTDBAR) — Offset 138h.....           | 417 |
| 4.2.43 | Fixed-Range MTRR Format 4K-C8000 (MTRR_FIX4K_C8000_REG_0_0_0_VTDBAR) — Offset 140h.....           | 417 |
| 4.2.44 | Fixed-Range MTRR Format 4K-D0000 (MTRR_FIX4K_D0000_REG_0_0_0_VTDBAR) — Offset 148h.....           | 417 |
| 4.2.45 | Fixed-Range MTRR Format 4K-D8000 (MTRR_FIX4K_D8000_REG_0_0_0_VTDBAR) — Offset 150h.....           | 417 |
| 4.2.46 | Fixed-Range MTRR Format 4K-E0000 (MTRR_FIX4K_E0000_REG_0_0_0_VTDBAR) — Offset 158h.....           | 417 |
| 4.2.47 | Fixed-Range MTRR Format 4K-E8000 (MTRR_FIX4K_E8000_REG_0_0_0_VTDBAR) — Offset 160h.....           | 418 |
| 4.2.48 | Fixed-Range MTRR Format 4K-F0000 (MTRR_FIX4K_F0000_REG_0_0_0_VTDBAR) — Offset 168h.....           | 418 |
| 4.2.49 | Fixed-Range MTRR Format 4K-F8000 (MTRR_FIX4K_F8000_REG_0_0_0_VTDBAR) — Offset 170h.....           | 418 |
| 4.2.50 | Variable-Range MTRR Format Physical Base 0 (MTRR_PHYS-BASE0_REG_0_0_0_VTDBAR) — Offset 180h ..... | 418 |



|          |   |            |
|----------|---|------------|
| 4.2.51   | Variable-Range MTRR Format Physical Mask 0 (MTRR_PHYS-MASK0_REG_0_0_0_VTDBAR) — Offset 188h | 419        |
| 4.2.52   | Variable-Range MTRR Format Physical Base 1 (MTRR_PHYS-BASE1_REG_0_0_0_VTDBAR) — Offset 190h | 419        |
| 4.2.53   | Variable-Range MTRR Format Physical Mask 1 (MTRR_PHYS-MASK1_REG_0_0_0_VTDBAR) — Offset 198h | 420        |
| 4.2.54   | Variable-Range MTRR Format Physical Base 2 (MTRR_PHYS-BASE2_REG_0_0_0_VTDBAR) — Offset 1A0h | 420        |
| 4.2.55   | Variable-Range MTRR Format Physical Mask 2 (MTRR_PHYS-MASK2_REG_0_0_0_VTDBAR) — Offset 1A8h | 421        |
| 4.2.56   | Variable-Range MTRR Format Physical Base 3 (MTRR_PHYS-BASE3_REG_0_0_0_VTDBAR) — Offset 1B0h | 421        |
| 4.2.57   | Variable-Range MTRR Format Physical Mask 3 (MTRR_PHYS-MASK3_REG_0_0_0_VTDBAR) — Offset 1B8h | 422        |
| 4.2.58   | Variable-Range MTRR Format Physical Base 4 (MTRR_PHYS-BASE4_REG_0_0_0_VTDBAR) — Offset 1C0h | 422        |
| 4.2.59   | Variable-Range MTRR Format Physical Mask 4 (MTRR_PHYS-MASK4_REG_0_0_0_VTDBAR) — Offset 1C8h | 423        |
| 4.2.60   | Variable-Range MTRR Format Physical Base 5 (MTRR_PHYS-BASE5_REG_0_0_0_VTDBAR) — Offset 1D0h | 423        |
| 4.2.61   | Variable-Range MTRR Format Physical Mask 5 (MTRR_PHYS-MASK5_REG_0_0_0_VTDBAR) — Offset 1D8h | 424        |
| 4.2.62   | Variable-Range MTRR Format Physical Base 6 (MTRR_PHYS-BASE6_REG_0_0_0_VTDBAR) — Offset 1E0h | 424        |
| 4.2.63   | Variable-Range MTRR Format Physical Mask 6 (MTRR_PHYS-MASK6_REG_0_0_0_VTDBAR) — Offset 1E8h | 425        |
| 4.2.64   | Variable-Range MTRR Format Physical Base 7 (MTRR_PHYS-BASE7_REG_0_0_0_VTDBAR) — Offset 1F0h | 425        |
| 4.2.65   | Variable-Range MTRR Format Physical Mask 7 (MTRR_PHYS-MASK7_REG_0_0_0_VTDBAR) — Offset 1F8h | 426        |
| 4.2.66   | Variable-Range MTRR Format Physical Base 8 (MTRR_PHYS-BASE8_REG_0_0_0_VTDBAR) — Offset 200h | 426        |
| 4.2.67   | Variable-Range MTRR Format Physical Mask 8 (MTRR_PHYS-MASK8_REG_0_0_0_VTDBAR) — Offset 208h | 427        |
| 4.2.68   | Variable-Range MTRR Format Physical Base 9 (MTRR_PHYS-BASE9_REG_0_0_0_VTDBAR) — Offset 210h | 427        |
| 4.2.69   | Variable-Range MTRR Format Physical Mask 9 (MTRR_PHYS-MASK9_REG_0_0_0_VTDBAR) — Offset 218h | 428        |
| 4.2.70   | Fault Recording Register Low [0] (FRCDL_REG_0_0_0_VTDBAR) — Offset 400h.<br>429             |            |
| 4.2.71   | Fault Recording Register High [0] (FRCDH_REG_0_0_0_VTDBAR) — Offset 408h<br>429             |            |
| 4.2.72   | Invalidate Address Register (IVA_REG_0_0_0_VTDBAR) — Offset 500h                            | 431        |
| 4.2.73   | IOTLB Invalidate Register (IOTLB_REG_0_0_0_VTDBAR) — Offset 508h                            | 432        |
| <b>5</b> | <b>PCI Express* Controller Registers (D1:F0-2, D6:F0)</b>                                   | <b>435</b> |
| 5.1      | Device Identifiers (ID) — Offset 0h   | 439        |
| 5.2      | Device Command (CMD) — Offset 4h  | 439        |
| 5.3      | Primary Status (PSTS) — Offset 6h   | 440        |
| 5.4      | Revision ID (RID_CC) — Offset 8h  | 441        |
| 5.5      | Cache Line Size (CLS) — Offset Ch   | 442        |
| 5.6      | Primary Latency Timer (PLT) — Offset Dh   | 442        |
| 5.7      | Header Type (HTYPE) — Offset Eh   | 443        |
| 5.8      | Bus Numbers (BNUM_SLT) — Offset 18h   | 443        |
| 5.9      | I/O Base And Limit (IOBL) — Offset 1Ch  | 444        |
| 5.10     | Secondary Status (SSTS) — Offset 1Eh  | 445        |
| 5.11     | Memory Base And Limit (MBL) — Offset 20h  | 445        |



|      |  |     |
|------|--|-----|
| 5.12 | Prefetchable Memory Base And Limit (PMBL) — Offset 24h.....          | 446 |
| 5.13 | Prefetchable Memory Base Upper 32 Bits (PMBU32) — Offset 28h.....    | 447 |
| 5.14 | Prefetchable Memory Limit Upper 32 Bits (PMLU32) — Offset 2Ch.....   | 447 |
| 5.15 | Capabilities List Pointer (CAPP) — Offset 34h.....                   | 447 |
| 5.16 | Interrupt Information (INTR) — Offset 3Ch.....                       | 448 |
| 5.17 | Bridge Control (BCTRL) — Offset 3Eh.....                             | 449 |
| 5.18 | Capabilities List (CLIST) — Offset 40h.....                          | 450 |
| 5.19 | PCI Express Capabilities (XCAP) — Offset 42h.....                    | 451 |
| 5.20 | Device Capabilities (DCAP) — Offset 44h.....                         | 452 |
| 5.21 | Device Control (DCTL) — Offset 48h.....                              | 453 |
| 5.22 | Device Status (DSTS) — Offset 4Ah.....                               | 454 |
| 5.23 | Link Capabilities (LCAP) — Offset 4Ch.....                           | 455 |
| 5.24 | Link Control (LCTL) — Offset 50h.....                                | 457 |
| 5.25 | Link Status (LSTS) — Offset 52h.....                                 | 459 |
| 5.26 | Slot Capabilities (SLCAP) — Offset 54h.....                          | 460 |
| 5.27 | Slot Control (SLCTL) — Offset 58h.....                               | 461 |
| 5.28 | Slot Status (SLSTS) — Offset 5Ah.....                                | 462 |
| 5.29 | Root Control (RCTL) — Offset 5Ch.....                                | 463 |
| 5.30 | Root Status (RSTS) — Offset 60h.....                                 | 464 |
| 5.31 | Device Capabilities 2 (DCAP2) — Offset 64h.....                      | 465 |
| 5.32 | Device Control 2 (DCTL2) — Offset 68h.....                           | 466 |
| 5.33 | Device Status 2 (DSTS2) — Offset 6Ah.....                            | 469 |
| 5.34 | Link Capabilities 2 (LCAP2) — Offset 6Ch.....                        | 469 |
| 5.35 | Link Control 2 (LCTL2) — Offset 70h.....                             | 470 |
| 5.36 | Link Status 2 (LSTS2) — Offset 72h.....                              | 473 |
| 5.37 | Slot Capabilities 2 (SLCAP2) — Offset 74h.....                       | 474 |
| 5.38 | Slot Control 2 (SLCTL2) — Offset 78h.....                            | 474 |
| 5.39 | Slot Status 2 (SLSTS2) — Offset 7Ah.....                             | 474 |
| 5.40 | Message Signaled Interrupt Identifiers (MID) — Offset 80h.....       | 474 |
| 5.41 | Message Signaled Interrupt Message (MC) — Offset 82h.....            | 475 |
| 5.42 | Message Signaled Interrupt Message Address (MA) — Offset 84h.....    | 475 |
| 5.43 | Message Signaled Interrupt Message Data (MD) — Offset 88h.....       | 476 |
| 5.44 | Subsystem Vendor Capability (SVCAP) — Offset 90h.....                | 476 |
| 5.45 | Subsystem Vendor IDs (SVID) — Offset 94h.....                        | 477 |
| 5.46 | Power Management Capability (PMCAP) — Offset A0h.....                | 477 |
| 5.47 | PCI Power Management Capabilities (PMC) — Offset A2h.....            | 478 |
| 5.48 | PCI Power Management Control (PMCS) — Offset A4h.....                | 479 |
| 5.49 | Advanced Error Extended (AECH) — Offset 100h.....                    | 480 |
| 5.50 | Uncorrectable Error Status (UES) — Offset 104h.....                  | 481 |
| 5.51 | Uncorrectable Error Mask (UEM) — Offset 108h.....                    | 482 |
| 5.52 | Uncorrectable Error Severity (UEV) — Offset 10Ch.....                | 483 |
| 5.53 | Correctable Error Status (CES) — Offset 110h.....                    | 484 |
| 5.54 | Correctable Error Mask (CEM) — Offset 114h.....                      | 485 |
| 5.55 | Advanced Error Capabilities And Control (AECC) — Offset 118h.....    | 486 |
| 5.56 | Header Log (HL_DW1) — Offset 11Ch.....                               | 487 |
| 5.57 | Header Log (HL_DW2) — Offset 120h.....                               | 488 |
| 5.58 | Header Log (HL_DW3) — Offset 124h.....                               | 488 |
| 5.59 | Header Log (HL_DW4) — Offset 128h.....                               | 488 |
| 5.60 | Root Error Command (REC) — Offset 12Ch.....                          | 489 |
| 5.61 | Root Error Status (RES) — Offset 130h.....                           | 489 |
| 5.62 | Error Source Identification (ESID) — Offset 134h.....                | 490 |
| 5.63 | PTM Extended Capability Header (PTMECH) — Offset 150h.....           | 491 |
| 5.64 | PTM Capability Register (PTMCAPR) — Offset 154h.....                 | 491 |
| 5.65 | PTM Control Register (PTMCTLR) — Offset 158h.....                    | 492 |
| 5.66 | L1 Sub-States Extended Capability Header (L1SECH) — Offset 200h..... | 493 |

|       |   |     |
|-------|---|-----|
| 5.67  | L1 Sub-States Capabilities (L1SCAP) — Offset 204h .....   | 494 |
| 5.68  | L1 Sub-States Control 1 (L1SCTL1) — Offset 208h .....   | 496 |
| 5.69  | L1 Sub-States Control 2 (L1SCTL2) — Offset 20Ch .....   | 497 |
| 5.70  | ACS Extended Capability Header (ACSECH) — Offset 220h .....   | 498 |
| 5.71  | ACS Capability Register (ACSCAPR) — Offset 224h .....   | 498 |
| 5.72  | ACS Control Register (ACSCTRL) — Offset 226h .....  | 499 |
| 5.73  | Port VC Capability Register 1 (PVCCR1) — Offset 284h .....  | 500 |
| 5.74  | DPC Extended Capability Header (DPCECH) — Offset A00h .....   | 501 |
| 5.75  | DPC Capability Register (DPCCAPR) — Offset A04h .....   | 502 |
| 5.76  | DPC Control Register (DPCCTRL) — Offset A06h .....  | 503 |
| 5.77  | DPC Status Register (DPCSR) — Offset A08h .....   | 504 |
| 5.78  | DPC Error Source ID Register (DPCESIDR) — Offset A0Ah .....   | 505 |
| 5.79  | RP PIO Status Register (RPPIOSR) — Offset A0Ch .....  | 506 |
| 5.80  | RP PIO Mask Register (RPPIOMR) — Offset A10h .....  | 507 |
| 5.81  | RP PIO Severity Register (RPPIOVR) — Offset A14h .....  | 508 |
| 5.82  | RP PIO SysError Register (RPPIOSER) — Offset A18h .....   | 509 |
| 5.83  | RP PIO Exception Register (RPPIOER) — Offset A1Ch .....   | 510 |
| 5.84  | RP PIO Header Log DW1 Register (RPPIOHLR_DW1) — Offset A20h .....   | 510 |
| 5.85  | RP PIO Header Log DW2 Register (RPPIOHLR_DW2) — Offset A24h .....   | 511 |
| 5.86  | RP PIO Header Log DW3 Register (RPPIOHLR_DW3) — Offset A28h .....   | 511 |
| 5.87  | RP PIO Header Log DW4 Register (RPPIOHLR_DW4) — Offset A2Ch .....   | 512 |
| 5.88  | Secondary PCI Express Extended Capability Header (SPEECH) — Offset A30h .....                                 | 512 |
| 5.89  | Link Control 3 (LCTL3) — Offset A34h .....  | 513 |
| 5.90  | Lane Error Status (LES) — Offset A38h .....   | 514 |
| 5.91  | Lane 0 And Lane 1 Equalization Control (L01EC) — Offset A3Ch .....  | 515 |
| 5.92  | Lane 2 And Lane 3 Equalization Control (L23EC) — Offset A40h .....  | 517 |
| 5.93  | Lane 4 And Lane 5 Equalization Control (L45EC) — Offset A44h .....  | 518 |
| 5.94  | Lane 6 And Lane 7 Equalization Control (L67EC) — Offset A48h .....  | 519 |
| 5.95  | Lane 8 And Lane 9 Equalization Control (L89EC) — Offset A4Ch .....  | 521 |
| 5.96  | Lane 10 And Lane 11 Equalization Control (L1011EC) — Offset A50h .....  | 522 |
| 5.97  | Lane 12 And Lane 13 Equalization Control (L1213EC) — Offset A54h .....  | 523 |
| 5.98  | Lane 14 And Lane 15 Equalization Control (L1415EC) — Offset A58h .....  | 525 |
| 5.99  | Data Link Feature Extended Capability Header (DLFECH) — Offset A90h .....                                     | 526 |
| 5.100 | Data Link Feature Capabilities Register (DLFCAP) — Offset A94h .....  | 527 |
| 5.101 | Data Link Feature Status Register (DLFSTS) — Offset A98h .....  | 527 |
| 5.102 | Physical Layer 16.0 GT/s Extended Capability Header (PL16GECH) — Offset A9Ch .....                            | 528 |
| 5.103 | Physical Layer 16.0 GT/s Capability Register (PL16CAP) — Offset AA0h .....                                    | 529 |
| 5.104 | Physical Layer 16.0 GT/s Control Register (PL16CTL) — Offset AA4h .....                                       | 529 |
| 5.105 | Physical Layer 16.0 GT/s Status Register (PL16S) — Offset AA8h .....  | 529 |
| 5.106 | Physical Layer 16.0 GT/s Local Data Parity Mismatch Status Register (PL16LDPMS) — Offset AACH .....           | 530 |
| 5.107 | Physical Layer 16.0 GT/s First Retimer Data Parity Mismatch Status Register (PL16FRD-PMS) — Offset AB0h ..... | 530 |
| 5.108 | Physical Layer 16.0 GT/s Second Retimer Data Parity Mismatch Status Register (PL16SRDPMS) — Offset AB4h ..... | 531 |
| 5.109 | Physical Layer 16.0 GT/s Extra Status Register (PL16ES) — Offset AB8h .....                                   | 531 |
| 5.110 | Physical Layer 16.0 GT/s Lane 01 Equalization Control Register (PL16L01EC) — Offset ABCh .....                | 532 |
| 5.111 | Physical Layer 16.0 GT/s Lane 23 Equalization Control Register (PL16L23EC) — Offset ABEh .....                | 532 |
| 5.112 | Physical Layer 16.0 GT/s Lane 45 Equalization Control Register (PL16L45EC) — Offset AC0h .....                | 533 |
| 5.113 | Physical Layer 16.0 GT/s Lane 67 Equalization Control Register (PL16L67EC) — Offset AC2h .....                | 534 |
| 5.114 | Physical Layer 16.0 GT/s Lane 89 Equalization Control Register (PL16L89EC) — Offset                           |     |

|  |            |
|--|------------|
| AC4h .....   | 535        |
| 5.115 Physical Layer 16.0 GT/s Lane 1011 Equalization Control Register (PL16L1011EC) — Offset AC6h .....   | 536        |
| 5.116 Physical Layer 16.0 GT/s Lane 1213 Equalization Control Register (PL16L1213EC) — Offset AC8h .....   | 537        |
| 5.117 Physical Layer 16.0 GT/s Lane 1415 Equalization Control Register (PL16L1415EC) — Offset ACAh .....   | 538        |
| 5.118 Physical Layer 16.0 GT/s Margining Extended Capability Header (PL16MECH) — Offset EDCh .....         | 539        |
| 5.119 Physical Layer 16.0 GT/s Margining Port Capabilities and Port Status (PL16MPCPS) — Offset EE0h ..... | 540        |
| 5.120 Physical Layer 16.0 GT/s Lane0 Margin Control and Status Register (PL16L0MCS) — Offset EE4h .....    | 541        |
| 5.121 Physical Layer 16.0 GT/s Lane1 Margin Control and Status Register (PL16L1MCS) — Offset EE8h .....    | 542        |
| 5.122 Physical Layer 16.0 GT/s Lane2 Margin Control and Status Register (PL16L2MCS) — Offset EECh .....    | 542        |
| 5.123 Physical Layer 16.0 GT/s Lane3 Margin Control and Status Register (PL16L3MCS) — Offset EF0h .....    | 542        |
| 5.124 Physical Layer 16.0 GT/s Lane4 Margin Control and Status Register (PL16L4MCS) — Offset EF4h .....    | 542        |
| 5.125 Physical Layer 16.0 GT/s Lane5 Margin Control and Status Register (PL16L5MCS) — Offset EF8h .....    | 542        |
| 5.126 Physical Layer 16.0 GT/s Lane6 Margin Control and Status Register (PL16L6MCS) — Offset EFCh .....    | 543        |
| 5.127 Physical Layer 16.0 GT/s Lane7 Margin Control and Status Register (PL16L7MCS) — Offset F00h .....    | 543        |
| 5.128 Physical Layer 16.0 GT/s Lane8 Margin Control and Status Register (PL16L8MCS) — Offset F04h .....    | 543        |
| 5.129 Physical Layer 16.0 GT/s Lane9 Margin Control and Status Register (PL16L9MCS) — Offset F08h .....    | 543        |
| 5.130 Physical Layer 16.0 GT/s Lane10 Margin Control and Status Register (PL16L10MCS) — Offset F0Ch .....  | 543        |
| 5.131 Physical Layer 16.0 GT/s Lane11 Margin Control and Status Register (PL16L11MCS) — Offset F10h .....  | 543        |
| 5.132 Physical Layer 16.0 GT/s Lane12 Margin Control and Status Register (PL16L12MCS) — Offset F14h .....  | 544        |
| 5.133 Physical Layer 16.0 GT/s Lane13 Margin Control and Status Register (PL16L13MCS) — Offset F18h .....  | 544        |
| 5.134 Physical Layer 16.0 GT/s Lane14 Margin Control and Status Register (PL16L14MCS) — Offset F1Ch .....  | 544        |
| 5.135 Physical Layer 16.0 GT/s Lane15 Margin Control and Status Register (PL16L15MCS) — Offset F20h .....  | 544        |
| <b>6 Dynamic Tuning Technology Registers (D4:F0) .....</b>   | <b>545</b> |
| 6.1 Vendor ID (VID_0_4_0_PCI) — Offset 0h .....  | 545        |
| 6.2 Device ID (DID_0_4_0_PCI) — Offset 2h .....  | 546        |
| 6.3 PCI Command (PCICMD_0_4_0_PCI) — Offset 4h .....   | 546        |
| 6.4 PCI Status (PCISTS_0_4_0_PCI) — Offset 6h .....  | 547        |
| 6.5 Revision ID (RID_0_4_0_PCI) — Offset 8h .....  | 549        |
| 6.6 Class Code (CC_0_4_0_PCI) — Offset 9h .....  | 549        |
| 6.7 Extended Class Code (CC_0_4_0_NOPI_PCI) — Offset Ah .....  | 550        |
| 6.8 Cache Line Size Register (CLS_0_4_0_PCI) — Offset Ch .....   | 550        |
| 6.9 Master Latency Timer (MLT_0_4_0_PCI) — Offset Dh .....   | 551        |
| 6.10 Header Type (HDR_0_4_0_PCI) — Offset Eh .....   | 551        |
| 6.11 Built In Self Test (BIST_0_4_0_PCI) — Offset Fh .....   | 551        |
| 6.12 Thermal Controller Base Address (TMBAR_0_4_0_PCI) — Offset 10h .....                                  | 552        |



|          |   |            |
|----------|---|------------|
| 6.13     | Subsystem Vendor ID (SVID_0_4_0_PCI) — Offset 2Ch.....                | 553        |
| 6.14     | Subsystem ID (SID_0_4_0_PCI) — Offset 2Eh.....                        | 553        |
| 6.15     | Capability Pointer (CAPPOINT_0_4_0_PCI) — Offset 34h.....             | 554        |
| 6.16     | Interrupt Line Register (INTRLINE_0_4_0_PCI) — Offset 3Ch.....        | 554        |
| 6.17     | Interrupt Pin Register (INTRPIN_0_4_0_PCI) — Offset 3Dh.....          | 555        |
| 6.18     | Minimum Guaranteed (MINGNT_0_4_0_PCI) — Offset 3Eh.....               | 555        |
| 6.19     | Maximum Latency (MAXLAT_0_4_0_PCI) — Offset 3Fh.....                  | 556        |
| 6.20     | Device Enable (DEVEN_0_4_0_PCI) — Offset 54h.....                     | 556        |
| 6.21     | Capabilities A (CAPID0_A_0_4_0_PCI) — Offset E4h.....                 | 558        |
| 6.22     | Capabilities B (CAPID0_B_0_4_0_PCI) — Offset E8h.....                 | 561        |
| <b>7</b> | <b>Gauss Newton Algorithm Registers (D8:F0) .....</b>                 | <b>565</b> |
| 7.1      | Vendor & Device ID (IDENTIFICATION) — Offset 0h.....                  | 566        |
| 7.2      | Device Control (DCTRL) — Offset 4h.....                               | 566        |
| 7.3      | Device Status (DSTS) — Offset 6h.....                                 | 567        |
| 7.4      | Revision ID & Class Codes (RID_DLCO) — Offset 8h.....                 | 569        |
| 7.5      | Cache Line Size (CLS) — Offset Ch.....                                | 569        |
| 7.6      | Header Type (HTYPE) — Offset Eh.....                                  | 570        |
| 7.7      | Built-in Self Test (BIST) — Offset Fh.....                            | 570        |
| 7.8      | GNA Base Address Low (GNABAL) — Offset 10h.....                       | 571        |
| 7.9      | GNA Base Address High (GNABAH) — Offset 14h.....                      | 572        |
| 7.10     | Sub System Vendor Identifiers (SSVI) — Offset 2Ch.....                | 572        |
| 7.11     | Sub System Identifiers (SSI) — Offset 2Eh.....                        | 573        |
| 7.12     | Capabilities Pointers (CAPP) — Offset 34h.....                        | 573        |
| 7.13     | Interrupt Line (INTL) — Offset 3Ch.....                               | 574        |
| 7.14     | Interrupt Pin Register (INTP) — Offset 3Dh.....                       | 574        |
| 7.15     | Min Grant And Min Latency Register (MINGNTLAT) — Offset 3Eh.....      | 575        |
| 7.16     | Override Configuration Control (OVRCFGCTL) — Offset 40h.....          | 575        |
| 7.17     | Message Signaled Interrupt Capability ID (MSICAPID) — Offset 90h..... | 576        |
| 7.18     | Message Signaled Interrupt Message Control (MC) — Offset 92h.....     | 577        |
| 7.19     | Message Signaled Interrupt Message Address (MA) — Offset 94h.....     | 577        |
| 7.20     | Message Signaled Interrupt Message Data (MD) — Offset 98h.....        | 578        |
| 7.21     | D0i3 Capability ID (D0I3CAPID) — Offset A0h.....                      | 578        |
| 7.22     | D0i3 Capability (D0I3CAP) — Offset A2h.....                           | 579        |
| 7.23     | D0i3 Vendor Extended Capability Register (D0I3VSEC) — Offset A4h..... | 579        |
| 7.24     | D0i3 SW LTR Pointer Register (D0I3SWLTRPTR) — Offset A8h.....         | 580        |
| 7.25     | D0i3 DevIdle Pointer Register (D0I3DEVIDLEPTR) — Offset ACh.....      | 580        |
| 7.26     | D0i3 DevIdle Power On Latency (D0I3DEVIDLEPOL) — Offset B0h.....      | 581        |
| 7.27     | D0i3 Power Control Enables Register (PCE) — Offset B2h.....           | 582        |
| 7.28     | Power Management Capability ID (PMCAPID) — Offset DCh.....            | 582        |
| 7.29     | Power Management Capability (PMCAP) — Offset DEh.....                 | 583        |
| 7.30     | Power Management Control Status (PMCS) — Offset E0h.....              | 584        |
| 7.31     | FLR Capability ID (FLRCAPID) — Offset F0h.....                        | 585        |
| 7.32     | FLR Capability Length And Version (FLRMISC) — Offset F2h.....         | 585        |
| 7.33     | FLR Control Register (FLRCTL) — Offset F4h.....                       | 586        |
| 7.34     | FLR Status Register (FLRSTS) — Offset F5h.....                        | 586        |

## Revision History

---

| Revision Number | Description   | Revision Date |
|-----------------|---|---------------|
| 001             | <ul style="list-style-type: none"><li>Initial release</li></ul> | March 2021    |
| 002             | <ul style="list-style-type: none"><li>Revision Update</li></ul> | May 2021      |

§ §

# 1 Introduction

---

This is Volume 2 of the 11th Generation Intel® Core™ Processor Families Datasheet. Volume 2 provides register information for the processor.

Refer #[634648](#) for the 11th Generation Intel® Core™ Processor Families 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    | <b>Read Only:</b> These bits can only be read by software, writes have no effect. The value of the bits is determined by the hardware only.  |
| RW    | <b>Read / Write:</b> These bits can be read and written by software.   |
| RW1C  | <b>Read / Write 1 to Clear:</b> 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  | <b>Read / Write 0 to Clear:</b> 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  | <b>Read / Write 1 to Set:</b> 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 | <b>Reserved and Preserved:</b> 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 | <b>Reserved and Zero:</b> These bits are reserved for future RW1C implementations. Software should use 0 for writes.   |
| WO    | <b>Write Only:</b> These bits can only be written by software, reads return zero.  |
| RC    | <b>Read Clear:</b> These bits can only be read by software, but a read causes the bits to be cleared. Hardware sets these bits.  |
| RSW1C | <b>Read Set / Write 1 to Clear:</b> 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   | <b>Read Clear / Write:</b> 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)           | <b>Sticky:</b> 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                   | <b>Key:</b> These bits control the ability to write other bits (identified with a 'Lock' modifier)                             |
| -L                 | RW                   | <b>Lock:</b> Hardware can make these bits "Read Only" using a separate configuration bit or other logic.                       |
|                    | WO                   |  |
| -O                 | RW                   | <b>Once:</b> After reset, these bits can only be written by software once, after which they become "Read Only".                |
|                    | WO                   |  |
| -FW                | RO                   | <b>Firmware Write:</b> The value of these bits can be updated by processor hardware mechanisms that may be firmware dependent. |
| -V                 | RO                   | <b>Variant:</b> 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 1: Host-PCI Express\* Bridge – 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 1 is a multi-function device consisting of three functions (0, 1, and 2). Device 1 contains the standard PCI-to-PCI bridge registers and the standard PCI Express/PCI configuration 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 Tuning Technology (DTT) - Logically, this device appears as a PCI device residing on PCI Bus 0. Device 4 contains the configuration registers for the DTT device.
- Device 6: Host-PCI Express\* Bridge – 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 6 contains the standard PCI-to-PCI bridge registers and the standard PCI Express/PCI configuration registers.
- 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>



**Table 2-3. Processor PCI Devices and Functions**

| Description                        | Device | Function |
|------------------------------------|--------|----------|
| HOST and DRAM Controller           | 0      | 0        |
| PCI Express* Controller (x16 PCIe) | 1      | 0        |
| PCI Express* Controller (x8 PCIe)  | 1      | 1        |
| PCI Express* Controller (x4 PCIe)  | 1      | 2        |
| PCI Express* Controller (x4 PCIe)  | 6      | 0        |
| Processor Graphics                 | 2      | 0        |
| Dynamic Tuning Technology          | 4      | 0        |
| Gauss Newton Algorithm Device      | 8      | 0        |
| Trace Hub                          | 9      | 0        |

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.

## 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)

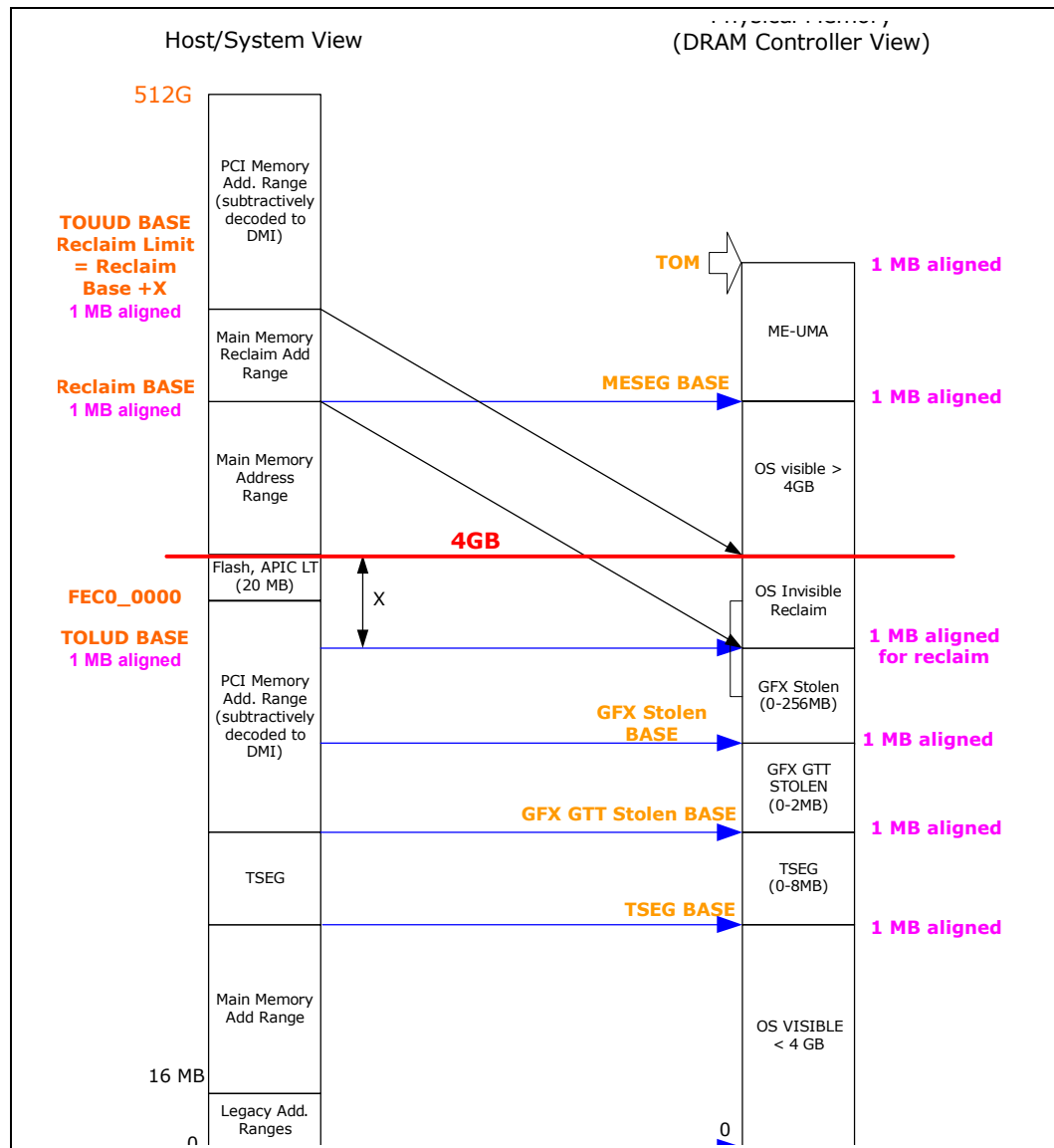


- DMIBAR – This window is used to access registers associated with the processor/PCH Serial Interconnect (DMI) register memory range. (4 KB window).
- VTDPVC0BAR - Memory mapped range for VT-d configuration
- GFXVTBAR - Memory mapped range for VT configuration of the processor graphics device (4KB window).
- 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**



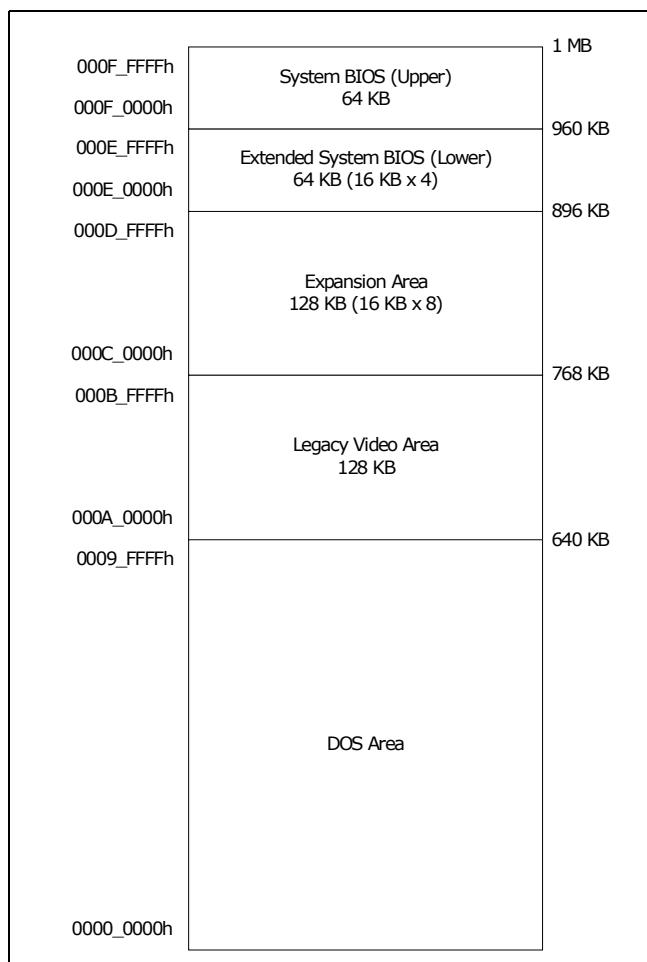
## 2.4 DOS Legacy Address Range

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.

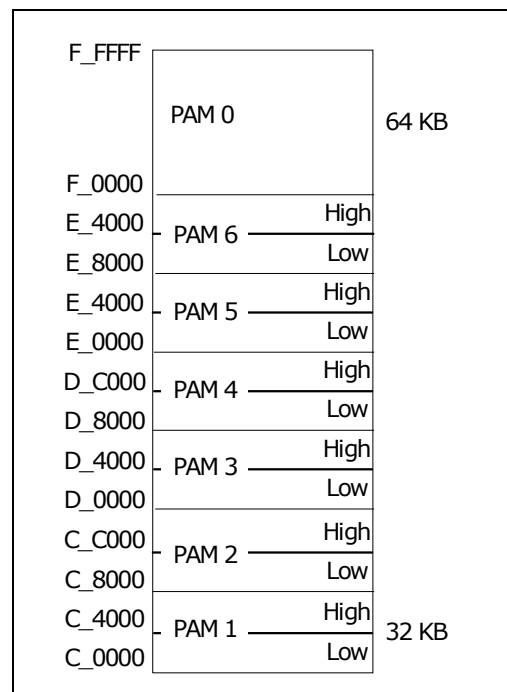
### 2.4.2.2 Monochrome Adapter (MDA) Range

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 deasserted.

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

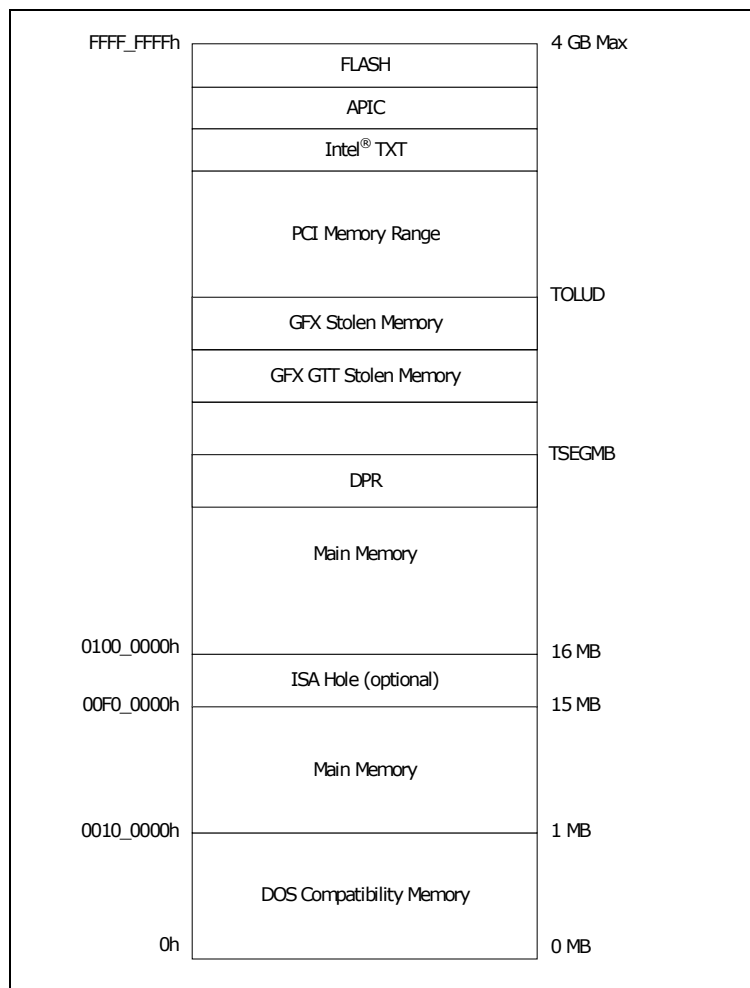
This address range extends from 1 MB to the top of Low Usable physical memory that is permitted to be accessible by the processor (as programmed in the TOLUD register). The processor will route all addresses within this range to the DRAM unless it falls into the optional TSEG, optional ISA Hole or optional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

This address range is divided into two sub-ranges:

- 1 MB to TSEGMB
- TSEGMB to TOLUD

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:

$$\text{TSEGMB} = \text{TOLUD} - \text{DSM SIZE} - \text{GSM SIZE} - \text{TSEG SIZE}$$

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)

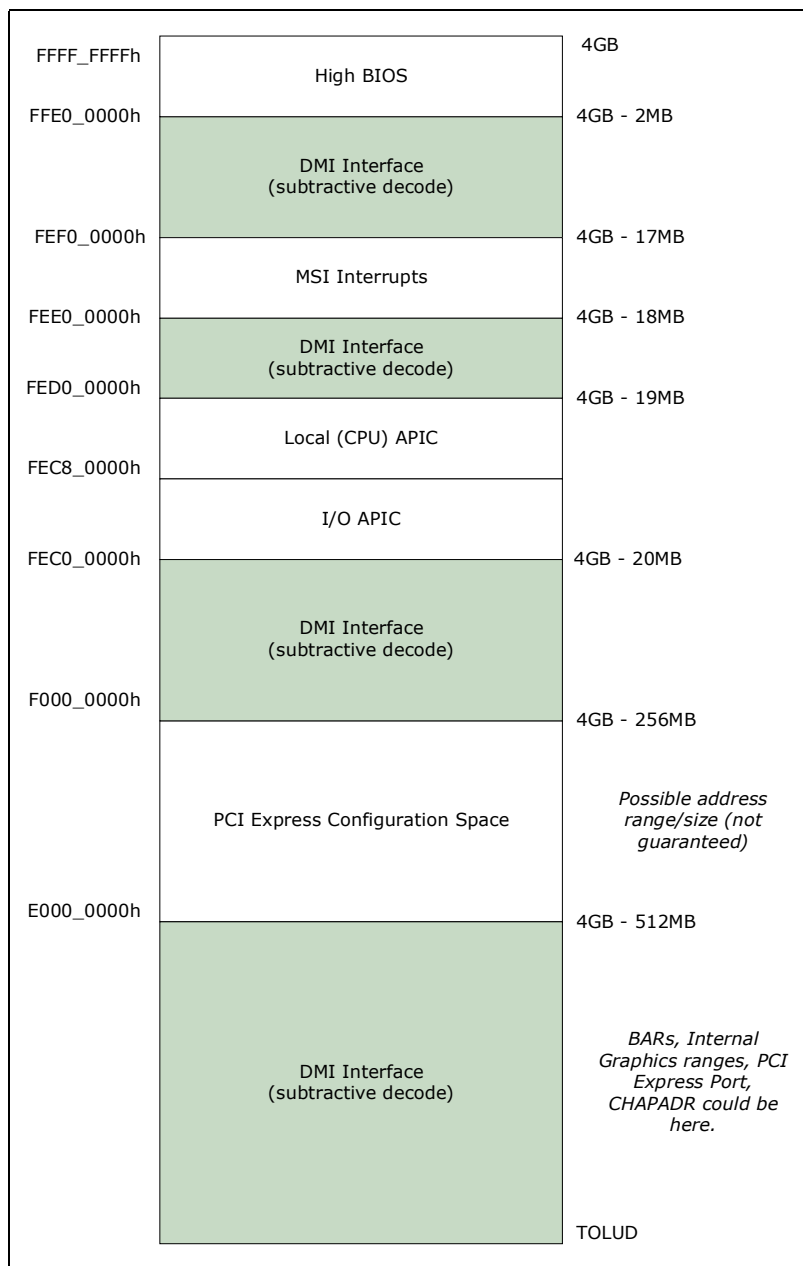
**In an Intel VT enable configuration, there are exceptions to this rule:**

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<sup>®</sup> Management Engine (Intel<sup>®</sup> ME) stolen memory. The Intel<sup>®</sup> ME stolen size register reflects the total amount of physical memory stolen by the Intel<sup>®</sup> ME. The Intel<sup>®</sup> ME stolen memory is located at the top of physical memory. The Intel<sup>®</sup> ME stolen memory base is calculated by subtracting the amount of memory stolen by the Intel<sup>®</sup> 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<sup>®</sup> 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<sup>®</sup> 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 GTTMADR 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 accesses 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:

$$\text{I/O\_Base\_Address} \leq \text{processor I/O Cycle Address} \leq \text{I/O\_Limit\_Address}$$

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

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.

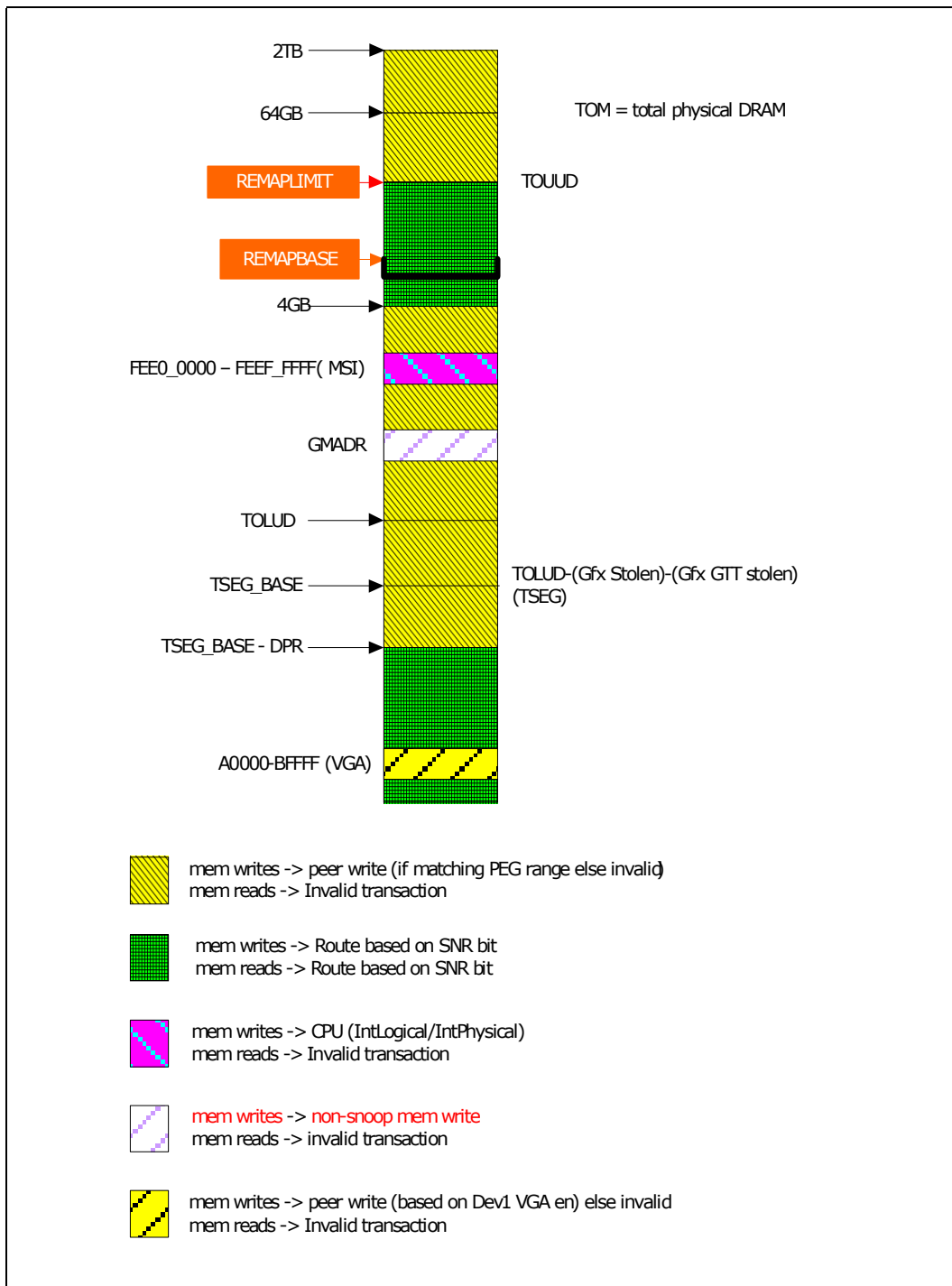
For reads, the processor will provide separate completion status for each naturally-aligned 64-byte block or, if chaining is enabled, each 128-byte block. If the starting address of a transaction hits a valid address, the portion of a request that hits that target device (PCI Express\* or DRAM) will 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<sup>®</sup> ME accesses and Intel<sup>®</sup> High Definition Audio (Intel<sup>®</sup> HD Audio) TC1 access bandwidth.
  - Processor Graphics GMADR writes and GMADR reads are not supported.
- VCm accesses
  - VCm access only map to Intel<sup>®</sup> 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<sup>®</sup> ME accesses its dedicated DRAM stolen space.
  - DMI block will decode these transactions to ensure only Intel<sup>®</sup> 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:

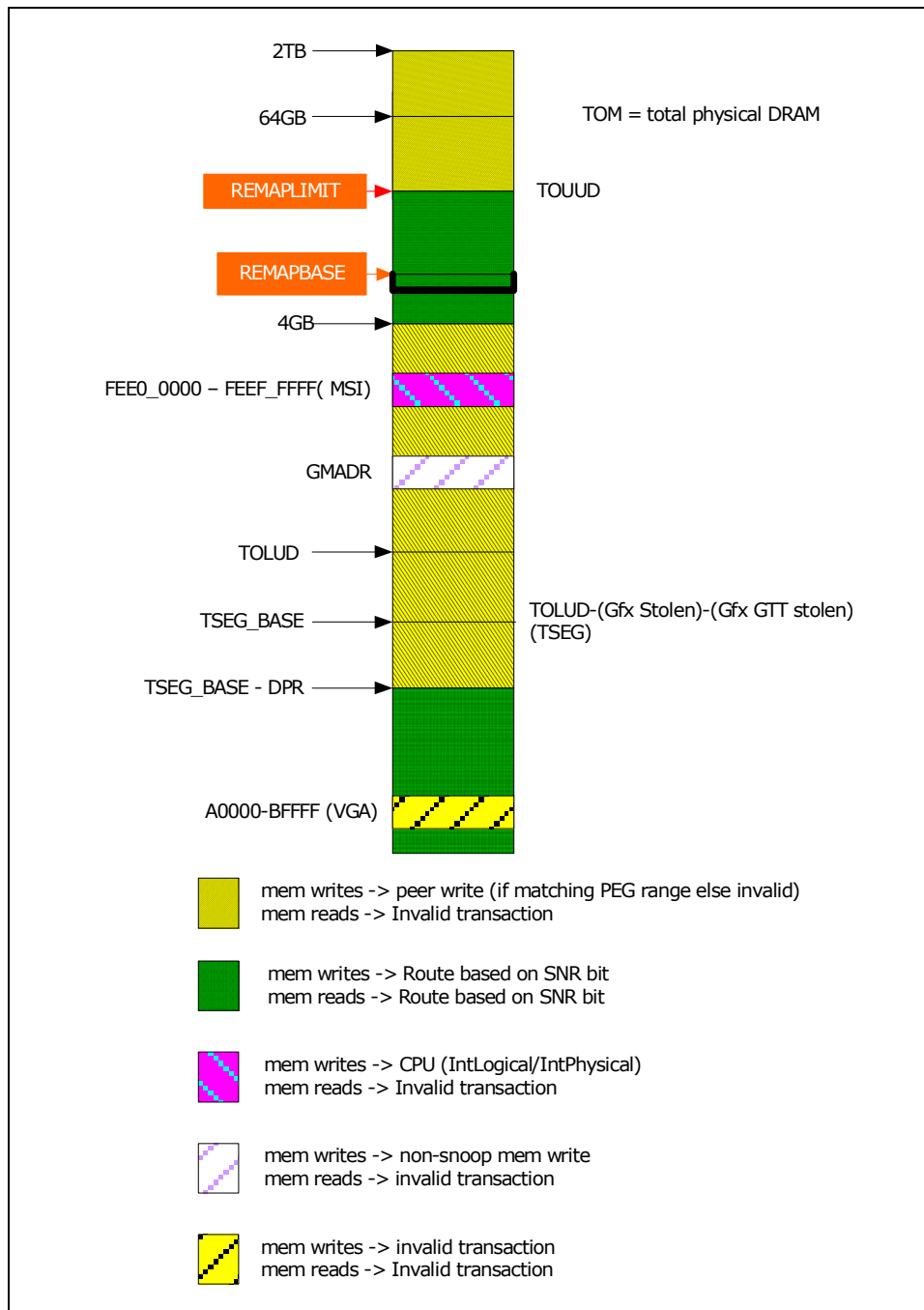
- Reads: Sent to DRAM address 000C\_0000h (non-snooped) and will return "unsuccessful completion".
- Writes: Sent to DRAM address 000C\_0000h (non-snooped) with byte enables all disabled Peer writes from PEG to DMI are not supported.

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<br>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    |
| 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.

### 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     | 4            | Device Identifiers (ID)                                   | 00008086h         |
| 4h     | 2            | Device Command (CMD)                                      | 0006h             |
| 6h     | 2            | Primary Status (PSTS)                                     | 0090h             |
| 8h     | 4            | Revision ID (RID_CC)                                      | 060000F0h         |
| Eh     | 1            | Header Type (HTYPE)                                       | 00h               |
| 1Eh    | 2            | Secondary Status (SSTS)                                   | 0000h             |
| 2Ch    | 4            | Subsystem Vendor IDs (SVD)                                | 00000000h         |
| 34h    | 1            | Capabilities List Pointer (CAPP)                          | E0h               |
| 3Eh    | 1            | Bridge Control (BCTRL)                                    | 00h               |
| 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             |
| 54h    | 4            | Device Enable (DEVEN_0_0_0_PCI)                           | 0000FFFFh         |
| 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 |



| Offset | Size (Bytes) | Register Name (Register Symbol)                 | Default Value     |
|--------|--------------|---|-------------------|
| 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 Device Identifiers (ID) – Offset 0h

Device ID and Vendor ID

| Type | Size   | Offset               | Default   |
|------|--------|----------------------|-----------|
| PCI  | 32 bit | [B:0, D:0, 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<br>RO/V    | <b>Device Identification (DID):</b><br>Processor Device ID. Value is SKU specific. |

| Bit Range | Default & Access | Field Name (ID): Description                            |
|-----------|------------------|---|
| 15:0      | 8086h<br>RO      | <b>Vendor Identification (VID):</b><br>Indicates Intel. |

### 3.1.3 Device Command (CMD) – Offset 4h

Device Command

| 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<br>RO         | <b>Reserved</b>  |
| 9         | 0h<br>RO         | <b>Fast Back to Back Enable (FBE):</b><br>Reserved   |
| 8         | 0h<br>RW         | <b>SERR# Enable (SEE):</b><br>When set, enables the root port to generate an SERR# message when PSTS.SSE is set.   |
| 7         | 0h<br>RO         | <b>Wait Cycle Control (WCC):</b><br>Reserved   |
| 6         | 0h<br>RW         | <b>Parity Error Response Enable (PERE):</b><br>Indicates that the device is capable of reporting parity errors as a master on the backbone.  |
| 5         | 0h<br>RO         | <b>VGA Palette Snoop (VGA_PSE):</b><br>Reserved  |
| 4         | 0h<br>RO         | <b>Memory Write and Invalidate Enable (MWIE):</b><br>Reserved  |
| 3         | 0h<br>RO         | <b>Special Cycle Enable (SCE):</b><br>Reserved   |
| 2         | 1h<br>RO         | <b>Bus Master Enable (BME):</b><br>When set, allows the root port to forward Memory and I/O Read/Write cycles onto the backbone from a PCI-Express device.<br>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.<br>The forwarding of Requests other than Memory or I/O requests is not controlled by this bit. |
| 1         | 1h<br>RO         | <b>Memory Space Enable (MSE):</b><br>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.   |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 0         | 0h<br>RO         | <b>I/O Space Enable (IOSE):</b><br>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. |

### 3.1.4 Primary Status (PSTS) – Offset 6h

Primary Status

| 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<br>RW/1C/V    | <b>Detected Parity Error (DPE):</b><br>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<br>RW/1C/V    | <b>Signaled System Error (SSE):</b><br>Set when the root port signals a system error to the internal SERR# logic.  |
| 13        | 0h<br>RW/1C/V    | <b>Received Master Abort (RMA):</b><br>Set when the root port receives a completion with unsupported request status from the backbone.   |
| 12        | 0h<br>RW/1C/V    | <b>Received Target Abort (RTA):</b><br>Set when the root port receives a completion with completer abort from the backbone.  |
| 11        | 0h<br>RW/1C/V    | <b>Signaled Target Abort (STA):</b><br>Set whenever the root port forwards a target abort received from the downstream device onto the backbone.   |
| 10:9      | 0h<br>RO         | <b>Primary DEVSEL# Timing Status (PDTs):</b><br>Reserved   |
| 8         | 0h<br>RW/1C/V    | <b>Master Data Parity Error Detected (DPD):</b><br>Set when the root port receives a completion with a data parity error on the backbone and PCMD.PERE is set.   |
| 7         | 1h<br>RO         | <b>Primary Fast Back to Back Capable (PFBC):</b><br>Reserved   |
| 6         | 0h<br>RO         | <b>Reserved</b>  |
| 5         | 0h<br>RO         | <b>Primary 66 MHz Capable (PC66):</b><br>Reserved  |
| 4         | 1h<br>RO         | <b>Capabilities List (CLIST):</b><br>Indicates the presence of a capabilities list.  |
| 3         | 0h<br>RO/V       | <b>Interrupt Status (IS):</b><br>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. |

| Bit Range | Default & Access | Field Name (ID): Description |
|-----------|------------------|------------------------------|
| 2:0       | 0h<br>RO         | <b>Reserved</b>              |

### 3.1.5 Revision ID (RID\_CC) – Offset 8h

Revision ID

| Type | Size   | Offset               | Default  |
|------|--------|----------------------|----------|
| PCI  | 32 bit | [B:0, D:0, F:0] + 8h | 06000F0h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| R           | R          | R         |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 31:24     | 06h<br>RO        | <b>Base Class Code (BCC):</b><br>Indicates the device is a bridge device.  |
| 23:16     | 00h<br>RO/V      | <b>Sub-Class Code (SCC):</b><br>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<br>RO/V      | <b>Programming Interface (PI):</b><br>PCI-to-PCI bridge.   |
| 7:0       | F0h<br>RO/V      | <b>Revision ID (RID):</b><br>Indicates the revision of the bridge.<br>The lower nibble, RID[7:0] of this register tracks the Revision ID of the SOC through Set ID Message received from Sideband interface. |

### 3.1.6 Header Type (HTYPE) – Offset Eh

Header Type

| 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         | 0h<br>RO         | <b>Multi-function Device (MFD):</b><br>This bit is '1' to indicate a multi-function device. |



| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 6:0       | 00h<br>RO/V      | <b>Header Type (HTYPE):</b><br>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. |

### 3.1.7 Secondary Status (SSTS) – Offset 1Eh

Secondary Status

| Type | Size   | Offset                | Default |
|------|--------|-----------------------|---------|
| PCI  | 16 bit | [B:0, D:0, 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<br>RW/1C/V    | <b>Detected Parity Error (DPE):</b><br>Set when the port receives a poisoned TLP.   |
| 14        | 0h<br>RW/1C/V    | <b>Received System Error (RSE):</b><br>Set when the port receives an ERR_FATAL or ERR_NONFATAL message from the device.   |
| 13        | 0h<br>RW/1C/V    | <b>Received Master Abort (RMA):</b><br>Set when the port receives a completion with 'Unsupported Request' status from the device.   |
| 12        | 0h<br>RW/1C/V    | <b>Received Target Abort (RTA):</b><br>Set when the port receives a completion with 'Completion Abort' status from the device.  |
| 11        | 0h<br>RW/1C/V    | <b>Signaled Target Abort (STA):</b><br>Set when the port generates a completion with 'Completion Abort' status to the device.   |
| 10:9      | 0h<br>RO/V       | <b>Secondary DEVSEL# Timing Status (SDTS):</b><br>Reserved  |
| 8         | 0h<br>RW/1C/V    | <b>Data Parity Error Detected (DPD):</b><br>Set when the BCTRL.PERE, and either of the following two conditions occurs:<br>Port receives completion marked poisoned.<br>Port poisons a write request to the secondary side. |
| 7         | 0h<br>RO/V       | <b>Secondary Fast Back to Back Capable (SFBC):</b><br>Reserved  |
| 6         | 0h<br>RO         | <b>Reserved</b>   |
| 5         | 0h<br>RO         | <b>Secondary 66 MHz Capable (SC66):</b><br>Reserved   |
| 4:0       | 0h<br>RO         | <b>Reserved</b>   |



### 3.1.8 Subsystem Vendor IDs (SVD) – Offset 2Ch

Subsystem Vendor IDs

| Type | Size   | Offset                | Default   |
|------|--------|-----------------------|-----------|
| PCI  | 32 bit | [B:0, D:0, 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<br>RW/L    | <p><b>Subsystem ID (SSID):</b><br/>           Values for the Subsystem ID are vendor specific. Subsystem ID values, in conjunction with the Subsystem Vendor ID, form a unique identifier for the PCI product. Subsystem ID and Device ID values are distinct and unrelated to each other, and software should not assume any relationship between them.<br/>           This register is Read-Only if LPCR.SRL field is set<br/> <b>Locked by:</b> LPCR.SRL</p>   |
| 15:0      | 0000h<br>RW/L    | <p><b>Subsystem Vendor ID (SVID):</b><br/>           The Subsystem Vendor ID register is used to uniquely identify the add-in card adapter or subsystem where the PCI Express component resides.<br/>           They provide a mechanism for vendors to distinguish their products from one another even though the assemblies may have the same PCI Express component on them (and, therefore, the same Vendor ID and Device ID).<br/>           This register is Read-Only if LPCR.SRL field is set<br/> <b>Locked by:</b> LPCR.SRL</p> |

### 3.1.9 Capabilities List Pointer (CAPP) – Offset 34h

Capabilities List Pointer



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

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 7:0       | E0h<br>RW/O      | <p><b>Capabilities Pointer (PTR):</b><br/>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.</p> <p>Capability Linked List (Default Settings)<br/>Offset   Capability   Next Pointer<br/>40h   PCI Express   80h<br/>80h   Message Signaled Interrupt (MSI)   90h<br/>90h   Subsystem Vendor   A0h<br/>A0h   PCI Power Management   00h</p> <p>Extended PCIe Capability Linked List<br/>Offset   Capability   Next Pointer<br/>100h   Advanced Error Reporting   000h<br/>140h   Access Control Services   000h<br/>200h   L1 Sub-states   000h<br/>220h   Secondary PCI Express Capability   000h</p> |

### 3.1.10 Bridge Control (BCTRL) – Offset 3Eh

Bridge Control

| Type | Size  | Offset                | Default |
|------|-------|-----------------------|---------|
| PCI  | 8 bit | [B:0, D:0, F:0] + 3Eh | 00h     |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 7:2       | 0h<br>RO         | <b>Reserved</b>  |
| 1         | 0h<br>RW         | <p><b>SERR# Enable (SE):</b><br/>When set, ERR_COR, ERR_NONFATAL, and ERR_FATAL messages received are forwarded to the backbone. When cleared, they are not.</p> |
| 0         | 0h<br>RO         | <b>Reserved</b>  |

### 3.1.11 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<br>RO         | <b>Reserved</b>  |
| 38:12     | 0000000h<br>RW   | <b>PXPEPBAR:</b><br>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<br>RO         | <b>Reserved</b>  |
| 0         | 0h<br>RW         | <b>PXPEPBAR Enable (PXPEPBAREN):</b><br>0: PXPEPBAR is disabled and does not claim any memory<br>1: PXPEPBAR memory mapped accesses are claimed and decoded appropriately<br>This register is locked by Intel TXT.   |

### 3.1.12 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<br>RO         | <b>Reserved</b>  |
| 38:16     | 000000h<br>RW    | <b>MCHBAR:</b><br>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<br>RO         | <b>Reserved</b>  |
| 0         | 0h<br>RW         | <b>MCHBAREN:</b><br>0: MCHBAR is disabled and does not claim any memory<br>1: MCHBAR memory mapped accesses are claimed and decoded appropriately<br>This register is locked in Intel TXT mode.  |

### 3.1.13 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<br>RW/L      | <b>GMS:</b><br>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.<br>This register is also Intel TXT lockable.<br>Hardware does not clear or set any of these bits automatically based on IGD being disabled/enabled.<br>BIOS Requirement: BIOS must not set this field to 0h if IVD (bit 1 of this register) is 0.<br><b>Locked by:</b> GGC_0_0_0_PCI.GGCLCK |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 7:6       | 0h<br>RW/L       | <b>GGMS:</b><br>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.<br>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.<br>Hardware functionality in case of programming this value to Reserved is not guaranteed.<br><b>Locked by:</b> GGC_0_0_0_PCI.GGCLCK |
| 5:3       | 0h<br>RO         | <b>Reserved</b>  |
| 2         | 0h<br>RW/L       | <b>VAMEN:</b><br>Enables the use of the iGFX engines for Versatile Acceleration.<br>1 - iGFX engines are in Versatile Acceleration Mode. Device 2 Class Code is 048000h.<br>0 - iGFX engines are in iGFX Mode. Device 2 Class Code is 030000h.<br><b>Locked by:</b> GGC_0_0_0_PCI.GGCLCK   |
| 1         | 0h<br>RW/L       | <b>IVD:</b><br>0: Enable. Device 2 (IGD) claims VGA memory and IO cycles, the Sub-Class Code within Device 2 Class Code register is 00.<br>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.<br>BIOS Requirement: BIOS must not set this bit to 0 if the GMS field (bits 7:3 of this register) pre-allocates no memory.<br><b>Locked by:</b> GGC_0_0_0_PCI.GGCLCK   |
| 0         | 0h<br>RW/L       | <b>GGCLCK:</b><br>When set to 1b, this bit will lock all bits in this register.<br><b>Locked by:</b> GGC_0_0_0_PCI.GGCLCK  |

### 3.1.14 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 | 0000FFFFh |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | R          | R         |

| Bit Range | Default & Access | Field Name (ID): Description |
|-----------|------------------|------------------------------|
| 31:16     | 0h<br>RO         | <b>Reserved</b>              |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 15        | 1h<br>RW/L       | <p><b>D8EN:</b><br/>0: Bus 0 Device 8 is disabled and not visible.<br/>1: Bus 0 Device 8 is enabled and visible.<br/>This bit will be set to 0b and remain 0b if Device 8 capability is disabled.<br/><b>Locked by:</b> CAPID0_B_0_0_0_PCI.GMM_DIS</p>   |
| 14        | 1h<br>RW/L       | <p><b>D14F0EN:</b><br/>VMD Enable -<br/>0: Bus 0 Device 14 Function 0 is disabled and hidden.<br/>1: Bus 0 Device 14 Function 0 is enabled and visible.<br/><b>Locked by:</b> CAPID0_B_0_0_0_PCI.VMD_DIS</p>   |
| 13        | 1h<br>RW/L       | <p><b>D6EN:</b><br/>0: Bus 0 Device 6 Function 0 is disabled and not visible.<br/>1: Bus 0 Device 6 Function 0 is enabled and visible.<br/>This bit will be set to 0b and remain 0b if Device 6 Function 0 capability is disabled.<br/><b>Locked by:</b> CAPID0_A_0_0_0_PCI.PEG60D</p>                                     |
| 12        | 1h<br>RW/L       | <p><b>D9EN:</b><br/>0: Bus 0 Device 9 is disabled and not visible.<br/>1: Bus 0 Device 9 is enabled and visible.<br/>This bit will be set to 0b and remain 0b if Device 9 capability is disabled.<br/><b>Locked by:</b> CAPID0_B_0_0_0_PCI.NPK_DIS</p>   |
| 11        | 1h<br>RW/L       | <p><b>D10EN:</b><br/>Device10 enable<br/>0: Bus 0 Device 10 is disabled and not visible.<br/>1: Bus 0 Device 10 is enabled and visible.<br/>This bit will be set to 0b and remain 0b if Device 10 capability is disabled.<br/><b>Locked by:</b> CAPID0_B_0_0_0_PCI.DEVICE10_DIS</p>  |
| 10        | 1h<br>RW/L       | <p><b>D5EN:</b><br/>0: Bus 0 Device 5 is disabled and not visible.<br/>1: Bus 0 Device 5 is enabled and visible.<br/>This bit will be set to 0b and remain 0b if Device 5 capability is disabled.<br/><b>Locked by:</b> CAPID0_B_0_0_0_PCI.IMGU_DIS</p>  |
| 9         | 1h<br>RW/L       | <p><b>D11F1EN:</b><br/>Device11 function 1 enable<br/>0: Bus 0 Device 11 function 1 is disabled and not visible.<br/>1: Bus 0 Device 11 function 1 is enabled and visible.<br/>This bit will be set to 0b and remain 0b if Device 11F1 capability is disabled.<br/><b>Locked by:</b> CAPID0_B_0_0_0_PCI.DEVICE11F1_DIS</p> |
| 8         | 1h<br>RW/L       | <p><b>D11F0EN:</b><br/>Device11 function 0 enable<br/>0: Bus 0 Device 11 function 0 is disabled and not visible.<br/>1: Bus 0 Device 11 function 0 is enabled and visible.<br/>This bit will be set to 0b and remain 0b if Device 11F0 capability is disabled.<br/><b>Locked by:</b> CAPID0_B_0_0_0_PCI.DEVICE11F0_DIS</p> |
| 7         | 1h<br>RW/L       | <p><b>D4EN:</b><br/>0: Bus 0 Device 4 is disabled and not visible.<br/>1: Bus 0 Device 4 is enabled and visible.<br/>This bit will be set to 0b and remain 0b if Device 4 capability is disabled.<br/><b>Locked by:</b> CAPID0_A_0_0_0_PCI.CDD</p>   |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 6         | 1h<br>RW/L       | <b>D3F7EN:</b><br>NVMe - Device 3 function 7 enable<br>0: Bus 0 Device 3 function 7 is disabled and hidden<br>1: Bus 0 Device 3 function 7 is enabled and visible<br>This bit will be set to 0b and remain 0b if Device 3 capability is disabled.<br><b>Locked by:</b> CAPID0_A_0_0_0_PCI.NVME_F7D |
| 5         | 1h<br>RW/L       | <b>D3F0EN:</b><br>NVMe - Device 3 function 0 enable<br>0: Bus 0 Device 3 function 0 is disabled and hidden<br>1: Bus 0 Device 3 function 0 is enabled and visible<br>This bit will be set to 0b and remain 0b if Device 3 capability is disabled.<br><b>Locked by:</b> CAPID0_A_0_0_0_PCI.NVME_F0D |
| 4         | 1h<br>RW/L       | <b>D2EN:</b><br>0: Bus 0 Device 2 is disabled and hidden<br>1: Bus 0 Device 2 is enabled and visible<br>This bit will be set to 0b and remain 0b if Device 2 capability is disabled.<br><b>Locked by:</b> CAPID0_A_0_0_0_PCI.IGD   |
| 3         | 1h<br>RW/L       | <b>D1F0EN:</b><br>0: Bus 0 Device 1 Function 0 is disabled and hidden.<br>1: Bus 0 Device 1 Function 0 is enabled and visible.<br>This bit will be set to 0b and remain 0b if PEG10 capability is disabled.<br><b>Locked by:</b> CAPID0_A_0_0_0_PCI.PEG10D   |
| 2         | 1h<br>RW/L       | <b>D1F1EN:</b><br>0: Bus 0 Device 1 Function 1 is disabled and hidden.<br>1: Bus 0 Device 1 Function 1 is enabled and visible.<br><b>Locked by:</b> CAPID0_A_0_0_0_PCI.PEG11D  |
| 1         | 1h<br>RW/L       | <b>D1F2EN:</b><br>0: Bus 0 Device 1 Function 2 is disabled and hidden.<br>1: Bus 0 Device 1 Function 2 is enabled and visible.<br><b>Locked by:</b> CAPID0_A_0_0_0_PCI.PEG12D  |
| 0         | 1h<br>RO         | <b>DOEN:</b><br>Bus 0 Device 0 Function 0 may not be disabled and is therefore hardwired to 1.   |

### 3.1.15 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 | 0000001h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | R          | R         |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 31:20     | 000h<br>RW/L     | <p><b>PCMBASE:</b><br/>           Sizes supported: 1M, 2M, 4M and 8M.<br/>           Base value programmed (from Top of Stolen Memory) itself defines the size of the WOPCM.<br/>           Separate WOPCM size programming is redundant information and not required.<br/>           Default 1M size programming. 4M recommended.<br/>           This register is locked (becomes read-only) when PAVPE = 1b.<br/> <b>Locked by:</b> PAVPC_0_0_0_PCI.PAVPLCK</p>   |
| 19:7      | 0h<br>RO         | <b>Reserved</b>   |
| 6         | 0h<br>RW/L       | <p><b>ASMFEN:</b><br/>           ASMF method enabled<br/>           0b Disabled (default).<br/>           1b Enabled.<br/>           This register is locked when PAVPLCK is set.<br/> <b>Locked by:</b> PAVPC_0_0_0_PCI.PAVPLCK</p>  |
| 5         | 0h<br>RO         | <b>Reserved</b>   |
| 4         | 0h<br>RW/L       | <p><b>OVTATTACK:</b><br/>           Override of Unsolicited Connection State Attack and Terminate.<br/>           0: Disable Override. Attack Terminate allowed.<br/>           1: Enable Override. Attack Terminate disallowed.<br/>           This register bit is locked when PAVPE is set.<br/> <b>Locked by:</b> PAVPC_0_0_0_PCI.PAVPLCK</p>   |
| 3         | 0h<br>RW/L       | <p><b>HVYMODESEL:</b><br/>           This bit is applicable only for PAVP2 operation mode or for PAVP3 mode only if the per-App memory configuration is disabled.<br/>           0: Lite Mode (Non-Serpent mode)<br/>           1: Serpent Mode<br/>           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.<br/> <b>Locked by:</b> PAVPC_0_0_0_PCI.PAVPLCK</p> |
| 2         | 0h<br>RW/L       | <p><b>PAVP Lock (PAVPLCK):</b><br/>           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).<br/> <b>Locked by:</b> PAVPC_0_0_0_PCI.PAVPLCK</p>  |
| 1         | 0h<br>RW/L       | <p><b>PAVPE:</b><br/>           0: PAVP functionality is disabled.<br/>           1: PAVP functionality is enabled.<br/>           This register is locked when PAVPLCK is set.<br/> <b>Locked by:</b> PAVPC_0_0_0_PCI.PAVPLCK</p>  |



| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 0         | 1h<br>RW/L       | <p><b>PCME:</b><br/>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.<br/>This register is locked when PAVPLOCK is set.<br/>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.<br/>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.<br/>For non-PAVP3 Mode, even for Lite mode configuration, this bit should be programmed to 1 and HVYMODESEL = 0).<br/>This bit should always be programmed to 1 if bits 1 and 2 (PAVPE and PAVP lock bits) are both set.<br/>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.<br/><b>Locked by:</b> PAVPC_0_0_0_PCI.PAVPLCK</p> |

### 3.1.16 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<br>RW/V/L   | <p><b>TOPOFDPR:</b><br/>Top address + 1 of DPR. This is the base of TSEG. Bits 19:0 of the BASE reported here are 0x0_0000.</p> |
| 19:12     | 0h<br>RO         | <b>Reserved</b>   |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 11:4      | 00h<br>RW/L      | <p><b>DPRSIZE:</b><br/>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p><b>Locked by:</b> DPR_0_0_0_PCI.LOCK</p> |
| 3         | 0h<br>RO         | <b>Reserved</b>  |
| 2         | 0h<br>RW/L       | <p><b>EPM:</b><br/>This field controls DMA accesses to the DMA Protected Range (DPR) region.<br/>0: DPR is disabled<br/>1: DPR is enabled. All DMA requests accessing DPR region are blocked.<br/>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.</p> <p><b>Locked by:</b> DPR_0_0_0_PCI.LOCK</p>  |
| 1         | 0h<br>RW/V/L     | <p><b>PRS:</b><br/>This field indicates the status of DPR.<br/>0: DPR protection disabled<br/>1: DPR protection enabled</p>  |
| 0         | 0h<br>RW/L       | <p><b>LOCK:</b><br/>All bits which may be updated by SW in this register are locked down when this bit is set.</p> <p><b>Locked by:</b> DPR_0_0_0_PCI.LOCK</p>   |

### 3.1.17 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<br>RO         | <b>Reserved</b>  |
| 38:31     | 00h<br>RW        | <p><b>PCIEXBAR:</b><br/>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:<br/>PCI Express Base Address + Segment Number*256MB+ Bus Number * 1MB + Device Number * 32KB + Function Number * 4KB<br/>This address is the beginning of the 4KB space that contains both the PCI compatible configuration space and the PCI Express extended configuration space.</p> |
| 30        | 0h<br>RW/V       | <p><b>ADMSK1024:</b><br/>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.</p>   |
| 29        | 0h<br>RW/V       | <p><b>ADMSK512:</b><br/>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.</p>  |
| 28        | 0h<br>RW/V       | <p><b>ADMSK256:</b><br/>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.</p>  |
| 27        | 0h<br>RW/V       | <p><b>ADMSK128:</b><br/>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.</p>  |
| 26        | 0h<br>RW/V       | <p><b>ADMSK64:</b><br/>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.</p>   |
| 25:4      | 0h<br>RO         | <b>Reserved</b>  |

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

### 3.1.18 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<br>RO         | <b>Reserved</b>  |
| 38:12     | 0000000h<br>RW   | <b>DMIBAR:</b><br>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<br>RO         | <b>Reserved</b>  |

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

### 3.1.19 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<br>RO         | <b>Reserved</b>   |
| 5:4       | 0h<br>RW/L       | <b>HIENABLE:</b><br>This field controls the steering of read and write cycles that address the BIOS area from 0F_0000h to 0F_FFFFh.<br>00: DRAM Disabled. All accesses are directed to DMI.<br>01: Read Only. All reads are sent to DRAM, all writes are forwarded to DMI.<br>10: Write Only. All writes are sent to DRAM, all reads are serviced by DMI.<br>11: Normal DRAM Operation. All reads and writes are serviced by DRAM.<br><b>Locked by:</b> PAM0_0_0_0_PCI.LOCK |
| 3:1       | 0h<br>RO         | <b>Reserved</b>   |



| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 0         | 0h<br>RW/L       | <b>LOCK:</b><br>If this bit is set, all of the PAM* registers are locked (cannot be written)<br><b>Locked by:</b> PAM0_0_0_0_PCI.LOCK |

### 3.1.20 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<br>RO         | <b>Reserved</b>   |
| 5:4       | 0h<br>RW/L       | <b>HIENABLE:</b><br>This field controls the steering of read and write cycles that address the BIOS area from 0C_4000h to 0C_7FFFh.<br>00: DRAM Disabled. All accesses are directed to DMI.<br>01: Read Only. All reads are sent to DRAM, all writes are forwarded to DMI.<br>10: Write Only. All writes are sent to DRAM, all reads are serviced by DMI.<br>11: Normal DRAM Operation. All reads and writes are serviced by DRAM.<br><b>Locked by:</b> PAM0_0_0_0_PCI.LOCK |
| 3:2       | 0h<br>RO         | <b>Reserved</b>   |

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

### 3.1.21 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<br>RO         | <b>Reserved</b>              |

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

### 3.1.22 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<br>RO         | <b>Reserved</b>  |
| 5:4       | 0h<br>RW/L       | <b>HIENABLE:</b><br>This field controls the steering of read and write cycles that address the BIOS area from 0D4000h to 0D7FFFh.<br>00: DRAM Disabled. All accesses are directed to DMI.<br>01: Read Only. All reads are sent to DRAM, all writes are forwarded to DMI.<br>10: Write Only. All writes are sent to DRAM, all reads are serviced by DMI.<br>11: Normal DRAM Operation. All reads and writes are serviced by DRAM.<br><b>Locked by:</b> PAM0_0_0_0_PCI.LOCK                            |
| 3:2       | 0h<br>RO         | <b>Reserved</b>  |
| 1:0       | 0h<br>RW/L       | <b>LOENABLE:</b><br>This field controls the steering of read and write cycles that address the BIOS area from 0D0000h to 0D3FFFh.<br>00: DRAM Disabled. All reads are sent to DRAM. All writes are forwarded to DMI.<br>01: Read Only. All reads are sent to DRAM. All writes are forwarded to DMI.<br>10: Write Only. All writes are sent to DRAM. All reads are serviced by DMI.<br>11: Normal DRAM Operation. All reads and writes are serviced by DRAM.<br><b>Locked by:</b> PAM0_0_0_0_PCI.LOCK |

### 3.1.23 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<br>RO         | <b>Reserved</b>  |
| 5:4       | 0h<br>RW/L       | <b>HIENABLE:</b><br>This field controls the steering of read and write cycles that address the BIOS area from 0DC000h to 0DFFFFh.<br>00: DRAM Disabled. All accesses are directed to DMI.<br>01: Read Only. All reads are sent to DRAM, all writes are forwarded to DMI.<br>10: Write Only. All writes are sent to DRAM, all reads are serviced by DMI.<br>11: Normal DRAM Operation. All reads and writes are serviced by DRAM.<br><b>Locked by:</b> PAM0_0_0_0_PCI.LOCK                            |
| 3:2       | 0h<br>RO         | <b>Reserved</b>  |
| 1:0       | 0h<br>RW/L       | <b>LOENABLE:</b><br>This field controls the steering of read and write cycles that address the BIOS area from 0D8000h to 0DBFFFh.<br>00: DRAM Disabled. All reads are sent to DRAM. All writes are forwarded to DMI.<br>01: Read Only. All reads are sent to DRAM. All writes are forwarded to DMI.<br>10: Write Only. All writes are sent to DRAM. All reads are serviced by DMI.<br>11: Normal DRAM Operation. All reads and writes are serviced by DRAM.<br><b>Locked by:</b> PAM0_0_0_0_PCI.LOCK |

### 3.1.24 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<br>RO         | <b>Reserved</b>  |
| 5:4       | 0h<br>RW/L       | <b>HIENABLE:</b><br>This field controls the steering of read and write cycles that address the BIOS area from 0E4000h to 0E7FFFh.<br>00: DRAM Disabled. All accesses are directed to DMI.<br>01: Read Only. All reads are sent to DRAM, all writes are forwarded to DMI.<br>10: Write Only. All writes are sent to DRAM, all reads are serviced by DMI.<br>11: Normal DRAM Operation. All reads and writes are serviced by DRAM.<br><b>Locked by:</b> PAM0_0_0_0_PCI.LOCK                            |
| 3:2       | 0h<br>RO         | <b>Reserved</b>  |
| 1:0       | 0h<br>RW/L       | <b>LOENABLE:</b><br>This field controls the steering of read and write cycles that address the BIOS area from 0E0000h to 0E3FFFh.<br>00: DRAM Disabled. All reads are sent to DRAM. All writes are forwarded to DMI.<br>01: Read Only. All reads are sent to DRAM. All writes are forwarded to DMI.<br>10: Write Only. All writes are sent to DRAM. All reads are serviced by DMI.<br>11: Normal DRAM Operation. All reads and writes are serviced by DRAM.<br><b>Locked by:</b> PAM0_0_0_0_PCI.LOCK |

### 3.1.25 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<br>RO         | <b>Reserved</b>  |
| 5:4       | 0h<br>RW/L       | <b>HIENABLE:</b><br>This field controls the steering of read and write cycles that address the BIOS area from 0EC000h to 0EFFFFh.<br>00: DRAM Disabled. All accesses are directed to DMI.<br>01: Read Only. All reads are sent to DRAM, all writes are forwarded to DMI.<br>10: Write Only. All writes are sent to DRAM, all reads are serviced by DMI.<br>11: Normal DRAM Operation. All reads and writes are serviced by DRAM.<br><b>Locked by:</b> PAM0_0_0_0_PCI.LOCK                            |
| 3:2       | 0h<br>RO         | <b>Reserved</b>  |
| 1:0       | 0h<br>RW/L       | <b>LOENABLE:</b><br>This field controls the steering of read and write cycles that address the BIOS area from 0E8000h to 0EBFFFh.<br>00: DRAM Disabled. All reads are sent to DRAM. All writes are forwarded to DMI.<br>01: Read Only. All reads are sent to DRAM. All writes are forwarded to DMI.<br>10: Write Only. All writes are sent to DRAM. All reads are serviced by DMI.<br>11: Normal DRAM Operation. All reads and writes are serviced by DRAM.<br><b>Locked by:</b> PAM0_0_0_0_PCI.LOCK |

### 3.1.26 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<br>RW         | <p><b>HEN:</b><br/>This field enables a memory hole in DRAM space. The DRAM that lies behind this space is not remapped.<br/>0: No memory hole.<br/>1: Memory hole from 15MB to 16MB.<br/>This bit is Intel TXT lockable.</p>  |
| 6:5       | 0h<br>RO         | <p><b>Reserved</b></p>   |
| 4         | 1h<br>RW         | <p><b>MDAPCIE:</b><br/>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.<br/>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.<br/>The behavior of this bit field is identical to bits [3:0]</p>   |
| 3         | 0h<br>RW         | <p><b>MDAP60:</b><br/>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.<br/>If device 1 function 2 VGA enable bit is not set, then accesses to IO address range x3BCh-x3BFh remain on the backbone.<br/>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.<br/>MDA resources are defined as the following:<br/>Memory: 0B0000h - 0B7FFFh<br/>I/O: 3B4h, 3B5h, 3B8h, 3B9h, 3BAh, 3BFh,<br/>(including ISA address aliases, A[15:10] are not used in decode)<br/>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.<br/>The following table shows the behavior for all combinations of MDA and VGA:<br/>VGAEN MDAP Description<br/>0 0 All References to MDA and VGA space are not claimed by Device 1 Function 2.<br/>0 1 Illegal combination<br/>1 0 All VGA and MDA references are routed to PCI Express Graphics Attach device 1 function 2.<br/>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.<br/>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.</p> |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 2         | 0h<br>RW         | <p><b>MDAP12:</b></p> <p>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.</p> <p>If device 1 function 2 VGA enable bit is not set, then accesses to IO address range x3BCh-x3BFh remain on the backbone.</p> <p>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.</p> <p>MDA resources are defined as the following:<br/>Memory: 0B0000h - 0B7FFFh<br/>I/O: 3B4h, 3B5h, 3B8h, 3B9h, 3BAh, 3BFh,<br/>(including ISA address aliases, A[15:10] are not used in decode)</p> <p>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.</p> <p>The following table shows the behavior for all combinations of MDA and VGA:<br/>VGAEN MDAP Description<br/>0 0 All References to MDA and VGA space are not claimed by Device 1 Function 2.<br/>0 1 Illegal combination<br/>1 0 All VGA and MDA references are routed to PCI Express Graphics Attach device 1 function 2.<br/>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.</p> <p>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.</p> |
| 1         | 0h<br>RW         | <p><b>MDAP11:</b></p> <p>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.</p> <p>If device 1 function 1 VGA enable bit is not set, then accesses to IO address range x3BCh-x3BFh remain on the backbone.</p> <p>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.</p> <p>MDA resources are defined as the following:<br/>Memory: 0B0000h - 0B7FFFh<br/>I/O: 3B4h, 3B5h, 3B8h, 3B9h, 3BAh, 3BFh,<br/>(including ISA address aliases, A[15:10] are not used in decode)</p> <p>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.</p> <p>The following table shows the behavior for all combinations of MDA and VGA:<br/>VGAEN MDAP Description<br/>0 0 All References to MDA and VGA space are not claimed by Device 1 Function 1.<br/>0 1 Illegal combination<br/>1 0 All VGA and MDA references are routed to PCI Express Graphics Attach device 1 function 1.<br/>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.</p> <p>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.</p> |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 0         | 0h<br>RW         | <p><b>MDAP10:</b></p> <p>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.</p> <p>If device 1 function 0 VGA enable bit is not set, then accesses to IO address range x3BCh-x3BFh remain on the backbone.</p> <p>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.</p> <p>MDA resources are defined as the following:<br/>Memory: 0B0000h - 0B7FFFh<br/>I/O: 3B4h, 3B5h, 3B8h, 3B9h, 3BAh, 3BFh,<br/>(including ISA address aliases, A[15:10] are not used in decode)</p> <p>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.</p> <p>The following table shows the behavior for all combinations of MDA and VGA:<br/>VGAEN MDAP Description<br/>0 0 All References to MDA and VGA space are not claimed by Device 1 Function 0.<br/>0 1 Illegal combination<br/>1 0 All VGA and MDA references are routed to PCI Express Graphics Attach device 1 function 0.<br/>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.</p> <p>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.</p> |

### 3.1.27 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<br>RO         | <b>Reserved</b>   |
| 38:20     | 7FFFFh<br>RW/L   | <p><b>TOM:</b></p> <p>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.</p> <p><b>Locked by:</b> TOM_0_0_0_PCI.LOCK</p> |



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

### 3.1.28 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<br>RO         | <b>Reserved</b>   |
| 38:20     | 00000h<br>RW/L   | <b>TOUUD:</b><br>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.<br>All the bits in this register are locked in Intel TXT mode.<br><b>Locked by:</b> TOUUD_0_0_0_PCI.LOCK |
| 19:1      | 0h<br>RO         | <b>Reserved</b>   |
| 0         | 0h<br>RW/L       | <b>LOCK:</b><br>This bit will lock all writable settings in this register, including itself.<br><b>Locked by:</b> TOUUD_0_0_0_PCI.LOCK  |



### 3.1.29 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<br>RW/L     | <b>BDSM:</b><br>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).<br><b>Locked by:</b> BDSM_0_0_0_PCI.LOCK |
| 19:1      | 0h<br>RO         | <b>Reserved</b>   |
| 0         | 0h<br>RW/L       | <b>LOCK:</b><br>This bit will lock all writable settings in this register, including itself.<br><b>Locked by:</b> BDSM_0_0_0_PCI.LOCK   |

### 3.1.30 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<br>RW/L     | <b>BGSM:</b><br>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).<br><b>Locked by:</b> BGSM_0_0_0_PCI.LOCK |
| 19:1      | 0h<br>RO         | <b>Reserved</b>  |
| 0         | 0h<br>RW/L       | <b>LOCK:</b><br>This bit will lock all writable settings in this register, including itself.<br><b>Locked by:</b> BGSM_0_0_0_PCI.LOCK  |

### 3.1.31 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<br>RW/L     | <b>TSEGMB:</b><br>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.<br><b>Locked by:</b> TSEGMB_0_0_0_PCI.LOCK |
| 19:1      | 0h<br>RO         | <b>Reserved</b>   |
| 0         | 0h<br>RW/L       | <b>LOCK:</b><br>This bit will lock all writable settings in this register, including itself.<br><b>Locked by:</b> TSEGMB_0_0_0_PCI.LOCK   |

### 3.1.32 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, 1 or 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<br>RW/L     | <p><b>TOLUD:</b><br/>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.</p> <p>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.</p> <p>This register must be 1MB aligned when reclaim is enabled.</p> <p><b>Locked by:</b> TOLUD_0_0_0_PCI.LOCK</p> |
| 19:1      | 0h<br>RO         | <b>Reserved</b>  |
| 0         | 0h<br>RW/L       | <p><b>LOCK:</b><br/>This bit will lock all writable settings in this register, including itself.</p> <p><b>Locked by:</b> TOLUD_0_0_0_PCI.LOCK</p>   |

### 3.1.33 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  |
|-----------|---------------------|---|
| 15:8      | 0h<br>RO            | <b>Reserved</b>   |
| 7         | 0h<br>RW/1C/V/<br>P | <b>IBECC Uncorrectable Error (IBECC_UC):</b><br>When this bit is set to 1 it indicates an uncorrectable error occurred in IBECC.  |
| 6         | 0h<br>RW/1C/V/<br>P | <b>IBECC Correctable Error (IBECC_COR):</b><br>When this bit is set to 1 it indicates a correctable error occurred in IBECC.  |
| 5         | 0h<br>RW/1C/V/<br>P | <b>Error on FMHC Unsupported Request Event (FMUR):</b><br>When this bit is set to 1 it indicates an unsupported request event occurred in FMHC (received from PCIE to Optane).  |
| 4         | 0h<br>RW/1C/V/<br>P | <b>FMCA:</b><br>When this bit is set to 1 it indicates a completer abort occurred in FMHC (received from PCIE to Optane).   |
| 3         | 0h<br>RW/1C/V/<br>P | <b>Media FMI Asynchronous Notification (FMIAN):</b><br>When this bit is set to 1 FMI Asynchronous Notification error event with Media dead or Health log critical notification has occurred in FMHC.  |
| 2         | 0h<br>RW/1C/V/<br>P | <b>FMI Thermal Event (FMITHERMERR):</b><br>When this bit is set to 1 it indicates a thermal event occurred in FMHC.   |
| 1         | 0h<br>RW/1C/V/<br>P | <b>Data Uncorrectable Error (DMERR):</b><br>If this bit is set to 1, a memory read data transfer had an uncorrectable multiple-bit error.<br>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.<br>Once this bit is set, the ECCERRLOGx fields are locked until the CPU clears this bit by writing a 1.<br>Software uses bits [1:0] to detect whether the logged error address is for a Single-bit or a Multiple-bit error.  |
| 0         | 0h<br>RW/1C/V/<br>P | <b>Data Single Bit Correctable Error (DSERR):</b><br>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.<br>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.<br>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.<br>A single bit error that occurs after a multibit error will set this bit but will not overwrite the other fields. |



### 3.1.34 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   |
|-----------|------------------|--|
| 15:8      | 0h<br>RO         | <b>Reserved</b>  |
| 7         | 0h<br>RW         | <b>IBECC Uncorrectable Error (IBECC_UC):</b><br>SERR on IBECC Uncorrectable error event<br>1: The Host Bridge generates an SERR special cycle over DMI when IBECC reports uncorrectable error.<br>0: Reporting of this condition via SERR messaging is disabled.   |
| 6         | 0h<br>RW         | <b>IBECC Correctable Error (IBECC_COR):</b><br>SERR on IBECC correctable error event<br>1: The Host Bridge generates an SERR special cycle over DMI when IBECC reports correctable error.<br>0: Reporting of this condition via SERR messaging is disabled.  |
| 5         | 0h<br>RW         | <b>SERR on FMHC Unsupported Request Event (FMUR):</b><br>SERR on FMHC unsupported request event<br>1: The Host Bridge generates an SERR special cycle over DMI when FMHC reports an unsupported request event.<br>0: Reporting of this condition via SERR messaging is disabled.   |
| 4         | 0h<br>RW         | <b>SERR on FMHC CA Event (FMCA):</b><br>SERR on FMHC CA event<br>1: The Host Bridge generates an SERR special cycle over DMI when FMHC reports a CA event.<br>0: Reporting of this condition via SERR messaging is disabled.   |
| 3         | 0h<br>RW         | <b>SERR on FMI Asynchronous Notification (FMIAN):</b><br>SERR on FMI Asynchronous Notification error event<br>1: The Host Bridge generates an SERR special cycle over DMI when FMHC reports a Asynchronous Notification error event with Media dead or Health log critical notification.<br>0: Reporting of this condition via SERR messaging is disabled. |
| 2         | 0h<br>RW         | <b>SERR on FMHC Thermal Event (FMITHERMERR):</b><br>SERR on FMHC thermal event<br>1: The Host Bridge generates an SERR special cycle over DMI when FMHC reports a thermal event.<br>0: Reporting of this condition via SERR messaging is disabled.   |

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

### 3.1.35 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  |
|-----------|------------------|---|
| 15:8      | 0h<br>RO         | <b>Reserved</b>   |
| 7         | 0h<br>RW         | <b>IBECC Uncorrectable Error (IBECC_UC):</b><br>SMI on IBECC Uncorrectable error event<br>1: The Host Bridge generates an SMI special cycle over DMI when IBECC reports uncorrectable error.<br>0: Reporting of this condition via SMI messaging is disabled. |
| 6         | 0h<br>RW         | <b>IBECC Correctable Error (IBECC_COR):</b><br>SMI on IBECC correctable error event<br>1: The Host Bridge generates an SMI special cycle over DMI when IBECC reports correctable error.<br>0: Reporting of this condition via SMI messaging is disabled.      |
| 5         | 0h<br>RW         | <b>SMI on FMHC Unsupported Request Event (FMUR):</b><br>1: The Host Bridge generates an SMI special cycle over DMI when FMHC reports an unsupported request event.<br>0: Reporting of this condition via SMI messaging is disabled.                           |
| 4         | 0h<br>RW         | <b>SMI on FMHC CA Event (FMCA):</b><br>SMI on FMHC CA event<br>1: The Host Bridge generates an SMI special cycle over DMI when FMHC reports a CA event.<br>0: Reporting of this condition via SMI messaging is disabled.                                      |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 3         | 0h<br>RW         | <b>SMI on FMI Asynchronous Notification (FMIAN):</b><br>SMI on FMI Asynchronous Notification error event<br>1: The Host Bridge generates an SMI special cycle over DMI when FMHC reports a Asynchronous Notification error event with Media dead or Health log critical notification.<br>0: Reporting of this condition via SMI messaging is disabled. |
| 2         | 0h<br>RW         | <b>SMI on FMHC Thermal Event (FMITHERMERR):</b><br>SMI on FMHC thermal event<br>1: The Host Bridge generates an SMI special cycle over DMI when FMHC reports a thermal event.<br>0: Reporting of this condition via SMI messaging is disabled.   |
| 1         | 0h<br>RW         | <b>SMI on Multiple Bit Error (DMESMI):</b><br>1: The Host generates an SMI DMI message when it detects a multiple-bit error reported by the DRAM controller.<br>0: Reporting of this condition via SMI messaging is disabled. For systems not supporting ECC this bit must be disabled.  |
| 0         | 0h<br>RW         | <b>Single Bit Error (DSESMI):</b><br>1: The Host generates an SMI DMI special cycle when the DRAM controller detects a single bit error.<br>0: Reporting of this condition via SMI messaging is disabled. For systems that do not support ECC this bit must be disabled.   |

### 3.1.36 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  |
|-----------|------------------|---|
| 15:8      | 0h<br>RO         | <b>Reserved</b>   |
| 7         | 0h<br>RW         | <b>IBECC Uncorrectable Error (IBECC_UC):</b><br>SCI on IBECC Uncorrectable error event<br>1: The Host Bridge generates an SCI special cycle over DMI when IBECC reports uncorrectable error.<br>0: Reporting of this condition via SCI messaging is disabled. |
| 6         | 0h<br>RW         | <b>IBECC Correctable Error (IBECC_COR):</b><br>SCI on IBECC correctable error event<br>1: The Host Bridge generates an SCI special cycle over DMI when IBECC reports correctable error.<br>0: Reporting of this condition via SCI messaging is disabled.      |



| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 5         | 0h<br>RW         | <b>SMI on FMHC Unsupported Request Event (FMUR):</b><br>SCI on FMHC unsupported request event<br>1: The Host Bridge generates an SCI special cycle over DMI when FMHC reports an unsupported request event.<br>0: Reporting of this condition via SCI messaging is disabled.   |
| 4         | 0h<br>RW         | <b>FMCA:</b><br>SCI on FMHC CA event<br>1: The Host Bridge generates an SCI special cycle over DMI when FMHC reports a CA event.<br>0: Reporting of this condition via SCI messaging is disabled.  |
| 3         | 0h<br>RW         | <b>SCI on FMI Asynchronous Notification (FMIAN):</b><br>SCI on FMI Asynchronous Notification error event<br>1: The Host Bridge generates an SCI special cycle over DMI when FMHC reports a Asynchronous Notification error event with Media dead or Health log critical notification.<br>0: Reporting of this condition via SCI messaging is disabled. |
| 2         | 0h<br>RW         | <b>FMITHERMERR:</b><br>SCI on FMHC thermal event<br>1: The Host Bridge generates an SCI special cycle over DMI when FMHC reports a thermal event.<br>0: Reporting of this condition via SCI messaging is disabled.   |
| 1         | 0h<br>RW         | <b>SCI on Multiple Bit Error (DMESCI):</b><br>1: The Host generates an SCI DMI message when it detects a multiple-bit error reported by the DRAM controller.<br>0: Reporting of this condition via SCI messaging is disabled. For systems not supporting ECC this bit must be disabled.  |
| 0         | 0h<br>RW         | <b>SCI on Single Bit Error (DSESCI):</b><br>1: The Host generates an SCI DMI special cycle when the DRAM controller detects a single bit error.<br>0: Reporting of this condition via SCI messaging is disabled. For systems that do not support ECC this bit must be disabled.  |

### 3.1.37 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 | 0000000h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access    | Field Name (ID): Description             |
|-----------|---------------------|--|
| 31:0      | 00000000<br>h<br>RW | <b>SKPD:</b><br>1 DWORD of data storage. |



### 3.1.38 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<br>RW/L       | <b>NVME Device 3 Function 0 Disable (NVME_F0D):</b><br>0: Device 3 Function 0 and associated memory spaces are accessible.<br>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<br>RW/L       | <b>PCIe Device 1 Function 2 Disable (PEG12D):</b><br>0: Device 1 Function 2 and associated memory spaces are accessible.<br>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<br>RW/L       | <b>PCIe Device 1 Function 1 Disable (PEG11D):</b><br>0: Device 1 Function 1 and associated memory spaces are accessible.<br>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<br>RW/L       | <b>PCIe Device 1 Function 0 Disable (PEG10D):</b><br>0: Device 1 Function 0 and associated memory spaces are accessible.<br>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<br>RW/L       | <b>PCIe Link Width Up-config Disable (PELWUD):</b><br>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.<br>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<br>RW/L       | <b>DMI Width (DW):</b><br>0: DMI x4<br>1: DMI x2  |
| 25        | 0h<br>RW/L       | <b>DRAM ECC Disable (ECCDIS):</b><br>0: ECC is supported<br>1: ECC is not supported   |
| 24        | 0h<br>RW/L       | <b>Force DRAM ECC Enable (FDEE):</b><br>0: DRAM ECC optional via software.<br>1: DRAM ECC enabled. MCHBAR C0MISCCTL bit [0] and C1MISCCTL bit [0] are forced to 1 and Read-Only.  |
| 23        | 0h<br>RW/L       | <b>VT-d Disable (VTDD):</b><br>0: VT-d is supported<br>1: VT-d is not supported   |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 22        | 0h<br>RW/L       | <b>DMI GEN2 Disable (DMIG2DIS):</b><br>0: Capable of running DMI in Gen 2 mode<br>1: Not capable of running DMI in Gen 2 mode   |
| 21        | 0h<br>RW/L       | <b>PCIe Controller Gen 2 Disable (PEGG2DIS):</b><br>0: Capable of running any of the PEG controllers in Gen 2 mode<br>1: Not capable of running any of the PEG controllers in Gen 2 mode  |
| 20:19     | 0h<br>RW/L       | <b>DRAM Maximum Size per Channel (DDRSZ):</b><br>This field defines the maximum allowed memory size per channel.<br>0h: Unlimited (64GB per channel)<br>1h: Maximum 8GB per channel<br>2h: Maximum 4GB per channel<br>3h: Maximum 2GB per channel   |
| 18        | 0h<br>RW/L       | <b>PCIe Controller Device 6 Function 0 Disabled (PEG60D):</b><br>PCIe Controller Device 6 Function 0 is disabled<br>0: Device 6 Function 0 is supported<br>1: Device 6 Function 0 is not supported  |
| 17        | 0h<br>RW/L       | <b>DRAM 1N Timing Disable (D1NM):</b><br>0: Part is capable of supporting 1n mode timings on the DDR interface.<br>1: Part is not capable of supporting 1n mode. Only supported timings are 2n or greater.  |
| 16        | 0h<br>RO         | <b>Reserved</b>   |
| 15        | 0h<br>RW/L       | <b>DTT Device Disable (CDD):</b><br>0: DTT Device enabled.<br>1: DTT Device disabled.   |
| 14        | 0h<br>RW/L       | <b>2 DIMMs Per Channel Enable (DDPCD):</b><br>Allows Dual Channel operation but only supports 1 DIMM per channel.<br>0: 2 DIMMs per channel enabled<br>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<br>RW/L       | <b>X2APIC Enable (X2APIC_EN):</b><br>Extended Interrupt Mode.<br>0b: Hardware does not support Extended APIC mode.<br>1b: Hardware supports Extended APIC mode.   |
| 12        | 0h<br>RW/L       | <b>Dual Memory Channel Support (PDCD):</b><br>0: Capable of Dual Channel<br>1: Not Capable of Dual Channel - only single channel capable.   |
| 11        | 0h<br>RW/L       | <b>Internal Graphics Disable (IGD):</b><br>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.<br>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. |



| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 10        | 0h<br>RW/L       | <b>DID0 Override Enable (DID0OE):</b><br>0: Disable ability to override DID0 - For production<br>1: Enable ability to override DID - For debug and samples only   |
| 9:8       | 0h<br>RO         | <b>Reserved</b>   |
| 7:4       | 0h<br>RW/L       | <b>Compatibility Revision ID (CRID):</b><br>Compatibility Revision ID   |
| 3         | 0h<br>RW/L       | <b>Memory Overclocking (DDR_OVERCLOCK):</b><br>Memory Overclocking is enabled.<br>When supported, memory can be trained at higher than default maximum frequencies.<br>0: Memory Overclocking is not supported<br>1: Memory Overclocking is supported   |
| 2:1       | 0h<br>RO         | <b>Reserved</b>   |
| 0         | 0h<br>RW/L       | <b>NVME F7D (NVME_F7D):</b><br>0: Device 3 Function 7 and associated memory spaces are accessible.<br>1: Device 3 Function 7 (NVMe F7) and associated memory space are disabled by hardwiring the D3F7EN field, bit 6 of the SoC Device Enable register |

### 3.1.39 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<br>RW/L       | <b>Image Processing Unit (IPU) Disable (IPU_DIS):</b><br>0: Device 5 associated memory spaces are accessible.<br>1: Device 5 associated memory and IO spaces are disabled.  |
| 30        | 0h<br>RW/L       | <b>Trace Hub Disable (TRACE_HUB_DIS):</b><br>0: Trace Hub associated memory spaces are accessible.<br>1: Trace Hub associated memory and IO spaces are disabled.  |
| 29        | 0h<br>RW/L       | <b>Overclocking Enabled (OC_ENABLED):</b><br>0: Overclocking is Disabled<br>1: Overclocking is Enabled<br>If overclocking is enabled, MSR FLEX_RATIO.OC_BINS contains how many bits of over-clocking are supported.<br>The encoding is as follows:<br>0: Overclocking is Disabled<br>1-6: Turbo ratio limits can be incremented by this amount<br>7: Unlimited<br>If overclocking is disabled, FLEX_RATIO.OC_BINS is meaningless. |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 28        | 0h<br>RW/L       | <b>SMT Capability (SMT):</b><br>This setting indicates whether the processor is SMT (HyperThreading) capable.  |
| 27:25     | 0h<br>RW/L       | <b>Cache Size (CACHESZ):</b><br>This setting indicates the supporting cache sizes.   |
| 24        | 0h<br>RW/L       | <b>SVM Disable (SVM_DISABLE):</b><br>0: SVM enabled<br>1: SVM disabled   |
| 23:21     | 0h<br>RW/L       | <b>Memory 100MHz Reference Clock (PLL_REF100_CFG):</b><br>DDR Maximum Frequency Capability with 100MHz memory reference clock (ref_clk).<br>0: 100 MHz memory reference clock is not supported<br>1-6: Reserved<br>7: Unlimited  |
| 20        | 0h<br>RW/L       | <b>PCIe Gen 3 Disable (PEGG3_DIS):</b><br>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)<br>1: Not capable of running any of the PCIe controllers in Gen 3 mode  |
| 19        | 0h<br>RW/L       | <b>Processor Package Type (PKGTYP):</b><br>This setting indicates the CPU Package Type.  |
| 18        | 0h<br>RW/L       | <b>Additive Graphics Enabled (ADDGFXEN):</b><br>0: Additive Graphics is disabled<br>1: Additive Graphics is enabled  |
| 17        | 0h<br>RW/L       | <b>Additive Graphics Capability Disable (ADDGFXCAP):</b><br>0: Capable of Additive Graphics<br>1: Not capable of Additive Graphics   |
| 16        | 0h<br>RW/L       | <b>PCIe x16 Disable (PEGX16D):</b><br>0: Capable of x16 PCIe Port<br>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<br>RW/L       | <b>DMI Gen 3 Disable (DMIG3DIS):</b><br>DMI Gen 3 Disable  |
| 14:12     | 0h<br>RW/L       | <b>2 Level Memory Technology Support (LTECH):</b><br>0: 1LM<br>1: EDRAM0<br>3: EDRAM0+1<br>4: 2LM<br>Other values are reserved   |
| 11        | 0h<br>RW/L       | <b>HDCP Disable (HDCPD):</b><br>0: Capable of HDCP<br>1: HDCP Disabled   |
| 10        | 0h<br>RW/L       | <b>2 Level Memory Support (2LM_SUPPORTED):</b><br>0: 2 Level Memory (2LM) is not supported. Only 1LM is supported.<br>1: 2 Level Memory (2LM) is supported   |
| 9         | 0h<br>RO         | <b>Reserved</b>  |
| 8         | 0h<br>RW/L       | <b>GNA (GMM) Disable (GNA_DIS):</b><br>0: Device 8 associated memory spaces are accessible.<br>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.  |



| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 7         | 0h<br>RW/L       | <b>DDD:</b><br>0: Debug mode<br>1: Production mode   |
| 6:4       | 0h<br>RO         | <b>Reserved</b>  |
| 3         | 0h<br>RW/L       | <b>S/H OPI Enable (SH_OPI_EN):</b><br>Specifies if OPI or DMI are enabled for S/H models.<br>0: DMI is enabled<br>1: OPI is enabled  |
| 2         | 0h<br>RW/L       | <b>VMD Disable (VMD_DIS):</b><br>Indicates if VMD is disabled.   |
| 1         | 0h<br>RW/L       | <b>Global Single PCIe Lane (DPEGFX1):</b><br>This bit has no effect on Device 1 unless Device 1 is configured for at least two ports via PEGOCFGSEL strap.<br>0: All PCIe port widths do not depend on their respective BCTRL[VGAEN].<br>1: Each PCIe port width is limited to x1 operation when its respective BCTRL[VGAEN] is set to 1b. |
| 0         | 0h<br>RW/L       | <b>Single PCIe Lane (SPEGFX1):</b><br>This bit has no effect on Device 1 unless Device 1 is configured for a single port via PEGOCFGSEL strap.<br>0: Device 1 Function 0 width does not depend on its BCTRL[VGAEN].<br>1: Device 1 Function 0 width is limited to x1 operation when its respective BCTRL[VGAEN] is set to 1.               |

### 3.1.40 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<br>RO         | <b>Reserved</b>  |
| 28        | 0h<br>RW/L       | <b>PCIe Gen 4 Disable (PEGG4_DIS):</b><br>PCIe Gen 4 Disabled. This field will be strap selectable/modifiable to enable PCH Pairing capabilities.<br>0: Capable of running any of the Gen 4-compliant PEG controllers in Gen 4 mode (Devices 0/1/0, 0/1/1, 0/1/2, 0/6/0)<br>1: Not capable of running any of the PEG controllers in Gen 4 mode |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 27:23     | 00h<br>RW/L      | <b>Maximum DDR4 Frequency (MAX_DATA_RATE_DDR4):</b><br>DDR4 Maximum Frequency Capability in 266Mhz units.<br>This value is relevant only when CAPID0_A_0_0_0_PCI.DDR_OVERCLOCK is zero (DDR overclocking is not supported).<br>0: Unlimited<br>1-31: multiples of 266MHz   |
| 22        | 0h<br>RW/L       | <b>DDR4 Support (DDR4_EN):</b><br>0: DDR4 is not supported<br>1: DDR4 is supported   |
| 21:17     | 00h<br>RW/L      | <b>Maximum LPDDR4 Frequency (MAX_DATA_RATE_LPDDR4):</b><br>LPDDR4 Maximum Frequency Capability in 266Mhz units.<br>This value is relevant only when CAPID0_A_0_0_0_PCI.DDR_OVERCLOCK is zero (DDR overclocking is not supported).<br>0: Unlimited<br>1-31: multiples of 266MHz   |
| 16        | 0h<br>RW/L       | <b>LPDDR4 Support (LPDDR4_EN):</b><br>0: LPDDR4 memory is not supported<br>1: LPDDR4 memory is supported   |
| 15        | 0h<br>RW/L       | <b>IBECC EN (IBECC_EN):</b><br>IBECC1 on/off mode of work<br>0 - IBECC1 is off<br>1 - IBECC1 is on   |
| 14        | 0h<br>RW/L       | <b>Dynamic Memory Frequency Change Disable (QCLK_GV_DIS):</b><br>0: Dynamic Memory Frequency Change is enabled<br>1: Dynamic Memory Frequency Change is disabled   |
| 13:10     | 0h<br>RO         | <b>Reserved</b>  |
| 9         | 0h<br>RW/L       | <b>SGX Disabled (SGX_DIS):</b><br>Software Guard Extension (Intel® SGX) Disabled: Indicates that Intel® SGX is not available on this processor   |
| 8:7       | 0h<br>RW/L       | <b>BCLKOCRANGE:</b><br>BCLK (Base clock) Overclocking maximum frequency.<br><ul style="list-style-type: none"><li>• 0: BCLK overclocking is disabled</li><li>• 1: BCLK maximum frequency is 115MHz</li><li>• 2: BCLK maximum frequency is 130MHz</li><li>• 3: Unlimited BCLK maximum frequency</li></ul>               |
| 6         | 0h<br>RW/L       | <b>Internal Display Disabled (IDD):</b><br>Specifies whether the Internal Display is Disabled.<br>0: Intel Display is enabled<br>1: Intel Display is disabled  |
| 5         | 0h<br>RW/L       | <b>DISPLAY PIPE3 (DISPLAY_PIPE3):</b><br>0: 3rd Display is disabled<br>1: 3rd Display is enabled   |
| 4:0       | 00h<br>RW/L      | <b>Max Data Rate At GEAR1 (MAX_DATA_RATE_AT_GEAR1):</b><br>This field reports the maximum Data Rate of the memory controller in GEAR 1 in 266Mhz units.<br>This value is relevant only when CAPID0_A_0_0_0_PCI.DDR_OVERCLOCK is zero (DDR overclocking is not supported).<br>0: Unlimited<br>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

### 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            | Round-Trip Latency (SC_ROUNDTRIP_LATENCY_0_0_0_MCHBAR)         | 19191919191919h   |
| 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)                       | 00000000185000h   |
| 4080h  | 4            | ODT Matrix (SC_ODT_MATRIX_0_0_0_MCHBAR)                        | 00000000h         |
| 4088h  | 8            | Scheduler Configuration (SC_GS_CFG_0_0_0_MCHBAR)               | 0000000000001020h |
| 4198h  | 4            | DDRIO Power Mode Timing (SPID_LOW_POWER_CTL_0_0_0_MCHBAR)      | F8141442h         |
| 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)                       | 4602980Fh         |
| 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)             | 000000Fh          |
| 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            | TC LPDDR4x MISC 0 0 0 MCHBAR (TC_LPDDR4_MISC_0_0_0_MCHBAR)               | 00000056h         |
| 42C4h  | 4            | TC SREXITTP 0 0 0 MCHBAR (TC_SREXITTP_0_0_0_MCHBAR)                      | 00000000h         |
| 43FCh  | 4            | MCMNTS SPARE 0 0 0 MCHBAR (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 Memory Request Counter (PWM_GT_REQCOUNT_0_0_0_MCHBAR)                 | 00000000h         |
| 5044h  | 4            | IA Memory Request Counter (PWM_IA_REQCOUNT_0_0_0_MCHBAR)                 | 00000000h         |
| 5048h  | 4            | IO Memory Request Counter (PWM_IO_REQCOUNT_0_0_0_MCHBAR)                 | 00000000h         |
| 5050h  | 4            | RdCAS Counter (PWM_RDDATA_COUNT_0_0_0_MCHBAR)                            | 00000000h         |
| 5054h  | 4            | WrCAS Counter (PWM_WRDATA_COUNT_0_0_0_MCHBAR)                            | 00000000h         |
| 5058h  | 4            | Command 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)       | 00000001FFFFFFFh  |

| Offset | Size (Bytes) | Register Name (Register Symbol)                                   | Default Value     |
|--------|--------------|---|-------------------|
| 5400h  | 8            | Graphics VT Base Address Register (GFXVTBAR_0_0_0_MCHBAR_NCU)     | 0000000000000000h |
| 5410h  | 8            | VTDPVC0BAR Base Address Register (VTDPVC0BAR_0_0_0_MCHBAR_NCU)    | 0000000000000000h |
| 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<br>RW/L      | <b>tWRPRE Timing Parameter (TWRPRE):</b><br>Holds DDR timing parameter tWRPRE.<br>WR to PRE same bank minimum delay in tCK cycles.<br>Supported range is 18-159.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG  |
| 23:21     | 4h<br>RW/L       | <b>tPPD Timing Parameter (TPPD):</b><br>Holds DDR timing parameter tPPD (for LPDDR4x only).<br>PRE/PREALL to PRE/PREALL (same rank) minimum delay in tCK cycles.<br>This parameter is ignored for non LPDDR4x DRAM technology.<br>Supported range is 4-7.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG |
| 20:16     | 06h<br>RW/L      | <b>tRDPRE Timing Parameter (TRDPRE):</b><br>Holds DDR timing parameter tRDPRE.<br>RD to PRE same bank minimum delay in tCK cycles.<br>Supported range is 6-15<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG   |
| 15:9      | 1Ch<br>RW/L      | <b>tRAS Timing Parameter (TRAS):</b><br>Holds DDR timing parameter tRAS.<br>ACT to PRE same bank minimum delay in tCK cycles.<br>For DDR/LPDDR Supported range is 28-90<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG   |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 8:6       | 0h<br>RW/L       | <p><b>tRPab_ext Timing Parameter (TRPAB_EXT):</b><br/>           Holds the value of tRPab-tRPpb for LPDDR in tCK cycles.<br/>           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.<br/>           When using DDR4 this field should be programmed to 0.<br/>           For LPDDR4x the following restrictions apply: For single/dual rank sub channels tRP-tRPab_ext &gt; 6. For three/four ranks sub channels tRP-tRPab_ext &gt; 8.<br/>           Supported range is 0-6.<br/> <b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG</p> |
| 5:0       | 08h<br>RW/L      | <p><b>tRP Timing Parameter (TRP):</b><br/>           Holds DDR timing parameter tRP (and tRCD).<br/>           PRE to ACT same bank minimum delay in tCK cycles.<br/>           ACT to CAS (RD or WR) same bank minimum delay in tCK cycles.<br/>           Supported range is 8-59.<br/> <b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG</p>   |

### 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<br>RO         | <b>Reserved</b>  |
| 26:21     | 08h<br>RW/L      | <p><b>tRCD Write Timing Parameter (TRCD_WR):</b><br/>           Holds DDR timing parameter tRCD for writes in tCK cycles.<br/>           This field should be configured to be the same as TC_PRE_0_0_0_MCHBAR.tRP.<br/>           Supported range is 8-59<br/> <b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG</p>  |
| 20:18     | 2h<br>RW/L       | <p><b>Derating Extensions (DERATING_EXT):</b><br/>           Holds LPDDR timing parameters derating tRAS, tRRD, tRP and tRCD in tCK cycles.<br/>           When LPDDR is hot, this value is added to the appropriate timing parameters.<br/>           For non LP devices program the field to 0. Supported range is 0-4.<br/> <b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG</p> |
| 17:13     | 04h<br>RW/L      | <p><b>tRRD Different Group (TRRD_DG):</b><br/>           Holds DDR timing parameter tRRD.<br/>           ACT to ACT (different bank group in DDR4) minimum delay in tCK cycles.<br/>           Supported range is 4-22.<br/> <b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG</p>   |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 12:8      | 04h<br>RW/L      | <b>tRRD Same Group (TRRD_SG):</b><br>Holds DDR timing parameter tRRD/tRRD_L.<br>For DDR4 program tRRD_L.<br>ACT to ACT (same bank group in DDR4) minimum delay in tCK cycles.<br>Supported range is 4-22.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG |
| 7         | 0h<br>RO         | <b>Reserved</b>  |
| 6:0       | 10h<br>RW/L      | <b>tFAW Timing Parameter (TFAW):</b><br>Holds DDR timing parameter tFAW (four activates window). In tCK cycles<br>Supported range is 16-88.<br><b>Locked by:</b> 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<br>RO         | <b>Reserved</b>  |
| 29:24     | 04h<br>RW/L      | <b>tRDRD Different DIMM (TRDRD_DD):</b><br>Minimum delay from RD to RD to the other DIMM in tCK cycles<br>Supported range is 4-54.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG                  |
| 23:22     | 0h<br>RO         | <b>Reserved</b>  |
| 21:16     | 04h<br>RW/L      | <b>tRDRD Different Rank (TRDRD_DR):</b><br>Minimum delay from RD to RD to the other rank in the same DIMM in tCK cycles<br>Supported range is 4-54.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG |
| 15:14     | 0h<br>RO         | <b>Reserved</b>  |
| 13:8      | 04h<br>RW/L      | <b>tRDRD Different Group (TRDRD_DG):</b><br>DDR4: Minimum delay from RD to RD to the different bank group in tCK cycles<br>Supported range is 4-54.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG |
| 7:6       | 0h<br>RO         | <b>Reserved</b>  |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 5:0       | 04h<br>RW/L      | <b>tRDRD Same Group (TRDRD_SG):</b><br>DDR4: Minimum delay from RD to RD to the same bank group in tCK cycles<br>Supported range is 4-54.<br><b>Locked by:</b> 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<br>RO         | <b>Reserved</b>  |
| 29:24     | 04h<br>RW/L      | <b>tRDWR Different DIMM (TRDWR_DD):</b><br>Minimum delay from RD to WR to the other DIMM in tCK cycles<br>Supported range is 4-54.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG                  |
| 23:22     | 0h<br>RO         | <b>Reserved</b>  |
| 21:16     | 04h<br>RW/L      | <b>tRDWR Different Rank (TRDWR_DR):</b><br>Minimum delay from RD to WR to the other rank in the same DIMM in tCK cycles<br>Supported range is 4-54.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG |
| 15:14     | 0h<br>RO         | <b>Reserved</b>  |
| 13:8      | 04h<br>RW/L      | <b>tRDWR Different Group (TRDWR_DG):</b><br>DDR4: Minimum delay from RD to WR to the different bank group in tCK cycles<br>Supported range is 4-54.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG |
| 7:6       | 0h<br>RO         | <b>Reserved</b>  |
| 5:0       | 04h<br>RW/L      | <b>tRDWR Same Group (TRDWR_SG):</b><br>DDR4: Minimum delay from RD to WR to the same bank group in tCK cycles<br>Supported range is 4-54.<br><b>Locked by:</b> 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<br>RO         | <b>Reserved</b>  |
| 29:24     | 04h<br>RW/L      | <b>tWRRD Different DIMM (TWRRD_DD):</b><br>Minimum delay from WR to RD to the other DIMM in tCK cycles<br>Supported range is 4-54.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG                  |
| 23:22     | 0h<br>RO         | <b>Reserved</b>  |
| 21:16     | 04h<br>RW/L      | <b>tWRRD Different Rank (TWRRD_DR):</b><br>Minimum delay from WR to RD to the other rank in the same DIMM in tCK cycles<br>Supported range is 4-54.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG |
| 15        | 0h<br>RO         | <b>Reserved</b>  |
| 14:8      | 04h<br>RW/L      | <b>tWRRD Different Group (TWRRD_DG):</b><br>DDR4: Minimum delay from WR to RD to the different bank group in tCK cycles<br>Supported range is 4-65.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG |
| 7:0       | 04h<br>RW/L      | <b>tWRRD Same Group (TWRRD_SG):</b><br>DDR4: Minimum delay from WR to RD to the same bank group in tCK cycles<br>Supported range is 4-145.<br><b>Locked by:</b> 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<br>RO         | <b>Reserved</b>  |
| 29:24     | 04h<br>RW/L      | <b>tWRWR Different DIMM (TWRWR_DD):</b><br>Minimum delay from WR to WR to the other DIMM in tCK cycles<br>Supported range is 4-54.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG                  |
| 23:22     | 0h<br>RO         | <b>Reserved</b>  |
| 21:16     | 04h<br>RW/L      | <b>tWRWR Different Rank (TWRWR_DR):</b><br>Minimum delay from WR to WR to the other rank in the same DIMM in tCK cycles<br>Supported range is 4-54.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG |
| 15:14     | 0h<br>RO         | <b>Reserved</b>  |
| 13:8      | 04h<br>RW/L      | <b>tWRWR Different Group (TWRWR_DG):</b><br>DDR4: Minimum delay from WR to WR to the different bank group in tCK cycles<br>Supported range is 4-54.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG |
| 7:6       | 0h<br>RO         | <b>Reserved</b>  |
| 5:0       | 04h<br>RW/L      | <b>tWRWR Same Group (TWRWR_SG):</b><br>DDR4: Minimum delay from WR to WR to the same bank group in tCK cycles<br>Supported range is 4-54.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG           |

### 3.2.8 Round-Trip 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 | 19191919191919h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | R          | R         |

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



| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 15        | 0h<br>RO         | <b>Reserved</b>  |
| 14:8      | 19h<br>RW/L      | <b>Rank 1 Latency (RANK_1_LATENCY):</b><br>Latency from read command to rank 1 until first data chunk return to MC in QCLK cycles<br>Supported range is 19-120.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG |
| 7         | 0h<br>RO         | <b>Reserved</b>  |
| 6:0       | 19h<br>RW/L      | <b>Rank 0 Latency (RANK_0_LATENCY):</b><br>Latency from read command to rank 0 until first data chunk return to MC in QCLK cycles<br>Supported range is 19-120.<br><b>Locked by:</b> 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<br>RO         | <b>Reserved</b>   |
| 4         | 0h<br>RW/L       | <b>ECC Correction Disable (ECC_CORRECTION_DISABLE):</b><br>When set, disables ECC correction. In this mode the memory controller reports any error type as uncorrectable.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_DFT   |
| 3         | 0h<br>RO         | <b>Reserved</b>   |
| 2:0       | 0h<br>RW/L       | <b>Error Injection Mode (ECC_INJECT):</b><br>ECC error inject options: <ul style="list-style-type: none"> <li>• 000b: No ECC error injection.</li> <li>• 001b: Inject correctable ECC error on ECC_INJ_ADDR_COMPARE register match.</li> <li>• 011b: Inject correctable ECC error on ECC error insertion counter.</li> <li>• 101b: Inject non-recoverable ECC error on ECC_INJ_ADDR_COMPARE register match (same as on poison)</li> <li>• 111b: Inject non-recoverable ECC error on ECC error insertion counter (same as on poison)</li> </ul> <b>Locked by:</b> 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<br>RO/V/P     | <b>ERRBANK:</b><br>This field holds the Bank Address of the read transaction that had the ECC error.   |
| 28:27     | 0h<br>RO/V/P     | <b>ERRRANK:</b><br>This field holds the Rank ID of the read transaction that had the ECC error.  |
| 26:24     | 0h<br>RO/V/P     | <b>ERRCHUNK:</b><br>Holds the chunk number of the error stored in the register.  |
| 23:16     | 00h<br>RO/V/P    | <b>Error Syndrome (ERRSYND):</b><br>This field contains the error syndrome.<br>A value of 0xFF indicates that the error is due to poisoning.   |
| 15:2      | 0h<br>RO         | <b>Reserved</b>  |
| 1         | 0h<br>RO/V/P     | <b>Multi-Bit Error Status (MERRSTS):</b><br>This bit is set when an uncorrectable multiple-bit error occurs on a memory read data transfer.<br>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.<br>This bit is cleared when the corresponding bit in 0.0.0.PCI.ERRSTS is cleared.   |
| 0         | 0h<br>RO/V/P     | <b>Single Bit Error Status (CERRSTS):</b><br>This bit is set when a correctable single-bit error occurs on a memory read data transfer.<br>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.<br>A multiple bit error that occurs after this bit is set will override the address/error syndrome information.<br>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<br>RO         | <b>Reserved</b>  |
| 30:29     | 0h<br>RO/V/P     | <b>Error Bank Group (ERRBANKGROUP):</b><br>This field holds the DRAM bank group (for DDR4) address of the read transaction that had the ECC error. |
| 28:17     | 000h<br>RO/V/P   | <b>Error Column (ERRCOL):</b><br>This field holds the DRAM column address of the read transaction that had the ECC error.                          |
| 16:0      | 00000h<br>RO/V/P | <b>Error Row (ERRROW):</b><br>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<br>RO         | <b>Reserved</b>   |
| 39:32     | 04h<br>RW/L      | <b>TWRPDEN:</b><br>Holds DDR timing parameter tWRPDEN.<br>WR to power down minimum delay in tCK cycles.<br>Supported range is 4-159.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG |
| 31        | 0h<br>RO         | <b>Reserved</b>   |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 30:24     | 04h<br>RW/L      | <b>tRDPDEN Timing Parameter (TRDPDEN):</b><br>Holds DDR timing parameter for tRDPDEN.<br>RD to power down minimum delay in tCK cycles.<br>Supported range is 4-95.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG   |
| 23:22     | 1h<br>RW/L       | <b>tPRPDEN Timing Parameter (TPRPDEN):</b><br>Holds DDR timing parameter tPRPDEN.<br>PRE to power down minimum delay in tCK cycles.<br>Supported range is 1-3.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG   |
| 21:16     | 04h<br>RW/L      | <b>tXP Timing Parameter (TXPDLL):</b><br>Holds DDR timing parameter tXP.<br>Power up to RD/WR minimum delay in tCK cycles.<br>Applicable for DDR4 in case of exit from PPD when DRAM is configured to slow-exit mode.<br>Supported range is 4-63.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG  |
| 15:13     | 0h<br>RO         | <b>Reserved</b>   |
| 12:8      | 04h<br>RW/L      | <b>tXP Timing Parameter (TXP):</b><br>Holds DDR timing parameter tXP.<br>Power up to any command minimum delay in tCK cycles<br>Supported range is 4-16.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG   |
| 7:5       | 0h<br>RO         | <b>Reserved</b>   |
| 4:0       | 04h<br>RW/L      | <b>tCKE Timing Parameter (TCKE):</b><br>Holds DDR timing parameter tCKE.<br>Power down to power up (and vice versa) minimum delay in tCK cycles.<br>Note that for LPDDR4x this value is also used for tCKCKEL and tCKELCMD.<br>For LPDDR4x tSR (minimum self refresh time) is calculated to be tCKE*2.<br>Supported range is 4-16.<br><b>Locked by:</b> 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<br>RO         | <b>Reserved</b>  |
| 27:22     | 06h<br>RW/L      | <b>TCWL:</b><br>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 LPDDR4x the minimum supported value is 4. For DDR4 the minimum supported value is 5.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG |
| 21:16     | 05h<br>RW/L      | <b>TCL:</b><br>Holds DDR timing parameter tCL. Read command to data delay in tCK cycles. Supported range is 4-36.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG   |
| 15:0      | 0h<br>RO         | <b>Reserved</b>  |

### 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<br>RW/L       | <b>Write Rank 3 (WRITE_RANK_3):</b><br>Indicate which ranks should terminate when writing to rank 3 (bits 3:0 correspond to ODT pins 3:0.)<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG |
| 27:24     | 0h<br>RW/L       | <b>Write Rank 2 (WRITE_RANK_2):</b><br>Indicate which ranks should terminate when writing to rank 2 (bits 3:0 correspond to ODT pins 3:0).<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 23:20     | 0h<br>RW/L       | <b>Write Rank 1 (WRITE_RANK_1):</b><br>Indicate which ranks should terminate when writing to rank 1 (bits 3:0 correspond to ODT pins 3:0).<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG  |
| 19:16     | 0h<br>RW/L       | <b>Write Rank 0 (WRITE_RANK_0):</b><br>Indicate which ranks should terminate when writing to rank 0 (bits 3:0 correspond to ODT pins 3:0),<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG  |
| 15:12     | 0h<br>RW/L       | <b>Read Rank 3 (READ_RANK_3):</b><br>Indicate which ranks should terminate when reading from rank 3 (bits 3:0 correspond to ODT pins 3:0)<br>Note that according to DRAM spec the target rank should not be terminated.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG |
| 11:8      | 0h<br>RW/L       | <b>Read Rank 2 (READ_RANK_2):</b><br>Indicate which ranks should terminate when reading from rank 2 (bits 3:0 correspond to ODT pins 3:0)<br>Note that according to DRAM spec the target rank should not be terminated.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG |
| 7:4       | 0h<br>RW/L       | <b>Read Rank 1 (READ_RANK_1):</b><br>Indicate which ranks should terminate when reading from rank 1 (bits 3:0 correspond to ODT pins 3:0)<br>Note that according to DRAM spec the target rank should not be terminated.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG |
| 3:0       | 0h<br>RW/L       | <b>Read Rank 0 (READ_RANK_0):</b><br>Indicate which ranks should terminate when reading from rank 0 (bits 3:0 correspond to ODT pins 3:0)<br>Note that according to DRAM spec the target rank should not be terminated.<br><b>Locked by:</b> 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<br>RO         | <b>Reserved</b>   |
| 33:32     | 0h<br>RW/L       | <b>DDR4 1 DIMM per Channel (DDR4_1DPC):</b><br>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.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 31        | 0h<br>RW/L       | <b>GEAR2:</b><br>Indicate that MC is working in Gear-2 (Qclk is half the data transfer clock of the DRAM)<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG  |
| 30        | 0h<br>RW/L       | <b>No Gear2 Param Divide (NO_GEAR2_PARAM_DIVIDE):</b><br>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).<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG  |
| 29:28     | 0h<br>RW/L       | <b>x8 Device (X8_DEVICE):</b><br>DIMM is made out of X8 devices<br>LSB is for DIMM 0, MSB is for DIMM 1.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG   |
| 27:15     | 0h<br>RO         | <b>Reserved</b>   |
| 14:12     | 1h<br>RW/L       | <b>tCPDED Timing Parameter (TCPDED):</b><br>Holds DDR timing parameter tCPDED.<br>Power down to command bus tri-state delay in tCK cycles (for DDR4)<br>Supported range is 1-7 in 1N mode.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG   |
| 11:8      | 0h<br>RW/L       | <b>Address Mirror (ADDRESS_MIRROR):</b><br>DIMM routing causes address mirroring<br>For DDR4:<br>bit 0: DIMM 0 (rank 1 bus is mirrored)<br>bit 1: DIMM 1 (rank 3 bus is mirrored)<br>For LPDDR4x<br>bit 0: Sub channel 0 ranks 0 and 2 CA bus is mirrored.<br>bit 1: Sub channel 1 ranks 0 and 2 CA bus is mirrored.<br>bit 2: Sub channel 0 ranks 1 and 3 CA bus is mirrored.<br>bit 3: Sub channel 1 ranks 1 and 3 CA bus is mirrored.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG |
| 7:5       | 1h<br>RW/L       | <b>N to 1 Ratio (N_TO_1_RATIO):</b><br>When using N:1 command stretch mode, every how many B2B valid command cycles a bubble is required<br>Supported range is 1 to 7<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG  |
| 4:3       | 0h<br>RW/L       | <b>CMD Stretch (CMD_STRETCH):</b><br>Command stretch mode:<br>00b: 1N<br>01b: 2N<br>10b: 3N<br>11b: N:1<br>Notice that in Gear2 MC uses only the low phase of Dclk for commands, effectively doing a 2N by default.<br>setting 2N in Gear2 will result in 4N at DDR interface<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG  |
| 2:0       | 0h<br>RO         | <b>Reserved</b>   |



### 3.2.16 DDRIO Power Mode Timing (SPID\_LOW\_POWER\_CTL\_0\_0\_0\_MCHBAR) – Offset 4198h

This register holds DDRIO timing constraints regarding power modes latencies.

| Type | Size   | Offset         | Default   |
|------|--------|----------------|-----------|
| MMIO | 32 bit | MCHBAR + 4198h | F8141442h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | R          | R         |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 31        | 1h<br>RW/L       | <b>Self-refresh Enable (SELFREFRESH_ENABLE):</b><br>allow sending DDRIO self refresh mode indication<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG   |
| 30        | 1h<br>RW/L       | <b>Power Down Enable (POWERDOWN_ENABLE):</b><br>allow sending DDRIO CKE power down mode indication<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG   |
| 29        | 1h<br>RW/L       | <b>Idle Enable (IDLE_ENABLE):</b><br>allow sending DDRIO idle mode indication<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG  |
| 28        | 1h<br>RW/L       | <b>CKE Valid Enable (CKEVALID_ENABLE):</b><br>Allow deasserting cke_valid when not toggling CKE pins<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG   |
| 27:24     | 8h<br>RW/L       | <b>CKE Valid Length (CKEVALID_LENGTH):</b><br>cke_valid pulse length in DCLK cycles<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG  |
| 23:20     | 1h<br>RW/L       | <b>Self-Refresh Length (SELFREFRESH_LENGTH):</b><br>Minimum time allowed in self refresh mode<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG  |
| 19:16     | 4h<br>RW/L       | <b>Self-Refresh Latency (SELFREFRESH_LATENCY):</b><br>Exit latency from self refresh mode till command can be sent in DCLK cycles<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG  |
| 15:12     | 1h<br>RW/L       | <b>Power-Down Length (POWERDOWN_LENGTH):</b><br>Minimum time allowed in CKE power down mode<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG  |
| 11:8      | 4h<br>RW/L       | <b>Power-Down Latency (POWERDOWN_LATENCY):</b><br>Exit latency from CKE power down mode till command can be sent in DCLK cycles<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG  |
| 7:4       | 4h<br>RW/L       | <b>Idle Length (IDLE_LENGTH):</b><br>Minimum time allowed in idle mode<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG   |
| 3:1       | 1h<br>RW/L       | <b>idle latency (IDLE_LATENCY):</b><br>Exit latency from idle mode till command can be sent in DCLK cycles<br>Note that a value larger than 2 will prevent sending requests in two cycle bypass when in IDLE mode.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG |



| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 0         | 0h<br>RW/L       | <b>Raise CKE After Exit Latency (RAISE_CKE_AFTER_EXIT_LATENCY):</b><br>Delay raising of CKE on exit from power-down and self-refresh power modes until required latency has passed.<br>If this bit is clear then CKE exit (and tXP) happens in parallel of waking up the PHY, otherwise they happen back to back.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG |

### 3.2.17 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<br>RO         | <b>Reserved</b>   |
| 26:24     | 3h<br>RW/V/L     | <b>Rank 3 (RANK_3):</b><br>Rank 3 refresh rate<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_PWR_MNGMENT |
| 23:19     | 0h<br>RO         | <b>Reserved</b>   |
| 18:16     | 3h<br>RW/V/L     | <b>Rank 2 (RANK_2):</b><br>Rank 2 refresh rate<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_PWR_MNGMENT |
| 15:11     | 0h<br>RO         | <b>Reserved</b>   |
| 10:8      | 3h<br>RW/V/L     | <b>Rank 1 (RANK_1):</b><br>Rank 1 refresh rate<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_PWR_MNGMENT |
| 7:3       | 0h<br>RO         | <b>Reserved</b>   |
| 2:0       | 3h<br>RW/V/L     | <b>Rank 0 (RANK_0):</b><br>Rank 0 refresh rate<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_PWR_MNGMENT |



### 3.2.18 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

**Note:** Bit definitions are the same as LPDDR\_MR4\_RANK\_TEMPERATURE\_0\_0\_0\_MCHBAR, offset 4224h.

### 3.2.19 Refresh Parameters (TC\_RFP\_0\_0\_0\_MCHBAR) – Offset 4238h

Refresh parameters

| Type | Size   | Offset         | Default   |
|------|--------|----------------|-----------|
| MMIO | 32 bit | MCHBAR + 4238h | 4602980Fh |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | R          | R         |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 31:25     | 23h<br>RW/L      | <b>tREFI x9 (TREFIX9):</b><br>Maximum time allowed between refreshes to a rank (in intervals of 1024 DCLK cycles).<br>Should be programmed to $8 * tREFI / 1024$ (to allow for possible delays from ZQ or ISOC).<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG |
| 24:19     | 0h<br>RO         | <b>Reserved</b>   |
| 18        | 0h<br>RW/L       | <b>Always Refresh on MRS (ALWAYSREFONMRS):</b><br>Setting this bit will enable MRS refresh at the beginning of the flow, regardless of refresh debt.<br>Note: MRS can send refreshes.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG                            |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 17        | 1h<br>RW/L       | <b>High Priority Referesh on MRS (HPREFONMRS):</b><br>Setting this bit will enable MRS refresh at the beginning of MRS flow if the rank reached High Priority refresh WM.<br>Should be set by default, it's intended for System Agent SpeedStep as MC can enter Self refresh while owing refreshes.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG |
| 16        | 0h<br>RW/L       | <b>COUNTTREFIWHILEREFEENOFF:</b><br>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.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG               |
| 15:12     | 9h<br>RW/L       | <b>Refresh Panic Threshold (REFRESH_PANIC_WM):</b><br>tREFI count level in which the refresh priority is panic (default is 9). The Maximum value for this field is 9.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG   |
| 11:8      | 8h<br>RW/L       | <b>Refresh Priority Threshold (REFRESH_HP_WM):</b><br>tREFI count level that turns the refresh priority to high (default is 8)<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG  |
| 7:0       | 0Fh<br>RW/L      | <b>Rank Idle (OREF_RI):</b><br>Rank idle period that defines an opportunity for refresh, in DCLK cycles<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG   |

### 3.2.20 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<br>RO         | <b>Reserved</b>  |
| 25:16     | 0B4h<br>RW/L     | <b>tRFC Timing Parameter (TRFC):</b><br>Time of refresh: from beginning of refresh until next ACT or refresh is allowed (in tCK cycles, default is 180)<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG   |
| 15:0      | 1004h<br>RW/L    | <b>tREFI Timing Parameter (TREFI):</b><br>Defines the average period between refreshes and the rate that tREFI counter is incremented (in DCLK cycles).<br>It is suggested to set tREFI to a 2.8% lower value than the JEDEC spec<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG |



### 3.2.21 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<br>RO         | <b>Reserved</b>   |
| 11:0      | 200h<br>RW/L     | <b>tXSDLL Timing Parameter (TXSDLL):</b><br>Delay between DDR SR exit and the first command that requires data RD/WR from DDR.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG |

### 3.2.22 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   |
|-----------|------------------|--|
| 31:15     | 0h<br>RO         | <b>Reserved</b>  |
| 14        | 0h<br>RW/L       | <b>Enable Refresh Type Display (EN_REF_TYPE_DISPLAY):</b><br>This bit when set displays refresh type on the BA address pins.<br>000 = Stolen Refresh<br>100 = Opportunistic Refresh<br>010 = Hi Priority Refresh<br>001 = Panic Refresh<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 13        | 0h<br>RW/L       | <b>Disable Stolen Refresh (DISABLE_STOLEN_REFRESH):</b><br>This bit when set disables stolen refreshes<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG  |
| 12        | 0h<br>RW/L       | <b>Refresh Stagger Mode (REF_STAGGER_MODE):</b><br>This bit sets the refresh staggering mode<br>0b: Per DIMM refresh stagger.<br>1b: Per channel refresh stagger.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG |
| 11        | 0h<br>RW/L       | <b>Refresh Stagger Enable (REF_STAGGER_EN):</b><br>When set this bit enables refresh staggering.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG  |
| 10:0      | 000h<br>RW/L     | <b>Refresh Interval (REF_INTERVAL):</b><br>Refresh Interval period in DCLKS<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG   |

### 3.2.23 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<br>RW/L     | <b>tZQCAL Timing Parameter (TZQCAL):</b><br>tZQCAL in tCK (WCK for LPDDR5) cycles. Used for LP4/5 and DDR5.<br>Should typically be set to 1us in LPDDR<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG |
| 19:10     | 040h<br>RW/L     | <b>tZQCS Timing Parameter (TZQCS):</b><br>For DDR4 holds tCK value in DCLK cycles.<br>For LPDDR4x holds tZQLAT in DCLK cycles.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG                         |
| 9:0       | 0h<br>RO         | <b>Reserved</b>   |

### 3.2.24 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<br>RO         | <b>Reserved</b>  |
| 7:0       | 0Fh<br>RW/L      | <p><b>Rank Occupancy (RANK_OCCUPANCY):</b><br/>Indicates which ranks are occupied in the system.<br/>Non-enhanced channels:</p> <ul style="list-style-type: none"> <li>• Bit 0: Rank 0</li> <li>• Bit 1: Rank 1</li> <li>• Bit 2: Rank 2</li> <li>• Bit 3: Rank 3</li> </ul> <p>Enhanced channels:</p> <ul style="list-style-type: none"> <li>• Bit 0: Rank 0 = Sub channel 0 Rank 0</li> <li>• Bit 1: Rank 1 = Sub channel 0 Rank 1</li> <li>• Bit 2: Rank 2 = Sub channel 1 Rank 0</li> <li>• Bit 3: Rank 3 = Sub channel 1 Rank 1</li> <li>• Bit 4: Sub channel 0 Rank 2</li> <li>• Bit 5: Sub channel 0 Rank 3</li> <li>• Bit 6: Sub channel 1 Rank 2</li> <li>• Bit 7: Sub channel 1 Rank 3</li> </ul> <p>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.</p> <p><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG</p> |

### 3.2.25 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<br>RO         | <b>Reserved</b>   |
| 13:8      | 00h<br>RW/L      | <b>DIMM1 Idle Energy (DIMM1_IDLE_ENERGY):</b><br>This register defines the energy consumed by DIMM1 for one clock cycle when the DIMM is idle with CKE on.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_PWR_MNGMENT |
| 7:6       | 0h<br>RO         | <b>Reserved</b>   |
| 5:0       | 00h<br>RW/L      | <b>DIMM0 Idle Energy (DIMM0_IDLE_ENERGY):</b><br>This register defines the energy consumed by DIMM0 for one clock cycle when the DIMM is idle with CKE on.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_PWR_MNGMENT |

### 3.2.26 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<br>RO         | <b>Reserved</b>  |
| 13:8      | 00h<br>RW/L      | <b>DIMM1 Power-Down Energy (DIMM1_PD_ENERGY):</b><br>This register defines the energy consumed by DIMM1 for one clock cycle when the DIMM is idle with CKE off.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_PWR_MNGMENT |

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

### 3.2.27 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<br>RO         | <b>Reserved</b>  |
| 15:8      | 00h<br>RW/L      | <b>DIMM1 ACT Energy (DIMM1_ACT_ENERGY):</b><br>This register defines the combined energy contribution of activate and precharge commands.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_PWR_MNGMENT |
| 7:0       | 00h<br>RW/L      | <b>DIMM0 ACT Energy (DIMM0_ACT_ENERGY):</b><br>This register defines the combined energy contribution of activate and precharge commands.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_PWR_MNGMENT |

### 3.2.28 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<br>RO         | <b>Reserved</b>  |
| 15:8      | 00h<br>RW/L      | <b>DIMM1 RD Energy (DIMM1_RD_ENERGY):</b><br>This register defines the energy contribution of a read CAS command.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_PWR_MNGMENT |
| 7:0       | 00h<br>RW/L      | <b>DIMM0 RD Energy (DIMM0_RD_ENERGY):</b><br>This register defines the energy contribution of a read CAS command.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_PWR_MNGMENT |

### 3.2.29 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<br>RO         | <b>Reserved</b>   |
| 15:8      | 00h<br>RW/L      | <b>DIMM1 WR Energy (DIMM1_WR_ENERGY):</b><br>This register defines the energy contribution of a write CAS command.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_PWR_MNGMENT |
| 7:0       | 00h<br>RW/L      | <b>DIMM0 WR Energy (DIMM0_WR_ENERGY):</b><br>This register defines the energy contribution of a write CAS command.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_PWR_MNGMENT |



### 3.2.30 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\_0\_0\_0\_MCHBAR 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<br>RW/L | <b>COUNT:</b><br>Chunk count for error inject<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_DFT |

### 3.2.31 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<br>RO         | <b>Reserved</b>  |
| 12        | 0h<br>RW/L       | <b>Add 1Qclk delay (ADD_1QCLK_DELAY):</b><br>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<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG |
| 11:6      | 00h<br>RW/L      | <b>Increased To tCWL (ADD_TCWL):</b><br>the number of cycles (Dclk) increased to tCWL.<br>Make sure tCWL + Add_tCWL doesn't overflow.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG   |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 5:0       | 03h<br>RW/L      | <b>Decreased From tCWL (DEC_TCWL):</b><br>the number of cycles (Dclk) decreased from tCWL, configuring this number to be larger than tCWL is forbidden<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG |

### 3.2.32 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<br>RO         | <b>Reserved</b>   |
| 19:10     | 03Ch<br>RW/L     | <b>tRFCpb Timing Parameter (TRFCPB):</b><br>Refresh time in tCK (WCK for LPDDR5) for REFpb<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG   |
| 9:4       | 01h<br>RW/L      | <b>Per Bank Refresh Exit on Idle Count (PBR_EXIT_ON_IDLE_CNT):</b><br>Number of tREFI cycles to count before switching PBR off for better clock gating. A value of 0 means no Idle exit.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG |
| 3         | 0h<br>RW/L       | <b>Per Bank Refresh Disable on Hot (PBR_DISABLE_ON_HOT):</b><br>Disable PBR when LP4 is at 0.25xtREFI condition<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG  |
| 2         | 0h<br>RO         | <b>Reserved</b>   |
| 1         | 0h<br>RW/L       | <b>Per Bank Refresh Out-of-Order Disable (PBR_OOO_DIS):</b><br>Disable out of order scheduling of banks for LP4<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG  |
| 0         | 1h<br>RW/L       | <b>Per Bank Refresh Disable (PBR_DISABLE):</b><br>Disable PBR (per bank refresh) for LP4 (DDR4 force PBR off)<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG  |

### 3.2.33 TC LPDDR4x MISC 0 0 0 MCHBAR (TC\_LPDDR4\_MISC\_0\_0\_0\_MCHBAR) – Offset 4294h

Miscellaneous timing constrains of LPDDR4x

| 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<br>RO         | <b>Reserved</b>  |
| 6:0       | 56h<br>RW/L      | <b>TOSCO:</b><br>Delay between DQS_OSC counter stop to MR18/19 read<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG |

### 3.2.34 TC SREXITTP 0 0 0 MCHBAR (TC\_SREXITTP\_0\_0\_0\_MCHBAR) – Offset 42C4h

Self-refresh exit 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<br>RO         | <b>Reserved</b>  |
| 9:0       | 000h<br>RW/L     | <b>TXSR:</b><br>Exit self refresh to valid commands delay.<br>in LP4 configure this parameter for tXSR or tXSR abort if used.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_CONFIG |

### 3.2.35 MCMNTS SPARE 0 0 0 MCHBAR (MCMNTS\_SPARE\_0\_0\_0\_MCHBAR) – Offset 43FCh

Spare 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<br>RO         | <b>Reserved</b>  |
| 13:12     | 0h<br>RW/L       | <b>Decoder EBH (DECODER_EBH):</b><br>Enable address decoder Extended bank hashing.<br>Bit 0 - Enable XaB<br>Bit 1 - Enable XbB<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_DFT   |
| 11        | 0h<br>RO         | <b>Reserved</b>  |
| 10        | 0h<br>RW/L       | <b>DISLOWREFRATE:</b><br>Don't allow refresh rate lower than 1X<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_DFT  |
| 9         | 0h<br>RW/L       | <b>FORCEX4REF:</b><br>Force accelerated refreshes, four times the refresh number. Should be mutexed with ForceX2Ref<br>Constant X4 refreshes may block channel from entering self refresh. In case of staggered refreshes and fully occupied channel it can cause performance degradation.<br>Use with caution.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_DFT  |
| 8         | 0h<br>RW/L       | <b>FORCEX2REF:</b><br>Force accelerated refreshes, twice the refresh number. Should be mutexed with ForceX4Ref.<br>Constant X2 refreshes may block channel from entering self refresh.<br>In case of staggered refreshes and fully occupied channel it can cause a performance degradation.<br>Use with caution.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_DFT |
| 7:0       | 0h<br>RO         | <b>Reserved</b>  |

### 3.2.36 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<br>RO         | <b>Reserved</b>  |
| 19:12     | 00h<br>RW/L      | <b>Channel S Size (CH_S_SIZE):</b><br>Channel S size in multiplies of 0.5GB.<br>Supported range is 0GB - 64GB.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_ADDR_MAP   |
| 11:5      | 0h<br>RO         | <b>Reserved</b>  |
| 4         | 0h<br>RW/L       | <b>Channel L Mapping (CH_L_MAP):</b><br>Channel L mapping to physical channel.<br>0b: Channel 0<br>1b: Channel 1<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_ADDR_MAP   |
| 3         | 0h<br>RW/L       | <b>Enhanced Channel Mode (ECHM):</b><br>Enhanced channel mode for LPDDR4x indicate that the channel operates as two 32bit channels instead of one 64bit channel.<br>In this mode DIMM 0 is mapped to DQ bits 31:0 and DIMM 1 is mapped to DQ bits 63:32.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_ADDR_MAP |
| 2:0       | 0h<br>RW/L       | <b>DDR Type (DDR_TYPE):</b><br>Defines the DDR type:<br>0: DDR4<br>1: DDR5<br>2-7: Reserved<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_ADDR_MAP  |

### 3.2.37 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<br>RO         | <b>Reserved</b>  |
| 13:12     | 0h<br>RW/L       | <b>ECC Channel Configuration (ECC):</b><br>0: No ECC active in the channel.<br>1: ECC is active in IO, ECC logic is not active.<br>2: ECC is disabled in IO, but ECC logic is enabled.<br>3: ECC active in both IO and ECC logic.<br>Notes: <ul style="list-style-type: none"> <li>This field must be programmed identically for all populated channels.</li> <li>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.</li> </ul> <b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_ADDR_MAP |
| 11:9      | 0h<br>RO         | <b>Reserved</b>  |
| 8         | 0h<br>RW/L       | <b>Enhanced Interleaving Mode (EIM):</b><br>0b: Disabled<br>1b: Enabled<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_ADDR_MAP  |
| 7:5       | 0h<br>RO         | <b>Reserved</b>  |
| 4         | 0h<br>RW/L       | <b>Rank Interleaving (RI):</b><br>Rank interleaving enable bit<br>0 - Disabled<br>1 - Enabled<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_ADDR_MAP  |
| 3:1       | 0h<br>RO         | <b>Reserved</b>  |
| 0         | 0h<br>RW/L       | <b>DIMM L Mapping (DIMM_L_MAP):</b><br>Virtual DIMM L mapping to physical DIMM<br>0b: DIMM0<br>1b: DIMM1<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_ADDR_MAP   |

### 3.2.38 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.



### 3.2.39 Channel 0 DIMM Characteristics (MAD\_DIMM\_CHO\_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<br>RO         | <b>Reserved</b>  |
| 29        | 0h<br>RW/L       | <b>DLS BGO on Bit 11 (DLS_BGO_ON_BIT_11):</b><br>when set, BG[0] will be placed on bit 11 of the channel address instead of bit 6.<br>CAS[7] will take zone address 6.<br>0b: CAS[7] = zoneaddr[11], BG[0] = zoneaddr[6].<br>1b: CAS[7] = zoneaddr[6], BG[0] = zoneaddr[11].<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_ADDR_MAP |
| 28        | 0h<br>RO         | <b>Reserved</b>  |
| 27:26     | 0h<br>RW/L       | <b>DIMM S Number of Ranks (DSNOR):</b><br>DIMM S number of ranks<br>0b: 1 Rank<br>1b: 2 Ranks<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_ADDR_MAP  |
| 25:24     | 0h<br>RW/L       | <b>DIMM S Width (DSW):</b><br>Width of DDR chips<br>0: X8 chips<br>1: X16 chips<br>2: X32 chips<br>3: Reserved<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_ADDR_MAP   |
| 23        | 0h<br>RO         | <b>Reserved</b>  |
| 22:16     | 00h<br>RW/L      | <b>DIMM S Size (DIMM_S_SIZE):</b><br>Size of DIMM S in 0.5GB multiples.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_ADDR_MAP  |
| 15:11     | 0h<br>RO         | <b>Reserved</b>  |
| 10:9      | 0h<br>RW/L       | <b>DIMM L Number of Ranks (DLNOR):</b><br>0: 1 Rank<br>1: 2 Ranks<br>In ERM (enhanced rank mode):<br>2: 3 ranks<br>3: 4 ranks<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_ADDR_MAP  |



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

### 3.2.40 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.

### 3.2.41 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<br>RO         | <b>Reserved</b>  |
| 28        | 0h<br>RW/L       | <b>Hash Mode (HASH_MODE):</b><br>Encoding:<br>0b: Use address bit-6 for channel selection.<br>1b: Use the channel hash function as defined in the other fields of this register.<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_ADDR_MAP |
| 27        | 0h<br>RO         | <b>Reserved</b>  |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 26:24     | 0h<br>RW/L       | <p><b>Hash LSB Mask Bit (HASH_LSB_MASK_BIT):</b><br/>           This field specifies the MC Channel interleave bit.<br/>           The following encoding is used:<br/>           0: Addr[6]<br/>           1: Addr[7]<br/>           2: Addr[8]<br/>           3: Addr[9]<br/>           4: Addr[10]<br/>           5: Addr[11]<br/>           6: Addr[12]<br/>           7: Addr[13]<br/>           For example, setting this field to 2 will interleave the channels at a 4 cacheline granularity.<br/>           BIOS should set this field same as the lowest selected bit in the Mask field of this register.<br/>           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.<br/> <b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_ADDR_MAP</p> |
| 23:20     | 0h<br>RO         | <b>Reserved</b>   |
| 19:6      | 0000h<br>RW/L    | <p><b>Hash Mask (HASH_MASK):</b><br/>           The 14-bit mask corresponds to memory request Addr[19:6].<br/>           Setting a mask bit to 1 will include that particular address bit in the channel XOR function.<br/>           For example, if the mask is set to 0C04h, then Channel = Addr[17] Addr[16] Addr[8]<br/> <b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_ADDR_MAP</p>  |
| 5:0       | 0h<br>RO         | <b>Reserved</b>   |

### 3.2.42 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<br>RO         | <b>Reserved</b>   |
| 28        | 0h<br>RW/L       | <p><b>Enhanced Hash Mode (EHASH_MODE):</b><br/>           Encoding:<br/>           0: Use address bit-6 for channel selection.<br/>           1: Use the channel Ehash function as defined in the other fields of this register<br/> <b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_ADDR_MAP</p> |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 27        | 0h<br>RO         | <b>Reserved</b>  |
| 26:24     | 0h<br>RW/L       | <p><b>Enhanced Hash LSB Mask Bit (EHASH_LSB_MASK_BIT):</b><br/>This specifies the MC Enhanced Channel interleave bit.<br/>The following encoding is used:</p> <ul style="list-style-type: none"> <li>• 000b: Addr[6]</li> <li>• 001b: Addr[7]</li> <li>• 010b: Addr[8]</li> <li>• 011b: Addr[9]</li> <li>• 100b: Addr[10]</li> <li>• 101b: Addr[11]</li> <li>• 110b: Addr[12]</li> <li>• 111b: Addr[13]</li> </ul> <p>For example, setting this field to 10b will interleave the channels at a 4 cache line granularity.<br/>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.<br/>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.<br/>Examples:</p> <ul style="list-style-type: none"> <li>• HASH_LSB_MASK_BIT = 0x2: physical Addr[8]</li> <li>• EHASH_LSB_MASK_BIT = 0x2: channel address[8], physical address [9]</li> </ul> <p><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_ADDR_MAP</p> |
| 23:20     | 0h<br>RO         | <b>Reserved</b>  |
| 19:6      | 0000h<br>RW/L    | <p><b>Enhanced Hash Mask (EHASH_MASK):</b><br/>The 14 bit mask corresponds to memory request Addr[19:6].<br/>Setting a mask bit to 1 will include that particular address bit in the channel XOR function.<br/>For example, if the mask is set to 14'h0C04, then Channel = Addr[17] Addr[16] Addr[8]<br/>The addresses above refer to channel addresses.<br/>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.<br/>Examples:</p> <ul style="list-style-type: none"> <li>• HASH_LSB_MASK_BIT = 0x2: physical Addr[8]</li> <li>• EHASH_LSB_MASK_BIT=0x2: channel address[8], physical address [9]</li> </ul> <p><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_ADDR_MAP</p>   |
| 5:0       | 0h<br>RO         | <b>Reserved</b>  |

### 3.2.43 GT Memory 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<br>RW/V/L | <b>COUNT:</b><br>Number of accesses<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_PWR_MNGMENT |

### 3.2.44 IA Memory 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.

### 3.2.45 IO Memory 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.

### 3.2.46 **RdCAS 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.

### 3.2.47 **WrCAS 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.

### 3.2.48 **Command Counter (PWM\_COMMAND\_COUNT\_0\_0\_0\_MCHBAR) – Offset 5058h**

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

Used for accurate memory bandwidth calculations.

**Note:** Bit definitions are the same as [PWM\\_GT\\_REQCOUNT\\_0\\_0\\_0\\_MCHBAR](#), offset 5040h.

### 3.2.49 **Self Refresh Mode Control (PM\_SREF\_CONFIG\_0\_0\_0\_MCHBAR) – Offset 5060h**

Defines if and when DDR can go into SR

| 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<br>RO         | <b>Reserved</b>              |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 15:0      | 0200h<br>RW/V/L  | <b>Idle Timer (IDLE_TIMER):</b><br>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.<br>Supported range is 512 to 64K-1<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_PWR_MNGMENT |

### 3.2.50 Address Compare for ECC Error Inject (ECC\_INJ\_ADDR\_COMPARE\_0\_0\_0\_MCHBAR) – Offset 5088h

Error injection is issued 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]

| 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<br>RO               | <b>Reserved</b>   |
| 32:0      | 00000000<br>0h<br>RW/L | <b>ADDRESS:</b><br>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[31:0]<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_DFT |

### 3.2.51 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<br>RO         | <b>Reserved</b>   |
| 38:20     | 7FFFFh<br>RW     | <b>Remap Base Address (REMAPBASE):</b><br>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<br>RO         | <b>Reserved</b>   |

### 3.2.52 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<br>RO         | <b>Reserved</b>              |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 38:20     | 00000h<br>RW     | <b>Remap Limit (REMAPLMT):</b><br>The value in this register defines the upper boundary of the Remap window. The Remap window is inclusive of this address.<br>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.<br>When the value in this register is less than the value programmed into the Remap Base register, the Remap window is disabled.<br>These Bits are Intel TXT lockable. |
| 19:0      | 0h<br>RO         | <b>Reserved</b>   |

### 3.2.53 Address Mask for ECC Error Inject (ECC\_INJ\_ADDR\_MASK\_0\_0\_0\_MCHBAR) – Offset 5158h

Error injection is issued when  $ECC\_INJ\_ADDR\_COMPARE\_0\_0\_0\_MCHBAR[32:0] = ADDR[38:6] \text{ AND } ECC\_INJ\_ADDR\_MASK\_0\_0\_0\_MCHBAR[32:0]$

| 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<br>RO           | <b>Reserved</b>   |
| 32:0      | 1FFFFFFFFh<br>RW/L | <b>ADDRESS:</b><br>Inject error when $ECC\_INJ\_ADDR\_COMPARE\_0\_0\_0\_MCHBAR[32:0] = ADDR[38:6] \text{ AND } ECC\_INJ\_ADDR\_MASK\_0\_0\_0\_MCHBAR[32:0]$<br><b>Locked by:</b> MC_LOCK_0_0_0_MCHBAR.LOCK_MC_DFT |

### 3.2.54 Graphics 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 LT 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<br>RO         | <b>Reserved</b>   |
| 38:12     | 0000000h<br>RW/V | <b>Graphics VT Base Address Register (GFXVTBAR):</b><br>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 LT mode. |
| 11:1      | 0h<br>RO         | <b>Reserved</b>   |
| 0         | 0h<br>RW/V/L     | <b>GFXVTBAREN:</b><br>0: GFX-VTBAR is disabled and does not claim any memory<br>1: GFX-VTBAR memory mapped accesses are claimed and decoded appropriately<br>This bit will remain 0 if VTd capability is disabled.<br><b>Locked by:</b> CAPID0_A_0_0_0_PCI.VTDD   |

### 3.2.55 VTDPVC0BAR Base Address Register (VTDPVC0BAR\_0\_0\_0\_MCHBAR\_NCU) – Offset 5410h

This is the base address for the DMI/PEG 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/PEG VC0 configuration space is disabled and must be enabled by writing a 1 to VC0BAREN.

All the bits in this register are locked in LT 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<br>RO         | <b>Reserved</b>   |
| 38:12     | 0000000h<br>RW/V | <b>VTVC0BAR:</b><br>This field corresponds to bits 38 to 12 of the base address DMI/PEG 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/PEG VC0 register set. All the Bits in this register are locked in LT mode. |
| 11:1      | 0h<br>RO         | <b>Reserved</b>   |
| 0         | 0h<br>RW/V/L     | <b>VTVC0BAREN:</b><br>0: VC0BAR is disabled and does not claim any memory<br>1: VC0BAR memory mapped accesses are claimed and decoded appropriately<br>This bit will remain 0 if VTd capability is disabled.<br><b>Locked by:</b> CAPID0_A_0_0_0_PCI.VTDD   |

### 3.2.56 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<br>RO          | <b>Reserved</b>  |
| 38:10     | 00000000h<br>RW/L | <b>IA Exclusion IMR Base Address (IMRIAEXCBASE):</b><br>This register contains the base address of IA exclusion IMR.<br><b>Locked by:</b> IMRIAEXCBASE_MCHBAR_CBO_INGRESS.LOCK |
| 9:1       | 0h<br>RO          | <b>Reserved</b>  |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 0         | 0h<br>RW/L       | <b>LOCK:</b><br>This bit will lock all writable settings in this register, including itself.<br><b>Locked by:</b> IMRIAEXCBASE_MCHBAR_CBO_INGRESS.LOCK |

### 3.2.57 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<br>RO          | <b>Reserved</b>  |
| 38:10     | 00000000h<br>RW/L | <b>IA Exclusion IMR Limit Address (IMRIAEXCLIMIT):</b><br>This register contains the limit address of IA exclusion IMR.<br><b>Locked by:</b> IMRIAEXCLIMIT_MCHBAR_CBO_INGRESS.LOCK |
| 9:1       | 0h<br>RO          | <b>Reserved</b>  |
| 0         | 0h<br>RW/L        | <b>LOCK:</b><br>This bit will lock all writable settings in this register, including itself.<br><b>Locked by:</b> IMRIAEXCLIMIT_MCHBAR_CBO_INGRESS.LOCK                            |

### 3.2.58 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<br>RO              | <b>Reserved</b>  |
| 38:10     | 00000000<br>h<br>RW/L | <b>GT Exclusion IMR Base Address (IMRGTEXCBASE):</b><br>This register contains the base address of GT exclusion IMR.<br><b>Locked by:</b> IMRGTEXCBASE_MCHBAR_CBO_INGRESS.LOCK |
| 9:1       | 0h<br>RO              | <b>Reserved</b>  |
| 0         | 0h<br>RW/L            | <b>LOCK:</b><br>This bit will lock all writable settings in this register, including itself.<br><b>Locked by:</b> IMRGTEXCBASE_MCHBAR_CBO_INGRESS.LOCK                         |

### 3.2.59 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<br>RO              | <b>Reserved</b>  |
| 38:10     | 00000000<br>h<br>RW/L | <b>GT Exclusion IMR Limit Address (IMRGTEXCLIMIT):</b><br>This register contains the limit address of GT exclusion IMR.<br><b>Locked by:</b> IMRGTEXCLIMIT_MCHBAR_CBO_INGRESS.LOCK |
| 9:1       | 0h<br>RO              | <b>Reserved</b>  |
| 0         | 0h<br>RW/L            | <b>LOCK:</b><br>This bit will lock all writable settings in this register, including itself.<br><b>Locked by:</b> 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.

### 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_CO_ANY_SUM_0_0_0_MCHBAR_PCU)                   | 0000000000000000h |
| 5830h  | 8            | Cycle Sum of Any Active Core (PKG_IA_CO_ANY_0_0_0_MCHBAR_PCU)                        | 0000000000000000h |
| 5838h  | 8            | Cycle Sum of Active Graphics (PKG_GT_CO_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_CO_ANY_SLICE_0_0_0_MCHBAR_PCU)              | 0000000000000000h |
| 5850h  | 8            | Cycle Sum of All Active GT Slice (PKG_GT_CO_SLICES_SUM_0_0_0_MCHBAR_PCU)             | 0000000000000000h |
| 5858h  | 8            | Cycle Sum of Any GT Media Engine (PKG_GT_CO_ANY_MEDIA_0_0_0_MCHBAR_PCU)              | 0000000000000000h |
| 5860h  | 8            | Ratio Sum of Any Active Core (PKG_IA_CO_ANY_RATIO_0_0_0_MCHBAR_PCU)                  | 0000000000000000h |
| 5868h  | 8            | Ratio Sum of Active GT (PKG_GT_CO_ANY_RATIO_0_0_0_MCHBAR_PCU)                        | 0000000000000000h |
| 5870h  | 8            | Ratio Sum of Active GT Slice (PKG_GT_CO_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         |
| 5938h  | 4            | Package Power SKU Unit (PACKAGE_POWER_SKU_UNIT_0_0_0_MCHBAR_PCU)                     | 000A0E03h         |

| Offset | Size (Bytes) | Register Name (Register Symbol)  | Default Value     |
|--------|--------------|--|-------------------|
| 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 (PPO_EFFICIENT_CYCLES_0_0_0_MCHBAR_PCU)         | 00000000h         |
| 596Ch  | 4            | Power Plane 0 Thread Activity (PPO_THREAD_ACTIVITY_0_0_0_MCHBAR_PCU)           | 00000000h         |
| 597Ch  | 4            | Primary Plane 0 Temperature (PPO_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         |
| 5A20h  | 4            | BIOS 2 Level Memory Configuration (BIOS_2LM_CONFIG)                            | 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)             | 00000000000000h |

### 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<br>RW  | <b>POST Code (POSTCODE):</b><br>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<br>00000000<br>h<br>RO/V | <b>DATA:</b><br>The counter value is incremented as a function of the number of cores that reside in C0 and are active.<br>If N cores are simultaneously in C0, then the number of clock ticks that are incremented is N.<br>Counter rate is the Max Non-Turbo frequency (same as TSC). |

### 3.3.4 Cycle Sum of Any Active Core (PKG\_IA\_CO\_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<br>00000000<br>h<br>RO/V | <b>DATA:</b><br>This counter increments whenever one (or more) IA cores are active and in C0 state.<br>Counter rate is the Max Non-Turbo frequency (same as TSC). |

### 3.3.5 Cycle Sum of Active Graphics (PKG\_GT\_CO\_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<br>00000000<br>h<br>RO/V | <b>DATA:</b><br>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<br>00000000<br>h<br>RO/V | <b>DATA:</b><br>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<br>00000000<br>h<br>RO/V | <b>DATA:</b><br>This counter increments whenever a GT slice (one of more) is active.<br>Counter rate is the Crystal clock. |

### 3.3.8 Cycle Sum of All Active GT Slice (PKG\_GT\_CO\_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<br>00000000<br>h<br>RW/V/L | <b>DATA:</b><br>This counter increments by the sum of all active GT slices.<br>Counter rate is the Crystal clock. |

### 3.3.9 Cycle Sum of Any GT Media Engine (PKG\_GT\_CO\_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<br>00000000<br>h<br>RW/V/L | <b>DATA:</b><br>This counter increments whenever any GT media engine is active.<br>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<br>00000000<br>h<br>RO/V | <b>DATA:</b><br>This counter increments whenever one or more IA cores are active and in C0 state.<br>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<br>00000000<br>h<br>RO/V | <b>DATA:</b><br>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\_RATIO\_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<br>00000000<br>h<br>RO/V | <b>DATA:</b><br>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<br>RW/L       | <b>LOCKED:</b><br>When set, this entire register becomes read-only. This bit will typically be set by BIOS during boot.<br><b>Locked by:</b> DDR_RAPL_LIMIT_0_0_0_MCHBAR_PCU.LOCKED   |
| 62:48     | 0h<br>RO         | <b>Reserved</b>   |
| 47        | 0h<br>RW/L       | <b>Power Limitation #2 Enable (LIMIT2_ENABLE):</b><br>Power Limit 2 (PL2) enable bit for DDR domain.<br><b>Locked by:</b> DDR_RAPL_LIMIT_0_0_0_MCHBAR_PCU.LOCKED  |
| 46:32     | 0000h<br>RW/L    | <b>Power Limitation #2 (LIMIT2_POWER):</b><br>Power Limit 2 (PL2) for DDR domain in Watts.<br>Format is U11.3: Resolution 0.125W, Range 0-2047.875W.<br><b>Locked by:</b> DDR_RAPL_LIMIT_0_0_0_MCHBAR_PCU.LOCKED  |
| 31:24     | 0h<br>RO         | <b>Reserved</b>   |
| 23:22     | 0h<br>RW/L       | <b>Limitation #1 Time Window X (LIMIT1_TIME_WINDOW_X):</b><br>Power Limit 1 (PL1) time window X value, for DDR domain.<br>Actual time window for RAPL is: $(1/1024 \text{ seconds}) * (1+(X/4)) * (2Y)$<br><b>Locked by:</b> DDR_RAPL_LIMIT_0_0_0_MCHBAR_PCU.LOCKED |
| 21:17     | 00h<br>RW/L      | <b>Limitation #1 Time Window Y (LIMIT1_TIME_WINDOW_Y):</b><br>Power Limit 1 (PL1) time window Y value, for DDR domain.<br>Actual time window for RAPL is: $(1/1024 \text{ seconds}) * (1+(X/4)) * (2Y)$<br><b>Locked by:</b> DDR_RAPL_LIMIT_0_0_0_MCHBAR_PCU.LOCKED |
| 16        | 0h<br>RO         | <b>Reserved</b>   |
| 15        | 0h<br>RW/L       | <b>Power Limit 1 Enable (LIMIT1_ENABLE):</b><br>Power Limit 1 (PL1) enable bit for DDR domain.<br><b>Locked by:</b> DDR_RAPL_LIMIT_0_0_0_MCHBAR_PCU.LOCKED  |
| 14:0      | 0000h<br>RW/L    | <b>Power Limit 1 (LIMIT1_POWER):</b><br>Power Limit 1 (PL1) for DDR domain in Watts.<br>Format is U11.3: Resolution 0.125W, Range 0-2047.875W.<br><b>Locked by:</b> 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<br>RO/V/P | <b>COUNTS:</b><br>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<br>RO         | <b>Reserved</b>  |
| 29        | 0h<br>RW/OC/V    | <b>Turbo Attenuation Status (TURBO_ATTEN_LOG):</b><br>Indicates that the frequency has throttled due to rapid frequency changes that lead to a performance loss. |
| 28        | 0h<br>RW/OC/V    | <b>Maximum Turbo Log (MAX_TURBO_LIMIT_LOG):</b><br>Indicates that the frequency has throttled due to exceeding turbo limits.                                     |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 27        | 0h<br>RW/0C/V    | <b>PL2/PL3 Status (PBM_PL2_LOG):</b><br>Indicates that the frequency has throttled due to exceeding PL2, PSysPL2, PL3 or PSysPL3 power limits.                                   |
| 26        | 0h<br>RW/0C/V    | <b>PL1 Log (PBM_PL1_LOG):</b><br>Indicates that the frequency has throttled due to exceeding PL1 or PSysPL1 power limits.  |
| 25        | 0h<br>RW/0C/V    | <b>FIVR Thermal Design Current Log (FIVR_TDC_LOG):</b><br>Indicates that the frequency has throttled due to exceeding the FIVR Thermal Design Current limit.                     |
| 24        | 0h<br>RW/0C/V    | <b>Electrical Design Protection Log (EDP_LOG):</b><br>Indicates that the frequency has throttled due to exceeding the EDP limits. EDP limits are IccMax, PL4 and Voltage Limits. |
| 23        | 0h<br>RW/0C/V    | <b>VR Thermal Design Current Log (VR_TDC_LOG):</b><br>Indicates that the frequency has throttled due to exceeding the VR Thermal Design Current limit.                           |
| 22        | 0h<br>RW/0C/V    | <b>VR is Hot Log (VR_THERMALERT_LOG):</b><br>Indicates that the frequency has throttled due to a VR HOT event (any processor VR).  |
| 21        | 0h<br>RW/0C/V    | <b>Running Average Thermal Limit Log (RATL_LOG):</b><br>Indicates that the frequency has throttled due to RATL thermal throttling.   |
| 20        | 0h<br>RO         | <b>Reserved</b>  |
| 19        | 0h<br>RW/0C/V    | <b>PCS Log (PCS_LIMIT_LOG):</b><br>Indicates that the frequency has throttled due to exceeding PECEI power limits.   |
| 18        | 0h<br>RW/0C/V    | <b>DDR Power Log (PBM_DDR_LOG):</b><br>Indicates that the frequency has throttled due to exceeding DDR power limits.   |
| 17        | 0h<br>RW/0C/V    | <b>Thermal Log (THERMAL_LOG):</b><br>Indicates that the frequency has throttled due to thermals reaching TjMax.  |
| 16        | 0h<br>RW/0C/V    | <b>PROCHOT# Log (PROCHOT_LOG):</b><br>Indicates that the frequency has throttled due to PROCHOT# assertion.  |
| 15:14     | 0h<br>RO         | <b>Reserved</b>  |
| 13        | 0h<br>RO/V       | <b>Turbo Attenuation Status (TURBO_ATTEN):</b><br>Indicates that the frequency is throttled due to rapid frequency changes that lead to a performance loss.                      |
| 12        | 0h<br>RO/V       | <b>Maximum Turbo Status (MAX_TURBO_LIMIT):</b><br>Indicates that the frequency is throttled due to exceeding turbo limits.   |
| 11        | 0h<br>RO/V       | <b>PL2/3 Status (PBM_PL2):</b><br>Indicates that the frequency is throttled due to exceeding PL2, PSysPL2, PL3 or PSysPL3 power limits.  |
| 10        | 0h<br>RO/V       | <b>PL1 Status (PBM_PL1):</b><br>Indicates that the frequency is throttled due to exceeding PL1 or PSysPL1 power limits.  |
| 9         | 0h<br>RO/V       | <b>FIVR Thermal Design Current Status (FIVR_TDC):</b><br>Indicates that the frequency is throttled due to exceeding the FIVR Thermal Design Current limit.                       |
| 8         | 0h<br>RO/V       | <b>Electrical Design Protection Status (EDP):</b><br>Indicates that the frequency is throttled due to exceeding the EDP limits. EDP limits are IccMax, PL4 and Voltage Limits.   |
| 7         | 0h<br>RO/V       | <b>VR Thermal Design Current Status (VR_TDC):</b><br>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<br>RO/V       | <b>VR is Hot Status (VR_THERMALERT):</b><br>Indicates that the frequency is throttled due to a VR HOT event (any processor VR).  |
| 5         | 0h<br>RO/V       | <b>Running Average Thermal Limit Status (RATL):</b><br>Indicates that the frequency is throttled due to RATL thermal throttling. |
| 4         | 0h<br>RO         | <b>Reserved</b>  |
| 3         | 0h<br>RO/V       | <b>PCS Status (PCS_LIMIT):</b><br>Indicates that the frequency is throttled due to exceeding PECEI power limits.                 |
| 2         | 0h<br>RO/V       | <b>DDR Power Status (PBM_DDR):</b><br>Indicates that the frequency is throttled due to exceeding DDR power limits.               |
| 1         | 0h<br>RO/V       | <b>Thermal Status (THERMAL):</b><br>Indicates that the frequency is throttled due to thermals reaching TjMax.                    |
| 0         | 0h<br>RO/V       | <b>PROCHOT# Status (PROCHOT):</b><br>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<br>RO         | <b>Reserved</b>  |
| 30        | 0h<br>RW/0C/V    | <b>Minimum Supported Power Log (MSPE_LOG):</b><br>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<br>RW/0C/V    | <b>Maximum Turbo Log (MAX_TURBO_LIMIT_LOG):</b><br>Indicates that the frequency has throttled due to exceeding turbo limits.<br>When GT has more than 1 slice, the additional slices may cause GT to operate at a lower frequency. |
| 28        | 0h<br>RW/0C/V    | <b>Inefficient Operation Log (INEFFICIENT_OPERATION_LOG):</b><br>Indicates that the frequency has throttled due to efficiency concerns.  |
| 27        | 0h<br>RW/0C/V    | <b>PL2/PL3 Status (PBM_PL2_LOG):</b><br>Indicates that the frequency has throttled due to exceeding PL2, PSysPL2, PL3 or PSysPL3 power limits.   |
| 26        | 0h<br>RW/0C/V    | <b>PL1 Log (PBM_PL1_LOG):</b><br>Indicates that the frequency has throttled due to exceeding PL1 or PSysPL1 power limits.  |
| 25        | 0h<br>RO         | <b>Reserved</b>  |
| 24        | 0h<br>RW/0C/V    | <b>Electrical Design Protection Log (EDP_LOG):</b><br>Indicates that the frequency has throttled due to exceeding the EDP limits.<br>EDP limits are IccMax, PL4 and Voltage Limits.  |
| 23        | 0h<br>RW/0C/V    | <b>VR Thermal Design Current Log (VR_TDC_LOG):</b><br>Indicates that the frequency has throttled due to exceeding the VR Thermal Design Current limit.   |
| 22        | 0h<br>RW/0C/V    | <b>VR is Hot Log (VR_THERMALERT_LOG):</b><br>Indicates that the frequency has throttled due to a VR HOT event (any processor VR).  |
| 21        | 0h<br>RW/0C/V    | <b>Running Average Thermal Limit Log (RATL_LOG):</b><br>Indicates that the frequency has throttled due to RATL thermal throttling.   |
| 20        | 0h<br>RO         | <b>Reserved</b>  |
| 19        | 0h<br>RW/0C/V    | <b>PCS Log (PCS_LIMIT_LOG):</b><br>Indicates that the frequency has throttled due to exceeding PECI power limits.  |
| 18        | 0h<br>RW/0C/V    | <b>DDR Power Log (PBM_LIMIT_LOG):</b><br>Indicates that the frequency has throttled due to exceeding DDR power limits.   |
| 17        | 0h<br>RW/0C/V    | <b>Thermal Log (THERMAL_LOG):</b><br>Indicates that the frequency has throttled due to thermals reaching TjMax.  |
| 16        | 0h<br>RW/0C/V    | <b>PROCHOT# Log (PROCHOT_LOG):</b><br>Indicates that the frequency has throttled due to PROCHOT# assertion.  |
| 15        | 0h<br>RO         | <b>Reserved</b>  |
| 14        | 0h<br>RO/V       | <b>Minimum Supported Power Status (MSPE):</b><br>Indicates that the frequency is throttled due to the processor is running below the minimum supported power.  |
| 13        | 0h<br>RO/V       | <b>Maximum Turbo Status (MAX_TURBO_LIMIT):</b><br>Indicates that the frequency is throttled due to exceeding turbo limits.<br>When GT has more than 1 slice, the additional slices may cause GT to operate at a lower frequency.   |
| 12        | 0h<br>RO/V       | <b>Inefficient Operation Status (INEFFICIENT_OPERATION):</b><br>Indicates that the frequency is throttled due to efficiency concerns.  |
| 11        | 0h<br>RO/V       | <b>PL2/3 Status (PBM_PL2):</b><br>Indicates that the frequency is throttled due to exceeding PL2, PSysPL2, PL3 or PSysPL3 power limits.  |
| 10        | 0h<br>RO/V       | <b>PL1 Status (PBM_PL1):</b><br>Indicates that the frequency is throttled due to exceeding PL1 or PSysPL1 power limits.  |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 9         | 0h<br>RO         | <b>Reserved</b>  |
| 8         | 0h<br>RO/V       | <b>Electrical Design Protection Status (EDP):</b><br>Indicates that the frequency is throttled due to exceeding the EDP limits. EDP limits are IccMax, PL4 and Voltage Limits. |
| 7         | 0h<br>RO/V       | <b>VR Thermal Design Current Status (VR_TDC):</b><br>Indicates that the frequency is throttled due to exceeding the VR Thermal Design Current limit.                           |
| 6         | 0h<br>RO/V       | <b>VR is Hot Status (VR_THERMALERT):</b><br>Indicates that the frequency is throttled due to a VR HOT event (any processor VR).  |
| 5         | 0h<br>RO/V       | <b>Running Average Thermal Limit Status (RATL):</b><br>Indicates that the frequency is throttled due to RATL thermal throttling.   |
| 4         | 0h<br>RO         | <b>Reserved</b>  |
| 3         | 0h<br>RO/V       | <b>PCS Status (PCS_LIMIT):</b><br>Indicates that the frequency is throttled due to exceeding PECCI power limits.   |
| 2         | 0h<br>RO/V       | <b>DDR Power Status (PBM_DDR):</b><br>Indicates that the frequency is throttled due to exceeding DDR power limits.   |
| 1         | 0h<br>RO/V       | <b>Thermal Status (THERMAL):</b><br>Indicates that the frequency is throttled due to thermals reaching TjMax.  |
| 0         | 0h<br>RO/V       | <b>PROCHOT# Status (PROCHOT):</b><br>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<br>RO         | <b>Reserved</b>   |
| 55:40     | 0000h<br>RO/V    | <b>System Agent Voltage (SA_VOLTAGE):</b><br>Reports the System Agent voltage in u3.13 format. Conversion to Volts:<br>$V = SA\_VOLTAGE / 8192.0$ |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 39:32     | 20h<br>RO/V      | <b>PSF0 PLL Ratio (PSF0_RATIO):</b><br>Reports the PSF0 PLL ratio.<br>The PSF0 frequency is: Ratio * 16.67MHz.<br>The supported ratios are {32, 48, 64} = {533MHz, 800MHz, 1067MHz}.  |
| 31:24     | 00h<br>RO/V      | <b>RING UCLK PLL Ratio (UCLK_RATIO):</b><br>Used to calculate the ring's frequency.<br>Ring Frequency = UCLK_RATIO * BCLK<br>Notes: <ul style="list-style-type: none"> <li>BCLK is read from BCLK_FREQ_0_0_0_MCHBAR.BCLK_FREQ. Value is in KHz.</li> <li>In the above formula, BCLK is in MHz.</li> </ul>   |
| 23:18     | 00h<br>RO/V      | <b>IPU PS Ratio (IPU_PS_RATIO):</b><br>IPU PS RATIO.<br>The frequency is 25MHz * Ratio.   |
| 17:12     | 00h<br>RO/V      | <b>IPU IS Divisor (IPU_IS_DIVISOR):</b><br>The frequency is 1600MHz/Divisor.  |
| 11        | 0h<br>RO/V       | <b>On Package Interface (OPI) Link Speed (OPI_LINK_SPEED):</b><br>0: 2Gb/s<br>1: 4Gb/s  |
| 10        | 0h<br>RO/V       | <b>DDR QCLK Reference (QCLK_REFERENCE):</b><br>0: 133.34Mhz. In frequency calculations use 400.0MHz/3.0.<br>1: 100.00Mhz  |
| 9:2       | 00h<br>RO/V      | <b>DDR QCLK Ratio (QCLK_RATIO):</b><br>Reference clock is determined by the QCLK_REFERENCE field.<br>QCLK frequency calculation when QCLK_REFERENCE = 0 (133.34MHz):<br>QCLK frequency = QCLK_RATIO * BCLK * 4.0 / 3.0<br>QCLK frequency calculation when QCLK_REFERENCE = 1 (100MHz):<br>QCLK frequency = QCLK_RATIO * BCLK<br>Notes: <ul style="list-style-type: none"> <li>BCLK is read from BCLK_FREQ_0_0_0_MCHBAR.BCLK_FREQ. Value is in KHz.</li> <li>In the above formulas, BCLK is in MHz.</li> </ul> |
| 1:0       | 0h<br>RO/V       | <b>Last Display Engine Workpoint Request Served (LAST_DE_WP_REQ_SERVED):</b><br>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<br>RO         | <b>Reserved</b>   |
| 4:0       | 00h<br>RW        | <b>Priority Level (PRIPTP):</b><br>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<br>RO         | <b>Reserved</b>   |
| 4:0       | 10h<br>RW        | <b>Priority Level (SECPTP):</b><br>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<br>RO/V | <b>DATA:</b><br>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<br>RO         | <b>Reserved</b>  |
| 19:16     | Ah<br>RO/V       | <b>Time Unit (TIME_UNIT):</b><br>Time Units used for power control registers.<br>The actual unit value is calculated by $1 \text{ s} / \text{Power}(2, \text{TIME\_UNIT})$ .<br>The default value of Ah corresponds to 976 usec.             |
| 15:13     | 0h<br>RO         | <b>Reserved</b>  |
| 12:8      | 0Eh<br>RO/V      | <b>Energy Unit (ENERGY_UNIT):</b><br>Energy Units used for power control registers.<br>The actual unit value is calculated by $1 \text{ J} / \text{Power}(2, \text{ENERGY\_UNIT})$ .<br>The default value of 14 corresponds to Ux.14 number. |
| 7:4       | 0h<br>RO         | <b>Reserved</b>  |
| 3:0       | 3h<br>RO/V       | <b>Power Unit (PWR_UNIT):</b><br>Power Units used for power control registers.<br>The actual unit value is calculated by $1 \text{ W} / \text{Power}(2, \text{PWR\_UNIT})$ .<br>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<br>RO         | <b>Reserved</b>   |
| 28:20     | 000h<br>RO/V     | <b>Slices Ratio (SLICES_RATIO):</b><br>GT slices frequency:<br>SLICES_RATIO * 16.666Mhz.<br>When GT is in RC6 this frequency is zero.       |
| 19:11     | 000h<br>RO/V     | <b>Un-slice Ratio (UNSLICE_RATIO):</b><br>GT Un-slice frequency:<br>UNSLICE_RATIO * 16.666Mhz.<br>When GT is in RC6 this frequency is zero. |
| 10:0      | 000h<br>RO/V/P   | <b>Slices Voltage (SLICES_VOLTAGE):</b><br>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<br>RO/V | <b>DATA:</b><br>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<br>RO/V | <b>DATA:</b><br>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<br>RO         | <b>Reserved</b>                             |
| 7:0       | 00h<br>RO/V      | <b>DATA:</b><br>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<br>RO         | <b>Reserved</b>  |
| 7:0       | FFh<br>RW        | <b>RP0 State Limit (RPSTT_LIM):</b><br>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 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<br>RO         | <b>Reserved</b>  |
| 23:16     | 00h<br>RW/P      | <b>RPn Capability (RPN_CAP):</b><br>RPn is the lowest requestable RP state.<br>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<br>RW/P      | <b>RP1 Capability (RP1_CAP):</b><br>RP1 is the sustained RP state.<br>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<br>RW/P      | <b>RPO Capability (RPO_CAP):</b><br>RPO is the highest RP state.<br>This field indicates the maximum RPO PLL ratio for the Integrated Graphics Engine (GT).<br>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<br>RW/L       | <b>LOCKED:</b><br>When set, this entire register becomes read-only.<br><b>Locked by:</b> TEMPERATURE_TARGET.LOCKED  |
| 30        | 0h<br>RO         | <b>Reserved</b>   |
| 29:24     | 00h<br>RO/V      | <b>TjMax Tcc Offset (TJ_MAX_TCC_OFFSET):</b><br>Temperature offset in degrees (C) from the TjMax. Used for throttling temperature. Will not impact temperature reading.<br>If offset is allowed and set, the throttle will occur and reported at lower than TjMax.<br><b>Locked by:</b> TEMPERATURE_TARGET.LOCKED |
| 23:16     | 00h<br>RO/V      | <b>Thermal Junction Maximum Temperature (TJMAX):</b><br>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<br>RO/V      | <b>Fan Temperature Offset (FAN_TEMP_TARGET_OFST):</b><br>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<br>RO/V       | <b>Tcc Offset Clamping Bit (TCC_OFFSET_CLAMPING_BIT):</b><br>When enabled will allow RATL throttling below P1<br><b>Locked by:</b> TEMPERATURE_TARGET.LOCKED  |
| 6:0       | 00h<br>RO/V      | <b>Tcc Offset Time Window (TCC_OFFSET_TIME_WINDOW):</b><br>Describes the RATL averaging time window<br><b>Locked by:</b> 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<br>RW/L       | <b>Package Limitation #2 Lock (PKG_PWR_LIM_LOCK):</b><br>When set, all settings in this register are locked and are treated as Read Only.<br>This bit will typically set by BIOS during boot time or resume from Sx.<br><b>Locked by:</b> PACKAGE_RAPL_LIMIT_0_0_0_MCHBAR_PCU.PKG_PWR_LIM_LOCK   |
| 62:48     | 0h<br>RO         | <b>Reserved</b>  |
| 47        | 0h<br>RW/L       | <b>Package Limitation #2 Enable (PKG_PWR_LIM_2_EN):</b><br>This bit enables/disables Package Limitation #2 (PL2).<br>0b: Package Power Limit 2 is Disabled<br>1b: Package Power Limit 2 is Enabled<br><b>Locked by:</b> PACKAGE_RAPL_LIMIT_0_0_0_MCHBAR_PCU.PKG_PWR_LIM_LOCK   |
| 46:32     | 0000h<br>RW/L    | <b>Package Power Limitation #2 (PKG_PWR_LIM_2):</b><br>This field indicates the power limitation #2.<br>The unit of measurement is defined in MSR PACKAGE_POWER_SKU_UNIT[PWR_UNIT].<br><b>Locked by:</b> PACKAGE_RAPL_LIMIT_0_0_0_MCHBAR_PCU.PKG_PWR_LIM_LOCK  |
| 31:24     | 0h<br>RO         | <b>Reserved</b>  |
| 23:17     | 00h<br>RW/L      | <b>Package Limitation #1 Time Window (PKG_PWR_LIM_1_TIME):</b><br>Specifies the time window used to calculate average power for PL1 and PL2.<br>The timing interval window is Floating Point number given by $1.x * power(2,y)$ .<br>$x = \text{PKG\_PWR\_LIM\_1\_TIME}[23:22]$<br>$y = \text{PKG\_PWR\_LIM\_1\_TIME}[21:17]$<br>The unit of measurement is defined in MSR PACKAGE_POWER_SKU_UNIT[TIME_UNIT].<br>The maximal time window is bounded by MSR PACKAGE_POWER_SKU[PKG_MAX_WIN].<br>The minimum time window is 1 unit of measurement (as defined above).<br><b>Locked by:</b> PACKAGE_RAPL_LIMIT_0_0_0_MCHBAR_PCU.PKG_PWR_LIM_LOCK |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 16        | 0h<br>RW/L       | <b>Package Clamping limitation #1 (PKG_CLMP_LIM_1):</b><br>Allows going below P1.<br>0b: Power limit throttling is limited between base frequency (P1) and Max turbo frequency (P0).<br>1b: Power limit throttling is not limited.<br><b>Locked by:</b> PACKAGE_RAPL_LIMIT_0_0_0_MCHBAR_PCU.PKG_PWR_LIM_LOCK |
| 15        | 0h<br>RW/L       | <b>Package Power Limit 1 Enable (PKG_PWR_LIM_1_EN):</b><br>This bit enables/disables Package Power Limit 1.<br>0b: Package Power Limit 1 is Disabled<br>1b: Package Power Limit 1 is Enabled<br><b>Locked by:</b> PACKAGE_RAPL_LIMIT_0_0_0_MCHBAR_PCU.PKG_PWR_LIM_LOCK                                       |
| 14:0      | 0000h<br>RW/L    | <b>Package Power Limit 1 (PKG_PWR_LIM_1):</b><br>This field indicates the power limitation #1 (PL1).<br>The unit of measurement is defined in PACKAGE_POWER_SKU_UNIT_MSR[PWR_UNIT].<br><b>Locked by:</b> 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<br>RO/V       | <b>VALID:</b><br>This bit indicates that the TEMPERATURE field is valid.<br>It is set by PCU if the temperature is within valid thermal sensor range.   |
| 30:27     | 1h<br>RO         | <b>RESOLUTION:</b><br>Supported resolution in degrees C.  |
| 26:23     | 0h<br>RO         | <b>Reserved</b>   |
| 22:16     | 00h<br>RO/V      | <b>TEMPERATURE:</b><br>This is a temperature offset in degrees C below the TjMax temperature.<br>This number is meaningful only if VALID bit in this register is set.   |
| 15        | 0h<br>RW/OC/V    | <b>Cross Domain Limit Log (CROSS_DOMAIN_LIMIT_LOG):</b><br>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.<br>This bit is sticky, software may clear this bit by writing a zero (0). |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 14        | 0h<br>RO/V       | <b>Cross Domain Limit Status (CROSS_DOMAIN_LIMIT_STATUS):</b><br>If set (1), indicates another hardware domain (e.g. processor graphics) is currently limiting energy efficiency optimizations in the processor core domain.  |
| 13        | 0h<br>RW/0C/V    | <b>Current Limit Log (CURRENT_LIMIT_LOG):</b><br>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). |
| 12        | 0h<br>RO/V       | <b>Current Limit Status (CURRENT_LIMIT_STATUS):</b><br>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<br>RW/0C/V    | <b>Power Limitation Log (POWER_LIMITATION_LOG):</b><br>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<br>RO/V       | <b>Power Limitation Status (POWER_LIMITATION_STATUS):</b><br>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<br>RW/0C/V    | <b>Threshold2 Log (THRESHOLD2_LOG):</b><br>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<br>RO/V       | <b>Threshold2 Status (THRESHOLD2_STATUS):</b><br>Indicates that the current temperature is higher than or equal to Threshold 2 temperature.   |
| 7         | 0h<br>RW/0C/V    | <b>Threshold1 Log (THRESHOLD1_LOG):</b><br>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<br>RO/V       | <b>Threshold1 Status (THRESHOLD1_STATUS):</b><br>Indicates that the current temperature is higher than or equal to Threshold 1 temperature.   |
| 5         | 0h<br>RW/0C/V    | <b>Out Of Specification Log (OUT_OF_SPEC_LOG):</b><br>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<br>RO/V       | <b>Out Of Specification Status (OUT_OF_SPEC_STATUS):</b><br>Status bit indicating that the processor is operating out of its thermal specification. Once set, this bit only clears on a reset.  |
| 3         | 0h<br>RW/0C/V    | <b>PROCHOT# Log (PROCHOT_LOG):</b><br>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<br>RO/V       | <b>PROCHOT# Status (PROCHOT_STATUS):</b><br>Status bit indicating that PROCHOT# is currently being asserted.  |
| 1         | 0h<br>RW/0C/V    | <b>Thermal Monitor Log (THERMAL_MONITOR_LOG):</b><br>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<br>RO/V       | <b>Thermal Monitor Status (THERMAL_MONITOR_STATUS):</b><br>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<br>RO         | <b>Reserved</b>  |
| 24        | 0h<br>RW         | <b>Power Interrupt Enable (POWER_INT_ENABLE):</b><br>When this bit is set, a thermal interrupt will be sent upon throttling due to power limitations.  |
| 23        | 0h<br>RW         | <b>Threshold2 Interrupt Enable (THRESHOLD_2_INT_ENABLE):</b><br>Controls the generation of a thermal interrupt whenever the Thermal Threshold 2 Temperature is crossed.  |
| 22:16     | 00h<br>RW        | <b>Threshold2 Relative Temperature (THRESHOLD_2_REL_TEMP):</b><br>This value indicates the offset in degrees below TjMax Temperature that should trigger a Thermal Threshold 2 trip.   |
| 15        | 0h<br>RW         | <b>Threshold1 Interrupt Enable (THRESHOLD_1_INT_ENABLE):</b><br>Controls the generation of a thermal interrupt whenever the Thermal Threshold 1 Temperature is crossed.  |
| 14:8      | 00h<br>RW        | <b>Threshold1 Relative Temperature (THRESHOLD_1_REL_TEMP):</b><br>This value indicates the offset in degrees below TjMax Temperature that should trigger a Thermal Threshold 1 trip.   |
| 7:5       | 0h<br>RO         | <b>Reserved</b>  |
| 4         | 0h<br>RW         | <b>Out Of Spec Interrupt Enable (OUT_OF_SPEC_INT_ENABLE):</b><br>Thermal interrupt enable for the critical temperature condition which is stored in the Critical Temperature Status bit in IA32_THERM_STATUS.  |
| 3         | 0h<br>RO         | <b>Reserved</b>  |
| 2         | 0h<br>RW         | <b>Bidirectional PROCHOT# Interrupt Enable (PROCHOT_INT_ENABLE):</b><br>If set, a thermal interrupt is delivered on the rising edge of PROCHOT#.   |
| 1         | 0h<br>RW         | <b>Low Temperature Interrupt Enable (LOW_TEMP_INT_ENABLE):</b><br>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<br>RW         | <b>High Temperature Interrupt Enable (HIGH_TEMP_INT_ENABLE):</b><br>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<br>RO         | <b>Reserved</b>  |
| 30        | 0h<br>RW         | <b>Force MDID Override (FORCE_MDID_OVERRIDE):</b><br>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<br>RW         | <b>Disable MDID Evaluation (DISABLE_MDID_EVALUATION):</b><br>Send a value of disabled to the PCH for the MDID field.   |
| 28:8      | 000000h<br>RW    | <b>Next Device Activity (NEXT_DEVICE_ACTIVITY):</b><br>These are in 1us increments and can report a maximum value of approximately 2 seconds   |
| 7         | 0h<br>RW         | <b>Interrupt or Memory (IM):</b><br>0: Interrupt. This is a hint for the idle duration time to the next interrupt.<br>1: Memory. This is a hint for the idle duration time to the next snoop cycle.  |
| 6         | 0h<br>RW         | <b>Opportunistic or Deterministic (OD):</b><br>0: Opportunistic. This is an opportunistic hint as suggested by the sub-system.<br>1: Deterministic. This is a deterministic hint as suggested by the sub-system.   |
| 5:2       | 0h<br>RO         | <b>Reserved</b>  |
| 1         | 0h<br>RW         | <b>VALID:</b><br>0: This Idle Duration Override CSR is not valid<br>1: This Idle Duration Override CSR is valid  |
| 0         | 0h<br>RO         | <b>Reserved</b>  |

### 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<br>00000000<br>h<br>RO/V | <b>DATA:</b><br>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<br>00000000<br>h<br>RO/V | <b>DATA:</b><br>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<br>RW  | <b>DATA:</b><br>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 BIOS 2 Level Memory Configuration (BIOS\_2LM\_CONFIG) – Offset 5A20h

This register is used by BIOS to specify 2 Level Memory (2LM) configurations.



| Type | Size   | Offset         | Default   |
|------|--------|----------------|-----------|
| MMIO | 32 bit | MCHBAR + 5A20h | 00000000h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 31:1      | 0h<br>RO         | <b>Reserved</b>  |
| 0         | 0h<br>RW         | <b>NM Flush Required (NM_FLUSH_REQUIRED):</b><br>This bit is set by BIOS to indicate if NM Flush is required as part of PKGS/Reset entry.<br>0: NM Retain is required as part of PKGS/Reset entry<br>1: NM Flush is required as part of PKGS/Reset entry |

### 3.3.41 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<br>00000000<br>h<br>RW/P | <b>SKPD:</b><br>64bit of data storage. |

### 3.3.42 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<br>RW/V | <b>DATA:</b><br>This field contains the data associated with specific commands. |

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



### 3.3.44 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<br>RO         | <b>Reserved</b>   |
| 1         | 0h<br>RW         | <b>PCIe Enumeration Done (PCIE_ENUMERATION_DONE):</b><br>This will be set after PCIe enumeration is done.<br>If it is set, the PCU will look at the following bits in DEVEN_0_0_0_PCI:<br>1: D1F2EN<br>2: D1F1EN<br>3: D1F0EN<br>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.<br>Note: Implicit assumption - this bit is asserted prior to (or with) asserting RST_CPL. |
| 0         | 0h<br>RW/1S      | <b>Reset Complete (RST_CPL):</b><br>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.<br>It is expected that this bit will be set just before BIOS transfer of control to the OS.<br>0b: Not ready<br>1b: BIOS PM configuration complete                             |

### 3.3.45 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<br>RW         | <b>RUN/BUSY Bit (RUN_BUSY):</b><br>This bit indicates that the BIOS request is pending.<br>BIOS sets this bit together with a command in the lower bits of this register.<br>The PCU may only clear this bit after the BIOS request has been served or observed.  |
| 30:17     | 0h<br>RO         | <b>Reserved</b>   |
| 16        | 0h<br>RW         | <b>Gear Type (GEAR_TYPE):</b><br>0h: Gear1 (Default) - DDR bus clock is the same as QCLK<br>1h: Gear2 - DDR PHY bus clock is double of QCLK   |
| 15:12     | 0h<br>RO         | <b>Reserved</b>   |
| 11:8      | 0h<br>RW         | <b>Reference Clock Type (REQ_TYPE):</b><br>Request Type: <ul style="list-style-type: none"> <li>0h: MC frequency request for 133MHz Qclk granularity.</li> <li>1h: MC frequency request for 100MHz Qclk granularity.</li> </ul> All other values are reserved.  |
| 7:0       | 00h<br>RW        | <b>Request Data (REQ_DATA):</b><br>This field holds the memory controller frequency request (QCLK). Each bin is 133/100MHz and not 266/200MHz.<br>This interface replaces the usage of DCLK ratios and Odd Ratio.<br>QCLK frequency is determined by the MC reference clock (MC_FREQ_TYPE) as well as BCLK.<br>0h: MC PLL shutdown<br>1h-2h: Reserved<br>3h-FFh: QCLK ratio in 133.33MHz or 100MHz increments |

### 3.3.46 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<br>RO         | <b>Reserved</b>  |
| 16        | 0h<br>RW/L       | <b>Gear Type (GEAR_TYPE):</b> <ul style="list-style-type: none"> <li>0 - Gear1 (Default) - DDR bus clock is the same as QCLK</li> <li>1 - Gear2 - DDR PHY bus clock is double of QCLK</li> </ul>   |
| 15:12     | 0h<br>RO         | <b>Reserved</b>  |
| 11:8      | 0h<br>RW/L       | <b>Reference Clock Type (MC_FREQ_TYPE):</b><br>This field holds the memory controller frequency Type. <ul style="list-style-type: none"> <li>0h: MC frequency request for 133MHz Qclk granularity.</li> <li>1h: MC frequency request for 100MHz Qclk granularity.</li> </ul> All other values are reserved.  |
| 7:0       | 00h<br>RW/L      | <b>Memory Controller Frequency (MC_FREQ):</b><br>This field holds the memory controller frequency (QCLK).<br>Each bin is 133/100MHz and not 266/200MHz.<br>This interface replaces the usage of DCLK ratios and Odd Ratio.<br>QCLK frequency is determined by the MC reference clock (MC_FREQ_TYPE) as well as BCLK.<br>0: Memory Controller PLL shutdown<br>1h-2h: Reserved<br>3h-FFh: QCLK ratio in 133.33MHz or 100MHz increments |

### 3.3.47 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<br>RO         | <b>Reserved</b>  |
| 15        | 0h<br>RW         | <b>Force Memory Master DLL When Display Engine is Active (MDLL_ON_DE):</b><br>Force memory master DLL on when the Display Engine is active.<br>This includes cases where memory is not accessed.<br>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.<br>0b: Display Engine wakes up memory DLL using the Self Refresh exit indication only<br>1b: Force Memory DLL on when the Display Engine is active                       |
| 14        | 0h<br>RW         | <b>Force Memory Controller PLL When Display Engine is Active (MPLL_ON_DE):</b><br>Force Memory PLLs (MCPLL and GDPLL) on when the Display Engine is active.<br>This includes cases where memory is not accessed.<br>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.<br>0b: Display Engine wakes up Memory PLLs using the Self Refresh exit indication only<br>1b: Force Memory PLLs on when the Display Engine is active |
| 13        | 1h<br>RW         | <b>System Agent Clock Gating Memory Controller PLL (SACG_MPLL):</b><br>When this bit is set to 1b, FCLK will never be gated when the memory controller PLL is ON.<br>Otherwise, FCLK gating policies are not affected by the locking of the memory controller PLLs.  |
| 12        | 0h<br>RW         | <b>Non-Snoop Wake Self Refresh Exit (NSWAKE_SREXIT):</b><br>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.<br>Otherwise, the Non-Snoop indication will not affect the Self Refresh exit policy.   |
| 11        | 0h<br>RW         | <b>System Agent Clock Gating Self Refresh Exit (SACG_SREXIT):</b><br>The Display Engine can indicate to the PCU that it wants the Memory Controller to exit self-refresh.<br>When this bit is set to 1b, this request from the Display Engine will cause FCLK to be ungated.<br>Otherwise, this request from the Display Engine has no effect on FCLK gating.  |
| 10        | 0h<br>RW         | <b>Master DLL Shutdown Power State Enable (MDLL_OFF_SEN):</b><br>This bit indicates when the Memory Master DLL may be shutdown based on link active power states.<br>0b: Memory DLL may be shut down in L1 and deeper sleep states.<br>1b: Memory DLL may be shut down in L0s and deeper sleep states.   |
| 9         | 0h<br>RW         | <b>Memory Controller PLL Shutdown Power State Enable (MPLL_OFF_SEN):</b><br>This bit indicates when the Memory PLLs (MCPLL and GDPLL) may be shutdown based on link active power states.<br>0b: Memory PLLs may be shut down in L1 and deeper sleep states.<br>1b: Memory PLLs may be shut down in L0s and deeper sleep states.  |



| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 8         | 1h<br>RW         | <b>System Agent Clock Gating Power State Enable (SACG_SEN):</b><br>This bit indicates when the System Agent clock gating is possible based on link active power states.<br>0b: System Agent clock gating is allowed in L1 and deeper sleep states.<br>1b: System Agent clock gating is allowed in L0s and deeper sleep states. |
| 7:3       | 0h<br>RO         | <b>Reserved</b>  |
| 2         | 1h<br>RW         | <b>PCIe PLL Shutdown Enable (PPLL_OFF_ENA):</b><br>This bit is used to enable shutting down the PCIe/DMI PLL.<br>0b: PLL shutdown is not allowed<br>1b: PLL shutdown is allowed  |
| 1         | 1h<br>RW         | <b>Memory Controller PLL Shutdown Enable (MPLL_OFF_ENA):</b><br>This bit is used to enable shutting down the Memory Controller PLLs (MCPLL and GDPLL).<br>0b: PLL shutdown is not allowed<br>1b: PLL shutdown is allowed   |
| 0         | 0h<br>RW         | <b>System Agent Clock Gating Enable (SACG_ENA):</b><br>This bit is used to enable or disable the System Agent Clock Gating (FCLK).<br>0b: System Agent Clock Gating is Not Allowed<br>1b: System Agent Clock Gating is Allowed   |

### 3.3.48 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<br>RO         | <b>Reserved</b>  |
| 7:0       | 00h<br>RO/V      | <b>TDP Ratio (TDP_RATIO):</b><br>Nominal TDP level ratio to be used for this specific processor (in units of 100MHz).<br>Note: A value of 0 in this field indicates invalid/undefined TDP point. |



### 3.3.49 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<br>RO         | <b>Reserved</b>  |
| 62:48     | 0000h<br>RO/V    | <b>Minimum Package Power (PKG_MIN_PWR):</b><br>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<br>RO         | <b>Reserved</b>  |
| 46:32     | 0000h<br>RO/V    | <b>Maximum Package Power (PKG_MAX_PWR):</b><br>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]. |
| 31:24     | 0h<br>RO         | <b>Reserved</b>  |
| 23:16     | 00h<br>RO/V      | <b>TDP Ratio (TDP_RATIO):</b><br>TDP ratio for this Configurable TDP Level.  |
| 15        | 0h<br>RO         | <b>Reserved</b>  |
| 14:0      | 0000h<br>RO/V    | <b>Package TDP (PKG_TDP):</b><br>Power Limit (PL1) for this Configurable TDP level. Units defined in MSR PACKAGE_POWER_SKU[PWR_UNIT]. Similar to PACKAGE_POWER_SKU[PKG_TDP].   |

### 3.3.50 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.

### 3.3.51 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<br>RW/L       | <b>Configurable TDP Lock (CONFIG_TDP_LOCK):</b><br>Configurable TDP level select lock.<br>0b: Unlocked.<br>1b: Locked till next reset.<br><b>Locked by:</b> CONFIG_TDP_CONTROL.CONFIG_TDP_LOCK   |
| 30:2      | 0h<br>RO         | <b>Reserved</b>  |
| 1:0       | 0h<br>RW/L       | <b>TDP Level (TDP_LEVEL):</b><br>Select Configurable TDP level:<br>0h: Nominal TDP level (default)<br>1h: Level from CONFIG_TDP_LEVEL_1<br>2h: Level from CONFIG_TDP_LEVEL_2<br>3h: Reserved<br><b>Locked by:</b> CONFIG_TDP_CONTROL.CONFIG_TDP_LOCK |

### 3.3.52 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<br>RW/L       | <b>Turbo Activation Ratio Lock (TURBO_ACTIVATION_RATIO_LOCK):</b><br>Locks this register until the next reset.<br>0b: Unlocked<br>1b: Locked<br><b>Locked by:</b> TURBO_ACTIVATION_RATIO.TURBO_ACTIVATION_RATIO_LOCK   |
| 30:8      | 0h<br>RO         | <b>Reserved</b>  |
| 7:0       | 00h<br>RW/L      | <b>Maximum Non-Turbo Ratio (MAX_NON_TURBO_RATIO):</b><br>CPU will treat any P-state request above this ratio as a request for max turbo<br>0 is special encoding which disables the feature.<br><b>Locked by:</b> TURBO_ACTIVATION_RATIO.TURBO_ACTIVATION_RATIO_LOCK |

### 3.3.53 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<br>RO         | <b>Reserved</b>  |
| 0         | 0h<br>RW/L       | <b>Memory Runtime Timing Overclocking Enabled (MC_TIMING_RUNTIME_OC_ENABLED):</b><br>Adjusting memory timing values for overclocking is enabled. |



### 3.3.54 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<br>RO          | <b>Reserved</b>  |
| 31:0      | 00000000h<br>RW/L | <b>BCLK Frequency (BCLK_FREQ):</b><br>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.

### 3.4.1 Summary of Registers

**Table 3-5. Summary of MCHBAR Registers**

| Offset | Size (Bytes) | Register Name (Register Symbol)                                | Default Value |
|--------|--------------|--|---------------|
| 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     |

### 3.4.2 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<br>RO         | <b>Reserved</b>  |
| 12        | 1h<br>RW/L       | <b>Thunderbolt DMA2 Enable (TBT_DMA2_EN):</b><br>0: DMA2 is disabled and hidden.<br>1: DMA2 is enabled and visible.<br><b>Locked by:</b> CAPID0_D_0_0_0_MCHBAR.TC_TBT_DMA2_DIS |
| 11        | 1h<br>RW/L       | <b>Thunderbolt DMA1 Enable (TBT_DMA1_EN):</b><br>0: DMA1 is disabled and hidden.<br>1: DMA1 is enabled and visible.<br><b>Locked by:</b> CAPID0_D_0_0_0_MCHBAR.TC_TBT_DMA1_DIS |
| 10        | 1h<br>RW/L       | <b>Thunderbolt DMA0 Enable (TBT_DMA0_EN):</b><br>0: DMA0 is disabled and hidden.<br>1: DMA0 is enabled and visible.<br><b>Locked by:</b> CAPID0_D_0_0_0_MCHBAR.TC_TBT_DMA0_DIS |



| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 9         | 1h<br>RW/L       | <b>xDCI Enable (XDCI_EN):</b><br>0: xDCI is disabled and hidden.<br>1: xDCI is enabled and visible.<br><b>Locked by:</b> CAPID0_D_0_0_0_MCHBAR.TC_XDCI_DIS               |
| 8         | 1h<br>RW/L       | <b>xHCI Enable (XHCI_EN):</b><br>0: xHCI is disabled and hidden.<br>1: xHCI is enabled and visible.<br><b>Locked by:</b> CAPID0_D_0_0_0_MCHBAR.TC_XHCI_DIS               |
| 7         | 1h<br>RW/L       | <b>PCIE7 Enable (PCIE7_EN):</b><br>0: TypeC PCIE Root Port 7 is disabled<br>1: TypeC PCIE Root Port 7 is enabled<br><b>Locked by:</b> CAPID0_D_0_0_0_MCHBAR.TC_PCIE7_DIS |
| 6         | 1h<br>RW/L       | <b>PCIE6 Enable (PCIE6_EN):</b><br>0: TypeC PCIE Root Port 6 is disabled<br>1: TypeC PCIE Root Port 6 is enabled<br><b>Locked by:</b> CAPID0_D_0_0_0_MCHBAR.TC_PCIE6_DIS |
| 5         | 1h<br>RW/L       | <b>PCIE5 Enable (PCIE5_EN):</b><br>0: TypeC PCIE Root Port 5 is disabled<br>1: TypeC PCIE Root Port 5 is enabled<br><b>Locked by:</b> CAPID0_D_0_0_0_MCHBAR.TC_PCIE5_DIS |
| 4         | 1h<br>RW/L       | <b>PCIE4 Enable (PCIE4_EN):</b><br>0: TypeC PCIE Root Port 4 is disabled<br>1: TypeC PCIE Root Port 4 is enabled<br><b>Locked by:</b> CAPID0_D_0_0_0_MCHBAR.TC_PCIE4_DIS |
| 3         | 1h<br>RW/L       | <b>PCIE3 Enable (PCIE3_EN):</b><br>0: TypeC PCIE Root Port 3 is disabled<br>1: TypeC PCIE Root Port 3 is enabled<br><b>Locked by:</b> CAPID0_D_0_0_0_MCHBAR.TC_PCIE3_DIS |
| 2         | 1h<br>RW/L       | <b>PCIE2 Enable (PCIE2_EN):</b><br>0: TypeC PCIE Root Port 2 is disabled<br>1: TypeC PCIE Root Port 2 is enabled<br><b>Locked by:</b> CAPID0_D_0_0_0_MCHBAR.TC_PCIE2_DIS |
| 1         | 1h<br>RW/L       | <b>PCIE1 Enable (PCIE1_EN):</b><br>0: TypeC PCIE Root Port 1 is disabled<br>1: TypeC PCIE Root Port 1 is enabled<br><b>Locked by:</b> CAPID0_D_0_0_0_MCHBAR.TC_PCIE1_DIS |
| 0         | 1h<br>RW/L       | <b>PCIE0 Enable (PCIE0_EN):</b><br>0: TypeC PCIE Root Port 0 is disabled<br>1: TypeC PCIE Root Port 0 is enabled<br><b>Locked by:</b> CAPID0_D_0_0_0_MCHBAR.TC_PCIE0_DIS |

### 3.4.3 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<br>RO         | <b>Reserved</b>   |
| 16        | 0h<br>RW/L       | <b>TypeC Sub-system IOM Microcontroller Disable (IOM_DIS):</b><br>0b: Type C IOM is Enabled<br>1b: Type C IOM is Disabled |
| 15:13     | 0h<br>RO         | <b>Reserved</b>   |
| 12        | 0h<br>RW/L       | <b>TypeC Sub-system Thunderbolt DMA2 Disable (TC_TBT_DMA2_DIS):</b><br>Indicates if Type-C DMA2 device is disabled.       |
| 11        | 0h<br>RW/L       | <b>TypeC Sub-system Thunderbolt DMA1 Disable (TC_TBT_DMA1_DIS):</b><br>Indicates if Type-C DMA1 device is disabled.       |
| 10        | 0h<br>RW/L       | <b>TypeC Sub-system Thunderbolt DMA0 Disable (TC_TBT_DMA0_DIS):</b><br>Indicates if Type-C DMA0 device is disabled.       |
| 9         | 0h<br>RW/L       | <b>TypeC Sub-system USB xDCI Disable (TC_XDCI_DIS):</b><br>Indicates if Type-C XDCI device is disabled.                   |
| 8         | 0h<br>RW/L       | <b>TypeC Sub-system USB xHCI Disable (TC_XHCI_DIS):</b><br>Indicates if Type-C XHCI device is disabled.                   |
| 7         | 0h<br>RW/L       | <b>TypeC Sub-system PCIE7 Disable (TC_PCIE7_DIS):</b><br>PCIE7 disable.   |
| 6         | 0h<br>RW/L       | <b>TypeC Sub-system PCIE6 Disable (TC_PCIE6_DIS):</b><br>PCIE6 disable.   |
| 5         | 0h<br>RW/L       | <b>TypeC Sub-system PCIE5 Disable (TC_PCIE5_DIS):</b><br>PCIE5 disable.   |
| 4         | 0h<br>RW/L       | <b>TypeC Sub-system PCIE4 Disable (TC_PCIE4_DIS):</b><br>PCIE4 disable.   |
| 3         | 0h<br>RW/L       | <b>TypeC Sub-system PCIE3 Disable (TC_PCIE3_DIS):</b><br>PCIE3 disable.   |
| 2         | 0h<br>RW/L       | <b>TypeC Sub-system PCIE2 Disable (TC_PCIE2_DIS):</b><br>PCIE2 disable.   |
| 1         | 0h<br>RW/L       | <b>TypeC Sub-system PCIE1 Disable (TC_PCIE1_DIS):</b><br>PCIE1 disable.   |
| 0         | 0h<br>RW/L       | <b>TypeC Sub-system PCIE0 Disable (TC_PCIE0_DIS):</b><br>PCIE0 root port is disabled.                                     |



## 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.

### 3.5.1 Summary of Registers

Table 3-6. Summary of DMIBAR Registers

| Offset | Size (Bytes) | Register Name (Register Symbol)                 | Default Value |
|--------|--------------|---|---------------|
| 0h     | 4            | Device Identifiers (ID)                         | 00008086h     |
| 4h     | 2            | Device Command (CMD)                            | 0006h         |
| 6h     | 2            | Primary Status (PSTS)                           | 0090h         |
| 8h     | 4            | Revision ID (RID_CC)                            | 060000F0h     |
| Eh     | 1            | Header Type (HTYPE)                             | 00h           |
| 1Eh    | 2            | Secondary Status (SSTS)                         | 0000h         |
| 2Ch    | 4            | Subsystem Vendor IDs (SVD)                      | 00000000h     |
| 34h    | 1            | Capabilities List Pointer (CAPP)                | E0h           |
| 3Eh    | 1            | Bridge Control (BCTRL)                          | 00h           |
| 44h    | 1            | Device Capabilities (DCAP)                      | 01h           |
| 48h    | 2            | Device Control (DCTL)                           | 0020h         |
| 4Ah    | 2            | Device Status (DSTS)                            | 0010h         |
| 4Ch    | 4            | Link Capabilities (LCAP)                        | 01714C10h     |
| 50h    | 2            | Link Control (LCTL)                             | 0040h         |
| 52h    | 2            | Link Status (LSTS)                              | 1011h         |
| 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         |



| Offset | Size (Bytes) | Register Name (Register Symbol)                                | Default Value |
|--------|--------------|--|---------------|
| 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     |
| 284h   | 4            | Port VC Capability Register 1 (PVCCR1)                         | 00000000h     |
| 288h   | 4            | Port VC Capability 2 (PVCC2)                                   | 00000000h     |
| 28Ch   | 2            | Port VC Control (PVCC)   | 0000h         |
| 28Eh   | 2            | Port VC Status (PVCS)  | 0000h         |
| 290h   | 4            | Virtual Channel 0 Resource Capability (V0VCRC)                 | 00000000h     |
| 294h   | 4            | Virtual Channel 0 Resource Control (V0CTL)                     | 80000001h     |
| 29Ah   | 2            | Virtual Channel 0 Resource Status (V0STS)                      | 0000h         |
| 29Ch   | 4            | Virtual Channel 1 Resource Capability (V1VCRC)                 | 00000000h     |
| 2A0h   | 4            | Virtual Channel 1 Resource Control (V1CTL)                     | 00000000h     |
| 2A6h   | 2            | Virtual Channel 1 Resource Status (V1STS)                      | 0000h         |
| 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     |
| A90h   | 4            | Data Link Feature Extended Capability Header (DLFECH)          | 00000000h     |
| A94h   | 4            | Data Link Feature Capabilities Register (DLFCAP)               | 80000000h     |
| A98h   | 4            | Data Link Feature Status Register (DLFSTS)                     | 00000000h     |
| A9Ch   | 4            | Physical Layer 16.0 GT/s Extended Capability Header (PL16GECH) | 00000000h     |

| Offset | Size (Bytes) | Register Name (Register Symbol)   | Default Value |
|--------|--------------|---|---------------|
| AA0h   | 4            | Physical Layer 16.0 GT/s Capability Register (PL16CAP)                                    | 00000000h     |
| AA4h   | 4            | Physical Layer 16.0 GT/s Control Register (PL16CTL)                                       | 00000000h     |
| AA8h   | 4            | Physical Layer 16.0 GT/s Status Register (PL16S)  | 00000000h     |
| AACH   | 4            | Physical Layer 16.0 GT/s Local Data Parity Mismatch Status Register (PL16LDPMS)           | 00000000h     |
| AB0h   | 4            | Physical Layer 16.0 GT/s First Retimer Data Parity Mismatch Status Register (PL16FRDPMS)  | 00000000h     |
| AB4h   | 4            | Physical Layer 16.0 GT/s Second Retimer Data Parity Mismatch Status Register (PL16SRDPMS) | 00000000h     |
| AB8h   | 4            | Physical Layer 16.0 GT/s Extra Status Register (PL16ES)                                   | 00000000h     |
| ABCh   | 2            | Physical Layer 16.0 GT/s Lane 01 Equalization Control Register (PL16L01EC)                | FFFFh         |
| ABEh   | 2            | Physical Layer 16.0 GT/s Lane 23 Equalization Control Register (PL16L23EC)                | FFFFh         |
| AC0h   | 2            | Physical Layer 16.0 GT/s Lane 45 Equalization Control Register (PL16L45EC)                | FFFFh         |
| AC2h   | 2            | Physical Layer 16.0 GT/s Lane 67 Equalization Control Register (PL16L67EC)                | FFFFh         |
| AC4h   | 2            | Physical Layer 16.0 GT/s Lane 89 Equalization Control Register (PL16L89EC)                | FFFFh         |
| AC6h   | 2            | Physical Layer 16.0 GT/s Lane 1011 Equalization Control Register (PL16L1011EC)            | FFFFh         |
| AC8h   | 2            | Physical Layer 16.0 GT/s Lane 1213 Equalization Control Register (PL16L1213EC)            | FFFFh         |
| ACAh   | 2            | Physical Layer 16.0 GT/s Lane 1415 Equalization Control Register (PL16L1415EC)            | FFFFh         |
| D00h   | 4            | Device ID Override (DIDOVR)   | 00000000h     |
| EDCh   | 4            | Physical Layer 16.0 GT/s Margining Extended Capability Header (PL16MECH)                  | 00010027h     |
| EE0h   | 4            | Physical Layer 16.0 GT/s Margining Port Capabilities and Port Status (PL16MPCCPS)         | 00000000h     |
| EE4h   | 4            | Physical Layer 16.0 GT/s Lane0 Margin Control and Status Register (PL16L0MCS)             | 00009C38h     |
| EE8h   | 4            | Physical Layer 16.0 GT/s Lane1 Margin Control and Status Register (PL16L1MCS)             | 00009C38h     |
| EECh   | 4            | Physical Layer 16.0 GT/s Lane2 Margin Control and Status Register (PL16L2MCS)             | 00009C38h     |
| EF0h   | 4            | Physical Layer 16.0 GT/s Lane3 Margin Control and Status Register (PL16L3MCS)             | 00009C38h     |
| EF4h   | 4            | Physical Layer 16.0 GT/s Lane4 Margin Control and Status Register (PL16L4MCS)             | 00009C38h     |
| EF8h   | 4            | Physical Layer 16.0 GT/s Lane5 Margin Control and Status Register (PL16L5MCS)             | 00009C38h     |
| EFCh   | 4            | Physical Layer 16.0 GT/s Lane6 Margin Control and Status Register (PL16L6MCS)             | 00009C38h     |
| F00h   | 4            | Physical Layer 16.0 GT/s Lane7 Margin Control and Status Register (PL16L7MCS)             | 00009C38h     |
| F04h   | 4            | Physical Layer 16.0 GT/s Lane8 Margin Control and Status Register (PL16L8MCS)             | 00009C38h     |
| F08h   | 4            | Physical Layer 16.0 GT/s Lane9 Margin Control and Status Register (PL16L9MCS)             | 00009C38h     |
| F0Ch   | 4            | Physical Layer 16.0 GT/s Lane10 Margin Control and Status Register (PL16L10MCS)           | 00009C38h     |

| Offset | Size (Bytes) | Register Name (Register Symbol)   | Default Value |
|--------|--------------|---|---------------|
| F10h   | 4            | Physical Layer 16.0 GT/s Lane11 Margin Control and Status Register (PL16L11MCS) | 00009C38h     |
| F14h   | 4            | Physical Layer 16.0 GT/s Lane12 Margin Control and Status Register (PL16L12MCS) | 00009C38h     |
| F18h   | 4            | Physical Layer 16.0 GT/s Lane13 Margin Control and Status Register (PL16L13MCS) | 00009C38h     |
| F1Ch   | 4            | Physical Layer 16.0 GT/s Lane14 Margin Control and Status Register (PL16L14MCS) | 00009C38h     |
| F20h   | 4            | Physical Layer 16.0 GT/s Lane15 Margin Control and Status Register (PL16L15MCS) | 00009C38h     |

### 3.5.2 Device Identifiers (ID) – Offset 0h

Device ID and Vendor ID

| Type | Size   | Offset      | Default   |
|------|--------|-------------|-----------|
| MMIO | 32 bit | DMIBAR + 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<br>RO/V    | <b>Device Identification (DID):</b><br>See the Device ID table in the first volume of this document. |
| 15:0      | 8086h<br>RO      | <b>Vendor Identification (VID):</b><br>Indicates Intel.  |

### 3.5.3 Device Command (CMD) – Offset 4h

Device Command

| Type | Size   | Offset      | Default |
|------|--------|-------------|---------|
| MMIO | 16 bit | DMIBAR + 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<br>RO         | <b>Reserved</b>              |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 9         | 0h<br>RO         | <b>Fast Back to Back Enable (FBE):</b><br>This field is reserved per PCI-Express spec.  |
| 8         | 0h<br>RW         | <b>SERR# Enable (SEE):</b><br>When set, enables the root port to generate an SERR# message when PSTS.SSE is set.  |
| 7         | 0h<br>RO         | <b>Wait Cycle Control (WCC):</b><br>This field is reserved per PCI-Express spec.  |
| 6         | 0h<br>RW         | <b>Parity Error Response Enable (PERE):</b><br>Indicates that the device is capable of reporting parity errors as a master on the backbone.   |
| 5         | 0h<br>RO         | <b>VGA Palette Snoop (VGA_PSE):</b><br>This field is reserved per PCI-Express spec.   |
| 4         | 0h<br>RO         | <b>Memory Write and Invalidate Enable (MWIE):</b><br>This field is reserved per PCI-Express spec.   |
| 3         | 0h<br>RO         | <b>Special Cycle Enable (SCE):</b><br>This field is reserved per PCI-Express and PCI bridge spec.   |
| 2         | 1h<br>RO         | <b>Bus Master Enable (BME):</b><br>When set, allows the root port to forward Memory and I/O Read/Write cycles onto the backbone from a PCI-Express device.<br>When this bit is 0b, Memory and I/O requests received at a Root Port must be handled as Unsupported Requests (UR).<br>This bit does not affect forwarding of Completions in either the Upstream or Downstream direction.<br>The forwarding of Requests other than Memory or I/O requests is not controlled by this bit. |
| 1         | 1h<br>RO         | <b>Memory Space Enable (MSE):</b><br>When set, memory cycles within the range specified by the memory base and limit registers can be forwarded to the PCI-Express device.<br>When cleared, these memory cycles are master aborted on the backbone.   |
| 0         | 0h<br>RO         | <b>I/O Space Enable (IOSE):</b><br>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.<br>When cleared, these cycles are master aborted on the backbone.  |

### 3.5.4 Primary Status (PSTS) – Offset 6h

Primary Status

| Type | Size   | Offset      | Default |
|------|--------|-------------|---------|
| MMIO | 16 bit | DMIBAR + 6h | 0090h   |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 15        | 0h<br>RW/1C/V    | <b>Detected Parity Error (DPE):</b><br>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<br>RW/1C/V    | <b>Signaled System Error (SSE):</b><br>Set when the root port signals a system error to the internal SERR# logic.  |
| 13        | 0h<br>RW/1C/V    | <b>Received Master Abort (RMA):</b><br>Set when the root port receives a completion with unsupported request status from the backbone.   |
| 12        | 0h<br>RW/1C/V    | <b>Received Target Abort (RTA):</b><br>Set when the root port receives a completion with completer abort from the backbone.  |
| 11        | 0h<br>RW/1C/V    | <b>Signaled Target Abort (STA):</b><br>Set whenever the root port forwards a target abort received from the downstream device onto the backbone.   |
| 10:9      | 0h<br>RO         | <b>Primary DEVSEL# Timing Status (PDTS):</b><br>This field is reserved per PCI-Express spec  |
| 8         | 0h<br>RW/1C/V    | <b>Master Data Parity Error Detected (DPD):</b><br>Set when the root port receives a completion with a data parity error on the backbone and PCMD.PERE is set.   |
| 7         | 1h<br>RO         | <b>Primary Fast Back to Back Capable (PFBC):</b><br>This field is reserved per PCI-Express spec.   |
| 6         | 0h<br>RO         | <b>Reserved</b>  |
| 5         | 0h<br>RO         | <b>Primary 66 MHz Capable (PC66):</b><br>This field is reserved per PCI-Express spec.  |
| 4         | 1h<br>RO         | <b>Capabilities List (CLIST):</b><br>Indicates the presence of a capabilities list.  |
| 3         | 0h<br>RO/V       | <b>Interrupt Status (IS):</b><br>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<br>RO         | <b>Reserved</b>  |

### 3.5.5 Revision ID (RID\_CC) – Offset 8h

Revision ID



| Type | Size   | Offset      | Default   |
|------|--------|-------------|-----------|
| MMIO | 32 bit | DMIBAR + 8h | 060000F0h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| R           | R          | R         |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 31:24     | 06h<br>RO        | <b>Base Class Code (BCC):</b><br>Indicates the device is a bridge device.  |
| 23:16     | 00h<br>RO/V      | <b>Sub-Class Code (SCC):</b><br>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<br>RO/V      | <b>Programming Interface (PI):</b><br>PCI-to-PCI bridge.   |
| 7:0       | F0h<br>RO/V      | <b>Revision ID (RID):</b><br>Indicates the revision of the bridge.<br>The lower nibble, RID[7:0] of this register tracks the Revision ID of the SOC through Set ID Message received from Sideband interface. |

### 3.5.6 Header Type (HTYPE) – Offset Eh

Header Type

| Type | Size  | Offset      | Default |
|------|-------|-------------|---------|
| MMIO | 8 bit | DMIBAR + Eh | 00h     |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| R           | R          | R         |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 7         | 0h<br>RO         | <b>Multi-function Device (MFD):</b><br>This bit is '1' to indicate a multi-function device.  |
| 6:0       | 00h<br>RO/V      | <b>Header Type (HTYPE):</b><br>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. |

### 3.5.7 Secondary Status (SSTS) – Offset 1Eh

Secondary Status

| Type | Size   | Offset       | Default |
|------|--------|--------------|---------|
| MMIO | 16 bit | DMIBAR + 1Eh | 0000h   |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 15        | 0h<br>RW/1C/V    | <b>Detected Parity Error (DPE):</b><br>Set when the port receives a poisoned TLP.  |
| 14        | 0h<br>RW/1C/V    | <b>Received System Error (RSE):</b><br>Set when the port receives an ERR_FATAL or ERR_NONFATAL message from the device.  |
| 13        | 0h<br>RW/1C/V    | <b>Received Master Abort (RMA):</b><br>Set when the port receives a completion with 'Unsupported Request' status from the device.  |
| 12        | 0h<br>RW/1C/V    | <b>Received Target Abort (RTA):</b><br>Set when the port receives a completion with 'Completion Abort' status from the device.   |
| 11        | 0h<br>RW/1C/V    | <b>Signaled Target Abort (STA):</b><br>Set when the port generates a completion with 'Completion Abort' status to the device.  |
| 10:9      | 0h<br>RO/V       | <b>Secondary DEVSEL# Timing Status (SDTS):</b><br>This field is reserved per PCI-Express spec<br>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<br>RW/1C/V    | <b>Data Parity Error Detected (DPD):</b><br>Set when the BCTRL.PERE, and either of the following two conditions occurs:<br>Port receives completion marked poisoned.<br>Port poisons a write request to the secondary side.  |
| 7         | 0h<br>RO/V       | <b>Secondary Fast Back to Back Capable (SFBC):</b><br>This field is reserved per PCI Express spec<br>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<br>RO         | <b>Reserved</b>  |
| 5         | 0h<br>RO         | <b>Secondary 66 MHz Capable (SC66):</b><br>This field is reserved per PCI Express spec   |
| 4:0       | 0h<br>RO         | <b>Reserved</b>  |

### 3.5.8 Subsystem Vendor IDs (SVD) – Offset 2Ch

Subsystem Vendor IDs



| Type | Size   | Offset       | Default   |
|------|--------|--------------|-----------|
| MMIO | 32 bit | DMIBAR + 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<br>RW/L    | <p><b>Subsystem ID (SSID):</b><br/>           Values for the Subsystem ID are vendor specific. Subsystem ID values, in conjunction with the Subsystem Vendor ID, form a unique identifier for the PCI product. Subsystem ID and Device ID values are distinct and unrelated to each other, and software should not assume any relationship between them.<br/>           This register is Read-Only if LPCR.SRL field is set<br/> <b>Locked by:</b> LPCR.SRL</p>  |
| 15:0      | 0000h<br>RW/L    | <p><b>Subsystem Vendor ID (SVID):</b><br/>           The Subsystem Vendor ID register is used to uniquely identify the addin cardadapter or subsystem where the PCI Express component resides. They provide a mechanism for vendors to distinguish their products from one another even though the assemblies may have the same PCI Express component on them (and, therefore, the same Vendor ID and Device ID).<br/>           This register is Read-Only if LPCR.SRL field is set<br/> <b>Locked by:</b> LPCR.SRL</p> |

### 3.5.9 Capabilities List Pointer (CAPP) – Offset 34h

Capabilities List Pointer



| Type | Size  | Offset       | Default |
|------|-------|--------------|---------|
| MMIO | 8 bit | DMIBAR + 34h | E0h     |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 7:0       | E0h<br>RW/O      | <p><b>Capabilities Pointer (PTR):</b><br/>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.</p> <p>Capability Linked List (Default Settings)<br/>Offset   Capability   Next Pointer<br/>40h   PCI Express   80h<br/>80h   Message Signaled Interrupt (MSI)   90h<br/>90h   Subsystem Vendor   A0h<br/>A0h   PCI Power Management   00h<br/>Extended PCIe Capability Linked List<br/>Offset   Capability   Next Pointer<br/>100h   Advanced Error Reporting   000h<br/>140h   Access Control Services   000h<br/>200h   L1 Sub-states   000h<br/>220h   Secondary PCI Express Capability   000h</p> |

### 3.5.10 Bridge Control (BCTRL) – Offset 3Eh

Bridge Control

| Type | Size  | Offset       | Default |
|------|-------|--------------|---------|
| MMIO | 8 bit | DMIBAR + 3Eh | 00h     |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 7:2       | 0h<br>RO         | <b>Reserved</b>  |
| 1         | 0h<br>RW         | <p><b>SERR# Enable (SE):</b><br/>When set, ERR_COR, ERR_NONFATAL, and ERR_FATAL messages received are forwarded to the backbone. When cleared, they are not.</p> |
| 0         | 0h<br>RO         | <b>Reserved</b>  |



### 3.5.11 Device Capabilities (DCAP) – Offset 44h

Device Capabilities

| Type | Size  | Offset       | Default |
|------|-------|--------------|---------|
| MMIO | 8 bit | DMIBAR + 44h | 01h     |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 7:3       | 0h<br>RO         | <b>Reserved</b>  |
| 2:0       | 1h<br>RW/O       | <b>Max Payload Size Supported (MPS):</b><br>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.<br>000b: 128 bytes max payload size.<br>001b: 256 bytes max payload size.<br>010b: 512 bytes max payload size.<br>011b: 1024 bytes max payload size.<br>100b: 2048 bytes max payload size.<br>101b: 4096 bytes max payload size.<br>110b: Reserved.<br>111b: Reserved.<br>This field applies only to the PCIe link interface. |

### 3.5.12 Device Control (DCTL) – Offset 48h

Device Control

| Type | Size   | Offset       | Default |
|------|--------|--------------|---------|
| MMIO | 16 bit | DMIBAR + 48h | 0020h   |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 15        | 0h<br>RO         | <b>Reserved</b>  |
| 14:12     | 0h<br>RO         | <b>Max Read Request Size (MRRS):</b><br>Hardwired to 0.<br>This field applies only to the PCIe link interface. |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 11        | 0h<br>RO         | <b>Enable No Snoop (ENS):</b><br>Not supported. The root port will never issue non-snoop requests.  |
| 10        | 0h<br>RW/P       | <b>Aux Power PM Enable (APME):</b><br>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<br>RO         | <b>Phantom Functions Enable (PFE):</b><br>Not supported   |
| 8         | 0h<br>RO         | <b>Extended Tag Field Enable (ETFE):</b><br>Not supported   |
| 7:5       | 1h<br>RW         | <b>Max Payload Size (MPS):</b><br>The root port supports up to 256B max payload.<br>Programming this field to any values greater than DCAP.MPS will result in aliasing to 128B max payload size.<br>000b: 128 bytes max payload size.<br>001b: 256 bytes max payload size.<br>010b: 512 bytes max payload size.<br>011b: 1024 bytes max payload size.<br>100b: 2048 bytes max payload size.<br>101b: 4096 bytes max payload size.<br>110b: Reserved.<br>111b: Reserved.<br>This field applies only to the PCIe link interface.<br>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<br>RO         | <b>Enable Relaxed Ordering (ERO):</b><br>Not supported  |
| 3         | 0h<br>RW         | <b>Unsupported Request Reporting Enable (URE):</b><br>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<br>RW         | <b>Fatal Error Reporting Enable (FEE):</b><br>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<br>RW         | <b>Non-Fatal Error Reporting Enable (NFE):</b><br>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<br>RW         | <b>Correctable Error Reporting Enable (CEE):</b><br>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.   |

### 3.5.13 Device Status (DSTS) – Offset 4Ah

Device Status



| Type | Size   | Offset       | Default |
|------|--------|--------------|---------|
| MMIO | 16 bit | DMIBAR + 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<br>RO         | <b>Reserved</b>   |
| 5         | 0h<br>RO         | <b>Transactions Pending (TDP):</b><br>This bit has no meaning for the root port since it never initiates a non-posted request with its own Requester ID.  |
| 4         | 1h<br>RO         | <b>AUX Power Detected (APD):</b><br>The root port contains AUX power for wakeup   |
| 3         | 0h<br>RW/1C/V    | <b>Unsupported Request Detected (URD):</b><br>Indicates an unsupported request was detected.  |
| 2         | 0h<br>RW/1C/V    | <b>Fatal Error Detected (FED):</b><br>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<br>RW/1C/V    | <b>Non-Fatal Error Detected (NFED):</b><br>Indicates a non-fatal error was detected. Set when an received a non-fatal error occurred from a poisoned TLP, unexpected completions, unsupported requests, completer abort, or completer timeout         |
| 0         | 0h<br>RW/1C/V    | <b>Correctable Error Detected (CED):</b><br>Indicates a correctable error was detected.<br>Set when received an internal correctable error from receiver errors / framing errors, TLP CRC error, DLLP CRC error, replay num rollover, replay timeout. |

### 3.5.14 Link Capabilities (LCAP) – Offset 4Ch

Link Capabilities

| Type | Size   | Offset       | Default   |
|------|--------|--------------|-----------|
| MMIO | 32 bit | DMIBAR + 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<br>RO/V      | <p><b>Port Number (PN):</b><br/>Indicates the port number for the root port. This value is different for each implemented port:<br/>Port # Value of PN field<br/>1 01h<br/>2 02h<br/>3 03h<br/>:<br/>:<br/>X 0Xh<br/>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.</p>   |
| 23        | 0h<br>RO         | <b>Reserved</b>   |
| 22        | 1h<br>RW/O       | <p><b>ASPM Optionality Compliance (ASPMOC):</b><br/>This bit must be set to 1b for PCIe 3.0 compliant port.<br/>Components implemented against certain earlier versions of this specification will have this bit set to 0b.<br/>Software is permitted to use the value of this bit to help determine whether to enable ASPM or whether to run ASPM compliance tests.</p>  |
| 21        | 1h<br>RO         | <p><b>Link Bandwidth Notification Capability (LBNC):</b><br/>This port supports Link Bandwidth Notification status and interrupt mechanisms.</p>  |
| 20        | 1h<br>RO         | <p><b>Link Active Reporting Capable (LARC):</b><br/>This port supports the optional capability of reporting the DL_Active state of the Data Link Control and Management State Machine.</p>  |
| 19        | 0h<br>RO         | <p><b>Surprise Down Error Reporting Capable (SDERC):</b><br/>Set to '0' to indicate the Root Port does not support Surprise Down Error Reporting</p>  |
| 18        | 0h<br>RO         | <p><b>Clock Power Management (CPM):</b><br/>0' Indicates that root ports do not support the CLKREQ# mechanism.</p>  |
| 17:15     | 2h<br>RW/O       | <p><b>L1 Exit Latency (EL1):</b><br/>Indicates an exit latency of 2us to 4us.<br/>000b: Less than 1 us<br/>001b: 1 us to less than 2 us<br/>010b: 2 us to less than 4 us<br/>011b: 4 us to less than 8 us<br/>100b: 8 us to less than 16 us<br/>101b: 16 us to less than 32 us<br/>110b: 32 us to 64 us<br/>111b: More than 64 us<br/>Note: If power management (e.g PLL shutdown) is enabled, BIOS should program this latency to comprehend PLL lock latency.</p> |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 14:12     | 4h<br>RO/V       | <p><b>LOs Exit Latency (ELO):</b><br/>Indicates an exit latency based upon common-clock configuration:<br/>LCTL.CCC Value<br/>0 MPC.UCEL<br/>1 MPC.CCEL</p>  |
| 11:10     | 3h<br>RW/O       | <p><b>Active State Link PM Support (APMS):</b><br/>Indicates the level of active state power management on this link<br/>Bits Definition<br/>00 No ASPM Support<br/>01 L0s Supported<br/>10 L1 Supported<br/>11 L0s and L1 Supported<br/>Note: If STRPFUSECFG.ASPMDIS is 1, the default of this field is '01'. Otherwise, the default of this field is '11'.<br/>If STRPFUSECFG.ASPMDIS is 1, BIOS writing '11' to this field will have the same effect as writing '01'. '01' will be reflected on this register when read and the register will turn to Read-Only once written once.</p>  |
| 9:4       | 01h<br>RO/V      | <p><b>Maximum Link Width (MLW):</b><br/>Indicates the maximum link width of the link<br/>0x1: x1 Link Width<br/>0x2: x2 Link Width<br/>0x4: x4 Link Width<br/>0x8: x8 Link Width<br/>0x10: x16 Link Width</p>  |
| 3:0       | 0h<br>RO/V       | <p><b>Max Link Speed (MLS):</b><br/>This field indicates the maximum Link speed of the associated Port.<br/>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.<br/>Defined encodings are:<br/>0001b: Supported Link Speeds Vector field bit 0.<br/>0010b: Supported Link Speeds Vector field bit 1.<br/>0011b: Supported Link Speeds Vector field bit 2.<br/>0100b: Supported Link Speeds Vector field bit 3.<br/>0101b: Supported Link Speeds Vector field bit 4.<br/>0110b: Supported Link Speeds Vector field bit 5.<br/>0111b: Supported Link Speeds Vector field bit 6.<br/>All other encodings are reserved.<br/>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.<br/>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.<br/>Otherwise, this field reports a value of 0011b.</p> |

### 3.5.15 Link Control (LCTL) – Offset 50h

#### Link Control

| Type | Size   | Offset       | Default |
|------|--------|--------------|---------|
| MMIO | 16 bit | DMIBAR + 50h | 0040h   |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 15:12     | 0h<br>RO         | <b>Reserved</b>  |
| 11        | 0h<br>RW         | <b>Link Autonomous Bandwidth Interrupt Enable (LABIE):</b><br>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<br>RW         | <b>Link Bandwidth Management Interrupt Enable (LBMIE):</b><br>When Set, this bit enables the generation of an interrupt to indicate that the Link Bandwidth Management Status bit has been Set.<br>This bit is not applicable and is reserved for Endpoints, PCI Express-to-PCI/PCI-X bridges, and Upstream Ports of Switches.<br>Functions that do not implement the Link Bandwidth Notification Capability must hardwire this bit to 0b.<br>Default value of this bit is 0b.   |
| 9         | 0h<br>RW         | <b>Hardware Autonomous Width Disable (HAWD):</b><br>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.<br>Note: When operating as PCI Express, this bit defines the value of the Link Upconfigure Capability in TS2 Ordered Sets.<br>Default value of this bit is 0b.  |
| 8         | 0h<br>RO         | <b>Enable Clock Power Management (ECPM):</b><br>Reserved   |
| 7         | 0h<br>RW         | <b>Extended Sync (ES):</b><br>When set, forces extended transmission of FTS ordered sets in FTS and extra TS2 at exit from L1 prior to entering L0.  |
| 6         | 1h<br>RO         | <b>Common Clock Configuration (CCC):</b><br>Reserved   |
| 5         | 0h<br>WO         | <b>Retrain Link (RL):</b><br>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.<br>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<br>RW/L       | <b>Link Disable (LD):</b><br>When set, the root port will disable the link by directing the LTSSM to the Disabled state.<br>This register is read only when MPC.SRL field is set<br>This register is Read-Only if LPCR.SRL field is set<br><b>Locked by:</b> LPCR.SRL  |
| 3         | 0h<br>RW/O       | <b>Read Completion Boundary Control (RCBC):</b><br>Indicates the read completion boundary is 64 bytes.   |
| 2         | 0h<br>RO         | <b>Reserved</b>  |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 1:0       | 0h<br>RW         | <p><b>Active State Link PM Control (ASPM):</b><br/>Indicates whether the root port should enter L0s or L1 or both.</p> <p>Bits Definition</p> <p>00 Disabled<br/>01 L0s Entry Enabled<br/>10 L1 Entry Enabled<br/>11 L0s and L1 Entry Enabled</p> <p>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.</p> <p>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.</p> |

### 3.5.16 Link Status (LSTS) – Offset 52h

Link Status

| Type | Size   | Offset       | Default |
|------|--------|--------------|---------|
| MMIO | 16 bit | DMIBAR + 52h | 1011h   |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 15        | 0h<br>RW/1C/V    | <p><b>Link Autonomous Bandwidth Status (LABS):</b><br/>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.<br/>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.<br/>The default value of this bit is 0b.</p>   |
| 14        | 0h<br>RW/1C/V    | <p><b>Link Bandwidth Management Status (LBMS):</b><br/>This bit is Set by hardware to indicate that either of the following has occurred without the Port transitioning through DL_Down status:<br/>A Link retraining has completed following a write of 1b to the Retrain Link bit<br/>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.<br/>Hardware has changed Link speed or width to attempt to correct unreliable Link operation, either through an LTSSM timeout or a higher level process<br/>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.<br/>The default value of this bit is 0b.</p> |
| 13        | 0h<br>RO/V       | <p><b>Link Active (LA):</b><br/>Set to 1b when the Data Link Control and Management State Machine is in the DL_Active state, 0b otherwise.</p>  |



| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 12        | 1h<br>RO/V       | <b>Slot Clock Configuration (SCC):</b><br>In normal mode, Root Port uses the same reference clock as on the platform and does not generate its own clock.<br>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<br>RO/V       | <b>Link Training (LT):</b><br>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<br>RO         | <b>Reserved</b>  |
| 9:4       | 01h<br>RO/V      | <b>Negotiated Link Width (NLW):</b><br>Negotiated link width.<br>0x1: x1 Link Width<br>0x2: x2 Link Width<br>0x4: x4 Link Width<br>0x8: x8 Link Width<br>0x10: x16 Link Width<br>The value of this register is undefined if the link has not successfully trained.   |
| 3:0       | 1h<br>RO/V       | <b>Current Link Speed (CLS):</b><br>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.<br>Defined encodings are:<br>0001b: Supported Link Speeds Vector field bit 0.<br>0010b: Supported Link Speeds Vector field bit 1.<br>0011b: Supported Link Speeds Vector field bit 2.<br>0100b: Supported Link Speeds Vector field bit 3.<br>0101b: Supported Link Speeds Vector field bit 4.<br>0110b: Supported Link Speeds Vector field bit 5.<br>0111b: Supported Link Speeds Vector field bit 6.<br>All other encodings are reserved.<br>The value of this field is undefined if the link is not up. |

### 3.5.17 Root Control (RCTL) – Offset 5Ch

Root Control

| Type | Size   | Offset       | Default |
|------|--------|--------------|---------|
| MMIO | 16 bit | DMIBAR + 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<br>RO         | <b>Reserved</b>              |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 3         | 0h<br>RW         | <b>PME Interrupt Enable (PIE):</b><br>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<br>RW         | <b>System Error on Fatal Error Enable (SFE):</b><br>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 dependant on CMD.SEE being set.                   |
| 1         | 0h<br>RW         | <b>System Error on Non-Fatal Error Enable (SNE):</b><br>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 dependant on CMD.SEE being set.       |
| 0         | 0h<br>RW         | <b>System Error on Correctable Error Enable (SCE):</b><br>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 dependant on CMD.SEE being set. |

### 3.5.18 Root Status (RSTS) – Offset 60h

Root Status

| 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   |
|-----------|------------------|--|
| 31:18     | 0h<br>RO         | <b>Reserved</b>  |
| 17        | 0h<br>RO/V       | <b>PME Pending (PP):</b><br>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 requester ID will be updated, and this bit will be cleared. Root Ports have a one deep PME pending queue.                               |
| 16        | 0h<br>RW/1C/V    | <b>PME Status (PS):</b><br>Indicates that PME was asserted by the requester ID in RID. Subsequent PMEs are kept pending until this bit is cleared.   |
| 15:0      | 0000h<br>RO/V    | <b>PME Requester ID (RID):</b><br>Indicates the PCI requester ID of the last PME requester. 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. |

### 3.5.19 Device Capabilities 2 (DCAP2) – Offset 64h

Device Capabilities 2

| Type | Size   | Offset       | Default   |
|------|--------|--------------|-----------|
| MMIO | 32 bit | DMIBAR + 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<br>RO         | <b>Reserved</b>   |
| 19:18     | 2h<br>RW/O       | <p><b>Optimized Buffer Flush/Fill Supported (OBFFS):</b><br/>           00b: OBFF is not supported.<br/>           01b: OBFF is supported using Message signaling only.<br/>           10b: OBFF is supported using WAKE# signaling only.<br/>           11b: OBFF is supported using WAKE# and Message signaling.<br/>           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.<br/>           Note: OBFF is not supported. BIOS should program this field to 00b.</p> |
| 17:12     | 0h<br>RO         | <b>Reserved</b>   |
| 11        | 1h<br>RW/O       | <p><b>LTR Mechanism Supported (LTRMS):</b><br/>           A value of 1b indicates support for the optional Latency Tolerance Reporting (LTR) mechanism capability.<br/>           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.</p>  |
| 10        | 0h<br>RO         | <b>Reserved</b>   |
| 9         | 0h<br>RW/O       | <p><b>CAS Completer 128-bit Supported (AC128BS):</b><br/>           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.</p>  |
| 8         | 0h<br>RW/O       | <p><b>AtomicOp Completer 64-bit Supported (AC64BS):</b><br/>           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</p>  |
| 7         | 0h<br>RW/O       | <p><b>AtomicOp Completer 32-bit Supported (AC32BS):</b><br/>           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</p>  |
| 6         | 0h<br>RW/O       | <p><b>Atomic Routing Supported (ARS):</b><br/>           This bit must be set to 1b if the Port supports this optional capability</p>   |
| 5         | 1h<br>RO         | <p><b>ARI Forwarding Supported (AFS):</b><br/>           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.<br/>           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.</p>   |
| 4         | 1h<br>RO         | <p><b>Completion Timeout Disable Supported (CTDS):</b><br/>           A value of 1b indicates support for the Completion Timeout Disable mechanism.</p>   |



| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 3:0       | 7h<br>RO         | <p><b>Completion Timeout Ranges Supported (CTRS):</b><br/>           This field indicates device support for the optional Completion Timeout programmability mechanism. This mechanism allows system software to modify the Completion Timeout value.</p> <p>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.</p> <p>For all other devices this field is reserved and must be hardwired to 0000b.</p> <p>Four time value ranges are defined:<br/>           Range A: 50us to 10ms<br/>           Range B: 10ms to 250ms<br/>           Range C: 250ms to 4s<br/>           Range D: 4s to 64s</p> <p>Bits are set according to the table below to show timeout value ranges supported.<br/>           0000b Completion Timeout programming not supported.<br/>           0001b Range A<br/>           0010b Range B<br/>           0011b Ranges A &amp; B<br/>           0110b Ranges B &amp; C<br/>           0111b Ranges A, B &amp; C &lt;-- This is what Root Port supports<br/>           1110b Ranges B, C &amp; D<br/>           1111b Ranges A, B, C &amp; D<br/>           All other values are reserved.</p> |

### 3.5.20 Device Control 2 (DCTL2) – Offset 68h

Device Control 2

| Type | Size   | Offset       | Default |
|------|--------|--------------|---------|
| MMIO | 16 bit | DMIBAR + 68h | 0000h   |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 15        | 0h<br>RO         | <b>Reserved</b>  |
| 14:13     | 0h<br>RW         | <p><b>Optimized Buffer Flush/Fill Enable (OBFFEN):</b><br/>           Optimized Buffer Flush/Fill Enable (OBFFEN):<br/>           00b Disable OBFF mechanism.<br/>           01b Enable OBFF mechanism using Message signaling (Variation A).<br/>           10b Enable OBFF mechanism using Message signaling (Variation B).<br/>           11b Enable OBFF using WAKE# signaling.</p> <p>Note: Only encoding 00b and 11b are supported. The encoding of 01b or 10b would be aliased to 00b.<br/>           If DCAP2.OBFFS is clear, programming this field to any non-zero values will have no effect.</p> |
| 12:11     | 0h<br>RO         | <b>Reserved</b>  |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 10        | 0h<br>RW         | <p><b>LTR Mechanism Enable (LTREN):</b><br/>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.<br/>If DCAP2.LTRMS is clear, programming this field to any non-zero values will have no effect.</p>  |
| 9:8       | 0h<br>RO         | <b>Reserved</b>  |
| 7         | 0h<br>RW         | <p><b>AtomicOp Egress Blocking (AEB):</b><br/>Applicable and mandatory for Switch Upstream Ports, Switch Downstream Ports, and Root Ports that implement AtomicOp routing capability - otherwise must be hardwired to 0b.<br/>When this bit is Set, AtomicOp Requests that target going out this Egress Port must be blocked.</p>  |
| 6         | 0h<br>RW         | <p><b>AtomicOp Requester Enable (ARE):</b><br/>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.<br/>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.<br/>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.</p>  |
| 5         | 0h<br>RW         | <p><b>ARI Forwarding Enable (AFE):</b><br/>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.</p>   |
| 4         | 0h<br>RW         | <p><b>Completion Timeout Disable (CTD):</b><br/>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.<br/>Software is permitted to set or clear this bit at any time. When set, the Completion Timeout detection mechanism is disabled.<br/>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.</p> |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 3:0       | 0h<br>RW         | <p><b>Completion Timeout Value (CTV):</b></p> <p>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.</p> <p>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.</p> <p>The Root Port targeted configurable ranges are listed below, along with the range allowed by the PCI Express 2.0 specification.</p> <p>Defined encodings:</p> <p>0000b Default range: 40-50ms (spec range 50us to 50ms)<br/>           Values available if Range A (50us to 10 ms) programmability range is supported:<br/>           0001b 90-100us (spec range is 50us to 100us)<br/>           0010b 9-10ms (spec range is 1ms to 10 ms)<br/>           Values available if Range B (10ms to 250ms) programmability range is supported:<br/>           0101b 40-50ms (spec range is 16ms to 55ms)<br/>           0110b 160-170ms (spec range is 65ms to 210ms)<br/>           Values available if Range C (250ms to 4s) programmability range is supported:<br/>           1001b 400-500ms (spec range is 260ms to 900ms)<br/>           1010b 1.6-1.7s (spec range is 1s to 3.5s)<br/>           Values not defined above are Reserved.</p> <p>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.</p> |

### 3.5.21 Device Status 2 (DSTS2) – Offset 6Ah

Device Status 2

| Type | Size   | Offset       | Default |
|------|--------|--------------|---------|
| MMIO | 16 bit | DMIBAR + 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<br>RO         | <b>Reserved</b>              |

### 3.5.22 Link Capabilities 2 (LCAP2) – Offset 6Ch

Link Capabilities 2

| Type | Size   | Offset       | Default  |
|------|--------|--------------|----------|
| MMIO | 32 bit | DMIBAR + 6Ch | 000000Eh |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 31:25     | 0h<br>RO         | <b>Reserved</b>   |
| 24        | 0h<br>RW/O       | <p><b>Two Retimers Presence Detect Supported (TRPDS):</b><br/>When set to 1b, this bit indicates that the associated Port supports detection and reporting of two Retimers presence.<br/>This bit must be set to 1b in a Downstream Port when the Supported Link Speeds Vector of the Link Capabilities 2 register indicates support for a Link speed of 16.0 GT/s or higher. It is permitted to be set to 1b regardless of the supported Link speeds, and in Upstream Ports, if the Retimer Presence Detect Supported bit is also set to 1b.</p>   |
| 23        | 0h<br>RW/O       | <p><b>Retimer Presence Detect Supported (RPDS):</b><br/>When set to 1b, this bit indicates that the associated Port supports detection and reporting of Retimer presence.<br/>This bit must be set to 1b in a Downstream Port when the Supported Link Speeds Vector of the Link Capabilities 2 register indicates support for a Link speed of 16.0 GT/s or higher. It is permitted to be set to 1b regardless of the supported Link speeds and in Upstream Ports.</p>   |
| 22:16     | 00h<br>RW/O      | <p><b>Lower SKP OS Reception Supported Speeds Vector (LSOSRSS):</b><br/>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.<br/>Bit definitions within this field are:<br/>Bit 0 2.5 GT/s<br/>Bit 1 5.0 GT/s<br/>Bit 2 8.0 GT/s<br/>Bit 3 16.0 GT/s<br/>Bits 6:4 RsvdP<br/>Behavior is undefined if a bit is set in this field and the corresponding bit is not set in the Supported Link Speeds Vector.<br/>This register is Read-Only if LPCR.SRL field is set<br/><b>Locked by:</b> LPCR.SRL</p>  |
| 15:9      | 00h<br>RW/O      | <p><b>Lower SKP OS Generation Supported Speeds Vector (LSOGSSV):</b><br/>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.<br/>Bit definitions within this field are:<br/>Bit 0 2.5 GT/s<br/>Bit 1 5.0 GT/s<br/>Bit 2 8.0 GT/s<br/>Bit 3 16.0GT/s<br/>Bits 6:4 RsvdP<br/>Behavior is undefined if a bit is set in this field and the corresponding bit is not set in the Supported Link Speeds Vector.<br/>This register is Read-Only if LPCR.SRL field is set<br/><b>Locked by:</b> LPCR.SRL</p> |
| 8         | 0h<br>RO         | <p><b>Crosslink Supported (CS):</b><br/>No support for Crosslink.</p>   |



| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 7:1       | 07h<br>RO/V      | <b>Supported Link Speeds Vector (SLSV):</b><br>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.<br>Bit definitions within this field for PCI Express are:<br>Bit 0: 2.5 GT/s.<br>Bit 1: 5.0 GT/s.<br>Bit 2: 8.0 GT/s.<br>Bit 3: 16.0 GT/s<br>Bits 6:3: Reserved. |
| 0         | 0h<br>RO         | <b>Reserved</b>  |

### 3.5.23 Link Control 2 (LCTL2) – Offset 70h

Link Control 2

| Type | Size   | Offset       | Default |
|------|--------|--------------|---------|
| MMIO | 16 bit | DMIBAR + 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<br>RW/P       | <b>Compliance Preset/De-emphasis (CD):</b><br>For 8.0 GT/s and higher 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.<br>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.<br>Encodings:<br>0001b -3.5 dB<br>0000b -6 dB<br>When the Link is operating at 2.5 GT/s, the setting of this field has no effect.<br>The default value of this field is 0000b.<br>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<br>RW/P       | <b>Compliance SOS (CSOS):</b><br>When set to 1b, the LTSSM is required to send SKP Ordered Sets periodically in between the (modified) compliance patterns.<br>The default value of this bit is 0b.<br>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<br>RW/P       | <p><b>Enter Modified Compliance (EMC):</b><br/>When this bit is set to 1b, the device transmits Modified Compliance Pattern if the LTSSM enters Polling.Compliance substate.<br/>Default value of this bit is 0b.<br/>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.</p>  |
| 9:7       | 0h<br>RW/P       | <p><b>Transmit Margin (TM):</b><br/>This field controls the value of the non-deemphasized 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).<br/>Encodings:<br/>000b Normal operating range<br/>001b 800-1200 mV for full swing and 400-700 mV for half-swing<br/>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<br/>n - 111b reserved<br/>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.<br/>Default value of this field is 000b.<br/>Components that support only the 2.5 GT/s speed are permitted to hardwire this bit to 000b.<br/>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.</p> |
| 6         | 0h<br>RW/P       | <p><b>Selectable De-emphasis (SD):</b><br/>When the Link is operating at 5.0 GT/s speed, this bit selects the level of de-emphasis for an Upstream component.<br/>Encodings:<br/>1b -3.5 dB<br/>0b -6 dB<br/>When the Link is not operating at 5.0 GT/s speed, the setting of this bit has no effect.</p>   |
| 5         | 0h<br>RO         | <b>Reserved</b>   |
| 4         | 0h<br>RW/P       | <p><b>Enter Compliance (EC):</b><br/>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.<br/>Default value of this bit following Fundamental Reset is 0b.<br/>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.</p>  |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 3:0       | 1h<br>RW/V/P     | <p><b>Target Link Speed (TLS):</b><br/>           This field sets an upper limit on Link operational speed by restricting the values advertised by the upstream component in its training sequences.<br/>           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.<br/>           Defined encodings are:<br/>           0001b: Supported Link Speeds Vector field bit 0.<br/>           0010b: Supported Link Speeds Vector field bit 1.<br/>           0011b: Supported Link Speeds Vector field bit 2.<br/>           0100b: Supported Link Speeds Vector field bit 3.<br/>           0101b: Supported Link Speeds Vector field bit 4.<br/>           0110b: Supported Link Speeds Vector field bit 5.<br/>           0111b: Supported Link Speeds Vector field bit 6.<br/>           All other encodings are reserved.<br/>           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.<br/>           The default value of this field is GEN1.<br/>           Note: This register field could be used by a driver to limit the link speed to 2.5 GT/s or 5 GT/s data rate.</p> |

### 3.5.24 Link Status 2 (LSTS2) – Offset 72h

Link Status 2

| Type | Size   | Offset       | Default |
|------|--------|--------------|---------|
| MMIO | 16 bit | DMIBAR + 72h | 0000h   |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 15:8      | 0h<br>RO         | <b>Reserved</b>  |
| 7         | 0h<br>RO/V/P     | <p><b>Two Retimers Presence Detected (PX2RPD):</b><br/>           When set to 1b, this bit indicates that two Retimers were present during the most recent Link negotiation.<br/>           The default value of this bit is 0b.<br/>           This bit is required for Ports that have the Two Retimers Presence Detect Supported bit of the Link Capabilities 2 register set to 1b.<br/>           Ports that have the Two Retimers Presence Detect Supported bit set to 0b are permitted to hardwire this bit to 0b.</p> |
| 6         | 0h<br>RO/V/P     | <p><b>Retimer Presence Detected (RPD):</b><br/>           When set to 1b, this bit indicates that a Retimer was present during the most recent Link negotiation.<br/>           The default value of this bit is 0b.<br/>           This bit is required for Ports that have the Retimer Presence Detect Supported bit Set.<br/>           Ports that have the Retimer Presence Detect Supported bit of the Link Capabilities 2 register set to 0b are permitted to hardwire this bit to 0b.</p>                             |

| Bit Range | Default & Access    | Field Name (ID): Description   |
|-----------|---------------------|--|
| 5         | 0h<br>RW/1C/V/<br>P | <b>Link Equalization Request (LER):</b><br>This bit is set by hardware to request the 8.0 GT/s Link equalization process to be performed on the Link.  |
| 4         | 0h<br>RO/V/P        | <b>Equalization Phase 3 Successful (EQP3S):</b><br>When set to 1, this bit indicates that Phase 3 of the 8.0 GT/s Transmitter Equalization procedure has successfully completed.   |
| 3         | 0h<br>RO/V/P        | <b>Equalization Phase 2 Successful (EQP2S):</b><br>When set to 1, this bit indicates that Phase 2 of the 8.0 GT/s Transmitter Equalization procedure has successfully completed.   |
| 2         | 0h<br>RO/V/P        | <b>Equalization Phase 1 Successful (EQP1S):</b><br>When set to 1, this bit indicates that Phase 1 of the 8.0 GT/s Transmitter Equalization procedure has successfully completed.   |
| 1         | 0h<br>RO/V/P        | <b>Equalization Complete (EQC):</b><br>When set to 1, this bit indicates that the Transmitter Equalization procedure at the 8.0GT/s data rate has completed.   |
| 0         | 0h<br>RO/V          | <b>Current De-emphasis Level (CDL):</b><br>When the Link is operating at 5.0 GT/s speed, this bit reflects the level of de-emphasis.<br>Encodings:<br>1b -3.5 dB<br>0b -6 dB<br>The value in this bit is undefined when the Link is not operating at 5.0 GT/s speed. |

### 3.5.25 Slot Capabilities 2 (SLCAP2) – Offset 74h

Slot Capabilities 2

**Note:** Bit definitions are the same as [DSTS2, offset 6Ah](#).

### 3.5.26 Slot Control 2 (SLCTL2) – Offset 78h

Slot Control 2

**Note:** Bit definitions are the same as [DSTS2, offset 6Ah](#).

### 3.5.27 Slot Status 2 (SLSTS2) – Offset 7Ah

Slot Status 2

**Note:** Bit definitions are the same as [DSTS2, offset 6Ah](#).

### 3.5.28 Message Signaled Interrupt Identifiers (MID) – Offset 80h

Message Signaled Interrupt Identifiers

| Type | Size   | Offset       | Default |
|------|--------|--------------|---------|
| MMIO | 16 bit | DMIBAR + 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<br>RW/O      | <b>Next Pointer (NEXT):</b><br>Indicates the location of the next capability in the list.<br>The default value of this register is 90h which points to the Subsystem Vendor capability structure.<br>BIOS can determine which capabilities will be exposed by including or removing them from the capability linked list.<br>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       | 05h<br>RO        | <b>Capability ID (CID):</b><br>Capabilities ID indicates MSI.  |

### 3.5.29 Message Signaled Interrupt Message (MC) – Offset 82h

Message Signaled Interrupt Message

| Type | Size   | Offset       | Default |
|------|--------|--------------|---------|
| MMIO | 16 bit | DMIBAR + 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<br>RO         | <b>Reserved</b>   |
| 7         | 0h<br>RO         | <b>64 Bit Address Capable (C64):</b><br>Capable of generating a 32-bit message only.  |
| 6:4       | 0h<br>RW         | <b>Multiple Message Enable (MME):</b><br>These bits are RW for software compatibility, but only one message is ever sent by the root port.  |
| 3:1       | 0h<br>RO         | <b>Multiple Message Capable (MMC):</b><br>Only one message is required.   |
| 0         | 0h<br>RW         | <b>MSI Enable (MSIE):</b><br>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. |

### 3.5.30 Message Signaled Interrupt Message Address (MA) – Offset 84h

Message Signaled Interrupt Message Address

| Type | Size   | Offset       | Default   |
|------|--------|--------------|-----------|
| MMIO | 32 bit | DMIBAR + 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<br>RW  | <b>ADDR:</b><br>Lower 32 bits of the system specified message address, always DW aligned. |
| 1:0       | 0h<br>RO         | <b>Reserved</b>   |

### 3.5.31 Message Signaled Interrupt Message Data (MD) – Offset 88h

Message Signaled Interrupt Message Data

| 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  |
|-----------|------------------|---|
| 15:0      | 0000h<br>RW      | <b>DATA:</b><br>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. |

### 3.5.32 Subsystem Vendor Capability (SVCAP) – Offset 90h

Subsystem Vendor Capability

| Type | Size   | Offset       | Default |
|------|--------|--------------|---------|
| MMIO | 16 bit | DMIBAR + 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<br>RW/O      | <b>Next Capability (NEXT):</b><br>Indicates the location of the next capability in the list.<br>The default value of this register is A0h which points to the PCI Power Management capability structure.<br>BIOS can determine which capabilities will be exposed by including or removing them from the capability linked list.<br>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<br>RO        | <b>Capability Identifier (CID):</b><br>Value of 0Dh indicates this is a PCI bridge subsystem vendor capability.   |

### 3.5.33 Subsystem Vendor IDs (SVID) – Offset 94h

Subsystem Vendor IDs

| Type | Size   | Offset       | Default   |
|------|--------|--------------|-----------|
| MMIO | 32 bit | DMIBAR + 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<br>RW/O    | <b>Subsystem Identifier (SID):</b><br>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<br>RW/O    | <b>Subsystem Vendor Identifier (SVID):</b><br>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). |

### 3.5.34 Power Management Capability (PMCAP) – Offset A0h

Power Management Capability

| Type | Size   | Offset       | Default |
|------|--------|--------------|---------|
| MMIO | 16 bit | DMIBAR + 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<br>RO        | <b>Next Capability (NEXT):</b><br>Indicates this is the last item in the list.                           |
| 7:0       | 01h<br>RO        | <b>Capability Identifier (CID):</b><br>Value of 01h indicates this is a PCI power management capability. |

### 3.5.35 PCI Power Management Capabilities (PMC) – Offset A2h

PCI Power Management Capabilities

| Type | Size   | Offset       | Default |
|------|--------|--------------|---------|
| MMIO | 16 bit | DMIBAR + 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<br>RO        | <b>PMES:</b><br>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<br>RO         | <b>D2S:</b><br>The D2 state is not supported.  |
| 9         | 0h<br>RO         | <b>D1S:</b><br>The D1 state is not supported.  |
| 8:6       | 0h<br>RO         | <b>AC:</b><br>Reports 375mA maximum suspend well current required when in the D3COLD state.  |
| 5         | 0h<br>RO         | <b>Device Specific Initialization (DSI):</b><br>Indicates that no device-specific initialization is required.  |
| 4         | 0h<br>RO         | <b>Reserved</b>  |
| 3         | 0h<br>RO         | <b>PME Clock (PMEC):</b><br>Indicates that PCI clock is not required to generate PME#.   |
| 2:0       | 3h<br>RO         | <b>VS:</b><br>Indicates support for Revision 1.2 of the PCI Power Management Specification.  |



### 3.5.36 PCI Power Management Control (PMCS) – Offset A4h

PCI Power Management Control

| Type | Size   | Offset       | Default   |
|------|--------|--------------|-----------|
| MMIO | 32 bit | DMIBAR + 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<br>RO        | <b>DTA:</b><br>Reserved   |
| 23        | 0h<br>RO         | <b>Bus Power / Clock Control Enable (BPCE):</b><br>This field is reserved per PCI Express specification   |
| 22        | 0h<br>RO         | <b>B2/B3 Support (B23S):</b><br>This field is reserved per PCI Express specification.   |
| 21:16     | 0h<br>RO         | <b>Reserved</b>   |
| 15        | 0h<br>RO         | <b>PME Status (PMES):</b><br>Indicates a PME was received on the downstream link.   |
| 14:13     | 0h<br>RO         | <b>Data Scale (DSC):</b><br>Reserved  |
| 12:9      | 0h<br>RO         | <b>Data Select (DSEL):</b><br>Reserved  |
| 8         | 0h<br>RW/P       | <b>PME Enable (PMEE):</b><br>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<br>RO         | <b>Reserved</b>   |
| 3         | 1h<br>RW/O       | <b>No Soft Reset (NSR):</b><br>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.<br>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.<br>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<br>Uninitialized with only PME context preserved if PME is supported and enabled. |
| 2         | 0h<br>RO         | <b>Reserved</b>   |



| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 1:0       | 0h<br>RO         | <p><b>Power State (PS):</b><br/>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:<br/>00: D0 state<br/>11: D3HOT state</p> <p>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.</p> <p>If software attempts to write a '10' or '01' to these bits, the write will be ignored.</p> |

### 3.5.37 Advanced Error Extended (AECH) – Offset 100h

Advanced Error Extended

| Type | Size   | Offset        | Default   |
|------|--------|---------------|-----------|
| MMIO | 32 bit | DMIBAR + 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<br>RW/O     | <p><b>Next Capability Offset (NCO):</b><br/>Points to the next capability.</p>  |
| 19:16     | 0h<br>RW/O       | <p><b>Capability Version (CV):</b><br/>For systems that support AER, BIOS should write a 1h to this register else it should write 0</p> |
| 15:0      | 0000h<br>RW/O    | <p><b>Capability ID (CID):</b><br/>For systems that support AER, BIOS should write a 0001h to this register else it should write 0</p>  |

### 3.5.38 Uncorrectable Error Status (UES) – Offset 104h

Uncorrectable Error Status



| Type | Size   | Offset        | Default   |
|------|--------|---------------|-----------|
| MMIO | 32 bit | DMIBAR + 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<br>RO            | <b>Reserved</b>  |
| 26        | 0h<br>RW/1C/V/<br>P | <b>Poisoned TLP Egress Blocked Status (PTLPEBS):</b><br>Indicates that poisoned TLP Egress Blocked error has occurred.<br>Note: This bit can only be set if DPCCAPR.PTLPEBS = '1' and DPCCTLR.PTLPEBE = '1'.                       |
| 25        | 0h<br>RO            | <b>Reserved</b>  |
| 24        | 0h<br>RW/1C/V/<br>P | <b>AtomicOp Egress Blocked Status (AEBS):</b><br>AtomicOp Egress Blocked Status  |
| 23:22     | 0h<br>RO            | <b>Reserved</b>  |
| 21        | 0h<br>RW/1C/V/<br>P | <b>ACS Violation Status (AVS):</b><br>Indicates an ACS Violation is logged.  |
| 20        | 0h<br>RW/1C/V/<br>P | <b>Unsupported Request Error Status (URE):</b><br>Indicates an unsupported request was received.   |
| 19        | 0h<br>RO            | <b>ECRC Error Status (EE):</b><br>ECRC is not supported.   |
| 18        | 0h<br>RW/1C/V/<br>P | <b>Malformed TLP Status (MT):</b><br>Indicates a malformed TLP was received.   |
| 17        | 0h<br>RW/1C/V/<br>P | <b>Receiver Overflow Status (RO):</b><br>Indicates a receiver overflow occurred.   |
| 16        | 0h<br>RW/1C/V/<br>P | <b>Unexpected Completion Status (UC):</b><br>Indicates an unexpected completion was received.  |
| 15        | 0h<br>RW/1C/V/<br>P | <b>Completer Abort Status (CA):</b><br>Indicates a completer abort was received  |
| 14        | 0h<br>RW/1C/V/<br>P | <b>Completion Timeout Status (CT):</b><br>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<br>RO            | <b>Flow Control Protocol Error Status (FCPE):</b><br>Not supported.  |
| 12        | 0h<br>RW/1C/V/<br>P | <b>Poisoned TLP Status (PT):</b><br>Indicates a poisoned TLP was received.   |

| Bit Range | Default & Access    | Field Name (ID): Description   |
|-----------|---------------------|--|
| 11:6      | 0h<br>RO            | <b>Reserved</b>  |
| 5         | 0h<br>RO            | <b>Surprise Down Error Status (SDE):</b><br>Surprise Down is not supported.                      |
| 4         | 0h<br>RW/1C/V/<br>P | <b>Data Link Protocol Error Status (DLPE):</b><br>Indicates a data link protocol error occurred. |
| 3:1       | 0h<br>RO            | <b>Reserved</b>  |
| 0         | 0h<br>RO            | <b>Training Error Status (TE):</b><br>Not supported.   |

### 3.5.39 Uncorrectable Error Mask (UEM) – Offset 108h

Uncorrectable Error Mask

| Type | Size   | Offset        | Default  |
|------|--------|---------------|----------|
| MMIO | 32 bit | DMIBAR + 108h | 0000000h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 31:27     | 0h<br>RO         | <b>Reserved</b>   |
| 26        | 0h<br>RW/P       | <b>Poisoned TLP Egress Blocked Mask (PTLPEBM):</b><br>Mask for Poisoned TLP Egress Blocked error. |
| 25        | 0h<br>RO         | <b>Reserved</b>   |
| 24        | 0h<br>RW/P       | <b>AtomicOp Egress Blocked Mask (AEBM):</b><br>Mask for AtomicOp Egress Blocked                   |
| 23:22     | 0h<br>RO         | <b>Reserved</b>   |
| 21        | 0h<br>RW/P       | <b>ACS Violation Mask (AVM):</b><br>Mask for ACS Violation errors.                                |
| 20        | 0h<br>RW/P       | <b>Unsupported Request Error Mask (URE):</b><br>Mask for uncorrectable errors.                    |
| 19        | 0h<br>RO         | <b>ECRC Error Mask (EE):</b><br>ECRC is not supported.  |
| 18        | 0h<br>RW/P       | <b>Malformed TLP Mask (MT):</b><br>Mask for malformed TLPs  |
| 17        | 0h<br>RW/P       | <b>Receiver Overflow Mask (RO):</b><br>Mask for receiver overflows.                               |



| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 16        | 0h<br>RW/P       | <b>Unexpected Completion Mask (UC):</b><br>Mask for unexpected completions.         |
| 15        | 0h<br>RW/P       | <b>Completer Abort Mask (CM):</b><br>Mask for completer abort.                      |
| 14        | 0h<br>RW/P       | <b>Completion Timeout Mask (CT):</b><br>Mask for completion timeouts.               |
| 13        | 0h<br>RO         | <b>Flow Control Protocol Error Mask (FCPE):</b><br>Not supported.                   |
| 12        | 0h<br>RW/P       | <b>Poisoned TLP Mask (PT):</b><br>Mask for poisoned TLPs.                           |
| 11:6      | 0h<br>RO         | <b>Reserved</b>   |
| 5         | 0h<br>RO         | <b>Surprise Down Error Mask (SDE):</b><br>Surprise Down is not supported.           |
| 4         | 0h<br>RW/P       | <b>Data Link Protocol Error Mask (DLPE):</b><br>Mask for data link protocol errors. |
| 3:1       | 0h<br>RO         | <b>Reserved</b>   |
| 0         | 0h<br>RO         | <b>Training Error Mask (TE):</b><br>Not supported.                                  |

### 3.5.40 Uncorrectable Error Severity (UEV) – Offset 10Ch

Uncorrectable Error Severity

| Type | Size   | Offset        | Default   |
|------|--------|---------------|-----------|
| MMIO | 32 bit | DMIBAR + 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<br>RO         | <b>Reserved</b>   |
| 26        | 0h<br>RW/P       | <b>Poisoned TLP Egress Blocked Severity (PTLPEBS):</b><br>Severity for Poisoned TLP Egress Blocked error. |
| 25        | 0h<br>RO         | <b>Reserved</b>   |
| 24        | 0h<br>RW/P       | <b>AtomicOp Egress Blocked Severity (AEBS):</b><br>AtomicOp Egress Blocked Severity                       |
| 23:22     | 0h<br>RO         | <b>Reserved</b>   |
| 21        | 0h<br>RW/P       | <b>ACS Violation Severity (AVS):</b><br>Severity for ACS Violation.                                       |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 20        | 0h<br>RW/P       | <b>Unsupported Request Error Severity (URE):</b><br>Severity for unsupported request reception. |
| 19        | 0h<br>RO         | <b>ECRC Error Severity (EE):</b><br>ECRC is not supported.                                      |
| 18        | 1h<br>RW/P       | <b>Malformed TLP Severity (MT):</b><br>Severity for malformed TLP reception.                    |
| 17        | 1h<br>RW/P       | <b>Receiver Overflow Severity (RO):</b><br>Severity for receiver overflow occurrences.          |
| 16        | 0h<br>RW/P       | <b>Unexpected Completion Severity (UC):</b><br>Severity for unexpected completion reception.    |
| 15        | 0h<br>RW/P       | <b>Completer Abort Severity (CA):</b><br>Severity for completer abort.                          |
| 14        | 0h<br>RW/P       | <b>Completion Timeout Severity (CT):</b><br>Severity for completion timeout.                    |
| 13        | 0h<br>RO         | <b>Flow Control Protocol Error Severity (FCPE):</b><br>Not supported.                           |
| 12        | 0h<br>RW/P       | <b>Poisoned TLP Severity (PT):</b><br>Severity for poisoned TLP reception.                      |
| 11:6      | 0h<br>RO         | <b>Reserved</b>   |
| 5         | 0h<br>RO         | <b>Surprise Down Error Severity (SDE):</b><br>Surprise Down is not supported.                   |
| 4         | 1h<br>RW/P       | <b>Data Link Protocol Error Severity (DLPE):</b><br>Severity for data link protocol errors.     |
| 3:1       | 0h<br>RO         | <b>Reserved</b>   |
| 0         | 0h<br>RO         | <b>Training Error Severity (TE):</b><br>TE not supported.                                       |

### 3.5.41 Correctable Error Status (CES) – Offset 110h

Correctable Error Status

| Type | Size   | Offset        | Default   |
|------|--------|---------------|-----------|
| MMIO | 32 bit | DMIBAR + 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<br>RO         | <b>Reserved</b>              |

| Bit Range | Default & Access    | Field Name (ID): Description  |
|-----------|---------------------|---|
| 13        | 0h<br>RW/1C/V/<br>P | <b>Advisory Non-Fatal Error Status (ANFES):</b><br>When set, indicates that an Advisory Non-Fatal Error occurred. |
| 12        | 0h<br>RW/1C/V/<br>P | <b>Replay Timer Timeout Status (RTT):</b><br>Indicates the replay timer timed out.                                |
| 11:9      | 0h<br>RO            | <b>Reserved</b>   |
| 8         | 0h<br>RW/1C/V/<br>P | <b>Replay Number Rollover Status (RNR):</b><br>Indicates the replay number rolled over.                           |
| 7         | 0h<br>RW/1C/V/<br>P | <b>Bad DLLP Status (BD):</b><br>Indicates a bad DLLP was received.  |
| 6         | 0h<br>RW/1C/V/<br>P | <b>Bad TLP Status (BT):</b><br>Indicates a bad TLP was received.  |
| 5:1       | 0h<br>RO            | <b>Reserved</b>   |
| 0         | 0h<br>RW/1C/V/<br>P | <b>Receiver Error Status (RE):</b><br>Indicates a receiver error occurred.  |

### 3.5.42 Correctable Error Mask (CEM) – Offset 114h

Correctable Error Mask

| Type | Size   | Offset        | Default   |
|------|--------|---------------|-----------|
| MMIO | 32 bit | DMIBAR + 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<br>RO         | <b>Reserved</b>  |
| 13        | 1h<br>RW/P       | <b>Advisory Non-Fatal Error Mask (ANFEM):</b><br>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.<br>This register is set by default to enable compatibility with software that does not comprehend Role-Based Error Reporting. |
| 12        | 0h<br>RW/P       | <b>Replay Timer Timeout Mask (RTT):</b><br>Mask for replay timer timeout.  |
| 11:9      | 0h<br>RO         | <b>Reserved</b>  |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 8         | 0h<br>RW/P       | <b>Replay Number Rollover Mask (RNR):</b><br>Mask for replay number rollover. |
| 7         | 0h<br>RW/P       | <b>Bad DLLP Mask (BD):</b><br>Mask for bad DLLP reception.                    |
| 6         | 0h<br>RW/P       | <b>Bad TLP Mask (BT):</b><br>Mask for bad TLP reception.                      |
| 5:1       | 0h<br>RO         | <b>Reserved</b>   |
| 0         | 0h<br>RW/P       | <b>Receiver Error Mask (RE):</b><br>Mask for receiver errors.                 |

### 3.5.43 Advanced Error Capabilities And Control (AECC) – Offset 118h

Advanced Error Capabilities And Control

| Type | Size   | Offset        | Default   |
|------|--------|---------------|-----------|
| MMIO | 32 bit | DMIBAR + 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<br>RO         | <b>Reserved</b>   |
| 12        | 0h<br>RO         | <b>Completion Timeout Prefix/Header Log Capable (CTPHLC):</b><br>If set, this bit indicates that port records the prefix/header of Request TLPs that experience a Completion Timeout error.<br>Note: BIOS should program this bit before enable the Completion Timeout mechanism. |
| 11:9      | 0h<br>RO         | <b>Reserved</b>   |
| 8         | 0h<br>RO         | <b>ECRC Check Enable (ECE):</b><br>ECRC is not supported.   |
| 7         | 0h<br>RO         | <b>ECRC Check Capable (ECC):</b><br>ECRC is not supported.  |
| 6         | 0h<br>RO         | <b>ECRC Generation Enable (EGE):</b><br>ECRC is not supported.  |
| 5         | 0h<br>RO         | <b>ECRC Generation Capable (EGC):</b><br>ECRC is not supported.   |
| 4:0       | 00h<br>RO/V/P    | <b>First Error Pointer (FEP):</b><br>Identifies the bit position of the first error reported in the Uncorrectable Error Status Register.  |



### 3.5.44 Header Log (HL\_DW1) – Offset 11Ch

Header Log

| Type | Size   | Offset        | Default   |
|------|--------|---------------|-----------|
| MMIO | 32 bit | DMIBAR + 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<br>RO/V/P | <b>1st DWORD of TLP (DW1):</b><br>Byte0 && Byte1 && Byte2 && Byte3 |

### 3.5.45 Header Log (HL\_DW2) – Offset 120h

Header Log

| Type | Size   | Offset        | Default   |
|------|--------|---------------|-----------|
| MMIO | 32 bit | DMIBAR + 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<br>RO/V/P | <b>2nd DWORD of TLP (DW2):</b><br>Byte4 && Byte5 && Byte6 && Byte7 |

### 3.5.46 Header Log (HL\_DW3) – Offset 124h

Header Log



| Type | Size   | Offset        | Default   |
|------|--------|---------------|-----------|
| MMIO | 32 bit | DMIBAR + 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<br>RO/V/P | <b>3rd DWORD of TLP (DW3):</b><br>Byte8 && Byte9 && Byte10 && Byte11 |

### 3.5.47 Header Log (HL\_DW4) – Offset 128h

Header Log

| Type | Size   | Offset        | Default   |
|------|--------|---------------|-----------|
| MMIO | 32 bit | DMIBAR + 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<br>RO/V/P | <b>4th DWORD of TLP (DW4):</b><br>Byte12 && Byte13 && Byte14 && Byte15 |

### 3.5.48 Root Error Command (REC) – Offset 12Ch

Root Error Command

| Type | Size   | Offset        | Default   |
|------|--------|---------------|-----------|
| MMIO | 32 bit | DMIBAR + 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<br>RO         | <b>Reserved</b>  |
| 2         | 0h<br>RW         | <b>Fatal Error Reporting Enable (FERE):</b><br>When set, the root port will generate an interrupt when a fatal error is reported by the attached device.             |
| 1         | 0h<br>RW         | <b>Non-fatal Error Reporting Enable (NERE):</b><br>When set, the root port will generate an interrupt when a non-fatal error is reported by the attached device.     |
| 0         | 0h<br>RW         | <b>Correctable Error Reporting Enable (CERE):</b><br>When set, the root port will generate an interrupt when a correctable error is reported by the attached device. |

### 3.5.49 Root Error Status (RES) – Offset 130h

Root Error Status

| Type | Size   | Offset        | Default   |
|------|--------|---------------|-----------|
| MMIO | 32 bit | DMIBAR + 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<br>RO           | <b>Advanced Error Interrupt Message Number (AEMN):</b><br>Reserved  |
| 26:7      | 0h<br>RO            | <b>Reserved</b>   |
| 6         | 0h<br>RW/1C/V/<br>P | <b>Fatal Error Messages Received (FEMR):</b><br>Set when one or more Fatal Uncorrectable Error Messages have been received.         |
| 5         | 0h<br>RW/1C/V/<br>P | <b>Non-Fatal Error Messages Received (NFEMR):</b><br>Set when one or more Non-Fatal Uncorrectable error messages have been received |
| 4         | 0h<br>RW/1C/V/<br>P | <b>First Uncorrectable Fatal (FUF):</b><br>Set when the first Uncorrectable Error message received is for a fatal error.            |

| Bit Range | Default & Access    | Field Name (ID): Description  |
|-----------|---------------------|---|
| 3         | 0h<br>RW/1C/V/<br>P | <b>Multiple ERR_FATAL/NONFATAL Received (MENR):</b><br>Set when either a fatal or a non-fatal error is received and the ENR bit is already set. |
| 2         | 0h<br>RW/1C/V/<br>P | <b>ERR_FATAL/NONFATAL Received (ENR):</b><br>Set when either a fatal or a non-fatal error message is received.                                  |
| 1         | 0h<br>RW/1C/V/<br>P | <b>Multiple ERR_COR Received (MCR):</b><br>Set when a correctable error message is received and the CR bit is already set.                      |
| 0         | 0h<br>RW/1C/V/<br>P | <b>ERR_COR Received (CR):</b><br>Set when a correctable error message is received.  |

### 3.5.50 Error Source Identification (ESID) – Offset 134h

Error Source Identification

| Type | Size   | Offset        | Default   |
|------|--------|---------------|-----------|
| MMIO | 32 bit | DMIBAR + 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<br>RO/V/P  | <b>ERR_FATAL/NONFATAL Source Identification (EFNFSID):</b><br>Loaded with the requester ID indicated in the received ERR_FATAL or ERR_NONFATAL message when RES.ENR is first set, or the internal requester ID if an internally detected error. |
| 15:0      | 0000h<br>RO/V/P  | <b>ERR_COR Source Identification (ECSID):</b><br>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.                                 |

### 3.5.51 PTM Extended Capability Header (PTMECH) – Offset 150h

PTM Extended Capability Header

| Type | Size   | Offset        | Default   |
|------|--------|---------------|-----------|
| MMIO | 32 bit | DMIBAR + 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<br>RW/O     | <b>Next Capability Offset (NCO):</b><br>Points to the next capability.   |
| 19:16     | 0h<br>RW/O       | <b>Capability Version (CV):</b><br>For systems that support PTM Extended Capability, BIOS should write a 1h to this register else it should write 0. |
| 15:0      | 0000h<br>RW/O    | <b>Capability ID (CID):</b><br>For systems that support PTM Extended Capability, BIOS should write a 001Fh to this register else it should write 0.  |

### 3.5.52 Port VC Capability Register 1 (PVCCR1) – Offset 284h

Port VC Capability Register 1

| Type | Size   | Offset        | Default   |
|------|--------|---------------|-----------|
| MMIO | 32 bit | DMIBAR + 284h | 00000000h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 31:12     | 0h<br>RO         | <b>Reserved</b>   |
| 11:10     | 0h<br>RO         | <b>Function Arbitration Table Entry Size (FARES):</b><br>Indicates the size (in bits) of Function Arbitration table entry in the device.<br>Defined encodings are:<br>00b Size of Function Arbitration table entry is 1 bit<br>01b Size of Function Arbitration table entry is 2 bits<br>10b Size of Function Arbitration table entry is 4 bits<br>11b Size of Function Arbitration table entry is 8 bits |
| 9:8       | 0h<br>RO         | <b>Reference Clock (RC):</b><br>Indicates the reference clock for Virtual Channels that support time-based WRR Function Arbitration.<br>Defined encodings are:<br>00b 100 ns reference clock<br>01b 11b Reserved  |
| 7         | 0h<br>RO         | <b>Reserved</b>   |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 6:4       | 0h<br>RO         | <b>Low Priority Extended VC Count (LPEVCC):</b><br>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 minimum value of this field is 000b and the maximum value is Extended VC Count. |
| 3         | 0h<br>RO         | <b>Reserved</b>   |
| 2:0       | 0h<br>RW/O       | <b>Extended VC Count (EVCC):</b><br>Indicates the number of (extended) Virtual Channels in addition to the default VC supported by the device.<br>The minimum value of this field is zero (for devices that only support the default VC). The maximum value is seven.   |

### 3.5.53 Port VC Capability 2 (PVCC2) – Offset 288h

Port VC Capability 2

| Type | Size   | Offset        | Default  |
|------|--------|---------------|----------|
| MMIO | 32 bit | DMIBAR + 288h | 0000000h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| R           | R          | R         |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 31:24     | 00h<br>RO        | <b>VC Arbitration Table Offset (VCATO):</b><br>Indicates the location of the VC Arbitration Table.<br>This field contains the zero-based offset of the table in DQWORDS (16 bytes) from the base address of the MFVC Capability structure. A value of 00h indicates that the table is not present.   |
| 23:8      | 0h<br>RO         | <b>Reserved</b>  |
| 7:0       | 00h<br>RO        | <b>VC Arbitration Capability (VCAC):</b><br>Indicates the types of VC Arbitration supported by the device for the LPVC group. This field is valid for all devices that report a Low Priority Extended VC Count greater than 0.<br>Each bit location within this field corresponds to a VC Arbitration Capability defined below. When more than 1 bit in this field is Set, it indicates that the device can be configured to provide different VC arbitration services.<br>Defined bit positions are:<br>Bit 0 Hardware fixed arbitration scheme, e.g., Round Robin<br>Bit 1 Weighted Round Robin (WRR) arbitration with 32 phases<br>Bit 2 WRR arbitration with 64 phases<br>Bit 3 WRR arbitration with 128 phases<br>Bits 4-7 Reserved |

### 3.5.54 Port VC Control (PVCC) – Offset 28Ch

Port VC Control



| Type | Size   | Offset        | Default |
|------|--------|---------------|---------|
| MMIO | 16 bit | DMIBAR + 28Ch | 0000h   |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 15:4      | 0h<br>RO         | <b>Reserved</b>   |
| 3:1       | 0h<br>RW         | <b>VC Arbitration Select (VCAS):</b><br>Used by software to configure the VC arbitration by selecting one of the supported VC Arbitration schemes indicated by the VC Arbitration Capability field in the Port VC Capability register 2.<br>The permissible values of this field are numbers corresponding to one of the asserted bits in the VC Arbitration Capability field. This field cannot be modified when more than one VC in the LPVC group is enabled.  |
| 0         | 0h<br>WO         | <b>Load VC Arbitration Table (LVCAT):</b><br>Used by software to update the VC Arbitration Table. This bit is valid when the selected VC Arbitration uses the VC Arbitration Table.<br>Software Sets this bit to request hardware to apply new values programmed into VC Arbitration Table - Clearing this bit has no effect. Software checks the VC Arbitration Table Status bit to confirm that new values stored in the VC Arbitration Table are latched by the VC arbitration logic.<br>This bit always returns 0b when read. |

### 3.5.55 Port VC Status (PVCS) – Offset 28Eh

Port VC Status

| Type | Size   | Offset        | Default |
|------|--------|---------------|---------|
| MMIO | 16 bit | DMIBAR + 28Eh | 0000h   |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| R           | R          | R         |

| Bit Range | Default & Access | Field Name (ID): Description |
|-----------|------------------|------------------------------|
| 15:1      | 0h<br>RO         | <b>Reserved</b>              |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 0         | 0h<br>RO         | <p><b>VC Arbitration Table Status (VCATS):</b><br/>Indicates the coherency status of the VC Arbitration Table. This bit is valid when the selected VC uses the VC Arbitration Table.</p> <p>This bit is Set by hardware when any entry of the VC Arbitration Table is written by software. This bit is Cleared by hardware when hardware finishes loading values stored in the VC Arbitration Table after software sets the Load VC Arbitration Table bit in the Port VC Control register.</p> <p>Default value of this bit is 0b.</p> |

### 3.5.56 Virtual Channel 0 Resource Capability (V0VCRC) – Offset 290h

Virtual Channel 0 Resource Capability

| Type | Size   | Offset        | Default   |
|------|--------|---------------|-----------|
| MMIO | 32 bit | DMIBAR + 290h | 00000000h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 31:24     | 00h<br>RO        | <p><b>Function Arbitration Table Offset (FATO):</b><br/>Indicates the location of the Function Arbitration Table associated with the VC resource.</p> <p>This field contains the zero-based offset of the table in DQWORDS (16 bytes) from the base address of the MFVC Capability structure. A value of 00h indicates that the table is not present.</p>   |
| 23        | 0h<br>RO         | <b>Reserved</b>   |
| 22:16     | 00h<br>RW/O      | <p><b>Maximum Time Slots (MTS):</b><br/>Indicates the maximum number of time slots (minus 1) that the VC resource is capable of supporting when it is configured for time-based WRR Function Arbitration. For example, a value of 000 0000b in this field indicates the supported maximum number of time slots is 1 and a value of 111 1111b indicates the supported maximum number of time slots is 128.</p> <p>This field is valid only when the Function Arbitration Capability indicates that the VC resource supports time-based WRR Function Arbitration.</p> |
| 15:8      | 0h<br>RO         | <b>Reserved</b>   |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 7:0       | 00h<br>RO        | <p><b>Function Arbitration Capability (FAC):</b><br/>Indicates types of Function Arbitration supported by the VC resource.<br/>Each bit location within this field corresponds to a Function Arbitration Capability defined below. When more than 1 bit in this field is Set, it indicates that the VC resource can be configured to provide different arbitration services.<br/>Software selects among these capabilities by writing to the Function Arbitration Select field.<br/>Defined bit positions are:<br/>Bit 0 Non-configurable hardware-fixed arbitration scheme, e.g., Round Robin (RR)<br/>Bit 1 Weighted Round Robin (WRR) arbitration with 32 phases<br/>Bit 2 WRR arbitration with 64 phases<br/>Bit 3 WRR arbitration with 128 phases<br/>Bit 4 Time-based WRR with 128 phases<br/>Bit 5 WRR arbitration with 256 phases<br/>Bits 6-7 Reserved</p> |

### 3.5.57 Virtual Channel 0 Resource Control (VOCTL) – Offset 294h

Virtual Channel 0 Resource Control

| Type | Size   | Offset        | Default   |
|------|--------|---------------|-----------|
| MMIO | 32 bit | DMIBAR + 294h | 80000001h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 31        | 1h<br>RO         | <p><b>Virtual Channel Enable (EN):</b><br/>When Set, this bit enables a Virtual Channel (see note 1 for exceptions). The Virtual Channel is disabled when this bit is cleared.<br/>Software must use the VC Negotiation Pending bit to check whether the VC negotiation is complete.<br/>Default value of this bit is 1b for the first VC resource and 0b for other VC resource(s).<br/>Notes:<br/>1. This bit is hardwired to 1b for the default VC (VC0), i.e., writing to this field has no effect for VC0.<br/>2. To enable a Virtual Channel, the VC Enable bits for that Virtual Channel must be Set in both components on a Link.<br/>3. To disable a Virtual Channel, the VC Enable bits for that Virtual Channel must be Cleared in both components on a Link.<br/>4. Software must ensure that no traffic is using a Virtual Channel at the time it is disabled.<br/>5. Software must fully disable a Virtual Channel in both components on a Link before re-enabling the Virtual Channel.</p> |
| 30:27     | 0h<br>RO         | <b>Reserved</b>  |



| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 26:24     | 0h<br>RO         | <p><b>Virtual Channel Identifier (ID):</b><br/>This field assigns a VC ID to the VC resource.<br/>This field cannot be modified when the VC is already enabled.<br/>Note:<br/>For the first VC resource (default VC), this field is a read-only field that must be hardwired to 000b.</p>   |
| 23:20     | 0h<br>RO         | <b>Reserved</b>   |
| 19:17     | 0h<br>RW         | <p><b>Function Arbitration Select (FAS):</b><br/>This field configures the VC resource to provide a particular Function Arbitration service.<br/>The permissible value of this field is a number corresponding to one of the asserted bits in the Function Arbitration Capability field of the VC resource.</p>   |
| 16        | 0h<br>RW         | <p><b>Load Function Arbitration Table (LFAT):</b><br/>When Set, this bit updates the Function Arbitration logic from the Function Arbitration Table for the VC resource. This bit is only valid when the Function Arbitration Table is used by the selected Function Arbitration scheme (that is indicated by a Set bit in the Function Arbitration Capability field selected by Function Arbitration Select).<br/>Software sets this bit to signal hardware to update Function Arbitration logic with new values stored in the Function Arbitration Table - clearing this bit has no effect.<br/>Software uses the Function Arbitration Table Status bit to confirm whether the new values of Function Arbitration Table are completely latched by the arbitration logic.<br/>This bit always returns 0b when read.<br/>Default value of this bit is 0b.</p>   |
| 15:10     | 00h<br>RW/L      | <p><b>Extended TC/VC Map (ETVM):</b><br/>Defines the upper 8-bits of the VC0 16-bit TC/VC mapping registers. These registers use the PCI Express reserved TC[3] traffic class bit.<br/>This register is Read-Only if LPCR.SRL field is set<br/><b>Locked by:</b> LPCR.SRL</p>   |
| 9:8       | 0h<br>RO         | <b>Reserved</b>   |
| 7:1       | 00h<br>RW/L      | <p><b>Transaction Class / Virtual Channel Map (TVM):</b><br/>This field indicates the TCs that are mapped to the VC resource.<br/>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 1 bit in this field is Set, it indicates that multiple TCs are mapped to the VC resource.<br/>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.<br/>Default value of this field is FFh for the first VC resource and is 00h for other VC resources.<br/>Note:<br/>Bit 0 of this field is read-only. It must be hardwired to 1b for the default VC0 and hardwired to 0b for all other enabled VCs.<br/>This register is Read-Only if LPCR.SRL field is set<br/><b>Locked by:</b> LPCR.SRL</p> |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 0         | 1h<br>RO         | <p><b>Transaction Class / Virtual Channel Map TC0 (TVMT0):</b><br/>           This field indicates the TCs that are mapped to the VC resource.<br/>           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 1 bit in this field is Set, it indicates that multiple TCs are mapped to the VC resource.<br/>           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.<br/>           Default value of this field is FFh for the first VC resource and is 00h for other VC resources.<br/>           Note:<br/>           Bit 0 of this field is read-only. It must be hardwired to 1b for the default VC0 and hardwired to 0b for all other enabled VCs.</p> |

### 3.5.58 Virtual Channel 0 Resource Status (VOSTS) – Offset 29Ah

Virtual Channel 0 Resource Status

| Type | Size   | Offset        | Default |
|------|--------|---------------|---------|
| MMIO | 16 bit | DMIBAR + 29Ah | 0000h   |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| R           | R          | R         |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 15:2      | 0h<br>RO         | <b>Reserved</b>  |
| 1         | 0h<br>RO/V       | <p><b>VC Negotiation Pending (NP):</b><br/>           This bit indicates whether the Virtual Channel negotiation (initialization or disabling) is in pending state.<br/>           When this bit is Set by hardware, it indicates that the VC resource is still in the process of negotiation. This bit is Cleared by hardware after the VC negotiation is complete. For a nondefault Virtual Channel, software may use this bit when enabling or disabling the VC. For the default VC, this bit indicates the status of the process of Flow Control initialization.<br/>           Before using a Virtual Channel, software must check whether the VC Negotiation Pending bits for that Virtual Channel are Clear in both components on a Link.</p> |
| 0         | 0h<br>RO         | <p><b>Function Arbitration Table Status (FATS):</b><br/>           This bit indicates the coherency status of the Function Arbitration Table associated with the VC resource. This bit is valid only when the Function Arbitration Table is used by the selected Function Arbitration for the VC resource.<br/>           This bit is Set by hardware when any entry of the Function Arbitration Table is written to by software. This bit is Cleared by hardware when hardware finishes loading values stored in the Function Arbitration Table after software sets the Load FunctionArbitration Table bit.<br/>           Default value of this bit is 0b</p>  |

### 3.5.59 Virtual Channel 1 Resource Capability (V1VCRC) – Offset 29Ch

Virtual Channel 1 Resource Capability

**Note:** Bit definitions are the same as V0VCRC, offset 290h.

### 3.5.60 Virtual Channel 1 Resource Control (V1CTL) – Offset 2A0h

Virtual Channel 1 Resource Control

| Type | Size   | Offset        | Default   |
|------|--------|---------------|-----------|
| MMIO | 32 bit | DMIBAR + 2A0h | 00000000h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 31        | 0h<br>RW/L       | <b>Virtual Channel Enable (EN):</b><br>Enables the VC when set. Disables the VC when cleared.<br>This register is Read-Only if LPCR.SRL field is set<br><b>Locked by:</b> LPCR.SRL  |
| 30:28     | 0h<br>RO         | <b>Reserved</b>   |
| 27:24     | 0h<br>RW/L       | <b>Virtual Channel Identifier (ID):</b><br>Indicates the ID to use for this virtual channel<br>Note: BIOS is required to program VCID[3] to 0 when operating at DMI2.<br>This register is Read-Only if LPCR.SRL field is set<br><b>Locked by:</b> LPCR.SRL  |
| 23:20     | 0h<br>RO         | <b>Reserved</b>   |
| 19:17     | 0h<br>RW         | <b>Function Arbitration Select (FAS):</b><br>This field configures the VC resource to provide a particular Function Arbitration service.<br>The permissible value of this field is a number corresponding to one of the asserted bits in the Function Arbitration Capability field of the VC resource.  |
| 16        | 0h<br>RW         | <b>Load Function Arbitration Table (LFAT):</b><br>When Set, this bit updates the Function Arbitration logic from the Function Arbitration Table for the VC resource. This bit is only valid when the Function Arbitration Table is used by the selected Function Arbitration scheme (that is indicated by a Set bit in the Function Arbitration Capability field selected by Function Arbitration Select).<br>Software sets this bit to signal hardware to update Function Arbitration logic with new values stored in the Function Arbitration Table - clearing this bit has no effect.<br>Software uses the Function Arbitration Table Status bit to confirm whether the new values of Function Arbitration Table are completely latched by the arbitration logic.<br>This bit always returns 0b when read.<br>Default value of this bit is 0b. |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 15:10     | 00h<br>RW/L      | <b>Extended TC/VC Map (ETVM):</b><br>Defines the upper 8-bits of the VC0 16-bit TC/VC mapping registers. These registers use the PCI Express reserved TC[3] traffic class bit.<br>This register is Read-Only if LPCR.SRL field is set<br><b>Locked by:</b> LPCR.SRL  |
| 9:8       | 0h<br>RO         | <b>Reserved</b>  |
| 7:1       | 00h<br>RW/L      | <b>Transaction Class / Virtual Channel Map (TVM):</b><br>This field indicates the TCs that are mapped to the VC resource.<br>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 1 bit in this field is Set, it indicates that multiple TCs are mapped to the VC resource.<br>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.<br>Default value of this field is FFh for the first VC resource and is 00h for other VC resources.<br>Note:<br>Bit 0 of this field is read-only. It must be hardwired to 1b for the default VC0 and hardwired to 0b for all other enabled VCs.<br>This register is Read-Only if LPCR.SRL field is set<br><b>Locked by:</b> LPCR.SRL |
| 0         | 0h<br>RO         | <b>Reserved</b>  |

### 3.5.61 Virtual Channel 1 Resource Status (V1STS) – Offset 2A6h

Virtual Channel 1 Resource Status

**Note:** Bit definitions are the same as V0STS, offset 29Ah.

### 3.5.62 Secondary PCI Express Extended Capability Header (SPEECH) – Offset A30h

Secondary PCI Express Extended Capability Header

| Type | Size   | Offset        | Default   |
|------|--------|---------------|-----------|
| MMIO | 32 bit | DMIBAR + 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<br>RW/O     | <p><b>Next Capability Offset (NCO):</b><br/>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.<br/>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.<br/>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.</p> |
| 19:16     | 0h<br>RW/O       | <p><b>Capability Version (CV):</b><br/>This field is a PCI-SIG defined version number that indicates the version of the Capability structure present.<br/>For systems that support Secondary PCI Express Extended Capability, BIOS should write a 1h to this register else it should write 0.</p>  |
| 15:0      | 0000h<br>RW/O    | <p><b>PCI Express Extended Capability ID (PCIECID):</b><br/>This field is a PCI-SIG defined ID number that indicates the nature and format of the Extended Capability.<br/>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.</p>   |

### 3.5.63 Link Control 3 (LCTL3) – Offset A34h

Link Control 3

| Type | Size   | Offset        | Default   |
|------|--------|---------------|-----------|
| MMIO | 32 bit | DMIBAR + 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<br>RO         | <b>Reserved</b>              |



| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 15:9      | 00h<br>RW        | <p><b>Enable Lower SKP OS Generation Vector (ELSOSGV):</b><br/>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.<br/>Bit definitions within this field are:<br/>Bit 0 2.5 GT/s<br/>Bit 1 5.0 GT/s<br/>Bit 2 8.0 GT/s<br/>Bit 3 16.0 GT/s<br/>Bits 6:4 Rsvd<br/>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.</p> |
| 8:2       | 0h<br>RO         | <b>Reserved</b>   |
| 1         | 0h<br>RW/P       | <p><b>Link Equalization Request Interrupt Enable (LERIE):</b><br/>When set, this bit enables the generation of an interrupt to indicate that the Link Equalization Request bit has been set.</p>  |
| 0         | 0h<br>RW/1S/V    | <p><b>Perform Equalization (PE):</b><br/>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.<br/>This bit is cleared by Root Port upon entry to Link Equalization Phase 1.</p>  |

### 3.5.64 Lane Error Status (LES) – Offset A38h

Lane Error Status

| Type | Size   | Offset        | Default   |
|------|--------|---------------|-----------|
| MMIO | 32 bit | DMIBAR + 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<br>RO            | <b>Reserved</b>  |
| 15        | 0h<br>RW/1C/V/<br>P | <p><b>Lane 15 Error Status (L15ES):</b><br/>Lane 15 detected a Lane-based error.</p> |
| 14        | 0h<br>RW/1C/V/<br>P | <p><b>Lane 14 Error Status (L14ES):</b><br/>Lane 14 detected a Lane-based error.</p> |
| 13        | 0h<br>RW/1C/V/<br>P | <p><b>Lane 13 Error Status (L13ES):</b><br/>Lane 13 detected a Lane-based error.</p> |
| 12        | 0h<br>RW/1C/V/<br>P | <p><b>Lane 12 Error Status (L12ES):</b><br/>Lane 12 detected a Lane-based error.</p> |

| Bit Range | Default & Access    | Field Name (ID): Description   |
|-----------|---------------------|--|
| 11        | 0h<br>RW/1C/V/<br>P | <b>Lane 11 Error Status (L11ES):</b><br>Lane 11 detected a Lane-based error. |
| 10        | 0h<br>RW/1C/V/<br>P | <b>Lane 10 Error Status (L10ES):</b><br>Lane 10 detected a Lane-based error. |
| 9         | 0h<br>RW/1C/V/<br>P | <b>Lane 9 Error Status (L9ES):</b><br>Lane 9 detected a Lane-based error.    |
| 8         | 0h<br>RW/1C/V/<br>P | <b>Lane 8 Error Status (L8ES):</b><br>Lane 8 detected a Lane-based error.    |
| 7         | 0h<br>RW/1C/V/<br>P | <b>Lane 7 Error Status (L7ES):</b><br>Lane 7 detected a Lane-based error.    |
| 6         | 0h<br>RW/1C/V/<br>P | <b>Lane 6 Error Status (L6ES):</b><br>Lane 6 detected a Lane-based error.    |
| 5         | 0h<br>RW/1C/V/<br>P | <b>Lane 5 Error Status (L5ES):</b><br>Lane 5 detected a Lane-based error.    |
| 4         | 0h<br>RW/1C/V/<br>P | <b>Lane 4 Error Status (L4ES):</b><br>Lane 4 detected a Lane-based error.    |
| 3         | 0h<br>RW/1C/V/<br>P | <b>Lane 3 Error Status (L3ES):</b><br>Lane 3 detected a Lane-based error.    |
| 2         | 0h<br>RW/1C/V/<br>P | <b>Lane 2 Error Status (L2ES):</b><br>Lane 2 detected a Lane-based error.    |
| 1         | 0h<br>RW/1C/V/<br>P | <b>Lane 1 Error Status (L1ES):</b><br>Lane 1 detected a Lane-based error.    |
| 0         | 0h<br>RW/1C/V/<br>P | <b>Lane 0 Error Status (L0ES):</b><br>Lane 0 detected a Lane-based error.    |

### 3.5.65 Lane 0 And Lane 1 Equalization Control (L01EC) – Offset A3Ch

Lane 0 And Lane 1 Equalization Control



| Type | Size   | Offset        | Default  |
|------|--------|---------------|----------|
| MMIO | 32 bit | DMIBAR + A3Ch | 7F7F7F7h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 31        | 0h<br>RO         | <b>Reserved</b>  |
| 30:28     | 7h<br>RW         | <b>Upstream Port Lane 1 Receiver Preset Hint (UPL1RPH):</b><br>Field contains the Receiver Preset Hint value sent or received during Port 8 GT/s Link Equalization..<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 27:24     | Fh<br>RW         | <b>Upstream Port Lane 1 Transmitter Preset (UPL1TP):</b><br>Field contains the Transmit Preset value sent or received during Port 8 GT/s Link Equalization..<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ.         |
| 23        | 0h<br>RO         | <b>Reserved</b>  |
| 22:20     | 7h<br>RW         | <b>Downstream Port Lane 1 Receiver Preset Hint (DPL1RPH):</b><br>Receiver Preset Hint may be used as a hint for 8 GT/s receiver equalization by this Port when the Port is operating as a Downstream Port.   |
| 19:16     | Fh<br>RW         | <b>Downstream Port Lane 1 Transmitter Preset (DPL1TP):</b><br>Transmitter Preset used for 8 GT/s 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<br>RO         | <b>Reserved</b>  |
| 14:12     | 7h<br>RW         | <b>Upstream Port Lane 0 Receiver Preset Hint (UPLORPH):</b><br>Field contains the Receiver Preset Hint value sent or received during Port 8 GT/s Link Equalization..<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 11:8      | Fh<br>RW         | <b>Upstream Port Lane 0 Transmitter Preset (UPL0TP):</b><br>Field contains the Transmit Preset value sent or received during Port 8 GT/s Link Equalization..<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ.         |
| 7         | 0h<br>RO         | <b>Reserved</b>  |
| 6:4       | 7h<br>RW         | <b>Downstream Port Lane 0 Receiver Preset Hint (DPLORPH):</b><br>Receiver Preset Hint may be used as a hint for 8 GT/s 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<br>RW         | <b>Downstream Port Lane 0 Transmitter Preset (DPL0TP):</b><br>Transmitter Preset used for 8 GT/s 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. |

### 3.5.66 Lane 2 And Lane 3 Equalization Control (L23EC) – Offset A40h

Lane 2 And Lane 3 Equalization Control

| Type | Size   | Offset        | Default   |
|------|--------|---------------|-----------|
| MMIO | 32 bit | DMIBAR + A40h | 7F7F7F7Fh |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 31        | 0h<br>RO         | <b>Reserved</b>  |
| 30:28     | 7h<br>RW         | <b>Upstream Port Lane 3 Receiver Preset Hint (UPL3RPH):</b><br>Field contains the Receiver Preset Hint value sent or received during Port 8 GT/s Link Equalization..<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 27:24     | Fh<br>RW         | <b>Upstream Port Lane 3 Transmitter Preset Hint (UPL3TP):</b><br>Field contains the Transmit Preset value sent or received during Port 8 GT/s Link Equalization..<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ.    |
| 23        | 0h<br>RO         | <b>Reserved</b>  |
| 22:20     | 7h<br>RW         | <b>Downstream Port Lane 3 Receiver Preset Hint (DPL3RPH):</b><br>Receiver Preset Hint may be used as a hint for 8 GT/s receiver equalization by this Port when the Port is operating as a Downstream Port.   |
| 19:16     | Fh<br>RW         | <b>Downstream Port Lane 3 Transmitter Preset (DPL3TP):</b><br>Transmitter Preset used for 8 GT/s 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<br>RO         | <b>Reserved</b>  |
| 14:12     | 7h<br>RW         | <b>Upstream Port Lane 2 Receiver Preset Hint (UPL2RPH):</b><br>Field contains the Receiver Preset Hint value sent or received during Port 8 GT/s Link Equalization..<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 11:8      | Fh<br>RW         | <b>Upstream Port Lane 2 Transmitter Preset (UPL2TP):</b><br>Field contains the Transmit Preset value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 7         | 0h<br>RO         | <b>Reserved</b>   |
| 6:4       | 7h<br>RW         | <b>Downstream Port Lane 2 Receiver Preset Hint (DPL2RPH):</b><br>Receiver Preset Hint may be used as a hint for 8 GT/s receiver equalization by this Port when the Port is operating as a Downstream Port.  |
| 3:0       | Fh<br>RW         | <b>Downstream Port Lane 2 Transmitter Preset (DPL2TP):</b><br>Transmitter Preset used for 8 GT/s 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.   |

### 3.5.67 Lane 4 And Lane 5 Equalization Control (L45EC) – Offset A44h

Lane 4 And Lane 5 Equalization Control

| Type | Size   | Offset        | Default  |
|------|--------|---------------|----------|
| MMIO | 32 bit | DMIBAR + A44h | 7F7F7F7h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 31        | 0h<br>RO         | <b>Reserved</b>  |
| 30:28     | 7h<br>RW         | <b>Upstream Port Lane 5 Receiver Preset Hint (UPL5RPH):</b><br>Field contains the Receiver Preset Hint value sent or received during Port 8 GT/s Link Equalization..<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 27:24     | Fh<br>RW         | <b>Upstream Port Lane 5 Transmitter Preset (UPL5TP):</b><br>Field contains the Transmit Preset value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ.          |
| 23        | 0h<br>RO         | <b>Reserved</b>  |
| 22:20     | 7h<br>RW         | <b>Downstream Port Lane 5 Receiver Preset Hint (DPL5RPH):</b><br>Receiver Preset Hint may be used as a hint for 8 GT/s 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<br>RW         | <b>Downstream Port Lane 5 Transmitter Preset (DPL5TP):</b><br>Transmitter Preset used for 8 GT/s 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<br>RO         | <b>Reserved</b>  |
| 14:12     | 7h<br>RW         | <b>Upstream Port Lane 4 Receiver Preset Hint (UPL4RPH):</b><br>Field contains the Receiver Preset Hint value sent or received during Port 8 GT/s Link Equalization..<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 11:8      | Fh<br>RW         | <b>Upstream Port Lane 4 Transmitter Preset (UPL4TP):</b><br>Field contains the Transmit Preset value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ.          |
| 7         | 0h<br>RO         | <b>Reserved</b>  |
| 6:4       | 7h<br>RW         | <b>Downstream Port Lane 4 Receiver Preset Hint (DPL4RPH):</b><br>Receiver Preset Hint may be used as a hint for 8 GT/s receiver equalization by this Port when the Port is operating as a Downstream Port.   |
| 3:0       | Fh<br>RW         | <b>Downstream Port Lane 4 Transmitter Preset (DPL4TP):</b><br>Transmitter Preset used for 8 GT/s 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.  |

### 3.5.68 Lane 6 And Lane 7 Equalization Control (L67EC) – Offset A48h

Lane 6 And Lane 7 Equalization Control

| Type | Size   | Offset        | Default  |
|------|--------|---------------|----------|
| MMIO | 32 bit | DMIBAR + A48h | 7F7F7F7h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 31        | 0h<br>RO         | <b>Reserved</b>  |
| 30:28     | 7h<br>RW         | <b>Upstream Port Lane 7 Receiver Preset Hint (UPL7RPH):</b><br>Field contains the Receiver Preset Hint value sent or received during Port 8 GT/s Link Equalization..<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 27:24     | Fh<br>RW         | <b>Upstream Port Lane 7 Transmitter Preset (UPL7TP):</b><br>Field contains the Transmit Preset value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ.          |
| 23        | 0h<br>RO         | <b>Reserved</b>  |
| 22:20     | 7h<br>RW         | <b>Downstream Port Lane 7 Receiver Preset Hint (DPL7RPH):</b><br>Receiver Preset Hint may be used as a hint for 8 GT/s receiver equalization by this Port when the Port is operating as a Downstream Port.   |
| 19:16     | Fh<br>RW         | <b>Downstream Port Lane 7 Transmitter Preset (DPL7TP):</b><br>Transmitter Preset used for 8 GT/s 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<br>RO         | <b>Reserved</b>  |
| 14:12     | 7h<br>RW         | <b>Upstream Port Lane 6 Receiver Preset Hint (UPL6RPH):</b><br>Field contains the Receiver Preset Hint value sent or received during Port 8 GT/s Link Equalization..<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 11:8      | Fh<br>RW         | <b>Upstream Port Lane 6 Transmitter Preset (UPL6TP):</b><br>Field contains the Transmit Preset value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ.          |
| 7         | 0h<br>RO         | <b>Reserved</b>  |
| 6:4       | 7h<br>RW         | <b>Downstream Port Lane 6 Receiver Preset Hint (DPL6RPH):</b><br>Receiver Preset Hint may be used as a hint for 8 GT/s receiver equalization by this Port when the Port is operating as a Downstream Port.   |
| 3:0       | Fh<br>RW         | <b>Downstream Port Lane 6 Transmitter Preset (DPL6TP):</b><br>Transmitter Preset used for 8 GT/s 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.  |

### 3.5.69 Lane 8 And Lane 9 Equalization Control (L89EC) – Offset A4Ch

Lane 8 And Lane 9 Equalization Control

| Type | Size   | Offset        | Default  |
|------|--------|---------------|----------|
| MMIO | 32 bit | DMIBAR + A4Ch | 7F7F7F7h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 31        | 0h<br>RO         | <b>Reserved</b>  |
| 30:28     | 7h<br>RW         | <b>Upstream Port Lane 9 Receiver Preset Hint (UPL9RPH):</b><br>Field contains the Receiver Preset Hint value sent or received during Port 8 GT/s Link Equalization..<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 27:24     | Fh<br>RW         | <b>Upstream Port Lane 9 Transmitter Preset (UPL9TP):</b><br>Field contains the Transmit Preset value sent or received during Port 8 GT/s Link Equalization..<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ.         |
| 23        | 0h<br>RO         | <b>Reserved</b>  |
| 22:20     | 7h<br>RW         | <b>Downstream Port Lane 9 Receiver Preset Hint (DPL9RPH):</b><br>Receiver Preset Hint may be used as a hint for 8 GT/s receiver equalization by this Port when the Port is operating as a Downstream Port.   |
| 19:16     | Fh<br>RW         | <b>Downstream Port Lane 9 Transmitter Preset (DPL9TP):</b><br>Transmitter Preset used for 8 GT/s 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<br>RO         | <b>Reserved</b>  |
| 14:12     | 7h<br>RW         | <b>Upstream Port Lane 8 Receiver Preset Hint (UPL8RPH):</b><br>Field contains the Receiver Preset Hint value sent or received during Port 8 GT/s Link Equalization..<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 11:8      | Fh<br>RW         | <b>Upstream Port Lane 8 Transmitter Preset (UPL8TP):</b><br>Field contains the Transmit Preset value sent or received during Port 8 GT/s Link Equalization..<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ.         |
| 7         | 0h<br>RO         | <b>Reserved</b>  |
| 6:4       | 7h<br>RW         | <b>Downstream Port Lane 8 Receiver Preset Hint (DPL8RPH):</b><br>Receiver Preset Hint may be used as a hint for 8 GT/s 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<br>RW         | <b>Downstream Port Lane 8 Transmitter Preset (DPL8TP):</b><br>Transmitter Preset used for 8 GT/s 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. |

### 3.5.70 Lane 10 And Lane 11 Equalization Control (L1011EC) – Offset A50h

Lane 10 And Lane 11 Equalization Control

| Type | Size   | Offset        | Default  |
|------|--------|---------------|----------|
| MMIO | 32 bit | DMIBAR + A50h | 7F7F7F7h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 31        | 0h<br>RO         | <b>Reserved</b>  |
| 30:28     | 7h<br>RW         | <b>Upstream Port Lane 11 Receiver Preset Hint (UPL11RPH):</b><br>Field contains the Receiver Preset Hint value sent or received during Port 8 GT/s Link Equalization..<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 27:24     | Fh<br>RW         | <b>Upstream Port Lane 11 Transmitter Preset (UPL11TP):</b><br>Field contains the Transmit Preset value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ.          |
| 23        | 0h<br>RO         | <b>Reserved</b>  |
| 22:20     | 7h<br>RW         | <b>Downstream Port Lane 11 Receiver Preset Hint (DPL11RPH):</b><br>Receiver Preset Hint may be used as a hint for 8 GT/s receiver equalization by this Port when the Port is operating as a Downstream Port.   |
| 19:16     | Fh<br>RW         | <b>Downstream Port Lane 11 Transmitter Preset (DPL11TP):</b><br>Transmitter Preset used for 8 GT/s 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<br>RO         | <b>Reserved</b>  |
| 14:12     | 7h<br>RW         | <b>Upstream Port Lane 10 Receiver Preset Hint (UPL10RPH):</b><br>Field contains the Receiver Preset Hint value sent or received during Port 8 GT/s Link Equalization..<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 11:8      | Fh<br>RW         | <b>Upstream Port Lane 10 Transmitter Preset (UPL10TP):</b><br>Field contains the Transmit Preset value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 7         | 0h<br>RO         | <b>Reserved</b>   |
| 6:4       | 7h<br>RW         | <b>Downstream Port Lane 10 Receiver Preset Hint (DPL10RPH):</b><br>Receiver Preset Hint may be used as a hint for 8 GT/s receiver equalization by this Port when the Port is operating as a Downstream Port.  |
| 3:0       | Fh<br>RW         | <b>Downstream Port Lane 10 Transmitter Preset (DPL10TP):</b><br>Transmitter Preset used for 8 GT/s 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.   |

### 3.5.71 Lane 12 And Lane 13 Equalization Control (L1213EC) – Offset A54h

Lane 12 And Lane 13 Equalization Control

| Type | Size   | Offset        | Default  |
|------|--------|---------------|----------|
| MMIO | 32 bit | DMIBAR + A54h | 7F7F7F7h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 31        | 0h<br>RO         | <b>Reserved</b>  |
| 30:28     | 7h<br>RW         | <b>Upstream Port Lane 13 Receiver Preset Hint (UPL13RPH):</b><br>Field contains the Receiver Preset Hint value sent or received during Port 8 GT/s Link Equalization..<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 27:24     | Fh<br>RW         | <b>Upstream Port Lane 13 Transmitter Preset (UPL13TP):</b><br>Field contains the Transmit Preset value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ.          |
| 23        | 0h<br>RO         | <b>Reserved</b>  |
| 22:20     | 7h<br>RW         | <b>Downstream Port Lane 13 Receiver Preset Hint (DPL13RPH):</b><br>Receiver Preset Hint may be used as a hint for 8 GT/s 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<br>RW         | <b>Downstream Port Lane 13 Transmitter Preset (DPL13TP):</b><br>Transmitter Preset used for 8 GT/s 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<br>RO         | <b>Reserved</b>  |
| 14:12     | 7h<br>RW         | <b>Upstream Port Lane 12 Receiver Preset Hint (UPL12RPH):</b><br>Field contains the Receiver Preset Hint value sent or received during Port 8 GT/s Link Equalization..<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 11:8      | Fh<br>RW         | <b>Upstream Port Lane 12 Transmitter Preset (UPL12TP):</b><br>Field contains the Transmit Preset value sent or received during Port 8 GT/s Link Equalization..<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ.         |
| 7         | 0h<br>RO         | <b>Reserved</b>  |
| 6:4       | 7h<br>RW         | <b>Downstream Port Lane 12 Receiver Preset Hint (DPL12RPH):</b><br>Receiver Preset Hint may be used as a hint for 8 GT/s receiver equalization by this Port when the Port is operating as a Downstream Port.   |
| 3:0       | Fh<br>RW         | <b>Downstream Port Lane 12 Transmitter Preset (DPL12TP):</b><br>Transmitter Preset used for 8 GT/s 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.  |

### 3.5.72 Lane 14 And Lane 15 Equalization Control (L1415EC) – Offset A58h

Lane 14 And Lane 15 Equalization Control

| Type | Size   | Offset        | Default  |
|------|--------|---------------|----------|
| MMIO | 32 bit | DMIBAR + A58h | 7F7F7F7h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 31        | 0h<br>RO         | <b>Reserved</b>  |
| 30:28     | 7h<br>RW         | <b>Upstream Port Lane 15 Receiver Preset Hint (UPL15RPH):</b><br>Field contains the Receiver Preset Hint value sent or received during Port 8 GT/s Link Equalization..<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |



| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 27:24     | Fh<br>RW         | <b>Upstream Port Lane 15 Transmitter Preset (UPL15TP):</b><br>Field contains the Transmit Preset value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ.          |
| 23        | 0h<br>RO         | <b>Reserved</b>  |
| 22:20     | 7h<br>RW         | <b>Downstream Port Lane 15 Receiver Preset Hint (DPL15RPH):</b><br>Receiver Preset Hint may be used as a hint for 8 GT/s receiver equalization by this Port when the Port is operating as a Downstream Port.   |
| 19:16     | Fh<br>RW         | <b>Downstream Port Lane 15 Transmitter Preset (DPL15TP):</b><br>Transmitter Preset used for 8 GT/s 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<br>RO         | <b>Reserved</b>  |
| 14:12     | 7h<br>RW         | <b>Upstream Port Lane 14 Receiver Preset Hint (UPL14RPH):</b><br>Field contains the Receiver Preset Hint value sent or received during Port 8 GT/s Link Equalization..<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 11:8      | Fh<br>RW         | <b>Upstream Port Lane 14 Transmitter Preset (UPL14TP):</b><br>Field contains the Transmit Preset value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ.          |
| 7         | 0h<br>RO         | <b>Reserved</b>  |
| 6:4       | 7h<br>RW         | <b>Downstream Port Lane 14 Receiver Preset Hint (DPL14RPH):</b><br>Receiver Preset Hint may be used as a hint for 8 GT/s receiver equalization by this Port when the Port is operating as a Downstream Port.   |
| 3:0       | Fh<br>RW         | <b>Downstream Port Lane 14 Transmitter Preset (DPL14TP):</b><br>Transmitter Preset used for 8 GT/s 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.  |

### 3.5.73 Data Link Feature Extended Capability Header (DLFECH) – Offset A90h

Data Link Feature Extended Capability Header

| Type | Size   | Offset        | Default   |
|------|--------|---------------|-----------|
| MMIO | 32 bit | DMIBAR + A90h | 00000000h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 31:20     | 000h<br>RW/O     | <b>Next Capability Offset (NCO):</b><br>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.<br>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.<br>The bottom 2 bits of this offset are Reserved and must be implemented as 00b although software must mask them to allow for future uses of these bits. |
| 19:16     | 0h<br>RW/O       | <b>Capability Version (CV):</b><br>This field is a PCI-SIG defined version number that indicates the version of the Capability structure present.   |
| 15:0      | 0000h<br>RW/O    | <b>PCI Express Extended Capability ID (PCIECID):</b><br>This field is a PCI-SIG defined ID number that indicates the nature and format of the Extended Capability.  |

### 3.5.74 Data Link Feature Capabilities Register (DLFCAP) – Offset A94h

Data Link Feature Capabilities Register

| Type | Size   | Offset        | Default   |
|------|--------|---------------|-----------|
| MMIO | 32 bit | DMIBAR + A94h | 80000000h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 31        | 1h<br>RW/O       | <b>Data Link Feature Exchange Enable (DLFEE):</b><br>If set, this bit indicates that this Port will enter the DL_Feature negotiation state. Default is 1b.   |
| 30:23     | 0h<br>RO         | <b>Reserved</b>  |
| 22:1      | 000000h<br>RW/O  | <b>Local Feature Supported (LFS):</b><br>These bits indicate that the Downstream Port supports the associated Data Link Feature. For this version of this specification, this field is hardwired to 0. |
| 0         | 0h<br>RW/O       | <b>Local Scaled Flow Control Supported (LSFCS):</b><br>This bit indicates that the Port supports the Scaled Flow Control Feature.  |

### 3.5.75 Data Link Feature Status Register (DLFSTS) – Offset A98h

Data Link Feature Status Register

| Type | Size   | Offset        | Default   |
|------|--------|---------------|-----------|
| MMIO | 32 bit | DMIBAR + A98h | 00000000h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| R           | R          | R         |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 31        | 0h<br>RO/V       | <b>Data Link Feature Status Valid (DLFSV):</b><br>This bit indicates that the Downstream Port has received a Data Link Feature DLLP after the Link entered L0.<br>When this bit is 1b, bits 23:0 are frozen. Software must clear this bit to re-enable capturing information. This bit is cleared on DL_Down. |
| 30:23     | 0h<br>RO         | <b>Reserved</b>   |
| 22:1      | 000000h<br>RO/V  | <b>Remote Feature Supported (RFS):</b><br>These bits indicate that the Remote Port supports the corresponding Data Link Feature. These bits capture all information from the Data Link Feature DLLP even when this Port does not support the corresponding feature.   |
| 0         | 0h<br>RO/V       | <b>Remote Scaled Flow Control Supported (RSFCS):</b><br>This bit indicates that the Remote Port indicated it supports the Scaled Flow Control Feature   |

### 3.5.76 Physical Layer 16.0 GT/s Extended Capability Header (PL16GECH) – Offset A9Ch

Physical Layer 16.0 GT/s Extended Capability Header

| Type | Size   | Offset        | Default   |
|------|--------|---------------|-----------|
| MMIO | 32 bit | DMIBAR + A9Ch | 00000000h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 31:20     | 000h<br>RW/O     | <b>Next Capability Offset (NCO):</b><br>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.<br>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. |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 19:16     | 0h<br>RW/O       | <b>Capability Version (CV):</b><br>This field is a PCI-SIG defined version number that indicates the version of the Capability structure present.  |
| 15:0      | 0000h<br>RW/O    | <b>PCI Express Extended Capability ID (PCIECID):</b><br>This field is a PCI-SIG defined ID number that indicates the nature and format of the Extended Capability.<br>Extended Capability ID for the Physical Layer 16.0 GT/s Capability |

### 3.5.77 Physical Layer 16.0 GT/s Capability Register (PL16CAP) – Offset AA0h

Physical Layer 16.0 GT/s Capability Register

**Note:** Bit definitions are the same as [DSTS2](#), offset 6Ah.

### 3.5.78 Physical Layer 16.0 GT/s Control Register (PL16CTL) – Offset AA4h

Physical Layer 16.0 GT/s Control Register

**Note:** Bit definitions are the same as [DSTS2](#), offset 6Ah.

### 3.5.79 Physical Layer 16.0 GT/s Status Register (PL16S) – Offset AA8h

Physical Layer 16.0 GT/s Status Register

| Type | Size   | Offset        | Default   |
|------|--------|---------------|-----------|
| MMIO | 32 bit | DMIBAR + AA8h | 00000000h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access    | Field Name (ID): Description   |
|-----------|---------------------|--|
| 31:5      | 0h<br>RO            | <b>Reserved</b>  |
| 4         | 0h<br>RW/1C/V/<br>P | <b>Link Equalization Request 16.0 GT/s (LERG4):</b><br>This bit is Set by hardware to request the 16.0 GT/s Link equalization process to be performed on the Link.<br>The default value of this bit is 0b.                             |
| 3         | 0h<br>RO/V/P        | <b>Equalization 16.0 GT/s Phase 3 Successful (EQP3SG4):</b><br>When set to 1b, this bit indicates that Phase 3 of the 16.0 GT/s Transmitter Equalization procedure has successfully completed.<br>The default value of this bit is 0b. |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 2         | 0h<br>RO/V/P     | <b>Equalization 16.0 GT/s Phase 2 Successful (EQP2SG4):</b><br>When set to 1b, this bit indicates that Phase 2 of the 16.0 GT/s Transmitter Equalization procedure has successfully completed.<br>The default value of this bit is 0b. |
| 1         | 0h<br>RO/V/P     | <b>Equalization 16.0 GT/s Phase 1 Successful (EQP1SG4):</b><br>When set to 1b, this bit indicates that Phase 1 of the 16.0 GT/s Transmitter Equalization procedure has successfully completed.<br>The default value of this bit is 0b. |
| 0         | 0h<br>RO/V/P     | <b>Equalization 16.0 GT/s Complete (EQG4):</b><br>When set to 1b, this bit indicates that the Transmitter Equalization procedure at the 16.0 GT/s data rate has completed.<br>The default value of this bit is 0b.                     |

### 3.5.80 Physical Layer 16.0 GT/s Local Data Parity Mismatch Status Register (PL16LDPMS) – Offset AACH

Physical Layer 16.0 GT/s Local Data Parity Mismatch Status Register

| Type | Size   | Offset        | Default   |
|------|--------|---------------|-----------|
| MMIO | 32 bit | DMIBAR + AACH | 00000000h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access   | Field Name (ID): Description  |
|-----------|--------------------|---|
| 31:16     | 0h<br>RO           | <b>Reserved</b>   |
| 15:0      | 0000h<br>RW/1C/V/P | <b>Local Data Parity Mismatch Status (LDPMS):</b><br>Each bit indicates if the corresponding Lane detected a Data Parity mismatch. A value of 1b indicates that a mismatch was detected on the corresponding Lane Number.<br>The default value of each bit is 0b. |

### 3.5.81 Physical Layer 16.0 GT/s First Retimer Data Parity Mismatch Status Register (PL16FRDPMS) – Offset AB0h

Physical Layer 16.0 GT/s First Retimer Data Parity Mismatch Status Register

| Type | Size   | Offset        | Default   |
|------|--------|---------------|-----------|
| MMIO | 32 bit | DMIBAR + AB0h | 00000000h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access       | Field Name (ID): Description  |
|-----------|------------------------|---|
| 31:16     | 0h<br>RO               | <b>Reserved</b>   |
| 15:0      | 0000h<br>RW/1C/V/<br>P | <b>First Retimer Data Parity Mismatch Status (FRDPMS):</b><br>Each bit indicates if the corresponding Lane detected a Data Parity mismatch. A value of 1b indicates that a mismatch was detected on the corresponding Lane Number. The default value of each bit is 0b. |

### 3.5.82 Physical Layer 16.0 GT/s Second Retimer Data Parity Mismatch Status Register (PL16SRDPMS) – Offset AB4h

Physical Layer 16.0 GT/s Second Retimer Data Parity Mismatch Status Register

| Type | Size   | Offset        | Default   |
|------|--------|---------------|-----------|
| MMIO | 32 bit | DMIBAR + AB4h | 00000000h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access       | Field Name (ID): Description   |
|-----------|------------------------|--|
| 31:16     | 0h<br>RO               | <b>Reserved</b>  |
| 15:0      | 0000h<br>RW/1C/V/<br>P | <b>Second Retimer Data Parity Mismatch Status (SRDPMS):</b><br>Each bit indicates if the corresponding Lane detected a Data Parity mismatch. A value of 1b indicates that a mismatch was detected on the corresponding Lane Number. The default value of each bit is 0b. |

### 3.5.83 Physical Layer 16.0 GT/s Extra Status Register (PL16ES) – Offset AB8h

Physical Layer 16.0 GT/s Extra Status Register

**Note:** Bit definitions are the same as [DSTS2, offset 6Ah](#).

### 3.5.84 Physical Layer 16.0 GT/s Lane 01 Equalization Control Register (PL16L01EC) – Offset ABCh

Physical Layer 16.0 GT/s Lane 01 Equalization Control Register

| Type | Size   | Offset        | Default |
|------|--------|---------------|---------|
| MMIO | 16 bit | DMIBAR + ABCh | FFFFh   |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 15:12     | Fh<br>RW         | <b>Upstream Port 16 GT/s Port Lane 1 Transmitter Preset (UP16L1TP):</b><br>Field contains the Transmit Preset value sent or received during Port 16 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 11:8      | Fh<br>RW         | <b>Downstream Port 16 GT/s Lane 1 Transmitter Preset (DP16L1TP):</b><br>Transmitter Preset used for 16 GT/s 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.  |
| 7:4       | Fh<br>RW         | <b>Upstream Port 16 GT/s Port Lane 0 Transmitter Preset (UP16L0TP):</b><br>Field contains the Transmit Preset value sent or received during Port 16 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 3:0       | Fh<br>RW         | <b>Downstream Port 16 GT/s Lane 0 Transmitter Preset (DP16L0TP):</b><br>Transmitter Preset used for 16 GT/s 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.  |

### 3.5.85 Physical Layer 16.0 GT/s Lane 23 Equalization Control Register (PL16L23EC) – Offset ABEh

Physical Layer 16.0 GT/s Lane 23 Equalization Control Register



| Type | Size   | Offset        | Default |
|------|--------|---------------|---------|
| MMIO | 16 bit | DMIBAR + ABEh | FFFFh   |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 15:12     | Fh<br>RW         | <b>Upstream Port 16 GT/s Port Lane 3 Transmitter Preset (UP16L3TP):</b><br>Field contains the Transmit Preset value sent or received during Port 16 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 11:8      | Fh<br>RW         | <b>Downstream Port 16 GT/s Lane 3 Transmitter Preset (DP16L3TP):</b><br>Transmitter Preset used for 16 GT/s 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.  |
| 7:4       | Fh<br>RW         | <b>Upstream Port 16 GT/s Port Lane 2 Transmitter Preset (UP16L2TP):</b><br>Field contains the Transmit Preset value sent or received during Port 16 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 3:0       | Fh<br>RW         | <b>Downstream Port 16 GT/s Lane 2 Transmitter Preset (DP16L2TP):</b><br>Transmitter Preset used for 16 GT/s 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.  |

### 3.5.86 Physical Layer 16.0 GT/s Lane 45 Equalization Control Register (PL16L45EC) – Offset AC0h

Physical Layer 16.0 GT/s Lane 45 Equalization Control Register



| Type | Size   | Offset        | Default |
|------|--------|---------------|---------|
| MMIO | 16 bit | DMIBAR + AC0h | FFFFh   |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 15:12     | Fh<br>RW         | <b>Upstream Port 16 GT/s Port Lane 5 Transmitter Preset (UP16L5TP):</b><br>Field contains the Transmit Preset value sent or received during Port 16 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 11:8      | Fh<br>RW         | <b>Downstream Port 16 GT/s Lane 5 Transmitter Preset (DP16L5TP):</b><br>Transmitter Preset used for 16 GT/s 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.  |
| 7:4       | Fh<br>RW         | <b>Upstream Port 16 GT/s Port Lane 4 Transmitter Preset (UP16L4TP):</b><br>Field contains the Transmit Preset value sent or received during Port 16 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 3:0       | Fh<br>RW         | <b>Downstream Port 16 GT/s Lane 4 Transmitter Preset (DP16L4TP):</b><br>Transmitter Preset used for 16 GT/s 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.  |

### 3.5.87 Physical Layer 16.0 GT/s Lane 67 Equalization Control Register (PL16L67EC) – Offset AC2h

Physical Layer 16.0 GT/s Lane 67 Equalization Control Register



| Type | Size   | Offset        | Default |
|------|--------|---------------|---------|
| MMIO | 16 bit | DMIBAR + AC2h | FFFFh   |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 15:12     | Fh<br>RW         | <b>Upstream Port 16 GT/s Port Lane 7 Transmitter Preset (UP16L7TP):</b><br>Field contains the Transmit Preset value sent or received during Port 16 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 11:8      | Fh<br>RW         | <b>Downstream Port 16 GT/s Lane 7 Transmitter Preset (DP16L7TP):</b><br>Transmitter Preset used for 16 GT/s 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.  |
| 7:4       | Fh<br>RW         | <b>Upstream Port 16 GT/s Port Lane 6 Transmitter Preset (UP16L6TP):</b><br>Field contains the Transmit Preset value sent or received during Port 16 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 3:0       | Fh<br>RW         | <b>Downstream Port 16 GT/s Lane 6 Transmitter Preset (DP16L6TP):</b><br>Transmitter Preset used for 16 GT/s 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.  |

### 3.5.88 Physical Layer 16.0 GT/s Lane 89 Equalization Control Register (PL16L89EC) – Offset AC4h

Physical Layer 16.0 GT/s Lane 89 Equalization Control Register

| Type | Size   | Offset        | Default |
|------|--------|---------------|---------|
| MMIO | 16 bit | DMIBAR + AC4h | FFFFh   |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 15:12     | Fh<br>RW         | <b>Upstream Port 16 GT/s Port Lane 9 Transmitter Preset (UP16L9TP):</b><br>Field contains the Transmit Preset value sent or received during Port 16 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 11:8      | Fh<br>RW         | <b>Downstream Port 16 GT/s Lane 9 Transmitter Preset (DP16L9TP):</b><br>Transmitter Preset used for 16 GT/s 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.  |
| 7:4       | Fh<br>RW         | <b>Upstream Port 16 GT/s Port Lane 8 Transmitter Preset (UP16L8TP):</b><br>Field contains the Transmit Preset value sent or received during Port 16 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 3:0       | Fh<br>RW         | <b>Downstream Port 16 GT/s Lane 8 Transmitter Preset (DP16L8TP):</b><br>Transmitter Preset used for 16 GT/s 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.  |

### 3.5.89 Physical Layer 16.0 GT/s Lane 1011 Equalization Control Register (PL16L1011EC) – Offset AC6h

Physical Layer 16.0 GT/s Lane 1011 Equalization Control Register



| Type | Size   | Offset        | Default |
|------|--------|---------------|---------|
| MMIO | 16 bit | DMIBAR + AC6h | FFFFh   |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 15:12     | Fh<br>RW         | <b>Upstream Port 16 GT/s Port Lane 11 Transmitter Preset (UP16L11TP):</b><br>Field contains the Transmit Preset value sent or received during Port 16 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 11:8      | Fh<br>RW         | <b>Downstream Port 16 GT/s Lane 11 Transmitter Preset (DP16L11TP):</b><br>Transmitter Preset used for 16 GT/s 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.  |
| 7:4       | Fh<br>RW         | <b>Upstream Port 16 GT/s Port Lane 10 Transmitter Preset (UP16L10TP):</b><br>Field contains the Transmit Preset value sent or received during Port 16 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 3:0       | Fh<br>RW         | <b>Downstream Port 16 GT/s Lane 10 Transmitter Preset (DP16L10TP):</b><br>Transmitter Preset used for 16 GT/s 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.  |

### 3.5.90 Physical Layer 16.0 GT/s Lane 1213 Equalization Control Register (PL16L1213EC) – Offset AC8h

Physical Layer 16.0 GT/s Lane 1213 Equalization Control Register

| Type | Size   | Offset        | Default |
|------|--------|---------------|---------|
| MMIO | 16 bit | DMIBAR + AC8h | FFFFh   |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 15:12     | Fh<br>RW         | <b>Upstream Port 16 GT/s Port Lane 13 Transmitter Preset (UP16L13TP):</b><br>Field contains the Transmit Preset value sent or received during Port 16 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 11:8      | Fh<br>RW         | <b>Downstream Port 16 GT/s Lane 13 Transmitter Preset (DP16L13TP):</b><br>Transmitter Preset used for 16 GT/s 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.  |
| 7:4       | Fh<br>RW         | <b>Upstream Port 16 GT/s Port Lane 12 Transmitter Preset (UP16L12TP):</b><br>Field contains the Transmit Preset value sent or received during Port 16 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 3:0       | Fh<br>RW         | <b>Downstream Port 16 GT/s Lane 12 Transmitter Preset (DP16L12TP):</b><br>Transmitter Preset used for 16 GT/s 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.  |

### 3.5.91 Physical Layer 16.0 GT/s Lane 1415 Equalization Control Register (PL16L1415EC) – Offset ACAh

Physical Layer 16.0 GT/s Lane 1415 Equalization Control Register

| Type | Size   | Offset        | Default |
|------|--------|---------------|---------|
| MMIO | 16 bit | DMIBAR + ACAh | FFFh    |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 15:12     | Fh<br>RW         | <b>Upstream Port 16 GT/s Port Lane 15 Transmitter Preset (UP16L15TP):</b><br>Field contains the Transmit Preset value sent or received during Port 16 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 11:8      | Fh<br>RW         | <b>Downstream Port 16 GT/s Lane 15 Transmitter Preset (DP16L15TP):</b><br>Transmitter Preset used for 16 GT/s 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.  |
| 7:4       | Fh<br>RW         | <b>Upstream Port 16 GT/s Port Lane 14 Transmitter Preset (UP16L14TP):</b><br>Field contains the Transmit Preset value sent or received during Port 16 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 3:0       | Fh<br>RW         | <b>Downstream Port 16 GT/s Lane 14 Transmitter Preset (DP16L14TP):</b><br>Transmitter Preset used for 16 GT/s 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.  |

### 3.5.92 Device ID Override (DIDOVR) – Offset D00h

Device ID Override

| Type | Size   | Offset        | Default   |
|------|--------|---------------|-----------|
| MMIO | 32 bit | DMIBAR + D00h | 00000000h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 31:25     | 0h<br>RO         | <b>Reserved</b>   |
| 24        | 0h<br>RW/L       | <b>Device Identifier 0 Override Enable (DID0OVR):</b><br>When this register is set, the register field DID0OVR will override DID bit [6:0]<br>This register is Read-Only if LPCR.DIDOVR_LOCK field is set<br><b>Locked by:</b> LPCR.DIDOVR_LOCK |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 23:16     | 00h<br>RW        | <b>Device Identifier 0 Override (DID0OVR):</b><br>These bits will override the current DID bit[6:0] using the lower 7-bit of this register   |
| 15:9      | 0h<br>RO         | <b>Reserved</b>  |
| 8         | 0h<br>RW/L       | <b>Device Identifier 2 Override Enable (DID2OVRE):</b><br>When this register is set, the register field DID0OVR will override DID bit [6:0]<br>This register is Read-Only if LPCR.DIDOVR_LOCK field is set<br><b>Locked by:</b> LPCR.DIDOVR_LOCK |
| 7:0       | 00h<br>RW        | <b>Device Identifier 2 Override (DID2OVR):</b><br>These bits will override the current DID bit[6:0] using the lower 7-bit of this register   |

### 3.5.93 Physical Layer 16.0 GT/s Margining Extended Capability Header (PL16MECH) – Offset EDCh

Physical Layer 16.0 GT/s Margining Extended Capability Header

| Type | Size   | Offset        | Default   |
|------|--------|---------------|-----------|
| MMIO | 32 bit | DMIBAR + EDCh | 00010027h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 31:20     | 000h<br>RW/O     | <b>Next Capability Offset (NCO):</b><br>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.<br>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.<br>The bottom 2 bits of this offset are Reserved and must be implemented as 00b although software must mask them to allow for future uses of these bits. |
| 19:16     | 1h<br>RW/O       | <b>Capability Version (CV):</b><br>This field is a PCI-SIG defined version number that indicates the version of the Capability structure present.   |
| 15:0      | 0027h<br>RW/O    | <b>PCI Express Extended Capability ID (PCIECID):</b><br>This field is a PCI-SIG defined ID number that indicates the nature and format of the Extended Capability.<br>Extended Capability ID for the Physical Layer 16.0 GT/s Margining Capability  |

### 3.5.94 Physical Layer 16.0 GT/s Margining Port Capabilities and Port Status (PL16MPCPS) – Offset EE0h

Physical Layer 16.0 GT/s Margining Port Capabilities and Port Status

| Type | Size   | Offset        | Default   |
|------|--------|---------------|-----------|
| MMIO | 32 bit | DMIBAR + EE0h | 00000000h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 31:18     | 0h<br>RO         | <b>Reserved</b>  |
| 17        | 0h<br>RO/V       | <b>Margining Software Ready (MARGINSWRDY):</b><br>When Margining uses Driver Software is Set, then this bit, when Set, indicates that the required software has performed the required initialization. The value of this bit is Undefined if Margining users Driver Software is Clear.   |
| 16        | 0h<br>RO/V       | <b>Margining Ready (MARGINRDY):</b><br>Indicates when the Margining feature is ready to accept margining commands. Behavior is undefined if this bit is Clear and, for any Lane, any of the Receiver Number, Margin Type, Usage Model, or Margin Payload fields are written.<br>If Margining uses Driver Software is Set, Margining Ready must be Set no later than 100 ms after the later of Margining Software Ready becoming Set or the link training to 16.0 GT/s.<br>If Margining uses Driver Software is Clear, Margining Ready must be Set no later than 100 ms after the Link trains to 16.0 GT/s. |
| 15:1      | 0h<br>RO         | <b>Reserved</b>  |
| 0         | 0h<br>RW/O       | <b>Margining uses Driver Software (MARGINDRISW):</b><br>If Set, indicates that Margining is partially implemented using Device Driver software. Margining Software Ready indicates when this software is initialized. If Clear, Margining does not require device driver software. In this case the value read from Margining Software Ready is undefined  |

### 3.5.95 Physical Layer 16.0 GT/s Lane0 Margin Control and Status Register (PL16L0MCS) – Offset EE4h

Physical Layer 16.0 GT/s Lane0 Margin Control and Status Register

| Type | Size   | Offset        | Default   |
|------|--------|---------------|-----------|
| MMIO | 32 bit | DMIBAR + EE4h | 00009C38h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 31:24     | 00h<br>RO/V      | <b>Margin Payload Status (MPSTS):</b><br>This field is only meaningful, when the Margin Type<br>This field must be reset to the default value if the Port goes to DL_Down status. |



| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 23        | 0h<br>RO         | <b>Reserved</b>   |
| 22        | 0h<br>RO/V       | <b>Usage Model Status (UMS):</b><br>This field must be reset to the default value if the Port goes to DL_Down status.   |
| 21:19     | 0h<br>RO/V       | <b>Margin Type Status (MTS):</b><br>This field must be reset to the default value if the Port goes to DL_Down status.   |
| 18:16     | 0h<br>RO/V       | <b>Receiver Number Status (RNS):</b><br>This field must be reset to the default value if the Port goes to DL_Down status.   |
| 15:8      | 9Ch<br>RW        | <b>Margin Payload (MP):</b><br>This fields value is used in conjunction with the Margin Type field.<br>The default value is 9Ch.<br>This field must be reset to the default value if the Port goes to DL_Down status. |
| 7         | 0h<br>RO         | <b>Reserved</b>   |
| 6         | 0h<br>RW         | <b>Usage Model (UM):</b><br>The default value is 0b.<br>This field must be reset to the default value if the Port goes to DL_Down status.   |
| 5:3       | 7h<br>RW         | <b>Margin Type (MT):</b><br>The default value is 111b.<br>This field must be reset to the default value if the Port goes to DL_Down status.   |
| 2:0       | 0h<br>RW         | <b>Receiver Number (RN):</b><br>The default value is 000b.<br>This field must be reset to the default value if the Port goes to DL_Down status.   |

### 3.5.96 Physical Layer 16.0 GT/s Lane1 Margin Control and Status Register (PL16L1MCS) – Offset EE8h

Physical Layer 16.0 GT/s Lane1 Margin Control and Status Register

**Note:** Bit definitions are the same as [PL16L0MCS](#), offset EE4h.

### 3.5.97 Physical Layer 16.0 GT/s Lane2 Margin Control and Status Register (PL16L2MCS) – Offset EECh

Physical Layer 16.0 GT/s Lane2 Margin Control and Status Register

**Note:** Bit definitions are the same as [PL16L0MCS](#), offset EE4h.

### 3.5.98 Physical Layer 16.0 GT/s Lane3 Margin Control and Status Register (PL16L3MCS) – Offset EF0h

Physical Layer 16.0 GT/s Lane3 Margin Control and Status Register

**Note:** Bit definitions are the same as [PL16L0MCS](#), offset EE4h.

### 3.5.99 Physical Layer 16.0 GT/s Lane4 Margin Control and Status Register (PL16L4MCS) – Offset EF4h

Physical Layer 16.0 GT/s Lane4 Margin Control and Status Register



**Note:** Bit definitions are the same as [PL16L0MCS](#), offset EE4h.

### **3.5.100 Physical Layer 16.0 GT/s Lane5 Margin Control and Status Register (PL16L5MCS) – Offset EF8h**

Physical Layer 16.0 GT/s Lane5 Margin Control and Status Register

**Note:** Bit definitions are the same as [PL16L0MCS](#), offset EE4h.

### **3.5.101 Physical Layer 16.0 GT/s Lane6 Margin Control and Status Register (PL16L6MCS) – Offset EFCh**

Physical Layer 16.0 GT/s Lane6 Margin Control and Status Register

**Note:** Bit definitions are the same as [PL16L0MCS](#), offset EE4h.

### **3.5.102 Physical Layer 16.0 GT/s Lane7 Margin Control and Status Register (PL16L7MCS) – Offset F00h**

Physical Layer 16.0 GT/s Lane7 Margin Control and Status Register

**Note:** Bit definitions are the same as [PL16L0MCS](#), offset EE4h.

### **3.5.103 Physical Layer 16.0 GT/s Lane8 Margin Control and Status Register (PL16L8MCS) – Offset F04h**

Physical Layer 16.0 GT/s Lane8 Margin Control and Status Register

**Note:** Bit definitions are the same as [PL16L0MCS](#), offset EE4h.

### **3.5.104 Physical Layer 16.0 GT/s Lane9 Margin Control and Status Register (PL16L9MCS) – Offset F08h**

Physical Layer 16.0 GT/s Lane9 Margin Control and Status Register

**Note:** Bit definitions are the same as [PL16L0MCS](#), offset EE4h.

### **3.5.105 Physical Layer 16.0 GT/s Lane10 Margin Control and Status Register (PL16L10MCS) – Offset F0Ch**

Physical Layer 16.0 GT/s Lane10 Margin Control and Status Register

**Note:** Bit definitions are the same as [PL16L0MCS](#), offset EE4h.

### **3.5.106 Physical Layer 16.0 GT/s Lane11 Margin Control and Status Register (PL16L11MCS) – Offset F10h**

Physical Layer 16.0 GT/s Lane11 Margin Control and Status Register

**Note:** Bit definitions are the same as [PL16L0MCS](#), offset EE4h.

### **3.5.107 Physical Layer 16.0 GT/s Lane12 Margin Control and Status Register (PL16L12MCS) — Offset F14h**

Physical Layer 16.0 GT/s Lane12 Margin Control and Status Register

**Note:** Bit definitions are the same as PL16L0MCS, offset EE4h.

### **3.5.108 Physical Layer 16.0 GT/s Lane13 Margin Control and Status Register (PL16L13MCS) — Offset F18h**

Physical Layer 16.0 GT/s Lane13 Margin Control and Status Register

**Note:** Bit definitions are the same as PL16L0MCS, offset EE4h.

### **3.5.109 Physical Layer 16.0 GT/s Lane14 Margin Control and Status Register (PL16L14MCS) — Offset F1Ch**

Physical Layer 16.0 GT/s Lane14 Margin Control and Status Register

**Note:** Bit definitions are the same as PL16L0MCS, offset EE4h.

### **3.5.110 Physical Layer 16.0 GT/s Lane15 Margin Control and Status Register (PL16L15MCS) — Offset F20h**

Physical Layer 16.0 GT/s Lane15 Margin Control and Status Register

**Note:** Bit definitions are the same as PL16L0MCS, offset EE4h.



## 3.6 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.

### 3.6.1 Summary of Registers

Table 3-7. 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     | 4            | Egress Port Virtual Channel Control (EPPVCCTL_0_0_0_PXPEPBAR)                | 00000000h     |
| 10h    | 4            | Egress Port Virtual Channel 0 Resource Capability (EPVCORCAP_0_0_0_PXPEPBAR) | 00000001h     |
| 14h    | 4            | Egress Port Virtual Channel 0 Resource Control (EPVCORCTL_0_0_0_PXPEPBAR)    | 800000FFh     |
| 1Ah    | 2            | Egress Port Virtual Channel 0 Resource Status (EPVCORSTS_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 Capability 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     |
| 80h    | 4            | Egress Port Link Element Declaration 4 (EPLE4D_0_0_0_PXPEPBAR)               | 04000002h     |

| Offset | Size (Bytes) | Register Name (Register Symbol)   | Default Value |
|--------|--------------|---|---------------|
| 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     |
| A0h    | 4            | Miscellaneous Port Configuration PXPEPBAR (MPCP)                            | 00000000h     |

### 3.6.2 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<br>RO       | <b>Pointer to Next Capability (PNC):</b><br>This field contains the offset to the next PCI Express capability structure in the linked list of capabilities (Link Declaration Capability).<br>Bits [21:20] are reserved and software must mask them to allow for future uses of these bits |
| 19:16     | 1h<br>RO         | <b>PCI Express Virtual Channel Capability Version (PCIEVCCV):</b><br>Hardwired to 1 to indicate compliances with the 1.1 version of the PCI Express specification.<br>Note: This version does not change for 2.0 compliance.  |
| 15:0      | 0002h<br>RO      | <b>Extended Capability ID (ECID):</b><br>Value of 0002h identifies this linked list item (capability structure) as being for PCI Express Virtual Channel registers.   |

### 3.6.3 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<br>RO         | <b>Reserved</b>  |
| 11:10     | 0h<br>RO         | <b>Port Arbitration Table Entry Size (PATES):</b><br>Indicates that the size of the Port Arbitration table entry is 1 bit.   |
| 9:8       | 0h<br>RO         | <b>Reference Clock (RC):</b><br>Indicates the reference clock for Virtual Channels that support time-based WRR Port Arbitration. 00:100 ns   |
| 7         | 0h<br>RO         | <b>Reserved</b>  |
| 6:4       | 0h<br>RO         | <b>Low Priority Extended Virtual Channel Count (LPEVCC):</b><br>Indicates the number of Virtual Channels (extended).<br>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<br>RO         | <b>Reserved</b>  |
| 2:0       | 1h<br>RW/L       | <b>Extended Virtual Channel Count (EVCC):</b><br>Indicates the number of (extended) Virtual Channels in addition to the default Virtual Channel supported by the device.<br><b>Locked by:</b> MPCP.SRL   |

### 3.6.4 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<br>RO        | <b>VC Arbitration Table Offset (VCATO):</b><br>This field is reserved for Virtual Channel Arbitration Table Offset (VCATO) |

| Bit Range | Default & Access | Field Name (ID): Description |
|-----------|------------------|------------------------------|
| 23:0      | 0h<br>RO         | <b>Reserved</b>              |

### 3.6.5 Egress Port Virtual Channel Control (EPPVCCTL\_0\_0\_0\_PXPEPBAR) – Offset Ch

Egress Port Virtual Channel Control

| Type | Size   | Offset        | Default  |
|------|--------|---------------|----------|
| MMIO | 32 bit | PXPEPBAR + Ch | 0000000h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 31:4      | 0h<br>RO         | <b>Reserved</b>  |
| 3:1       | 0h<br>RW         | <b>VC Arbitration Select (VCAS):</b><br>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).<br>This field cannot be modified when more than one Virtual Channel in the LPVC group is enabled. |
| 0         | 0h<br>RO         | <b>Load Virtual Channel Arbitration Table (LVCAT):</b><br>This field is reserved for Load Virtual Channel Arbitration Table (LVCAT)  |

### 3.6.6 Egress Port Virtual Channel 0 Resource Capability (EPVCORCAP\_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<br>RO        | <b>Port Arbitration Table Offset (PATO):</b><br>No VC0 port arbitration necessary. |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 23        | 0h<br>RO         | <b>Reserved</b>   |
| 22:16     | 00h<br>RO        | <b>Maximum Time Slots (MTS):</b><br>No VC0 port arbitration necessary.  |
| 15        | 0h<br>RO         | <b>Reject Snoop Transactions (RSNPT):</b><br>0: Transactions with or without the No Snoop bit set within the TLP header are allowed on this VC.<br>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<br>RO         | <b>Reserved</b>   |
| 7:0       | 01h<br>RO        | <b>Port Arbitration Capability (PAC):</b><br>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.   |

### 3.6.7 Egress Port Virtual Channel 0 Resource Control (EPVCORCTL\_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 | 80000FFh |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 31        | 1h<br>RO         | <b>VC0 Enable (VCOE):</b><br>For VC0 this is hardwired to 1 and read only as VC0 can never be disabled.  |
| 30:27     | 0h<br>RO         | <b>Reserved</b>  |
| 26:24     | 0h<br>RO         | <b>VC0 ID (VCOID):</b><br>Assigns a Virtual Channel ID to the Virtual Channel resource. For VC0 this is hardwired to 0 and read only.  |
| 23:20     | 0h<br>RO         | <b>Reserved</b>  |
| 19:17     | 0h<br>RW         | <b>Port Arbitration Select (PAS):</b><br>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<br>RO         | <b>Reserved</b>  |



| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 7:1       | 7Fh<br>RW        | <b>TC/VC0 Map (TCVCOM):</b><br>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<br>RO         | <b>TC0/VC0 Map (TC0VCOM):</b><br>Traffic Class 0 is always routed to VC0.  |

### 3.6.8 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<br>RO         | <b>Reserved</b>   |
| 1         | 0h<br>RO/V       | <b>VC0 Negotiation Pending (VCONP):</b><br>0: The Virtual Channel negotiation is complete.<br>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<br>RO         | <b>Reserved</b>   |

### 3.6.9 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<br>RO        | <b>Port Arbitration Table Offset (PATO):</b><br>No VC0 port arbitration is necessary.   |
| 23        | 0h<br>RO         | <b>Reserved</b>   |
| 22:16     | 00h<br>RO        | <b>Maximum Time Slots (MTS):</b><br>No VC0 port arbitration is necessary.   |
| 15        | 1h<br>RO         | <b>Reject Snoop Transactions (RSNPT):</b><br>0: Transactions with or without the No Snoop bit set within the TLP header are allowed on this VC.<br>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<br>RO         | <b>Reserved</b>   |
| 7:0       | 01h<br>RO        | <b>Port Arbitration Capability (PAC):</b><br>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.   |

### 3.6.10 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<br>RW         | <p><b>VC1 Enable (VC1E):</b><br/>           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).<br/>           0: Virtual Channel is disabled.<br/>           1: Virtual Channel is enabled.<br/>           See exceptions in note below.<br/>           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.<br/>           Notes:<br/>           1. To enable a Virtual Channel, the Virtual Channel Enable bits for that Virtual Channel must be set in both Components on a Link.<br/>           2. To disable a Virtual Channel, the Virtual Channel Enable bits for that Virtual Channel must be cleared in both Components on a Link.<br/>           3. Software must ensure that no traffic is using a Virtual Channel at the time it is disabled.<br/>           4. Software must fully disable a Virtual Channel in both Components on a Link before re-enabling the Virtual Channel.</p> |
| 30:27     | 0h<br>RO         | <b>Reserved</b>   |
| 26:24     | 1h<br>RW         | <p><b>VC1 ID (VC1ID):</b><br/>           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.</p>   |
| 23:20     | 0h<br>RO         | <b>Reserved</b>   |
| 19:17     | 0h<br>RW         | <p><b>Port Arbitration Select (PAS):</b><br/>           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.</p>   |
| 16:8      | 0h<br>RO         | <b>Reserved</b>   |
| 7:1       | 00h<br>RW        | <p><b>TC/VC1 Map (TCVC1M):</b><br/>           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.</p>   |
| 0         | 0h<br>RO         | <p><b>TC0/VC1 Map (TC0VC1M):</b><br/>           Traffic Class 0 is always routed to VC0.</p>  |



### 3.6.11 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<br>RO         | <b>Reserved</b>  |
| 1         | 0h<br>RO/V       | <b>VC1 Negotiation Pending (VC1NP):</b><br>0: The Virtual Channel negotiation is complete.<br>1: The Virtual Channel resource is still in the process of negotiation (initialization or disabling).<br>For this non-default Virtual Channel, software may use this bit when enabling or disabling the VC.<br>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<br>RO         | <b>Port Arbitration Table Status (PATS):</b><br>This field is reserved for Port Arbitration Table Status (PATS)  |

### 3.6.12 Egress Port Capability Declaration (EPRCLDECH\_0\_0\_0\_PXPEPBAR) – Offset 40h

Egress Port Capability 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<br>RO       | <b>Pointer to Next Capability (PNC):</b><br>This value terminates the PCI Express extended capabilities list associated with this RCRB.  |
| 19:16     | 1h<br>RO         | <b>Link Declaration Capability Version (LDCV):</b><br>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<br>RO      | <b>Extended Capability ID (ECID):</b><br>Value of 5h identifies this linked list item (capability structure) as being for PCI Express Link Declaration Capability. |

### 3.6.13 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<br>RO        | <b>Port Number (PN):</b><br>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<br>RW/L      | <b>Component ID (CID):</b><br>Identifies the physical component that contains this Root Complex Element.<br>BIOS Requirement: Must be initialized according to guidelines in the PCI Express* Isochronous/Virtual Channel Support Hardware Programming Specification (HPS).<br><b>Locked by:</b> MPCP.SRL |
| 15:8      | 05h<br>RO        | <b>Number of Link Entries (NLE):</b><br>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<br>RO         | <b>Reserved</b>   |
| 3:0       | 1h<br>RO         | <b>Element Type (ET):</b><br>Indicates the type of the Root Complex Element. Value of 1 h represents a port to system memory.   |

### 3.6.14 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<br>RO        | <b>Target Port Number (TPN):</b><br>Specifies the port number associated with the element targeted by this link entry (DMI).<br>The target port number is with respect to the component that contains this element as specified by the target component ID.   |
| 23:16     | 00h<br>RW/L      | <b>Target Component ID (TCID):</b><br>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).<br><b>Locked by:</b> MPCP.SRL |
| 15:2      | 0h<br>RO         | <b>Reserved</b>   |
| 1         | 0h<br>RO         | <b>Link Type (LTYP):</b><br>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<br>RW/L       | <b>Link Valid (LV):</b><br>0: Link Entry is not valid and will be ignored.<br>1: Link Entry specifies a valid link.<br><b>Locked by:</b> MPCP.SRL   |

### 3.6.15 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<br>RW/L   | <b>Low Link Address (LLA):</b><br>Memory mapped base address of the RCRB that is the target element (DMI) for this link entry.<br><b>Locked by:</b> MPCP.SRL |

| Bit Range | Default & Access | Field Name (ID): Description |
|-----------|------------------|------------------------------|
| 11:0      | 0h<br>RO         | <b>Reserved</b>              |

### 3.6.16 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<br>RO         | <b>Reserved</b>  |
| 7:0       | 00h<br>RW/L      | <b>Upper Link Address (ULA):</b><br>Memory mapped base address of the RCRB that is the target element (DMI) for this link entry.<br><b>Locked by:</b> MPCP.SRL |

### 3.6.17 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<br>RO        | <b>Target Port Number (TPN):</b><br>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<br>RW/L      | <b>Target Component ID (TCID):</b><br>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.<br>BIOS Requirement: Must be initialized according to guidelines in the PCI Express* Isochronous/Virtual Channel Support Hardware Programming Specification (HPS).<br><b>Locked by:</b> MPCP.SRL |
| 15:2      | 0h<br>RO         | <b>Reserved</b>   |
| 1         | 1h<br>RO         | <b>Link Type (LTYP):</b><br>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<br>RW/L       | <b>Link Valid (LV):</b><br>0: Link Entry is not valid and will be ignored.<br>1: Link Entry specifies a valid link.<br><b>Locked by:</b> MPCP.SRL   |

### 3.6.18 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.

**Note:** Bit definitions are the same as EPLE1A\_0\_0\_0\_PXPEPBAR, offset 58h.

### 3.6.19 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.

**Note:** Bit definitions are the same as EPULE1A\_0\_0\_0\_PXPEPBAR, offset 5Ch.

### 3.6.20 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<br>RO        | <b>Target Port Number (TPN):</b><br>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<br>RW/L      | <b>Target Component ID (TCID):</b><br>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.<br>BIOS Requirement: Must be initialized according to guidelines in the PCI Express* Isochronous/Virtual Channel Support Hardware Programming Specification (HPS).<br><b>Locked by:</b> MPCP.SRL |
| 15:2      | 0h<br>RO         | <b>Reserved</b>   |
| 1         | 1h<br>RO         | <b>Link Type (LTYP):</b><br>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<br>RW/L       | <b>Link Valid (LV):</b><br>0: Link Entry is not valid and will be ignored.<br>1: Link Entry specifies a valid link.<br><b>Locked by:</b> MPCP.SRL   |

### 3.6.21 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.

**Note:** Bit definitions are the same as [EPLE1A\\_0\\_0\\_0\\_PXPEPBAR](#), offset 58h.

### 3.6.22 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<br>RO         | <b>Reserved</b>   |
| 7:0       | 00h<br>RW/L      | <b>Upper Link Address (ULA):</b><br>Memory mapped base address of the RCRB that is the target element (DMI) for this link entry<br><b>Locked by:</b> MPCP.SRL |

### 3.6.23 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<br>RO        | <b>Target Port Number (TPN):</b><br>Specifies the port number associated with the element targeted by this link entry (PEG1.2).<br>The target port number is with respect to the component that contains this element as specified by the target component ID.   |
| 23:16     | 00h<br>RW/L      | <b>Target Component ID (TCID):</b><br>Identifies the physical or logical component that is targeted by this link entry. A value of 0 is reserved. Component IDs start at 1.<br>This value is a mirror of the value in the Component ID field of all elements in this component.<br>BIOS Requirement: Must be initialized according to guidelines in the PCI Express* Isochronous/Virtual Channel Support Hardware Programming Specification (HPS).<br><b>Locked by:</b> MPCP.SRL |
| 15:2      | 0h<br>RO         | <b>Reserved</b>  |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 1         | 1h<br>RO         | <b>Link Type (LTYP):</b><br>Indicates that the link points to configuration space of the integrated device which controls the x16 root port for PEG1.<br>The link address specifies the configuration address (segment, bus, device, function) of the target root port. |
| 0         | 0h<br>RW/L       | <b>Link Valid (LV):</b><br>0: Link Entry is not valid and will be ignored.<br>1: Link Entry specifies a valid link.<br><b>Locked by:</b> MPCP.SRL   |

### 3.6.24 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.

**Note:** Bit definitions are the same as EPLE1A\_0\_0\_0\_PXPEPBAR, offset 58h.

### 3.6.25 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.

**Note:** Bit definitions are the same as EPULE1A\_0\_0\_0\_PXPEPBAR, offset 5Ch.

### 3.6.26 Egress Port Link Element Declaration 5 (EPL5D\_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<br>RO        | <b>Target Port Number (TPN):</b><br>Specifies the port number associated with the element targeted by this link entry (PEG6.0).<br>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<br>RW/L      | <b>Target Component ID (TCID):</b><br>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.<br>BIOS Requirement: Must be initialized according to guidelines in the PCI Express* Isochronous/Virtual Channel Support Hardware Programming Specification (HPS).<br><b>Locked by:</b> MPCP.SRL |
| 15:2      | 0h<br>RO         | <b>Reserved</b>   |
| 1         | 1h<br>RO         | <b>Link Type (LTYP):</b><br>Indicates that the link points to configuration space of the integrated device which controls the x16 root port for PEG1.<br>The link address specifies the configuration address (segment, bus, device, function) of the target root port.   |
| 0         | 0h<br>RW/L       | <b>Link Valid (LV):</b><br>0: Link Entry is not valid and will be ignored.<br>1: Link Entry specifies a valid link.<br><b>Locked by:</b> MPCP.SRL   |

### 3.6.27 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.

**Note:** Bit definitions are the same as EPLE1A\_0\_0\_0\_PXPEPBAR, offset 58h.

### 3.6.28 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<br>RO         | <b>Reserved</b>  |
| 7:0       | 00h<br>RW/L      | <b>Upper Link Address (ULA):</b><br>Upper Link Address: Memory mapped base address of the RCRB that is the target element (DMI) for this link entry.<br><b>Locked by:</b> MPCP.SRL |

### 3.6.29 Miscellaneous Port Configuration PXPEPBAR (MPCP) – Offset A0h

Miscellaneous Port Configuration PXPEPBAR

| Type | Size   | Offset         | Default   |
|------|--------|----------------|-----------|
| MMIO | 32 bit | PXPEPBAR + A0h | 00000000h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 31        | 0h<br>RW/O       | <b>Secured Register Lock (SRL):</b><br>When this bit is set, all the secured registers in PXPEPBAR will be locked and will be Read-Only. Refer to register description |
| 30:0      | 0h<br>RO         | <b>Reserved</b>  |



## 3.7 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.

### 3.7.1 Summary of Registers

**Table 3-8. 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         |
| A8h    | 4            | Invalidation Event Address Register (IEADDR_REG_0_0_0_VTDBAR)    | 00000000h         |

| Offset | Size (Bytes) | Register Name (Register Symbol)                                       | Default Value     |
|--------|--------------|---|-------------------|
| 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 |

### 3.7.2 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 | VTDPVCOBAR + 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<br>RO         | <b>Reserved</b>   |
| 7:4       | 1h<br>RO         | <b>Major Version Number (MAJOR):</b><br>Indicates supported architecture version.       |
| 3:0       | 0h<br>RO         | <b>Minor Version Number (MINOR):</b><br>Indicates supported architecture minor version. |

### 3.7.3 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<br>RO         | <b>Reserved</b>   |
| 56        | 0h<br>RO         | <b>First Level 64-KByte Page SupportP (FL1GP):</b><br>A value of 1 in this field indicates 1-GByte page size is supported for first-level translation.  |
| 55        | 1h<br>RO         | <b>Read Draining (DRD):</b> <ul style="list-style-type: none"> <li>0 = Hardware does not support draining of DMA read requests.</li> <li>1 = Hardware supports draining of DMA read requests.</li> </ul>  |
| 54        | 1h<br>RO         | <b>Write Draining (DWD):</b> <ul style="list-style-type: none"> <li>0 = Hardware does not support draining of DMA write requests.</li> <li>1 = Hardware supports draining of DMA write requests.</li> </ul>   |
| 53:48     | 12h<br>RO        | <b>Maximum Address Mask Value (MAMV):</b><br>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<br>RO        | <b>Number of Fault-Recording Registers (NFR):</b><br>Number of fault recording registers is computed as N+1, where N is the value reported in this field.<br>Implementations must support at least one fault recording register (NFR = 0) for each remapping hardware unit in the platform.<br>The maximum number of fault recording registers per remapping hardware unit is 256.  |
| 39        | 1h<br>RO         | <b>Page Selective Invalidation (PSI):</b> <ul style="list-style-type: none"> <li>0 = Hardware supports only domain and global invalidates for IOTLB.{*}1 = Hardware supports page selective, domain and global invalidates for IOTLB.</li> </ul> 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<br>RO         | <b>Reserved</b>   |



| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 37:34     | 3h<br>RO         | <p><b>Second Level Large Page Support (SLLPS):</b><br/>This field indicates the super page sizes supported by hardware.<br/>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:</p> <ul style="list-style-type: none"> <li>• 0 = 21-bit offset to page frame (2MB)</li> <li>• 1 = 30-bit offset to page frame (1GB)</li> <li>• 2 = 39-bit offset to page frame (512GB)</li> <li>• 3 = 48-bit offset to page frame (1TB)</li> </ul> <p>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.</p>  |
| 33:24     | 040h<br>RO       | <p><b>Fault-Recording Register Offset (FRO):</b><br/>This field specifies the location to the first fault recording register relative to the register base address of this remapping hardware unit.<br/>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 <math>X+(16*Y)</math>.</p>   |
| 23        | 0h<br>RO         | <b>Reserved</b>  |
| 22        | 1h<br>RO         | <p><b>Zero Length Read (ZLR):</b></p> <ul style="list-style-type: none"> <li>• 0 = Indicates the remapping hardware unit blocks (and treats as fault) zero length DMA read requests to write-only pages.</li> <li>• 1 = Indicates the remapping hardware unit supports zero length DMA read requests to write-only pages.</li> </ul> <p>DMA remapping hardware implementations are recommended to report ZLR field as Set.</p>   |
| 21:16     | 26h<br>RO        | <p><b>Maximum Guest Address Width (MGAW):</b><br/>This field indicates the maximum DMA virtual addressability supported by remapping hardware. The Maximum Guest Address Width (MGAW) is computed as <math>(N+1)</math>, 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.<br/>If the value in this field is X, untranslated and translated DMA requests to addresses above <math>2(x+1)-1</math> are always blocked by hardware. Translations requests to address above <math>2(x+1)-1</math> from allowed devices return a null Translation Completion Data Entry with <math>R=W=0</math>.<br/>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).<br/>Implementations are recommended to support MGAW at least equal to the physical addressability (host address width) of the platform.</p> |
| 15:13     | 0h<br>RO         | <b>Reserved</b>  |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 12:8      | 04h<br>RO        | <p><b>Supported Adjusted Guest Address Widths (SAGAW):</b></p> <p>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.</p> <p>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:</p> <ul style="list-style-type: none"> <li>• 0 = 30-bit AGAW (2-level page table)</li> <li>• 1 = 39-bit AGAW (3-level page table)</li> <li>• 2 = 48-bit AGAW (4-level page table)</li> <li>• 3 = 57-bit AGAW (5-level page table)</li> <li>• 4 = 64-bit AGAW (6-level page table)</li> </ul> <p>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.</p> |
| 7         | 0h<br>RO         | <p><b>Caching Mode (CM):</b></p> <ul style="list-style-type: none"> <li>• 0 = Not-present and erroneous entries are not cached in any of the remapping caches. Invalidation is 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.</li> <li>• 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.</li> </ul> <p>Hardware implementations of this architecture must support a value of 0 in this field.</p>  |
| 6         | 1h<br>RO         | <p><b>Protected High-Memory Region (PHMR):</b></p> <ul style="list-style-type: none"> <li>• 0 = Indicates protected high-memory region is not supported.</li> <li>• 1 = Indicates protected high-memory region is supported.</li> </ul>   |
| 5         | 1h<br>RO         | <p><b>Protected Low-Memory Region (PLMR):</b></p> <ul style="list-style-type: none"> <li>• 0 = Indicates protected low-memory region is not supported.</li> <li>• 1 = Indicates protected low-memory region is supported.</li> </ul>  |
| 4         | 0h<br>RO         | <p><b>Required Write-Buffer Flushing (RWBF):</b></p> <ul style="list-style-type: none"> <li>• 0 = Indicates no write-buffer flushing is needed to ensure changes to memory-resident structures are visible to hardware.</li> <li>• 1 = Indicates software must explicitly flush the write buffers to ensure updates made to memory-resident remapping structures are visible to hardware.</li> </ul>  |
| 3         | 0h<br>RO         | <p><b>Advanced Fault Logging (AFL):</b></p> <ul style="list-style-type: none"> <li>• 0 = Indicates advanced fault logging is not supported. Only primary fault logging is supported.</li> <li>• 1 = Indicates advanced fault logging is supported.</li> </ul>   |
| 2:0       | 2h<br>RO         | <p><b>Number of Domains Supported (ND):</b></p> <ul style="list-style-type: none"> <li>• 000b = Hardware supports 4-bit domain-ids with support for up to 16 domains.</li> <li>• 001b = Hardware supports 6-bit domain-ids with support for up to 64 domains.</li> <li>• 010b = Hardware supports 8-bit domain-ids with support for up to 256 domains.</li> <li>• 011b = Hardware supports 10-bit domain-ids with support for up to 1024 domains.</li> <li>• 100b = Hardware supports 12-bit domain-ids with support for up to 4K domains.</li> <li>• 100b = Hardware supports 14-bit domain-ids with support for up to 16K domains.</li> <li>• 110b = Hardware supports 16-bit domain-ids with support for up to 64K domains.</li> <li>• 111b = Reserved.</li> </ul>   |

### 3.7.4 Extended Capability Register (ECAP\_REG\_0\_0\_0\_VTD BAR) – Offset 10h

Register to report remapping hardware extended capabilities.

| Type | Size   | Offset           | Default          |
|------|--------|------------------|------------------|
| MMIO | 64 bit | VTDPVCOBAR + 10h | 000000000F050DAh |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| R           | R          | R         |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 63:41     | 0h<br>RO         | <b>Reserved</b>   |
| 40        | 0h<br>RO         | <b>Process Address Space ID Support (PASID):</b> <ul style="list-style-type: none"> <li>0 = Hardware does not support requests tagged with Process Address Space IDs.</li> <li>1 = Hardware supports requests tagged with Process Address Space IDs.</li> </ul>   |
| 39:35     | 00h<br>RO        | <b>PASID Size Supported (PSS):</b><br>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.<br>This field is valid only when PASID field is reported as Set. |
| 34        | 0h<br>RO         | <b>Extended Accessed Flag Support (EAFS):</b> <ul style="list-style-type: none"> <li>0 = Hardware does not support the extended-accessed (EA) bit in first-level paging-structure entries.</li> <li>1 = Hardware supports the extended accessed (EA) bit in first-level paging-structure entries.</li> </ul> This field is valid only when PASID field is reported as Set.  |
| 33        | 0h<br>RO         | <b>No Write Flag Support (NWFS):</b> <ul style="list-style-type: none"> <li>0 = Hardware ignores the No Write (NW) flag in Device-TLB translation requests, and behaves as if NW is always 0.</li> <li>1 = Hardware supports the No Write (NW) flag in Device-TLB translation requests.</li> </ul> This field is valid only when Device-TLB support (DT) field is reported as Set.  |
| 32        | 0h<br>RO         | <b>PASID-Only Translations (POT):</b> <ul style="list-style-type: none"> <li>0 = Hardware does not support PASID-only Translation Type in extended-context-entries.</li> <li>1 = Hardware supports PASID-only Translation Type in extended-context-entries.</li> </ul> This field is valid only when PASID field is reported as Set.  |
| 31        | 0h<br>RO         | <b>Supervisor Request Support (SRS):</b> <ul style="list-style-type: none"> <li>0 = H/W does not support requests-with-PASID seeking supervisor privilege.</li> <li>1 = H/W supports requests-with-PASID seeking supervisor privilege.</li> </ul> The field is valid only when PASID field is reported as Set.  |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 30        | 0h<br>RO         | <b>Execute Request Support (ERS):</b> <ul style="list-style-type: none"> <li>0 = H/W does not support requests-with-PASID seeking execute permission.</li> <li>1 = H/W supports requests-with-PASID seeking execute permission.</li> </ul> This field is valid only when PASID field is reported as Set.  |
| 29        | 0h<br>RO         | <b>Page Request Support (PRS):</b> <ul style="list-style-type: none"> <li>0 = Hardware does not support Page Requests.</li> <li>1 = Hardware supports Page Requests</li> </ul> This field is valid only when Device-TLB (DT) field is reported as Set.  |
| 28        | 0h<br>RO         | <b>ECAP Ignore (IGN):</b><br>Ignore this field  |
| 27        | 0h<br>RO         | <b>Deferred Invalidate Support (DIS):</b> <ul style="list-style-type: none"> <li>0 = Hardware does not support deferred invalidations of IOTLB and Device-TLB.</li> <li>1 = Hardware supports deferred invalidations of IOTLB and Device-TLB.</li> </ul> This field is valid only when PASID field is reported as Set.  |
| 26        | 0h<br>RO         | <b>Nested Translation Support (NEST):</b> <ul style="list-style-type: none"> <li>0 = Hardware does not support nested translations.</li> <li>1 = Hardware supports nested translations.</li> </ul> This field is valid only when PASID field is reported as Set.  |
| 25        | 0h<br>RO         | <b>Memory Type Support (MTS):</b> <ul style="list-style-type: none"> <li>0 = Hardware does not support Memory Type in first-level translation and Extended Memory type in second-level translation.</li> <li>1 = Hardware supports Memory Type in first-level translation and Extended Memory type in second-level translation.</li> </ul> This field is valid only when PASID and ECS fields are reported as Set.<br>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<br>RO         | <b>Extended Context Support (ECS):</b> <ul style="list-style-type: none"> <li>0 = Hardware does not support extended-root-entries and extended-context-entries.</li> <li>1 = Hardware supports extended-root-entries and extended-context-entries.</li> </ul> Implementations reporting PASID or PRS fields as Set, must report this field as Set.  |
| 23:20     | Fh<br>RO         | <b>Maximum Handle Mask Value (MHMV):</b><br>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).<br>This field is valid only when the IR field in Extended Capability register is reported as Set.  |
| 19:18     | 0h<br>RO         | <b>Reserved</b>   |
| 17:8      | 050h<br>RO       | <b>IOTLB Register Offset (IRO):</b><br>This field specifies the offset to the IOTLB registers relative to the register base address of this remapping hardware unit.<br>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<br>RO         | <b>Snoop Control (SC):</b> <ul style="list-style-type: none"> <li>0 = Hardware does not support 1-setting of the SNP field in the page-table entries.</li> <li>1 = Hardware supports the 1-setting of the SNP field in the page-table entries.</li> </ul>   |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 6         | 1h<br>RO         | <p><b>Pass Through (PT):</b></p> <ul style="list-style-type: none"> <li>0 = Hardware does not support pass-through translation type in context entries and extended-context-entries.</li> <li>1 = Hardware supports pass-through translation type in context entries and extended-context-entries.</li> </ul> <p>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.<br/>Hardware implementations supporting PASID must report a value of 1b in this field.</p>  |
| 5         | 0h<br>RO         | <b>Reserved</b>  |
| 4         | 1h<br>RO         | <p><b>Extended Interrupt Mode (EIM):</b></p> <ul style="list-style-type: none"> <li>0 = On Intel64 platforms, hardware supports only 8-bit APIC-IDs (xAPIC mode).</li> <li>1 = On Intel64 platforms, hardware supports 32-bit APIC-IDs (x2APIC mode).</li> </ul> <p>This field is valid only on Intel64 platforms reporting Interrupt Remapping support (IR field Set).</p>  |
| 3         | 1h<br>RO         | <p><b>Interrupt Remapping support (IR):</b></p> <ul style="list-style-type: none"> <li>0 = Hardware does not support interrupt remapping.</li> <li>1 = Hardware supports interrupt remapping.</li> </ul> <p>Implementations reporting this field as Set must also support Queued Invalidation (QI).</p>  |
| 2         | 0h<br>RO         | <p><b>Device-TLB Support (DT):</b></p> <ul style="list-style-type: none"> <li>0 = Hardware does not support device-IOTLBs.</li> <li>1 = Hardware supports Device-IOTLBs.</li> </ul> <p>Implementations reporting this field as Set must also support Queued Invalidation (QI).<br/>Hardware implementations supporting I/O Page Requests (PRS field Set in Extended Capability register) must report a value of 1b in this field.</p>  |
| 1         | 1h<br>RO         | <p><b>Queued Invalidation Support (QI):</b></p> <ul style="list-style-type: none"> <li>0 = Hardware does not support queued invalidations.</li> <li>1 = Hardware supports queued invalidations.</li> </ul>   |
| 0         | 0h<br>RO         | <p><b>Page-Walk Coherency (C):</b></p> <p>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.</p> <ul style="list-style-type: none"> <li>0 = Indicates hardware accesses to remapping structures are non-coherent.</li> <li>1 = Indicates hardware accesses to remapping structures are coherent.</li> </ul> <p>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.</p> |

### 3.7.5 Global Command Register (GCMD\_REG\_0\_0\_0\_VTD BAR) – 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<br>RW         | <p><b>Translation Enable (TE):</b><br/>Software writes to this field to request hardware to enable/disable DMA-remapping:</p> <ul style="list-style-type: none"> <li>0 = Disable DMA remapping.</li> <li>1 = Enable DMA remapping.</li> </ul> <p>Hardware reports the status of the translation enable operation through the TES field in the Global Status register.</p> <p>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.</p> <p>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.</p> <p>The value returned on a read of this field is undefined.</p>   |
| 30        | 0h<br>WO         | <p><b>Set Root Table Pointer (SRTP):</b><br/>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.</p> <p>Hardware reports the status of the Set Root Table Pointer operation through the RTPS field in the Global Status register.</p> <p>The Set Root Table Pointer operation must be performed before enabling or re-enabling (after disabling) DMA remapping through the TE field.</p> <p>.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.</p> <p>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.</p> <p>Clearing this bit has no effect. The value returned on read of this field is undefined.</p> |
| 29        | 0h<br>RO         | <p><b>Set Fault Log (SFL):</b><br/>This field is valid only for implementations supporting advanced fault logging.</p> <p>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.</p> <p>Hardware reports the status of the Set Fault Log operation through the FLS field in the Global Status register.</p> <p>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.</p> <p>Clearing this bit has no effect. The value returned on read of this field is undefined.</p>  |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 28        | 0h<br>RO         | <p><b>Enable Advanced Fault Logging (EAFL):</b><br/>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:</p> <ul style="list-style-type: none"> <li>0 = Disable advanced fault logging. In this case, translation faults are reported through the Fault Recording registers.</li> <li>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.</li> </ul> <p>The value returned on read of this field is undefined.</p>   |
| 27        | 0h<br>RO         | <p><b>Write Buffer Flush (WBF):</b><br/>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.</p>   |
| 26        | 0h<br>RW         | <p><b>Queued Invalidation Enable (QIE):</b><br/>This field is valid only for implementations supporting queued invalidations. Software writes to this field to enable or disable queued invalidations.</p> <ul style="list-style-type: none"> <li>0 = Disable queued invalidations.</li> <li>1 = Enable use of queued invalidations.</li> </ul> <p>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.</p>  |
| 25        | 0h<br>RW         | <p><b>Interrupt Remapping Enable (IRE):</b><br/>This field is valid only for implementations supporting interrupt remapping.</p> <ul style="list-style-type: none"> <li>0 = Disable interrupt-remapping hardware.</li> <li>1 = Enable interrupt-remapping hardware.</li> </ul> <p>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.</p> |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 24        | 0h<br>WO         | <p><b>Set Interrupt Remap Table Pointer (SIRTP):</b><br/>           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.</p> |
| 23        | 0h<br>RW         | <p><b>Compatibility Format Interrupt (CFI):</b><br/>           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.</p> <ul style="list-style-type: none"> <li>• 0 = Block Compatibility format interrupts.</li> <li>• 1 = Process Compatibility format interrupts as pass-through (bypass interrupt remapping).</li> </ul> <p>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.</p>  |
| 22:0      | 0h<br>RO         | <b>Reserved</b>  |

### 3.7.6 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<br>RO/V       | <p><b>Translation Enable Status (TES):</b><br/>This field indicates the status of DMA-remapping hardware.</p> <ul style="list-style-type: none"> <li>0 = DMA-remapping hardware is not enabled.</li> <li>1 = DMA-remapping hardware is enabled</li> </ul>  |
| 30        | 0h<br>RO/V       | <p><b>Root Table Pointer Status (RTPS):</b><br/>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.</p>  |
| 29        | 0h<br>RO         | <p><b>Fault Log Status (FLS):</b><br/>This field:</p> <ul style="list-style-type: none"> <li>Is cleared by hardware when software Sets the SFL field in the Global Command register.</li> <li>Is Set by hardware when hardware completes the Set Fault Log Pointer operation using the value provided in the Advanced Fault Log register.</li> </ul>   |
| 28        | 0h<br>RO         | <p><b>Advanced Fault Logging Status (AFLS):</b><br/>This field is valid only for implementations supporting advanced fault logging. It indicates the advanced fault logging status:</p> <ul style="list-style-type: none"> <li>0 = Advanced Fault Logging is not enabled.</li> <li>1 = Advanced Fault Logging is enabled.</li> </ul>   |
| 27        | 0h<br>RO         | <p><b>Write Buffer Flush Status (WBFS):</b><br/>This field is valid only for implementations requiring write buffer flushing. This field indicates the status of the write buffer flush command. It is:</p> <ul style="list-style-type: none"> <li>Set by hardware when software sets the WBF field in the Global Command register.</li> <li>Cleared by hardware when hardware completes the write buffer flushing operation.</li> </ul> |
| 26        | 0h<br>RO/V       | <p><b>Queued Invalidation Enable Status (QIES):</b><br/>This field indicates queued invalidation enable status.</p> <ul style="list-style-type: none"> <li>0 = queued invalidation is not enabled.</li> <li>1 = queued invalidation is enabled</li> </ul>  |
| 25        | 0h<br>RO/V       | <p><b>Interrupt Remapping Enable Status (IRES):</b><br/>This field indicates the status of Interrupt-remapping hardware.</p> <ul style="list-style-type: none"> <li>0 = Interrupt-remapping hardware is not enabled.</li> <li>1 = Interrupt-remapping hardware is enabled</li> </ul>   |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 24        | 0h<br>RO/V       | <b>Interrupt Remapping Pointer Status (IRTPS):</b><br>This field indicates the status of the interrupt remapping table pointer in hardware. This field is cleared by hardware when software sets the SIRTTP 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<br>RO/V       | <b>Compatibility Format Interrupt Status (CFIS):</b><br>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. <ul style="list-style-type: none"> <li>• 0 = Compatibility format interrupts are blocked.</li> <li>• 1 = Compatibility format interrupts are processed as pass-through (bypassing interrupt remapping).</li> </ul> |
| 22:0      | 0h<br>RO         | <b>Reserved</b>  |

### 3.7.7 Root Table Address Register (RTADDR\_REG\_0\_0\_0\_VTD BAR) – 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<br>00000h<br>RW | <b>Root Table Address (RTA):</b><br>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<br>RW                 | <b>Root Table Type (RTT):</b><br>This field specifies the type of root-table referenced by the Root Table Address (RTA) field: <ul style="list-style-type: none"> <li>• 0 = Root Table.</li> <li>• 1 = Extended Root Table</li> </ul>   |
| 10:0      | 0h<br>RO                 | <b>Reserved</b>   |

### 3.7.8 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 | 080000000000000h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 63        | 0h<br>RW/V       | <p><b>Invalidate Context Cache (ICC):</b><br/>           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.<br/>           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.<br/>           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.<br/>           Hardware implementations reporting write-buffer flushing requirement (RWBF=1 in Capability register) must implicitly perform a write buffer flush before invalidating the context cache.</p> |
| 62:61     | 0h<br>RW         | <p><b>Context Invalidation Request Granularity (CIRG):</b><br/>           Software provides the requested invalidation granularity through this field when setting the ICC field:</p> <ul style="list-style-type: none"> <li>• 00: Reserved.</li> <li>• 01: Global Invalidation request.</li> <li>• 10: Domain-selective invalidation request. The target domain-id must be specified in the DID field.</li> <li>• 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.</li> </ul> <p>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.</p>  |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 60:59     | 1h<br>RO/V       | <p><b>Context Actual Invalidation Granularity (CAIG):</b><br/>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).<br/>The following are the encodings for this field:</p> <ul style="list-style-type: none"> <li>• 00: Reserved.</li> <li>• 01: Global Invalidation performed. This could be in response to a global, domain-selective or device-selective invalidation request.</li> <li>• 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.</li> <li>• 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.</li> </ul> |
| 58:34     | 0h<br>RO         | <b>Reserved</b>   |
| 33:32     | 0h<br>RW         | <p><b>Function Mask (FM):</b><br/>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:</p> <ul style="list-style-type: none"> <li>• 00: No bits in the SID field masked.</li> <li>• 01: Mask most significant bit of function number in the SID field.</li> <li>• 10: Mask two most significant bit of function number in the SID field.</li> <li>• 11: Mask all three bits of function number in the SID field.</li> </ul> <p>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.</p>  |
| 31:16     | 0000h<br>RW      | <p><b>Source ID (SID):</b><br/>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.</p>   |
| 15:0      | 0000h<br>RW      | <p><b>Domain ID (DID):</b><br/>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.<br/>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.</p>  |

### 3.7.9 Fault Status Register (FSTS\_REG\_0\_0\_0\_VTD BAR) — 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<br>RO         | <b>Reserved</b>  |
| 15:8      | 00h<br>RO        | <b>Fault Record Index (FRI):</b><br>This field is valid only when the PPF field is Set.<br>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.<br>The value read from this field is undefined when the PPF field is clear.   |
| 7         | 0h<br>RW/1C      | <b>Page Request Overflow (PRO):</b><br>Hardware detected a Page Request Overflow error. Hardware implementations not supporting the Page Request Queue implement this bit as RsvdZ.  |
| 6         | 0h<br>RO         | <b>Invalidation Time-out Error (ITE):</b><br>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.<br>Hardware implementations not supporting device Device-IOTLBs implement this bit as RsvdZ.  |
| 5         | 0h<br>RO         | <b>Invalidation Completion Error (ICE):</b><br>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 the Fault Event Control register.<br>Hardware implementations not supporting Device-IOTLBs implement this bit as RsvdZ.  |
| 4         | 0h<br>RW/1C      | <b>Invalidation Queue Error (IQE):</b><br>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.<br>Hardware implementations not supporting queued invalidations implement this bit as RsvdZ. |
| 3         | 0h<br>RO         | <b>Advanced Pending Fault (APF):</b><br>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.<br>Software writing 1 to this field clears it. Hardware implementations not supporting advanced fault logging implement this bit as RsvdZ.   |
| 2         | 0h<br>RO         | <b>Advanced Fault Overflow (AFO):</b><br>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.<br>Software writing 1 to this field clears it.<br>Hardware implementations not supporting advanced fault logging implement this bit as RsvdZ.  |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 1         | 0h<br>RO/V       | <p><b>Primary Pending Fault (PPF):</b><br/>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.</p> <ul style="list-style-type: none"> <li>0 = No pending faults in any of the fault recording registers.</li> <li>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.</li> </ul> |
| 0         | 0h<br>RW/1C      | <p><b>Primary Fault Overflow (PFO):</b><br/>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.</p>   |

### 3.7.10 Fault Event Control Register (FECTL\_REG\_0\_0\_0\_VTD BAR) – 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<br>RW         | <p><b>Interrupt Mask (IM):</b></p> <ul style="list-style-type: none"> <li>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).</li> <li>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.</li> </ul> |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 30        | 0h<br>RO/V       | <p><b>Interrupt Pending (IP):</b><br/>Hardware sets the IP field whenever it detects an interrupt condition, which is defined as:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> <li>• Hardware detected error associated with the Invalidation Queue, setting the IQE field in the Fault Status register.</li> <li>• Hardware detected invalid Device-IOTLB invalidation completion, setting the ICE field in the Fault Status register.</li> <li>• Hardware detected Device-IOTLB invalidation completion time-out, setting the ITE field in the Fault Status register.</li> </ul> <p>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.</p> <p>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.</p> <p>The IP field is cleared by hardware as soon as the interrupt message pending condition is serviced. This could be due to either:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Software servicing all the pending interrupt status fields in the Fault Status register as follows: <ul style="list-style-type: none"> <li>- 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.</li> <li>- Software clearing other status fields in the Fault Status register by writing back the value read from the respective fields.</li> </ul> </li> </ul> |
| 29:0      | 0h<br>RO         | <b>Reserved</b>  |

### 3.7.11 Fault Event Data Register (FEDATA\_REG\_0\_0\_0\_VTD BAR) – Offset 3Ch

Register specifying the interrupt message data

| Type | Size   | Offset           | Default   |
|------|--------|------------------|-----------|
| MMIO | 32 bit | VTDPVCOBAR + 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<br>RW      | <b>Extended Interrupt Message Data (EIMD):</b><br>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<br>RW      | <b>Interrupt Message Data (IMD):</b><br>Data value in the interrupt request.  |

### 3.7.12 Fault Event Address Register (FEADDR\_REG\_0\_0\_0\_VTD BAR) – Offset 40h

Register specifying the interrupt message address.

| Type | Size   | Offset           | Default   |
|------|--------|------------------|-----------|
| MMIO | 32 bit | VTDPVCOBAR + 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<br>RW  | <b>Message Address (MA):</b><br>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<br>RO         | <b>Reserved</b>   |

### 3.7.13 Fault Event Upper Address Register (FEUADDR\_REG\_0\_0\_0\_VTD BAR) – 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<br>RW  | <b>Message Upper Address (MUA):</b><br>Hardware implementations supporting Extended Interrupt Mode are required to implement this register.<br>Hardware implementations not supporting Extended Interrupt Mode may treat this field as RsvdZ. |

### 3.7.14 Advanced Fault Log Register (AFLOG\_REG\_0\_0\_0\_VTD BAR) – 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     | 00000000<br>00000h<br>RO | <b>Fault Log Address (FLA):</b><br>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.<br>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<br>RO                 | <b>Fault Log Size (FLS):</b><br>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<br>RO                 | <b>Reserved</b>  |



### 3.7.15 Protected Memory Enable Register (PMEN\_REG\_0\_0\_0\_VTD BAR) – Offset 64h

Register to enable the DMA-protected memory regions setup through the PLMBASE,..PLMLIMIT, 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<br>RW         | <p><b>Enable Protected Memory (EPM):</b><br/>This field controls DMA accesses to the protected low-memory and protected high-memory regions.</p> <ul style="list-style-type: none"> <li>• 0 = Protected memory regions are disabled.</li> <li>• 1 = Protected memory regions are enabled. DMA requests accessing protected memory regions are handled as follows:               <ul style="list-style-type: none"> <li>- When DMA remapping is not enabled, all DMA requests accessing protected memory regions are blocked.</li> <li>- When DMA remapping is enabled:                   <ul style="list-style-type: none"> <li>• DMA requests processed as pass-through (Translation Type value of 10b in Context-Entry) and accessing the protected memory regions are blocked.</li> <li>• DMA requests with translated address (AT=10b) and accessing the protected memory regions are blocked.</li> <li>• 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.</li> </ul> </li> </ul> </li> </ul> <p>Remapping hardware access to the remapping structures are not subject to protected memory region checks.<br/>DMA requests blocked due to protected memory region violation are not recorded or reported as remapping faults.<br/>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.</p> |
| 30:1      | 0h<br>RO         | <b>Reserved</b>  |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 0         | 0h<br>RO/V       | <b>Protected Region Status (PRS):</b><br>This field indicates the status of protected memory region(s): <ul style="list-style-type: none"> <li>• 0 = Protected memory region(s) disabled.</li> <li>• 1 = Protected memory region(s) enabled.</li> </ul> |

### 3.7.16 Protected Low Memory Base Register (PLMBASE\_REG\_0\_0\_0\_VTD BAR) – 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<br>RW       | <b>Protected Low-Memory Base (PLMB):</b><br>This register specifies the base of protected low-memory region in system memory. |
| 19:0      | 0h<br>RO         | <b>Reserved</b>   |

### 3.7.17 Protected Low-Memory Limit Register (PLMLIMIT\_REG\_0\_0\_0\_VTD BAR) – 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<br>RW       | <b>Protected Low-Memory Limit (PLML):</b><br>This register specifies the last host physical address of the DMA-protected low-memory region in system memory. |
| 19:0      | 0h<br>RO         | <b>Reserved</b>  |

### 3.7.18 Protected High-Memory Base Register (PHMBASE\_REG\_0\_0\_0\_VTDDBAR) – 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<br>RO         | <b>Reserved</b>   |
| 38:20     | 00000h<br>RW     | <b>Protected High-Memory Base (PHMB):</b><br>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<br>RO         | <b>Reserved</b>   |

### 3.7.19 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<br>RO         | <b>Reserved</b>  |
| 38:20     | 00000h<br>RW     | <b>Protected High-Memory Limit (PHML):</b><br>This register specifies the last host physical address of the DMA-protected high-memory region in system memory<br>Hardware ignores and does not implement bits 63:HAW, where HAW is the host address width. |
| 19:0      | 0h<br>RO         | <b>Reserved</b>  |

### 3.7.20 Invalidation Queue Head Register (IQH\_REG\_0\_0\_0\_VTDDBAR) – 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<br>RO         | <b>Reserved</b>   |
| 18:4      | 0000h<br>RO/V    | <b>Queue Head (QH):</b><br>Specifies the offset (128-bit aligned) to the invalidation queue for the command that will be fetched next by hardware<br>Hardware resets this field to 0 whenever the queued invalidation is disabled (QIES field Clear in the Global Status register). |
| 3:0       | 0h<br>RO         | <b>Reserved</b>   |

### 3.7.21 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<br>RO         | <b>Reserved</b>  |
| 18:4      | 0000h<br>RW      | <b>Queue Tail (QT):</b><br>Specifies the offset (128-bit aligned) to the invalidation queue for the command that will be written next by software. |
| 3:0       | 0h<br>RO         | <b>Reserved</b>  |

### 3.7.22 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<br>RO         | <b>Reserved</b>  |
| 38:12     | 0000000h<br>RW   | <b>Invalidation Queue Base Address (IQA):</b><br>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<br>RO         | <b>Reserved</b>  |
| 2:0       | 0h<br>RW         | <b>Queue Size (QS):</b><br>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). |

### 3.7.23 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<br>RO         | <b>Reserved</b>   |
| 0         | 0h<br>RW/1C      | <b>Invalidation Wait Descriptor Complete (IWC):</b><br>Indicates completion of Invalidation Wait Descriptor with Interrupt Flag (IF) field Set. Hardware implementations not supporting queued invalidations implement this field as RsvdZ. |

### 3.7.24 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<br>RW         | <p><b>Interrupt Mask (IM):</b></p> <ul style="list-style-type: none"> <li>0= No masking of interrupt. When a invalidation event condition is detected, hardware issues an interrupt message (using the Invalidation Event Data &amp; Invalidation Event Address register values)</li> <li>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.</li> </ul>  |
| 30        | 0h<br>RO/V       | <p><b>Interrupt Pending (IP):</b><br/>Hardware sets the IP field whenever it detects an interrupt condition. Interrupt condition is defined as:</p> <ul style="list-style-type: none"> <li>An Invalidation Wait Descriptor with Interrupt Flag (IF) field Set completed, setting the IWC field in the Invalidation Completion Status register</li> <li>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</li> </ul> <p>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:</p> <ul style="list-style-type: none"> <li>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</li> <li>1= Software servicing the IWC field in the Invalidation Completion Status register.</li> </ul> |
| 29:0      | 0h<br>RO         | <b>Reserved</b>  |

### 3.7.25 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<br>RW      | <b>Extended Interrupt Message Data (EIMD):</b><br>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<br>RW      | <b>Interrupt Message Data (IMD):</b><br>Data value in the interrupt request.   |

### 3.7.26 Invalidation Event Address Register (IEADDR\_REG\_0\_0\_0\_VTD BAR) – 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\_VTD BAR, offset 40h.

### 3.7.27 Invalidation Event Upper Address Register (IEUADDR\_REG\_0\_0\_0\_VTD BAR) – 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<br>RW  | <b>Message Upper Address (MUA):</b><br>Hardware implementations supporting Queued Invalidation and Extended Interrupt Mode are required to implement this register. Hardware implementations not supporting Queued Invalidation or Extended Interrupt Mode may treat this field as RsvdZ. |

### 3.7.28 Interrupt Remapping Table Address Register (IRTA\_REG\_0\_0\_0\_VTD BAR) – 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<br>00000h<br>RW | <b>Interrupt Remapping Table Address (IRTA):</b><br>This field points to the base of 4KB aligned interrupt remapping table<br>Hardware ignores and does not implement bits 63:HAW, where HAW is the host address width<br>Reads of this field returns value that was last programmed to it.  |
| 11        | 0h<br>RW                 | <b>Extended Interrupt Mode Enable (EIME):</b><br>This field is used by hardware on Intel64 platforms as follows: <ul style="list-style-type: none"> <li>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</li> <li>1= x2APIC mode is active. Hardware interprets all 32-bits of Destination-ID field in the IRTEs</li> </ul> This field is implemented as RsvdZ on implementations reporting Extended Interrupt Mode (EIM) field as Clear in Extended Capability register. |
| 10:4      | 0h<br>RO                 | <b>Reserved</b>  |
| 3:0       | 0h<br>RW                 | <b>IRTA Size (S):</b><br>This field specifies the size of the interrupt remapping table.<br>The number of entries in the interrupt remapping table is $2(X+1)$ , where X is the value programmed in this field.  |

### 3.7.29 Page Request Status Register (PRESTS\_REG\_0\_0\_0\_VTD BAR) – 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<br>RO         | <b>Reserved</b>   |
| 0         | 0h<br>RO         | <b>Pending Page Request (PPR):</b><br>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_req_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. |

### 3.7.30 Page Request Event Control Register (PRECTL\_REG\_0\_0\_0\_VTDDBAR) – 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<br>RO         | <b>Interrupt Mask (IM):</b><br>Interrupt Mask <ul style="list-style-type: none"> <li>• 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)</li> <li>• 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.</li> </ul> |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 30        | 0h<br>RO         | <p><b>Interrupt Pending (IP):</b><br/>Interrupt Pending: Hardware sets the IP field whenever it detects an interrupt condition. Interrupt condition is defined as:</p> <ul style="list-style-type: none"> <li>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</li> <li>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</li> </ul> <p>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:</p> <ul style="list-style-type: none"> <li>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</li> <li>Software servicing the PPR field in the Page Request Event Status register.</li> </ul> |
| 29:0      | 0h<br>RO         | <b>Reserved</b>   |

### 3.7.31 Page Request Event Data Register (PREDATA\_REG\_0\_0\_0\_VTD BAR) – 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<br>RO      | <p><b>Extended Interrupt Message Data (EIMD):</b><br/>Extended Interrupt Message Data</p>  |
| 15:0      | 0000h<br>RO      | <p><b>Interrupt Message Data (IMD):</b><br/>Interrupt Message Data: Data value in the interrupt request. Software requirements for programming this register are described in VTd Spec</p> |

### 3.7.32 Page Request Event Address Register (PREADDR\_REG\_0\_0\_0\_VTD BAR) – 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<br>RO  | <b>Message Address (MA):</b><br>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<br>RO         | <b>Reserved</b>  |

### 3.7.33 Page Request Event Upper Address Register (PREUADDR\_REG\_0\_0\_0\_VTD BAR) – 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<br>RO  | <b>Message Upper Address (MUA):</b><br>Message Upper Address: This field specifies the upper address (bits.. 63:32) for the page request event interrupt. |

### 3.7.34 Fault Recording Register Low [0] (FRCDL\_REG\_0\_0\_0\_VTD BAR) – 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<br>00000h<br>RO/V | <b>Fault Info (FI):</b><br>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<br>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<br>This field is relevant only when the F field is Set. |
| 11:0      | 0h<br>RO                   | <b>Reserved</b>   |

### 3.7.35 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<br>RW/1C      | <b>FRCDH Fault (F):</b><br>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<br>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<br>RO/V       | <b>FRCDH Type (T):</b><br>Type of the faulted request: <ul style="list-style-type: none"> <li>• 0: Write request</li> <li>• 1: Read request or AtomicOp request</li> </ul> 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<br>RO/V       | <b>Address Type (AT):</b><br>This field captures the AT field from the faulted DMA request<br>Hardware implementations not supporting Device-IOTLBs (DI field Clear in Extended Capability register) treat this field as RsvdZ<br>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<br>RO/V   | <b>PASID Value (PN):</b><br>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<br>RO/V      | <b>Fault Reason (FR):</b><br>Reason for the fault<br>This field is relevant only when the F field is set.  |
| 31        | 0h<br>RO/V       | <b>PASID Present (PP):</b><br>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<br>RO/V       | <b>Execute Permission Requested (EXE):</b><br>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<br>RO/V       | <b>Privilege Mode Requested (PRIV):</b><br>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<br>RO         | <b>Reserved</b>  |
| 15:0      | 0000h<br>RO/V    | <b>Source Identifier (SID):</b><br>Requester-id associated with the fault condition<br>This field is relevant only when the F field is set.  |

### 3.7.36 Invalidate Address Register (IVA\_REG\_0\_0\_0\_VTD BAR) – 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<br>00000h<br>RW | <p><b>IVA Address (ADDR):</b><br/>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.<br/>A value returned on a read of this field is undefined<br/>A value returned on a read of this field is undefined</p>   |
| 11:7      | 0h<br>RO                 | <b>Reserved</b>   |
| 6         | 0h<br>RW                 | <p><b>Invalidation Hint (IH):</b><br/>The field provides hint to hardware about preserving or flushing the non-leaf (page-directory) entries that may be cached in hardware:</p> <ul style="list-style-type: none"> <li>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.</li> <li>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.</li> </ul> <p>A value returned on a read of this field is undefined</p> |
| 5:0       | 00h<br>RW                | <p><b>Address Mask (AM):</b><br/>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</p> <p>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.</p>  |

### 3.7.37 IOTLB Invalidate Register (IOTLB\_REG\_0\_0\_0\_VTD BAR) – 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<br>RW/V       | <p><b>Invalidate IOTLB (IVT):</b><br/>           Software requests IOTLB invalidation by setting this field. Software must also set the requested invalidation granularity by programming the IIRG field<br/>           Hardware clears the IVT field to indicate the invalidation request is complete.<br/>           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<br/>           Software must not submit IOTLB invalidation requests when there is a context-cache invalidation request pending at this remapping hardware unit.<br/>           Hardware implementations reporting write-buffer flushing requirement (RWBF=1 in Capability register) must implicitly perform a write buffer flushing before invalidating the IOTLB.</p>   |
| 62        | 0h<br>RO         | <b>Reserved</b>   |
| 61:60     | 0h<br>RW         | <p><b>IOTLB Invalidation Request Granularity (IIRG):</b><br/>           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</p> <ul style="list-style-type: none"> <li>• 00 = Reserved</li> <li>• 01 = Global invalidation request</li> <li>• 10 = Domain-selective invalidation request. The target domain-id must be specified in the DID field</li> <li>• 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</li> </ul> <p>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</p> |
| 59        | 0h<br>RO         | <b>Reserved</b>   |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 58:57     | 1h<br>RO/V       | <p><b>IOTLB Actual Invalidation Granularity (IAIG):</b><br/>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</p> <ul style="list-style-type: none"> <li>• 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</li> <li>• 01 = Global Invalidation performed. This could be in response to a global, domain-selective, or page-selective invalidation request</li> <li>• 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</li> <li>• 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.</li> </ul> |
| 56:50     | 0h<br>RO         | <b>Reserved</b>   |
| 49        | 0h<br>RW         | <p><b>Drain Reads (DR):</b><br/>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:</p> <ul style="list-style-type: none"> <li>• 0 = Hardware may complete the IOTLB invalidation without draining any translated DMA read requests</li> <li>• 1 = Hardware must drain DMA read requests.</li> </ul>  |
| 48        | 0h<br>RW         | <p><b>Drain Writes (DW):</b><br/>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:</p> <ul style="list-style-type: none"> <li>• 0 = Hardware may complete the IOTLB invalidation without draining DMA write requests</li> <li>• 1 = Hardware must drain relevant translated DMA write requests.</li> </ul>  |
| 47:32     | 0000h<br>RW      | <p><b>Domain ID (DID):</b><br/>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.<br/>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.</p>   |
| 31:0      | 0h<br>RO         | <b>Reserved</b>   |

# 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.

### 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)   | 9A40h         |
| 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           |
| 40h    | 2            | Capability Identifier (CAPID0_0_2_0_PCI)                                     | 7009h         |

| Offset | Size (Bytes) | Register Name (Register Symbol)  | Default Value |
|--------|--------------|--|---------------|
| 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)                             | 00000000h     |
| 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)                                | 1008000h      |
| 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     |
| 204h   | 2            | ATS Capability (ATS_CAP_0_2_0_PCI)                                       | 0060h         |

| Offset | Size (Bytes) | Register Name (Register Symbol)                               | Default Value |
|--------|--------------|---|---------------|
| 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     |
| 32Ah   | 2            | SRIOV Status (SRIOV_STS_0_2_0_PCI)                            | 0000h         |
| 32Ch   | 2            | SRIOV Initial VFs (SRIOV_INITVFS_0_2_0_PCI)                   | 0007h         |
| 32Eh   | 2            | SRIOV Total VFs (SRIOV_TOTVFS_0_2_0_PCI)                      | 0007h         |
| 334h   | 2            | First VF Offset (FIRST_VF_OFFSET_0_2_0_PCI)                   | 0001h         |
| 336h   | 2            | VF Stride (VF_STRIDE_0_2_0_PCI)                               | 0001h         |
| 33Ah   | 2            | VF Device ID (VF_DEVICEID_0_2_0_PCI)                          | 9A40h         |
| 33Ch   | 4            | Supported Page Sizes (SUPPORTED_PAGE_SIZES_0_2_0_PCI)         | 00000553h     |
| 340h   | 4            | System Page Sizes (SYSTEM_PAGE_SIZES_0_2_0_PCI)               | 00000001h     |
| 344h   | 4            | VF BAR0 Lower DWORD (VF_BAR0_LDW_0_2_0_PCI)                   | 00000004h     |
| 348h   | 4            | VF BAR0 Upper DWORD (VF_BAR0_UDW_0_2_0_PCI)                   | 00000000h     |
| 34Ch   | 4            | VF BAR1 LDW (VF_BAR1_LDW_0_2_0_PCI)                           | 0000000Ch     |
| 350h   | 4            | VF BAR1 UDW (VF_BAR1_UDW_0_2_0_PCI)                           | 00000000h     |
| 35Ch   | 4            | VF 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<br>RO      | <b>Vendor ID (VID):</b><br>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 | 9A40h   |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| R           | R          | R         |

| Bit Range | Default & Access | Field Name (ID): Description                                    |
|-----------|------------------|---|
| 15:7      | 134h<br>RO       | <b>Device ID MSB (DID_MSB):</b><br>Upper byte of the Device ID. |
| 6:0       | 40h<br>RO/V      | <b>Device ID LSB (DID_LSB):</b><br>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<br>RO         | <b>Reserved</b>   |
| 10        | 0h<br>RW/V       | <b>Interrupt Disable (INTDIS):</b><br>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<br>RO         | <b>Fast Back-To-Back (FB2B):</b><br>Not Implemented. Hardwired to 0.  |
| 8         | 0h<br>RO         | <b>SERR Enable (SEN):</b><br>Not Implemented. Hardwired to 0.   |
| 7         | 0h<br>RO         | <b>Wait Cycle Control (WCC):</b><br>Not Implemented. Hardwired to 0.  |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 6         | 0h<br>RO         | <b>Parity Error Enable (PER):</b><br>Not Implemented.<br>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<br>RO         | <b>Video Palette Snooping (VPS):</b><br>This bit is hardwired to 0 to disable snooping.   |
| 4         | 0h<br>RO         | <b>Memory Write and Invalidate Enable (MWIE):</b><br>Hardwired to 0.<br>The IGD does not support memory write and invalidate commands.  |
| 3         | 0h<br>RO         | <b>Special Cycle Enable (SCE):</b><br>This bit is hardwired to 0.<br>The IGD ignores Special cycles.  |
| 2         | 0h<br>RW/V       | <b>Bus Master Enable (BME):</b><br>0: Disable IGD bus mastering.<br>1: Enable the IGD to function as a PCI compliant master.  |
| 1         | 0h<br>RW/V       | <b>Memory Access Enable (MAE):</b><br>This bit controls the IGD's response to memory space accesses.<br>0: Disable.<br>1: Enable.   |
| 0         | 0h<br>RW/V/L     | <b>I/O Access Enable (IOAE):</b><br>This bit controls the IGD's response to I/O space accesses.<br>0: Disable.<br>1: Enable.<br>This field is read-only 0 if DEV2CTL[0].IOBARDIS at offset 58h is 1.<br><b>Locked by:</b> 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<br>RO         | <b>Detected Parity Error (DPE):</b><br>Since the IGD does not detect parity, this bit is always hardwired to 0.         |
| 14        | 0h<br>RO         | <b>Signaled System Error (SSE):</b><br>The IGD never asserts SERR#, therefore this bit is hardwired to 0.               |
| 13        | 0h<br>RO         | <b>Received Master Abort Status (RMAS):</b><br>The IGD never gets a Master Abort, therefore this bit is hardwired to 0. |



| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 12        | 0h<br>RO         | <b>Received Target Abort Status (RTAS):</b><br>The IGD never gets a Target Abort, therefore this bit is hardwired to 0.  |
| 11        | 0h<br>RO         | <b>Signaled Target Abort Status (STAS):</b><br>Hardwired to 0. The IGD does not use target abort semantics.  |
| 10:9      | 0h<br>RO         | <b>Device Select Timing (DEVT):</b><br>Hardwired to 00.  |
| 8         | 0h<br>RO         | <b>Master Data Parity Error Detected (DPD):</b><br>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<br>RO         | <b>Fast Back-To-Back (FB2B):</b><br>Hardwired to 0 to be compliant to PCI Express Base Spec (rev 3.0).   |
| 6         | 0h<br>RO         | <b>User Defined Format (UDF):</b><br>Hardwired to 0.   |
| 5         | 0h<br>RO         | <b>66MHz PCI Capable (C66):</b><br>Hardwired to 0.   |
| 4         | 1h<br>RO         | <b>Capability List (CLIST):</b><br>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<br>RO/V       | <b>Interrupt Status (INTSTS):</b><br>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<br>RO         | <b>Reserved</b>  |

#### 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<br>RO/V      | <b>Base Class Code (BCC):</b><br>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<br>RO/V      | <b>Sub-Class Code (SUBCC):</b><br>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<br>RO        | <b>Programming Interface (PI):</b><br>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<br>RO        | <b>Revision ID (RID):</b><br>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<br>RW        | <b>Cache Line Size Value (CLS):</b><br>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<br>RO        | <b>Master Latency Timer Count Value (MLTCV):</b><br>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<br>RO         | <b>Multi Function Status (MFUNC):</b><br>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<br>RO        | <b>Header Code (H):</b><br>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<br>RO         | <b>BIST Supported (BISTS):</b><br>BIST is not supported. This bit is hardwired to 0. |
| 6:0       | 0h<br>RO         | <b>Reserved</b>  |

#### 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<br>RW/V      | <b>Memory Base Address (MBA_0):</b><br>Set by the OS, these bits correspond to address signals [63:24]. |
| 23:4      | 00000h<br>RO     | <b>Address Mask (ADM):</b><br>Hardwired to 0s to indicate at least 16MB address range.                  |
| 3         | 0h<br>RO         | <b>Prefetchable Memory (PREFMEM):</b><br>Hardwired to 0 to prevent prefetching.                         |
| 2:1       | 2h<br>RO         | <b>Memory Type (MENTYP):</b><br>Hardwired to 2h to indicate 64 bit base address.                        |
| 0         | 0h<br>RO         | <b>Memory I/O Space (MIOS):</b><br>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<br>RW/V | <b>Memory Base Address (MBA_1):</b><br>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<br>RW/V/L     | <b>4096MB Address Mask (ADMSK4096):</b><br>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)<br><b>Locked by:</b> MSAC_0_2_0_PCI.APSZ4     |
| 30        | 0h<br>RW/V/L     | <b>2048MB Address Mask (ADMSK2048):</b><br>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)<br><b>Locked by:</b> MSAC_0_2_0_PCI.APSZ3 |
| 29        | 0h<br>RW/V/L     | <b>1024MB Address Mask (ADMSK1024):</b><br>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)<br><b>Locked by:</b> MSAC_0_2_0_PCI.APSZ2 |
| 28        | 0h<br>RW/V/L     | <b>512MB Address Mask (ADMSK512):</b><br>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)<br><b>Locked by:</b> MSAC_0_2_0_PCI.APSZ1    |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 27        | 0h<br>RW/V/L     | <b>256MB Address Mask (ADMSK256):</b><br>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)<br><b>Locked by:</b> MSAC_0_2_0_PCI.APSZ0 |
| 26:4      | 000000h<br>RO    | <b>Address Mask (ADM):</b><br>Hardwired to 0s to indicate at least 128MB address range.  |
| 3         | 1h<br>RO         | <b>Prefetchable Memory (PREFMEM):</b><br>Hardwired to 1 to enable prefetching.   |
| 2:1       | 2h<br>RO         | <b>Memory Type (MEMTYP):</b><br>Hardwired to 2h to indicate 64 bit base address.   |
| 0         | 0h<br>RO         | <b>Memory I/O Space (MIOS):</b><br>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<br>RW/V | <b>Memory Base Address (MBA):</b><br>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.

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<br>RO         | <b>Reserved</b>  |
| 15:6      | 000h<br>RW/V/L   | <b>IO Base Address (IOBASE):</b><br>Set by the OS, allowing the I/O Base to be located anywhere in 16bit I/O Address Space. Note: This field is RO 0's if DEV2CTL[0] IOBARDIS is 1b.<br><b>Locked by:</b> DEV2CTL_0_2_0_PCI.IOBARDIS |
| 5:3       | 0h<br>RO         | <b>Reserved</b>  |
| 2:1       | 0h<br>RO         | <b>Memory Type (MEMTYPE):</b><br>Hardwired to 0s to indicate 32-bit address.   |
| 0         | 1h<br>RO         | <b>Memory I/O Space (MIOS):</b><br>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<br>RW      | <b>Subsystem Vendor Id (SUBVID):</b><br>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<br>RW      | <b>Subsystem ID (SUBID):</b><br>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<br>RO      | <b>ROM Base Address (RBA):</b><br>Hardwired to 0's.                               |
| 17:11     | 00h<br>RO        | <b>Address Mask (ADMSK):</b><br>Hardwired to 0s to indicate 256 KB address range. |
| 10:1      | 0h<br>RO         | <b>Reserved</b>   |
| 0         | 0h<br>RO         | <b>ROM BIOS Enable (RBE):</b><br>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<br>RO        | <b>Capabilities Pointer Value (CPV):</b><br>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<br>RW        | <b>Interrupt Connection (INTCON):</b><br>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<br>RO        | <b>Interrupt Pin Value (INTPIN):</b><br>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<br>RO        | <b>Minimum Grant Value (MGV):</b><br>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<br>RO        | <b>Maximum Latency Value (MLV):</b><br>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<br>RO        | <b>Next Capability Pointer (NEXT_CAP):</b><br>This field is hardwired to point to the next PCI Capability structure, the PCIe Capabilities structure at 70h.                |
| 7:0       | 09h<br>RO        | <b>Capability Identifier (CAP_ID):</b><br>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<br>RO         | <b>Reserved</b>   |
| 11:8      | 1h<br>RO         | <b>CAPID Version (CAPID_VER):</b><br>This field is hardwired to the value 1h to identify the first revision of the CAPID register definition. |
| 7:0       | 0Ch<br>RO        | <b>CAPID Length (CAPIDLEN):</b><br>This field is hardwired to the value 0Ch to indicate the structure length (12 bytes).                      |

#### 4.1.26 Capabilities A (CAPIDO\_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 | 0000000h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| R           | R          | R         |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 31:25     | 0h<br>RO         | <b>Reserved</b>  |
| 24        | 0h<br>RO/V       | <b>Display FuSa Disabled (DISPLAY_FUSA_DIS):</b><br>0: Display FuSa is enabled<br>1: Display FuSa is disabled<br>Note: FuSa is an acronym for Functional Safety. |
| 23:4      | 0h<br>RO         | <b>Reserved</b>  |
| 3         | 0h<br>RO/V       | <b>VGT Enabled (VGT_EN):</b><br>0: VGT is disabled<br>1: VGT is enabled  |
| 2         | 0h<br>RO         | <b>Reserved</b>  |
| 1         | 0h<br>RO/V       | <b>SVM Disabled (SVMD):</b><br>0: SVM is enabled<br>1: SVM is disabled   |



| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 0         | 0h<br>RO/V       | <b>VTD Disable (VTDD):</b><br>0: VTD is enabled<br>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<br>RO         | <b>Reserved</b>              |

#### 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<br>RO/V      | <p><b>Graphics Memory Size (GMS):</b><br/>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.</p> <p>00h: 0MB<br/>01h - 10h: 32MB, 64MB, 96MB, ..., 512MB<br/>11h - 1Fh: Reserved<br/>20h: 1024MB<br/>21h - 2Fh: Reserved<br/>30h: 1536MB 31h - 3Fh: Reserved<br/>40h: 2048MB<br/>41h - EFh: Reserved<br/>F0h - FEh: 4MB, 8MB, 12MB, ..., 60MB<br/>FFh: Reserved Hardware functionality in case of programming this value to Reserved is not guaranteed.</p> |
| 7:6       | 0h<br>RO/V       | <p><b>Graphics Translation Table Memory Size (GGMS):</b><br/>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</p>  |
| 5:3       | 0h<br>RO         | <b>Reserved</b>  |
| 2         | 0h<br>RO/V       | <p><b>Versatile Acceleration Mode Enable (VAMEN):</b><br/>Enables the use of the iGFX engines for Versatile Acceleration.<br/>0: iGFX engines are in iGFX Mode. Device 2 Class Code is 030000h.<br/>1: iGFX engines are in Versatile Acceleration Mode. Device 2 Class Code is 038000h.</p>  |
| 1         | 0h<br>RO/V       | <p><b>IVD:</b><br/>0: Enable. Device 2 (IGD) claims VGA memory and IO cycles, the Sub-Class Code within Device 2 Class Code register is 00.<br/>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.<br/>BIOS Requirement: BIOS must not set this bit to 0 if the GMS field (bits 7:3 of this register) pre-allocates no memory.</p>  |
| 0         | 0h<br>RO         | <b>Reserved</b>  |



## 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<br>RO         | <b>Reserved</b>   |
| 14        | 0h<br>RO/V       | <b>CHAP Enable (D7EN):</b><br>0: Device 7 is disabled<br>1: Device 7 is enabled   |
| 13        | 0h<br>RO         | <b>Device 6 Enable (D6EN):</b><br>0: Device 6 is disabled<br>1: Device 6 is enabled   |
| 12:11     | 0h<br>RO         | <b>Reserved</b>   |
| 10        | 0h<br>RO         | <b>Device 5 Enable (D5EN):</b><br>0: Device 5 is disabled<br>1: Device 5 is enabled   |
| 9:8       | 0h<br>RO         | <b>Reserved</b>   |
| 7         | 1h<br>RO/V       | <b>Device 4 Enable (D4EN):</b><br>0: Device 4 is disabled<br>1: Device 4 is enabled   |
| 6         | 0h<br>RO         | <b>Reserved</b>   |
| 5         | 1h<br>RO/V       | <b>Device 3 Enable For Display HD Audio (D3EN):</b><br>0: Device 3 is disabled<br>1: Device 3 is enabled  |
| 4         | 1h<br>RO/V       | <b>Internal Graphics Engine (D2EN):</b><br>0: Bus 0 Device 2 is disabled and hidden<br>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<br>RO/V       | <b>PEG10 Enable (D1F0EN):</b><br>Device 1, Function 0 is enabled  |
| 2         | 1h<br>RO/V       | <b>PEG11 Enable (D1F1EN):</b><br>Device 1, Function 1 is enabled  |
| 1         | 1h<br>RO/V       | <b>PEG12 Enable (D1F2EN):</b><br>Device 1, Function 2 is enabled  |
| 0         | 1h<br>RO         | <b>Host Bridge Enable (D0EN):</b><br>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<br>RO         | <b>Reserved</b>   |
| 0         | 0h<br>RW         | <b>IO BAR Disable (IOBARDIS):</b><br>System BIOS can choose to disable and hide the IOBAR for systems that do not require legacy IOBAR access to GFX MMIO registers.<br>0b: IOBAR is enabled and exposed at offset 0x20 in Device 2 Configuration space (Default).<br>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 | 00000000h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | R          | R         |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 31:21     | 0h<br>RO         | <b>Reserved</b>  |
| 20        | 0h<br>RW/V       | <b>Untrusted Aperture Size Bit 4 (APSZ4):</b><br>Untrusted Aperture Size Bit 4 |
| 19        | 0h<br>RW/V       | <b>Untrusted Aperture Size Bit 3 (APSZ3):</b><br>Untrusted Aperture Size Bit 3 |
| 18        | 0h<br>RW/V       | <b>Untrusted Aperture Size Bit 2 (APSZ2):</b><br>Untrusted Aperture Size Bit 2 |
| 17        | 0h<br>RW/V       | <b>Untrusted Aperture Size Bit 1 (APSZ1):</b><br>Untrusted Aperture Size Bit 1 |
| 16        | 0h<br>RW/V       | <b>Untrusted Aperture Size Bit 0 (APSZ0):</b><br>Untrusted Aperture Size Bit 0 |
| 15:0      | 0h<br>RO         | <b>Reserved</b>  |

#### 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<br>RW/V | <b>Token Value (TOKEN_VALUE):</b><br>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<br>RO         | <b>Reserved</b>   |
| 0         | 0h<br>RO         | <b>GFX VTd Active (VTACT):</b><br>Reflects GFX VTd Mode is active.<br>1: GFX VTd Mode is active<br>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<br>RO        | <b>Next Capability Pointer (NEXT_PTR):</b><br>This field is hardwired to point to the next PCI Capability structure, the MSI Capabilities at ACh. |
| 7:0       | 10h<br>RO        | <b>Capability Identifier (CAP_ID):</b><br>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<br>RO         | <b>Reserved</b>  |
| 13:9      | 00h<br>RO        | <b>Interrupt Message Number (INTRMSG):</b><br>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<br>RO         | <b>Slot Implemented (SLOTIMP):</b><br>This field is hardwired to 0 for an endpoint device.   |
| 7:4       | 9h<br>RO         | <b>Device Type (DEV_TYPE):</b><br>This field is hardwired to 9h to indicate a Root Complex Integrated Endpoint.  |
| 3:0       | 2h<br>RO         | <b>Capability Version (CAP_VER):</b><br>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<br>RO         | <b>Reserved</b>   |
| 28        | 1h<br>RO         | <b>Functional Level Reset Capability (FLRCAP):</b><br>Hardwired to 1b to indicate the Function supports the optional Function Level Reset mechanism.    |
| 27:26     | 0h<br>RO         | <b>Captured Slot Power Limit Scale (PWR_LIM_SCALE):</b><br>Not applicable for a Root Complex Integrated Endpoint with no Link or Slot. Hardwired to 00b |
| 25:18     | 00h<br>RO        | <b>Captured Slot Power Limit Value (CSPLS):</b><br>Not applicable for a Root Complex Integrated Endpoint with no Link or Slot. Hardwired to 00h         |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 17:16     | 0h<br>RO         | <b>Reserved</b>   |
| 15        | 1h<br>RO         | <b>Role-Based Error Reporting (RBER):</b><br>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<br>RO         | <b>Reserved</b>   |
| 11:9      | 0h<br>RO         | <b>Endpoint L1 Acceptable Latency (EPL1AL):</b><br>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<br>RO         | <b>Endpoint L0S Acceptable Latency (EPL0AL):</b><br>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<br>RO         | <b>Extended Tag Field Supported (ETFS):</b><br>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<br>RO         | <b>Phantom Functions Supported (PFS):</b><br>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<br>RO         | <b>Max Payload Size Supported (MPSS):</b><br>This field indicates the maximum payload size that the Function can support for TLPs. Hardwired to 000b to represent 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<br>RW/V       | <b>Initiate Function Level Reset (INIT_FLR):</b><br>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. |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 14:12     | 0h<br>RO         | <b>Max Read Request Size (MRRS):</b><br>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<br>RO         | <b>Enable No Snoop (ENS):</b><br>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<br>RO         | <b>Aux Power PM Enable (APPME):</b><br>Functions that do not implement this capability hardwire this bit to 0b.   |
| 9         | 0h<br>RO         | <b>Phantom Functions Enable (PFE):</b><br>Functions that do not implement this capability hardwire this bit to 0b.  |
| 8         | 0h<br>RO         | <b>Extended Tag Field Enable (ETFE):</b><br>Functions that do not implement this capability hardwire this bit to 0b.  |
| 7:5       | 0h<br>RO         | <b>Max Payload Size (MPS):</b><br>Functions that support only the 128-byte max payload size are permitted to hardwire this field to 000b.   |
| 4         | 0h<br>RO         | <b>Enable Relaxed Ordering (ERO):</b><br>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<br>RO         | <b>Unsupported Request Response Enable (URRE):</b><br>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<br>RW/V       | <b>Fatal Error Enable (FEE):</b><br>This bit, in conjunction with other bits, controls sending ERR_FATAL Messages.  |
| 1         | 0h<br>RW/V       | <b>Non-Fatal Error Enable (NFEE):</b><br>This bit, in conjunction with other bits, controls sending ERR_NONFATAL Messages.  |
| 0         | 0h<br>RW/V       | <b>Correctable Error Enable (CEE):</b><br>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<br>RO         | <b>Reserved</b>              |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 5         | 0h<br>RO         | <b>Transactions Pending (TP):</b><br>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<br>RO         | <b>Aux Power Detected (APD):</b><br>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<br>RO         | <b>Unsupported Request Detected (URD):</b><br>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<br>RW/V       | <b>Fatal Error Detected (FED):</b><br>This bit indicates status of fatal errors detected. Errors are logged in this register regardless of whether error reporting is enabled or not in the Device Control Register.   |
| 1         | 0h<br>RW/V       | <b>Non-Fatal Error Detected (NFED):</b><br>This bit indicates status of non fatal errors detected. Errors are logged in this register regardless of whether error reporting is enabled or not in the Device Control Register.  |
| 0         | 0h<br>RW/V       | <b>Correctable Error Detected (CED):</b><br>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<br>RO        | <b>Pointer To Next Capability (POINTNEXT):</b><br>This is a hardwired pointer to the next item in the capabilities list.     |
| 7:0       | 05h<br>RO        | <b>Capability ID (CAPID):</b><br>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<br>RO         | <b>Reserved</b>   |
| 8         | 1h<br>RO         | <b>Per Vector Mask Capable (PVMASKCAP):</b><br>SR-IOV requires this capability.   |
| 7         | 0h<br>RO         | <b>64BIT Capable (CAP64B):</b><br>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<br>RW/V       | <b>Multiple Message Enable (MME):</b><br>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 requests 000: 1001: 2010: 4011: 8100: 16101: 32110: Reserved 111: Reserved |
| 3:1       | 0h<br>RO         | <b>Multiple Message Capable (MMC):</b><br>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.   |
| 0         | 0h<br>RW/V       | <b>MSI Enable (MSIEN):</b><br>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<br>RW/V | <b>Message Address Field (MESSADD):</b><br>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<br>RO          | <b>Force DWORD Align (FDWORD):</b><br>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<br>RW/V    | <b>Message Data (MESSDATA):</b><br>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<br>RO         | <b>Reserved</b>   |
| 0         | 0h<br>RW/V       | <b>Mask Bit For Vector 0 (MASKBIT):</b><br>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<br>RO         | <b>Reserved</b>  |
| 0         | 0h<br>RO/V       | <b>Pending Bit For Vector 0 (PENDBIT):</b><br>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<br>RO/V     | <b>Graphics Base Of Stolen Memory LSB (BDSM_LSB):</b><br>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<br>RO         | <b>Reserved</b>   |

#### 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<br>RO/V | <b>Graphics Base Of Stolen Memory MSB (BDSM_MSB):</b><br>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<br>RW     | <b>GFX-VTD Base Address Lower DWORD (GFXVTDBAR):</b><br>This field corresponds to bits 31 to 12 of the base address GFX-VTD configuration space.<br>BIOS will program this register resulting in a base address for a 4KB block of contiguous memory address space.<br>This register ensures that a naturally aligned 4KB space is allocated within the first 512GB of addressable memory space.<br>System Software uses this base address to program the GFX-VTD register set. |
| 11:1      | 0h<br>RO         | <b>Reserved</b>   |
| 0         | 0h<br>RW/V       | <b>GFX-VTBAR Enable (GFXVTDBAREN):</b><br>0: GFX-VTBAR is disabled and does not claim any memory.<br>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<br>RW  | <b>GFX-VTD Base Address Upper DWORD (GFXVTDBAR):</b><br>This field corresponds to bits 63 to 32 of the base address GFX-VTD configuration space.<br>BIOS will program this register, resulting in a base address for a 4KB block of contiguous memory address space.<br>This register ensures that a naturally aligned 4KB space is allocated within the first 512GB of addressable memory space.<br>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<br>RO        | <b>Next Capability Pointer (NEXT_PTR):</b><br>This is a hardwired pointer to the next item in the capabilities list. |
| 7:0       | 01h<br>RO        | <b>Capability Identifier (CAP_ID):</b><br>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<br>RO        | <b>PME Support (PMES):</b><br>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<br>RO         | <b>D2 Support (D2):</b><br>Hardwired to 0 to indicate the D2 power management state is not supported.   |
| 9         | 0h<br>RO         | <b>D1 Support (D1):</b><br>Hardwired to 0 to indicate that the D1 power management state is not supported.  |
| 8:6       | 0h<br>RO         | <b>Reserved</b>   |
| 5         | 1h<br>RO         | <b>Device Specific Initialization (DSI):</b><br>Hardwired to 1 to indicate that special initialization of the IGD is required before generic class device driver is to use it.  |
| 4         | 0h<br>RO         | <b>Reserved</b>   |
| 3         | 0h<br>RO         | <b>PME Clock (PMECLK):</b><br>Hardwired to 0 to indicate IGD does not support PME# generation.  |
| 2:0       | 2h<br>RO         | <b>Power Management Interface Version (VER):</b><br>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<br>RO         | <b>PME Status (PMESTS):</b><br>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<br>RO         | <b>Data Scale (DSCALE):</b><br>This field is hardwired to 00 to indicate IGD does not support data register.  |
| 12:9      | 0h<br>RO         | <b>Data Select (DSEL):</b><br>This field is hardwired to 0h to indicate IGD does not support data register.   |
| 8         | 0h<br>RO         | <b>PME Enable (PMEEN):</b><br>This bit is hardwired to 0 to indicate that PME# assertion from D3 (cold) is disabled.  |
| 7:2       | 0h<br>RO         | <b>Reserved</b>   |
| 1:0       | 0h<br>RW/V       | <b>Power State (PWRSTAT):</b><br>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<br>RW        | <b>Software Scratch Bits (SWSB):</b><br>Software Scratch Bits  |
| 7:1       | 00h<br>RW        | <b>Software Flag (SWF):</b><br>Used to indicate caller and SMI function desired, as well as return result.   |
| 0         | 0h<br>RW         | <b>Software SMI Event (GSSMIE):</b><br>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<br>RW        | <b>Graphics System Event Scratch Trigger 3 (GSE3):</b><br>Graphics System Event Scratch Trigger 3 |
| 23:16     | 00h<br>RW        | <b>Graphics System Event Scratch Trigger 2 (GSE2):</b><br>Graphics System Event Scratch Trigger 2 |
| 15:8      | 00h<br>RW        | <b>Graphics System Event Scratch Trigger 1 (GSE1):</b><br>Graphics System Event Scratch Trigger 1 |
| 7:0       | 00h<br>RW        | <b>Graphics System Event Scratch Trigger 0 (GSE0):</b><br>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<br>RW         | <b>SMI Or SCI Event Select (SMISCISEL):</b><br>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<br>RW      | <b>Software Scratch Bits (SCISB):</b><br>Read/write bits not used by hardware.   |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 0         | 0h<br>RW         | <b>Software SCI Event (GSSCIE):</b><br>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<br>RO/V     | <b>WOPCM Base LSB (WOPCMBASE_LSB):</b><br>Base value programmed (from Top of Stolen Memory). The programmed value must be consistent with the WOPCM Size programming.  |
| 19:9      | 0h<br>RO         | <b>Reserved</b>  |
| 8:7       | 0h<br>RO/V       | <b>WOPCM Size (WOPCMSIZE):</b><br>This register determines the WOPCM size. The programmed value must be consistent with the WOPCM base programming.<br>00b: 1MB (default)<br>01b: 2MB<br>10b: 4MB<br>11b: 8MB      |
| 6         | 0h<br>RO/V       | <b>ASMF Method Enable (ASMFEN):</b><br>0: Disable ASMF<br>1: Enable ASMF   |
| 5         | 0h<br>RO         | <b>Reserved</b>  |
| 4         | 0h<br>RO/V       | <b>Override Terminate Attack (OVTATTACK):</b><br>Override of unsolicited connection state attack and terminate<br>0: Disable override; attack terminate allowed<br>1: Enable override; attack terminate disallowed |
| 3         | 0h<br>RO/V       | <b>Heavy Mode Select (HVYMODSEL):</b><br>Heavy/light encryption mode select 0: Surface encryption is disabled - Light mode 1: Surface encryption is enabled  |
| 2         | 0h<br>RO/V       | <b>Lock Bit (LOCK):</b><br>BIOS will set this bit with bit 0 and/or bit 1.   |
| 1         | 0h<br>RO/V       | <b>PAVP Enable (PAVPE):</b><br>0: PAVP functionality disabled 1: PAVP functionality enabled  |



| Bit Range | Default & Access | Field Name (ID): Description                                  |
|-----------|------------------|---|
| 0         | 0h<br>RO/V       | <b>PCM Enable (PCME):</b><br>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<br>RO/V | <b>WOPCM Base MSB (WOPCMBASE_MSB):</b><br>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<br>RO       | <b>Stepping Revision ID MSB (SRID_MSB):</b><br>Upper 4 bit of the Stepping Revision ID. |
| 19:16     | 0h<br>RO         | <b>Stepping Revision ID LSB (SRID_LSB):</b><br>Lower 4 bit of the Stepping Revision ID. |
| 15:0      | 0h<br>RO         | <b>Reserved</b>   |

#### 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<br>RW  | <b>Device Switching Storage (DSS):</b><br>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<br>RO       | <b>Next Capability Offset (NCO):</b><br>This is a hardwired pointer to the next item in the capabilities list. |
| 19:16     | 1h<br>RO         | <b>Version ID (V):</b><br>Hardwired to capability version 1.   |
| 15:0      | 001Bh<br>RO      | <b>Capability ID (CAPID):</b><br>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<br>RO         | <b>Reserved</b>   |
| 12:8      | 14h<br>RO        | <b>Maximum PASID Width (MPW):</b><br>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<br>RO         | <b>Reserved</b>   |
| 2         | 0h<br>RO         | <b>Privilege Mode Supported (PMS):</b><br>Hardwired to 0, the Endpoint supports operating in Non-privileged mode only, and will never request privileged mode in requests-with-PASID. |
| 1         | 0h<br>RO         | <b>Execute Permission Supported (EPS):</b><br>Hardwired to 0, the Endpoint supports requests-with-PASID that requests execute permission.   |
| 0         | 0h<br>RO         | <b>Reserved</b>   |

#### 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<br>RO         | <b>Reserved</b>              |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 2         | 0h<br>RO         | <b>Privileged Mode Enable (PME):</b><br>Hardwired to 0, the Endpoint is not permitted to request privileged mode in requests-with-PASID.   |
| 1         | 0h<br>RW         | <b>Execute Permission Enable (EPE):</b><br>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<br>RW         | <b>PASID Enable (PE):</b><br>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<br>RO       | <b>Next Capability Offset (NCO):</b><br>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<br>RO         | <b>Version ID (V):</b><br>Hardwired to capability version 1.   |
| 15:0      | 000Fh<br>RO      | <b>Capability ID (CAPID):</b><br>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<br>RO         | <b>Reserved</b>   |
| 6         | 1h<br>RO         | <b>Global Invalidate Supported (GIS):</b><br>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<br>RO         | <b>Page Aligned Request (PAR):</b><br>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<br>RO        | <b>Invalidate Queue Depth (IQE):</b><br>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<br>RW         | <b>ATS Enable (AE):</b><br>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<br>RO         | <b>Reserved</b>   |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 4:0       | 00h<br>RW        | <b>Smallest Translation Unit (STU):</b><br>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 <sup>STU</sup> . A value of 0 indicates one block and value 1F indicates 2 <sup>31</sup> 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<br>RO/V     | <b>Next Capability Offset (NCO):</b><br>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<br>RO         | <b>Version ID (V):</b><br>Hardwired to capability version 1.  |
| 15:0      | 0013h<br>RO      | <b>Capability ID (CAPID):</b><br>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<br>RO         | <b>Reserved</b>   |
| 1         | 0h<br>RO         | <b>RST:</b><br>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<br>RW         | <b>Page-Request Enable (PRE):</b><br>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<br>RO         | <p><b>PRG Response PASID Required (PRPR):</b><br/>           If set, the Function expects a PASID TLP Prefix on PRG Response Messages when the corresponding page requests had a PASID TLP Prefix.<br/>           If Clear, the function does not expect PASID TLP Prefixes on any PRG Response Message.<br/>           Function behavior is undefined if this bit is Clear and the Function receives a PRG Response Message with a PASID TLP Prefix.<br/>           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.<br/>           This bit is RsvdZ if the Function does not support the PASID TLP Prefix.</p> |
| 14:9      | 0h<br>RO         | <b>Reserved</b>   |
| 8         | 1h<br>RO         | <p><b>S:</b><br/>           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.</p>  |
| 7:2       | 0h<br>RO         | <b>Reserved</b>   |
| 1         | 0h<br>RW/V       | <p><b>Unexpected Page Request Group Index (UPGRI):</b><br/>           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.</p>  |
| 0         | 0h<br>RW/V       | <p><b>Response Failure (RF):</b><br/>           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.</p>  |

#### 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<br>RO  | <b>Outstanding Page Request Capacity (OPRC):</b><br>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<br>RW  | <b>Outstanding Page Request Allocation (OPRA):</b><br>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<br>RO       | <b>Next Capability Offset (NEXT_0):</b><br>Next capability Offset. Value = 0x000 to indicate the end of the Extended Capability List |
| 19:16     | 1h<br>RO         | <b>Capability Version (CAP_VER):</b><br>Capability Version   |
| 15:0      | 0010h<br>RO      | <b>PCIe Extended Capability ID (PCIE_ECAP_ID):</b><br>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<br>RO       | <b>VF Migration Interrupt Message Number (VF_MIG_INTR_MSG_NUM):</b><br>Value: 0. VF Migration is not supported. |
| 20:2      | 0h<br>RO         | <b>Reserved</b>   |
| 1         | 0h<br>RO         | <b>ARI Capable Hierarchy Preserved (ARI_CAP_HIER_PRESERVED):</b><br>Value: Always 0. ARI is not supported.      |
| 0         | 0h<br>RO         | <b>VF Migration Capable (VF_MIG_CAP):</b><br>Value:0. VF Migration not supported.                               |

#### 4.1.72 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<br>RO         | <b>Reserved</b>   |
| 0         | 0h<br>RO         | <b>VF Migration Status (VF_MIG_STS):</b><br>VF Migration Status |

#### 4.1.73 SRIOV Initial VFs (SRIOV\_INITVFS\_0\_2\_0\_PCI) – Offset 32Ch

Defines Initial number of VFs 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<br>RO/V    | <b>Initial VFs (INITIAL_VFS):</b><br>For SR-IOV implementation, this value must exactly match the Total VFs |

#### 4.1.74 SRIOV Total VFs (SRIOV\_TOTVFS\_0\_2\_0\_PCI) – Offset 32Eh

Defines the Total number of VFs 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<br>RO      | <b>Total VFs (TOTAL_VFS):</b><br>Indicates the maximum number of VFs that could be associated with the PF |

#### 4.1.75 First VF Offset (FIRST\_VF\_OFFSET\_0\_2\_0\_PCI) – Offset 334h

Defines the offset of the function number from the PF to the first VF.

| 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<br>RO      | <b>First VF Offset Value (FIRST_VF_OFFSET):</b><br>Defines the routing ID offset of the first VF that is associated with the PF that contains this Capability structure. The first VFs 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. |

#### 4.1.76 VF Stride (VF\_STRIDE\_0\_2\_0\_PCI) – Offset 336h

Defines the stride of the function number from one VF 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<br>RO      | <b>VF Stride Value (VF_STRIDE):</b><br>Defines the Routing ID offset from one VF to the next one for all VFs associated with the PF that contains this Capability structure. The next VFs 16-bit Routing ID is calculated by adding the contents of this field to the Routing ID of the current VF, ignoring any carry, using unsigned 16-bit arithmetic. The value of this field is hardwired to 0001h. |

#### 4.1.77 VF 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 | 9A40h   |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| R           | R          | R         |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 15:0      | 9A40h<br>RO/V    | <b>VF Device ID (VF_DEVICEID):</b><br>Mirror the same device ID as the PF |

#### 4.1.78 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 | 00000553h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| R           | R          | R         |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 31:0      | 00000553h<br>RO  | <b>Supported Page Sizes Value (PAGE_SIZES):</b><br>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. |

#### 4.1.79 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<br>RO  | <p><b>Graphics System Event Scratch Trigger (SYS_PAGE_SIZES):</b><br/>           This field defines the page size the system will use to map the VFs memory addresses.<br/>           Software must set the value of the System Page Size to one of the page sizes set in the Supported Page Sizes field.<br/>           As with Supported Page Sizes, if bit n is Set in System Page Size, the VFs associated with this PF are required to support a page size of 2<sup>(n+12)</sup>.<br/>           For example, if bit 1 is Set, the system is using an 8-KB page size.<br/>           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.<br/>           The results are undefined if a bit is Set in System Page Size that is not Set in Supported Page Sizes.<br/>           When System Page Size is set, the VF associated with this PF is required to align all BAR resources 20 on a System Page Size boundary.<br/>           Each VF BAR<sub>n</sub> or VF BAR<sub>n</sub> pair shall be aligned on a System Page Size boundary.<br/>           Each VF BAR<sub>n</sub> or VF BAR<sub>n</sub> pair defining a non-zero address space shall be sized to consume an integer multiple of System Page Size bytes.<br/>           All data structures requiring page size alignment within a VF shall be aligned on a System Page Size boundary.<br/>           VF Enable must be zero when System Page Size is written.<br/>           The results are undefined if System Page Size is written when VF Enable is Set.<br/>           Default value is 1h (i.e., 4 KB), and that is the only value allowed for this implementation</p> |

#### 4.1.80 VF 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 VFs.

The HPA of the GTTMMADR for Virtual Function n = VF 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<br>RW/V      | <b>VF GTTMMADDR Lower DWORD (VF_GTTMMADDR_LDW):</b><br>VF GTTMMADDR Lower DWORD                |
| 23:4      | 00000h<br>RO     | <b>VF GTTMMADDR Lower DWORD Mask (VF_GTTMMADDR_LDW_MASK):</b><br>VF GTTMMADDR Lower DWORD Mask |
| 3         | 0h<br>RO         | <b>BAR is Prefetchable (PREFETCHABLE):</b><br>BAR is Prefetchable                              |
| 2:1       | 2h<br>RO         | <b>BAR Type (BAR_TYPE):</b><br>A value of 10 indicates a 64 bit BAR.                           |
| 0         | 0h<br>RO         | <b>Memory Space Indicator (MEM_SPACE_IND):</b><br>A value 0 indicates a memory space.          |

#### 4.1.81 VF 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 VFs

| 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<br>RW/V | <b>VF GTTMMADDR Upper DWORD (VF_GTTMMADDR_UDW):</b><br>VF GTTMMADDR Upper DWORD |

#### 4.1.82 VF 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 VFs.



| 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<br>RW/V       | <b>VF GMADDR Lower DWORD (VF_GMADDR_LDW):</b><br>VF GMADDR Lower DWORD                |
| 28:4      | 0000000h<br>RO   | <b>VF GMADDR Lower DWORD Mask (VF_GMADDR_LDW_MASK):</b><br>VF GMADDR Lower DWORD Mask |
| 3         | 1h<br>RO         | <b>BAR is Prefetchable (PREFETCHABLE):</b><br>BAR is Prefetchable                     |
| 2:1       | 2h<br>RO         | <b>BAR Type (BAR_TYPE):</b><br>A value of 10 indicates a 64 bit BAR.                  |
| 0         | 0h<br>RO         | <b>Memory Space Indicator (MEM_SPACE_IND):</b><br>A value 0 indicates a memory space. |

#### 4.1.83 VF 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 VFs

| 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<br>RW/V | <b>VF GMADDR Upper DWORD (VF_GMADDR_UDW):</b><br>VF GMADDR Upper DWORD |

#### 4.1.84 VF Migration State Array Offset (VF\_MIGST\_OFFSET\_0\_2\_0\_PCI) – Offset 35Ch

Defines offset from a PF BAR to the VF Migration State Array. VF 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.

### 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)             | 0000079E2FF050DFh |
| 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         |
| A8h    | 4            | Invalidation Event Address Register (IEADDR_REG_0_0_0_VTDBAR)    | 00000000h         |

| Offset | Size (Bytes) | Register Name (Register Symbol)  | Default Value     |
|--------|--------------|--|-------------------|
| 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 |
| 198h   | 8            | Variable-Range MTRR Format Physical Mask 1 (MTRR_PHYSMASK1_REG_0_0_0_VTDBAR) | 0000000000000000h |

| Offset | Size (Bytes) | Register Name (Register Symbol)  | Default Value     |
|--------|--------------|--|-------------------|
| 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<br>RO         | <b>Reserved</b>   |
| 7:4       | 4h<br>RO         | <b>Major Version Number (MAJOR):</b><br>Indicates supported architecture version.       |
| 3:0       | 0h<br>RO         | <b>Minor Version Number (MINOR):</b><br>Indicates supported architecture minor version. |

### 4.2.3 Capability Register (CAP\_REG\_0\_0\_0\_VTD BAR) – 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  |
|-----------|------------------|---|
| 63:61     | 0h<br>RO         | <b>Reserved</b>   |
| 60        | 0h<br>RO         | <b>First Level 5-level Paging (FL5LP):</b> <ul style="list-style-type: none"> <li>0: Hardware does not support 5-level paging for requests-with-PASID subject to first-level translation.</li> <li>1: Hardware supports 5-level paging for requests-with-PASID subject to first-level translation.</li> </ul>                                   |
| 59        | 1h<br>RO         | <b>Posted Interrupt Support (PI):</b> <ul style="list-style-type: none"> <li>0 = Hardware does not support Posting of Interrupts.</li> <li>1 = Hardware supports Posting of Interrupts.</li> </ul> Hardware implementations reporting this field as Set must also report Interrupt Remapping support (IR field in Extended Capability Register) |
| 58:57     | 0h<br>RO         | <b>Reserved</b>   |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 56        | 1h<br>RO         | <b>First Level 1-GByte Page Support (FL1GP):</b><br>A value of 1 in this field indicates 1-GByte page size is supported for first-level translation.  |
| 55        | 1h<br>RO         | <b>Read Draining (DRD):</b> <ul style="list-style-type: none"> <li>0 = Hardware does not support draining of DMA read requests.</li> <li>1 = Hardware supports draining of DMA read requests.</li> </ul>  |
| 54        | 1h<br>RO         | <b>Write Draining (DWD):</b> <ul style="list-style-type: none"> <li>0 = Hardware does not support draining of DMA write requests.</li> <li>1 = Hardware supports draining of DMA write requests.</li> </ul>   |
| 53:48     | 00h<br>RO        | <b>Maximum Address Mask Value (MAMV):</b><br>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<br>RO        | <b>Number of Fault-Recording Registers (NFR):</b><br>Number of fault recording registers is computed as N+1, where N is the value reported in this field.<br>Implementations must support at least one fault recording register (NFR = 0) for each remapping hardware unit in the platform.<br>The maximum number of fault recording registers per remapping hardware unit is 256.  |
| 39        | 0h<br>RO         | <b>Page Selective Invalidation (PSI):</b> <ul style="list-style-type: none"> <li>0 = Hardware supports only domain and global invalidates for IOTLB.</li> <li>1 = Hardware supports page selective, domain and global invalidates for IOTLB.</li> </ul> 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<br>RO         | <b>Reserved</b>   |
| 37:34     | 3h<br>RO         | <b>Second Level Large Page Support (SLLPS):</b><br>This field indicates the super page sizes supported by hardware.<br>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: <ul style="list-style-type: none"> <li>0 = 21-bit offset to page frame (2MB)</li> <li>1 = 30-bit offset to page frame (1GB)</li> <li>2 = 39-bit offset to page frame (512GB)</li> <li>3 = 48-bit offset to page frame (1TB)</li> </ul> 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<br>RO       | <b>Fault-Recording Register Offset (FRO):</b><br>This field specifies the location to the first fault recording register relative to the register base address of this remapping hardware unit.<br>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<br>RO         | <b>Reserved</b>   |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 22        | 1h<br>RO         | <p><b>Zero Length Read (ZLR):</b></p> <ul style="list-style-type: none"> <li>0 = Indicates the remapping hardware unit blocks (and treats as fault) zero length DMA read requests to write-only pages.</li> <li>1 = Indicates the remapping hardware unit supports zero length DMA read requests to write-only pages.</li> </ul> <p>DMA remapping hardware implementations are recommended to report ZLR field as Set.</p>   |
| 21:16     | 2Fh<br>RO        | <p><b>Maximum Guest Address Width (MGAW):</b></p> <p>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.</p> <p>If the value in this field is X, untranslated and translated DMA requests to addresses above <math>2(x+1)-1</math> are always blocked by hardware. Translations requests to address above <math>2(x+1)-1</math> from allowed devices return a null Translation Completion Data Entry with R=W=0.</p> <p>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).</p> <p>Implementations are recommended to support MGAW at least equal to the physical addressability (host address width) of the platform.</p> |
| 15:13     | 0h<br>RO         | <b>Reserved</b>  |
| 12:8      | 04h<br>RO        | <p><b>Supported Adjusted Guest Address Widths (SAGAW):</b></p> <p>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.</p> <p>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:</p> <ul style="list-style-type: none"> <li>0 = 30-bit AGAW (2-level page table)</li> <li>1 = 39-bit AGAW (3-level page table)</li> <li>2 = 48-bit AGAW (4-level page table)</li> <li>3 = 57-bit AGAW (5-level page table)</li> <li>4 = Reserved</li> </ul> <p>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.</p>  |
| 7         | 0h<br>RO         | <p><b>Caching Mode (CM):</b></p> <ul style="list-style-type: none"> <li>0 = Not-present and erroneous entries are not cached in any of the remapping caches. Invalidation 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.</li> <li>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.</li> </ul> <p>Hardware implementations of this architecture must support a value of 0 in this field.</p>  |
| 6         | 1h<br>RO         | <p><b>Protected High-Memory Region (PHMR):</b></p> <ul style="list-style-type: none"> <li>0 = Indicates protected high-memory region is not supported.</li> <li>1 = Indicates protected high-memory region is supported.</li> </ul>  |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 5         | 1h<br>RO         | <b>Protected Low-Memory Region (PLMR):</b> <ul style="list-style-type: none"> <li>0 = Indicates protected low-memory region is not supported.</li> <li>1 = Indicates protected low-memory region is supported.</li> </ul>  |
| 4         | 0h<br>RO         | <b>Required Write-Buffer Flushing (RWBF):</b> <ul style="list-style-type: none"> <li>0 = Indicates no write-buffer flushing is needed to ensure changes to memory-resident structures are visible to hardware.</li> <li>1 = Indicates software must explicitly flush the write buffers to ensure updates made to memory-resident remapping structures are visible to hardware.</li> </ul>  |
| 3         | 0h<br>RO         | <b>Advanced Fault Logging (AFL):</b> <ul style="list-style-type: none"> <li>0 = Indicates advanced fault logging is not supported. Only primary fault logging is supported.</li> <li>1 = Indicates advanced fault logging is supported.</li> </ul>   |
| 2:0       | 6h<br>RO         | <b>Number of Domains Supported (ND):</b> <ul style="list-style-type: none"> <li>000b = Hardware supports 4-bit domain-ids with support for up to 16 domains.</li> <li>001b = Hardware supports 6-bit domain-ids with support for up to 64 domains.</li> <li>010b = Hardware supports 8-bit domain-ids with support for up to 256 domains.</li> <li>011b = Hardware supports 10-bit domain-ids with support for up to 1024 domains.</li> <li>100b = Hardware supports 12-bit domain-ids with support for up to 4K domains.</li> <li>100b = Hardware supports 14-bit domain-ids with support for up to 16K domains.</li> <li>110b = Hardware supports 16-bit domain-ids with support for up to 64K domains.</li> <li>111b = Reserved.</li> </ul> |

#### 4.2.4 Extended Capability Register (ECAP\_REG\_0\_0\_0\_VTD BAR) – Offset 10h

Register to report remapping hardware extended capabilities.

| Type | Size   | Offset         | Default           |
|------|--------|----------------|-------------------|
| MMIO | 64 bit | GFXVTBAR + 10h | 0000079E2FF050DFh |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| R           | R          | R         |

| Bit Range | Default & Access | Field Name (ID): Description |
|-----------|------------------|------------------------------|
| 63:44     | 0h<br>RO         | <b>Reserved</b>              |



| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 43        | 0h<br>RO         | <p><b>PASID Support Limitation (PSL):</b></p> <p>This field is valid only when Process Address Space ID Support (PASID) field (bit 40) is reported as Set. When this field is reported as Set, extended context-entries with PASID Enable (PASIDE) field Set do not support Requests-without PASID.</p> <p>Hardware implementations must report a value of 0 in this field. Virtual implementations may report a value of 1 in this field to disallow guest software from using an extended-context-entry for both Virtual Address (VA) and I/O Virtual Address (IOVA) concurrently.</p> |
| 42        | 1h<br>RO         | <p><b>Page Request Draining Support (PDS):</b></p> <ul style="list-style-type: none"> <li>0 = Hardware does not support Page-Request Drain (PD) flag in Inv_wait_dsc.</li> <li>1 = Hardware supports Page-Request Drain (PD) flag in Inv_wait_dsc.</li> </ul> <p>This field is valid only when Device-TLB support field is reported as Set.</p>  |
| 41        | 1h<br>RO         | <p><b>Device-TLB Invalidation Throttle (DIT):</b></p> <ul style="list-style-type: none"> <li>0 = Hardware does not support Device-TLB Invalidation Throttling.</li> <li>1 = Hardware supports Device-TLB Invalidation Throttling.</li> </ul> <p>This field is valid only when Page Request Support (PRS) field is reported as Set.</p>   |
| 40        | 1h<br>RO         | <p><b>Process Address Space ID Support (PASID):</b></p> <ul style="list-style-type: none"> <li>0 = Hardware does not support requests tagged with Process Address Space IDs.</li> <li>1 = Hardware supports requests tagged with Process Address Space IDs.</li> </ul>   |
| 39:35     | 13h<br>RO        | <p><b>PASID Size Supported (PSS):</b></p> <p>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.</p> <p>This field is valid only when PASID field is reported as Set.</p>   |
| 34        | 1h<br>RO         | <p><b>Extended Accessed Flag Support (EAFS):</b></p> <ul style="list-style-type: none"> <li>0 = Hardware does not support the extended-accessed (EA) bit in first-level paging-structure entries.</li> <li>1 = Hardware supports the extended accessed (EA) bit in first-level paging-structure entries.</li> </ul> <p>This field is valid only when PASID field is reported as Set.</p>   |
| 33        | 1h<br>RO         | <p><b>No Write Flag Support (NWFS):</b></p> <ul style="list-style-type: none"> <li>0 = Hardware ignores the No Write (NW) flag in Device-TLB translation requests, and behaves as if NW is always 0.</li> <li>1 = Hardware supports the No Write (NW) flag in Device-TLB translation requests.</li> </ul> <p>This field is valid only when Device-TLB support (DT) field is reported as Set.</p>   |
| 32        | 0h<br>RO         | <b>Reserved</b>  |
| 31        | 0h<br>RO         | <p><b>Supervisor Request Support (SRS):</b></p> <ul style="list-style-type: none"> <li>0 = H/W does not support requests-with-PASID seeking supervisor privilege.</li> <li>1 = H/W supports requests-with-PASID seeking supervisor privilege.</li> </ul> <p>The field is valid only when PASID field is reported as Set.</p>   |
| 30        | 0h<br>RO         | <p><b>Execute Request Support (ERS):</b></p> <ul style="list-style-type: none"> <li>0 = H/W does not support requests-with-PASID seeking execute permission.</li> <li>1 = H/W supports requests-with-PASID seeking execute permission.</li> </ul> <p>This field is valid only when PASID field is reported as Set.</p>   |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 29        | 1h<br>RO         | <b>Page Request Support (PRS):</b> <ul style="list-style-type: none"> <li>0 = Hardware does not support Page Requests.</li> <li>1 = Hardware supports Page Requests</li> </ul> This field is valid only when Device-TLB (DT) field is reported as Set.  |
| 28        | 0h<br>RO         | <b>IGN:</b><br>Ignore this field  |
| 27        | 1h<br>RO         | <b>Deferred Invalidate Support (DIS):</b> <ul style="list-style-type: none"> <li>0 = Hardware does not support deferred invalidations of IOTLB and Device-TLB.</li> <li>1 = Hardware supports deferred invalidations of IOTLB and Device-TLB.</li> </ul> This field is valid only when PASID field is reported as Set.  |
| 26        | 1h<br>RO         | <b>Nested Translation Support (NEST):</b> <ul style="list-style-type: none"> <li>0 = Hardware does not support nested translations.</li> <li>1 = Hardware supports nested translations.</li> </ul> This field is valid only when PASID field is reported as Set.  |
| 25        | 1h<br>RO         | <b>Memory Type Support (MTS):</b> <ul style="list-style-type: none"> <li>0 = Hardware does not support Memory Type in first-level translation and Extended Memory type in second-level translation.</li> <li>1 = Hardware supports Memory Type in first-level translation and Extended Memory type in second-level translation.</li> </ul> This field is valid only when PASID and ECS fields are reported as Set.<br>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<br>RO         | <b>Extended Context Support (ECS):</b> <ul style="list-style-type: none"> <li>0 = Hardware does not support extended-root-entries and extended-context-entries.</li> <li>1 = Hardware supports extended-root-entries and extended-context-entries.</li> </ul> Implementations reporting PASID or PRS fields as Set, must report this field as Set.  |
| 23:20     | Fh<br>RO         | <b>Maximum Handle Mask Value (MHMV):</b><br>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).<br>This field is valid only when the IR field in Extended Capability register is reported as Set.  |
| 19:18     | 0h<br>RO         | <b>Reserved</b>   |
| 17:8      | 050h<br>RO       | <b>IOTLB Register Offset (IRO):</b><br>This field specifies the offset to the IOTLB registers relative to the register base address of this remapping hardware unit.<br>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<br>RO         | <b>Snoop Control (SC):</b> <ul style="list-style-type: none"> <li>0 = Hardware does not support 1-setting of the SNP field in the page-table entries.</li> <li>1 = Hardware supports the 1-setting of the SNP field in the page-table entries.</li> </ul>   |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 6         | 1h<br>RO         | <p><b>Pass Through (PT):</b></p> <ul style="list-style-type: none"> <li>0 = Hardware does not support pass-through translation type in context entries and extended-context-entries.</li> <li>1 = Hardware supports pass-through translation type in context entries and extended-context-entries.</li> </ul> <p>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.</p>  |
| 5         | 0h<br>RO         | <b>Reserved</b>  |
| 4         | 1h<br>RO         | <p><b>Extended Interrupt Mode (EIM):</b></p> <ul style="list-style-type: none"> <li>0 = On Intel64 platforms, hardware supports only 8-bit APIC-IDs (xAPIC mode).</li> <li>1 = On Intel64 platforms, hardware supports 32-bit APIC-IDs (x2APIC mode).</li> </ul> <p>This field is valid only on Intel64 platforms reporting Interrupt Remapping support (IR field Set).</p>  |
| 3         | 1h<br>RO         | <p><b>Interrupt Remapping support (IR):</b></p> <ul style="list-style-type: none"> <li>0 = Hardware does not support interrupt remapping.</li> <li>1 = Hardware supports interrupt remapping.</li> </ul> <p>Implementations reporting this field as Set must also support Queued Invalidation (QI).</p>  |
| 2         | 1h<br>RO         | <p><b>Device-TLB Support (DT):</b></p> <ul style="list-style-type: none"> <li>0 = Hardware does not support device-IOTLBs.</li> <li>1 = Hardware supports Device-IOTLBs.</li> </ul> <p>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.</p>  |
| 1         | 1h<br>RO         | <p><b>Queued Invalidation Support (QI):</b></p> <ul style="list-style-type: none"> <li>0 = Hardware does not support queued invalidations.</li> <li>1 = Hardware supports queued invalidations.</li> </ul>   |
| 0         | 1h<br>RO         | <p><b>Page-Walk Coherency (C):</b></p> <p>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.</p> <ul style="list-style-type: none"> <li>0 = Indicates hardware accesses to remapping structures are non-coherent.</li> <li>1 = Indicates hardware accesses to remapping structures are coherent.</li> </ul> <p>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.</p> |

#### 4.2.5 Global Command Register (GCMD\_REG\_0\_0\_0\_VTD BAR) – 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

Register to control r mapping hardware. If multiple control fields in this register need to be modified, software must serialize the modifications through multiple writes to this register

- 1. Tmp = Read GSTS\_REG
- 2. Status = (Tmp & 96FFFFFFh) // Reset the one-shot bits
- 3. Command = (Status | (Y << X))
- 4. Write Command to GCMD\_REG
- 5. Wait until GSTS\_REG[X] indicates command is serviced.

| 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<br>RW         | <p><b>Translation Enable (TE):</b><br/>Software writes to this field to request hardware to enable/disable DMA-remapping:</p> <ul style="list-style-type: none"> <li>• 0 = Disable DMA remapping.</li> <li>• 1 = Enable DMA remapping.</li> </ul> <p>Hardware reports the status of the translation enable operation through the TES field in the Global Status register.</p> <p>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.</p> <p>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.</p> <p>The value returned on a read of this field is undefined.</p>   |
| 30        | 0h<br>WO         | <p><b>Set Root Table Pointer (SRTP):</b><br/>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.</p> <p>Hardware reports the status of the Set Root Table Pointer operation through the RTPS field in the Global Status register.</p> <p>The Set Root Table Pointer operation must be performed before enabling or re-enabling (after disabling) DMA remapping through the TE field.</p> <p>.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.</p> <p>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.</p> <p>Clearing this bit has no effect. The value returned on read of this field is undefined.</p> |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 29        | 0h<br>RO         | <p><b>Set Fault Log (SFL):</b><br/>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.</p> <p>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.</p>   |
| 28        | 0h<br>RO         | <p><b>Enable Advanced Fault Logging (EAFL):</b><br/>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:</p> <ul style="list-style-type: none"> <li>• 0 = Disable advanced fault logging. In this case, translation faults are reported through the Fault Recording registers.</li> <li>• 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.</li> </ul> <p>The value returned on read of this field is undefined.</p>   |
| 27        | 0h<br>RO         | <p><b>Write Buffer Flush (WBF):</b><br/>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.</p>   |
| 26        | 0h<br>RW         | <p><b>Queued Invalidation Enable (QIE):</b><br/>This field is valid only for implementations supporting queued invalidations. Software writes to this field to enable or disable queued invalidations.</p> <ul style="list-style-type: none"> <li>• 0 = Disable queued invalidations.</li> <li>• 1 = Enable use of queued invalidations.</li> </ul> <p>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.</p>  |
| 25        | 0h<br>RW         | <p><b>Interrupt Remapping Enable (IRE):</b><br/>This field is valid only for implementations supporting interrupt remapping.</p> <ul style="list-style-type: none"> <li>• 0 = Disable interrupt-remapping hardware.</li> <li>• 1 = Enable interrupt-remapping hardware.</li> </ul> <p>Hardware reports the status of the interrupt remapping enable operation through the IRES field in the Global Status register.</p> <p>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.</p> <p>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.</p> |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 24        | 0h<br>WO         | <p><b>Set Interrupt Remap Table Pointer (SIRTP):</b><br/>           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.</p> |
| 23        | 0h<br>RW         | <p><b>Compatibility Format Interrupt (CFI):</b><br/>           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.</p> <ul style="list-style-type: none"> <li>• 0 = Block Compatibility format interrupts.</li> <li>• 1 = Process Compatibility format interrupts as pass-through (bypass interrupt remapping).</li> </ul> <p>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.</p>  |
| 22:0      | 0h<br>RO         | <b>Reserved</b>  |

#### 4.2.6 Global Status Register (GSTS\_REG\_0\_0\_0\_VTD BAR) — 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<br>RO/V       | <p><b>Translation Enable Status (TES):</b><br/>This field indicates the status of DMA-remapping hardware.</p> <ul style="list-style-type: none"> <li>0 = DMA-remapping hardware is not enabled.</li> <li>1 = DMA-remapping hardware is enabled</li> </ul>  |
| 30        | 0h<br>RO/V       | <p><b>Root Table Pointer Status (RTPS):</b><br/>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.</p>  |
| 29        | 0h<br>RO         | <p><b>Fault Log Status (FLS):</b><br/>This field:</p> <ul style="list-style-type: none"> <li>Is cleared by hardware when software Sets the SFL field in the Global Command register.</li> <li>Is Set by hardware when hardware completes the Set Fault Log Pointer operation using the value provided in the Advanced Fault Log register.</li> </ul>   |
| 28        | 0h<br>RO         | <p><b>Advanced Fault Logging Status (AFLS):</b><br/>This field is valid only for implementations supporting advanced fault logging. It indicates the advanced fault logging status:</p> <ul style="list-style-type: none"> <li>0 = Advanced Fault Logging is not enabled.</li> <li>1 = Advanced Fault Logging is enabled.</li> </ul>   |
| 27        | 0h<br>RO         | <p><b>Write Buffer Flush Status (WBFS):</b><br/>This field is valid only for implementations requiring write buffer flushing. This field indicates the status of the write buffer flush command. It is:</p> <ul style="list-style-type: none"> <li>Set by hardware when software sets the WBF field in the Global Command register.</li> <li>Cleared by hardware when hardware completes the write buffer flushing operation.</li> </ul> |
| 26        | 0h<br>RO/V       | <p><b>Queued Invalidation Enable Status (QIES):</b><br/>This field indicates queued invalidation enable status.</p> <ul style="list-style-type: none"> <li>0 = queued invalidation is not enabled.</li> <li>1 = queued invalidation is enabled</li> </ul>  |
| 25        | 0h<br>RO/V       | <p><b>Interrupt Remapping Enable Status (IRES):</b><br/>This field indicates the status of Interrupt-remapping hardware.</p> <ul style="list-style-type: none"> <li>0 = Interrupt-remapping hardware is not enabled.</li> <li>1 = Interrupt-remapping hardware is enabled</li> </ul>   |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 24        | 0h<br>RO/V       | <b>Interrupt Remapping Pointer Status (IRTPS):</b><br>This field indicates the status of the interrupt remapping table pointer in hardware. This field is cleared by hardware when software sets the SIRTTP 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<br>RO/V       | <b>Compatibility Format Interrupt Status (CFIS):</b><br>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. <ul style="list-style-type: none"> <li>0 = Compatibility format interrupts are blocked.</li> <li>1 = Compatibility format interrupts are processed as pass-through (bypassing interrupt remapping).</li> </ul> |
| 22:0      | 0h<br>RO         | <b>Reserved</b>  |

## 4.2.7 Root Table Address Register (RTADDR\_REG\_0\_0\_0\_VTD BAR) – 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<br>RO              | <b>Reserved</b>  |
| 51:12     | 00000000<br>00h<br>RW | <b>Root Table Address (RTA):</b><br>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 SRTTP field in the Global Command register. Reads of this register returns value that was last programmed to it. |
| 11        | 0h<br>RW              | <b>Root Table Type (RTT):</b><br>This field specifies the type of root-table referenced by the Root Table Address (RTA) field: <ul style="list-style-type: none"> <li>0 = Root Table.</li> <li>1 = Extended Root Table</li> </ul>  |
| 10:0      | 0h<br>RO              | <b>Reserved</b>  |





## 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<br>RW/V       | <p><b>Invalidate Context Cache (ICC):</b><br/>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.<br/>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.<br/>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.<br/>Hardware implementations reporting write-buffer flushing requirement (RWBF=1 in Capability register) must implicitly perform a write buffer flush before invalidating the context cache.</p> |
| 62:61     | 0h<br>RW         | <p><b>Context Invalidation Request Granularity (CIRG):</b><br/>Software provides the requested invalidation granularity through this field when setting the ICC field:</p> <ul style="list-style-type: none"> <li>• 00: Reserved.</li> <li>• 01: Global Invalidation request.</li> <li>• 10: Domain-selective invalidation request. The target domain-id must be specified in the DID field.</li> <li>• 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.</li> </ul> <p>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.</p>   |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 60:59     | 1h<br>RO/V       | <p><b>Context Actual Invalidation Granularity (CAIG):</b><br/>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).<br/>The following are the encodings for this field:</p> <ul style="list-style-type: none"> <li>• 00: Reserved.</li> <li>• 01: Global Invalidation performed. This could be in response to a global, domain-selective or device-selective invalidation request.</li> <li>• 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.</li> <li>• 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.</li> </ul> |
| 58:34     | 0h<br>RO         | <b>Reserved</b>   |
| 33:32     | 0h<br>RW         | <p><b>Function Mask (FM):</b><br/>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:</p> <ul style="list-style-type: none"> <li>• 00: No bits in the SID field masked.</li> <li>• 01: Mask most significant bit of function number in the SID field.</li> <li>• 10: Mask two most significant bit of function number in the SID field.</li> <li>• 11: Mask all three bits of function number in the SID field.</li> </ul> <p>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.</p>  |
| 31:16     | 0000h<br>RW      | <p><b>SID:</b><br/>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.</p>   |
| 15:0      | 0000h<br>RW      | <p><b>DID:</b><br/>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.<br/>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.</p>  |

#### 4.2.9 Fault Status Register (FSTS\_REG\_0\_0\_0\_VTD BAR) — 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<br>RO         | <b>Reserved</b>  |
| 15:8      | 00h<br>RO        | <b>Fault Record Index (FRI):</b><br>This field is valid only when the PPF field is Set.<br>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.<br>The value read from this field is undefined when the PPF field is clear.   |
| 7         | 0h<br>RW/1C      | <b>Page Request Overflow (PRO):</b><br>Hardware detected a Page Request Overflow error. Hardware implementations not supporting the Page Request Queue implement this bit as RsvdZ.  |
| 6         | 0h<br>RW/1C      | <b>Invalidation Time-out Error (ITE):</b><br>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.<br>Hardware implementations not supporting device Device-IOTLBs implement this bit as RsvdZ.  |
| 5         | 0h<br>RW/1C      | <b>Invalidation Completion Error (ICE):</b><br>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 the Fault Event Control register.<br>Hardware implementations not supporting Device-IOTLBs implement this bit as RsvdZ.  |
| 4         | 0h<br>RW/1C      | <b>Invalidation Queue Error (IQE):</b><br>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.<br>Hardware implementations not supporting queued invalidations implement this bit as RsvdZ. |
| 3         | 0h<br>RO         | <b>Advanced Pending Fault (APF):</b><br>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.<br>Software writing 1 to this field clears it. Hardware implementations not supporting advanced fault logging implement this bit as RsvdZ.   |
| 2         | 0h<br>RO         | <b>Advanced Fault Overflow (AFO):</b><br>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.<br>Software writing 1 to this field clears it.<br>Hardware implementations not supporting advanced fault logging implement this bit as RsvdZ.  |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 1         | 0h<br>RO/V       | <p><b>Primary Pending Fault (PPF):</b><br/>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.</p> <ul style="list-style-type: none"> <li>0 = No pending faults in any of the fault recording registers.</li> <li>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.</li> </ul> |
| 0         | 0h<br>RW/1C      | <p><b>Primary Fault Overflow (PFO):</b><br/>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.</p>   |

#### 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<br>RW         | <p><b>Interrupt Mask (IM):</b></p> <ul style="list-style-type: none"> <li>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).</li> <li>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.</li> </ul> |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 30        | 0h<br>RO/V       | <p><b>Interrupt Pending (IP):</b><br/>Hardware sets the IP field whenever it detects an interrupt condition, which is defined as:</p> <ul style="list-style-type: none"> <li>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.</li> <li>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.</li> <li>Hardware detected error associated with the Invalidation Queue, setting the IQE field in the Fault Status register.</li> <li>Hardware detected invalid Device-IOTLB invalidation completion, setting the ICE field in the Fault Status register.</li> <li>Hardware detected Device-IOTLB invalidation completion time-out, setting the ITE field in the Fault Status register.</li> </ul> <p>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.</p> <p>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.</p> <p>The IP field is cleared by hardware as soon as the interrupt message pending condition is serviced. This could be due to either:</p> <ul style="list-style-type: none"> <li>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.</li> <li>Software servicing all the pending interrupt status fields in the Fault Status register as follows: <ul style="list-style-type: none"> <li>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.</li> <li>Software clearing other status fields in the Fault Status register by writing back the value read from the respective fields.</li> </ul> </li> </ul> |
| 29:0      | 0h<br>RO         | <b>Reserved</b>  |

#### 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<br>RW      | <b>Extended Interrupt Message Data (EIMD):</b><br>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<br>RW      | <b>Interrupt Message Data (IMD):</b><br>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<br>RW  | <b>Message Address (MA):</b><br>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<br>RO         | <b>Reserved</b>   |

#### 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<br>RW  | <b>Message Upper Address (MUA):</b><br>Hardware implementations supporting Extended Interrupt Mode are required to implement this register.<br>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\_VTD BAR) – 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     | 00000000<br>00000h<br>RO | <b>Fault Log Address (FLA):</b><br>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.<br>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<br>RO                 | <b>Fault Log Size (FLS):</b><br>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<br>RO                 | <b>Reserved</b>  |

## 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, PLMLIMIT, 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<br>RW         | <p><b>Enable Protected Memory (EPM):</b><br/>This field controls DMA accesses to the protected low-memory and protected high-memory regions.</p> <ul style="list-style-type: none"> <li>0 = Protected memory regions are disabled.</li> <li>1 = Protected memory regions are enabled. DMA requests accessing protected memory regions are handled as follows: <ul style="list-style-type: none"> <li>When DMA remapping is not enabled, all DMA requests accessing protected memory regions are blocked.</li> <li>When DMA remapping is enabled: <ul style="list-style-type: none"> <li>DMA requests processed as pass-through (Translation Type value of 10b in Context-Entry) and accessing the protected memory regions are blocked.</li> <li>DMA requests with translated address (AT=10b) and accessing the protected memory regions are blocked.</li> <li>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.</li> </ul> </li> </ul> </li> </ul> <p>Remapping hardware access to the remapping structures are not subject to protected memory region checks.<br/>DMA requests blocked due to protected memory region violation are not recorded or reported as remapping faults.<br/>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.<br/>After writing to this field software must wait for the operation to be completed and reflected in the PRS status field (bit 0) before changing the value of this field again.</p> |
| 30:1      | 0h<br>RO         | <b>Reserved</b>  |



| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 0         | 0h<br>RO/V       | <b>Protected Region Status (PRS):</b><br>This field indicates the status of protected memory region(s): <ul style="list-style-type: none"> <li>• 0 = Protected memory region(s) disabled.</li> <li>• 1 = Protected memory region(s) enabled.</li> </ul> |

#### 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<br>RW       | <b>Protected Low-Memory Base (PLMB):</b><br>This register specifies the base of protected low-memory region in system memory. |
| 19:0      | 0h<br>RO         | <b>Reserved</b>   |

#### 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<br>RW       | <b>Protected Low-Memory Limit (PLML):</b><br>This register specifies the last host physical address of the DMA-protected low-memory region in system memory. |
| 19:0      | 0h<br>RO         | <b>Reserved</b>  |

#### 4.2.18 Protected High-Memory Base Register (PHMBASE\_REG\_0\_0\_0\_VTD BAR) – 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<br>RO         | <b>Reserved</b>   |
| 38:20     | 00000h<br>RW     | <b>Protected High-Memory Base (PHMB):</b><br>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<br>RO         | <b>Reserved</b>   |

#### 4.2.19 Protected High-Memory Limit Register (PHMLIMIT\_REG\_0\_0\_0\_VTD BAR) – 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<br>RO         | <b>Reserved</b>  |
| 38:20     | 00000h<br>RW     | <b>Protected High-Memory Limit (PHML):</b><br>This register specifies the last host physical address of the DMA-protected high-memory region in system memory<br>Hardware ignores and does not implement bits 63:HAW, where HAW is the host address width. |
| 19:0      | 0h<br>RO         | <b>Reserved</b>  |

## 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<br>RO         | <b>Reserved</b>   |
| 18:4      | 0000h<br>RO/V    | <b>Queue Head (QH):</b><br>Specifies the offset (128-bit aligned) to the invalidation queue for the command that will be fetched next by hardware<br>Hardware resets this field to 0 whenever the queued invalidation is disabled (QIES field Clear in the Global Status register). |
| 3:0       | 0h<br>RO         | <b>Reserved</b>   |



#### 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<br>RO         | <b>Reserved</b>  |
| 18:4      | 0000h<br>RW      | <b>Queue Tail (QT):</b><br>Specifies the offset (128-bit aligned) to the invalidation queue for the command that will be written next by software. |
| 3:0       | 0h<br>RO         | <b>Reserved</b>  |

#### 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<br>RO         | <b>Reserved</b>  |
| 38:12     | 0000000h<br>RW   | <b>Invalidation Queue Base Address (IQA):</b><br>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<br>RO         | <b>Reserved</b>  |
| 2:0       | 0h<br>RW         | <b>Queue Size (QS):</b><br>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 | 0000000h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 31:1      | 0h<br>RO         | <b>Reserved</b>   |
| 0         | 0h<br>RW/1C      | <b>Invalidation Wait Descriptor Complete (IWC):</b><br>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<br>RW         | <p><b>Interrupt Mask (IM):</b></p> <ul style="list-style-type: none"> <li>0= No masking of interrupt. When a invalidation event condition is detected, hardware issues an interrupt message (using the Invalidation Event Data &amp; Invalidation Event Address register values)</li> <li>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.</li> </ul>  |
| 30        | 0h<br>RO/V       | <p><b>Interrupt Pending (IP):</b><br/>Hardware sets the IP field whenever it detects an interrupt condition. Interrupt condition is defined as:</p> <ul style="list-style-type: none"> <li>An Invalidation Wait Descriptor with Interrupt Flag (IF) field Set completed, setting the IWC field in the Invalidation Completion Status register</li> <li>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</li> </ul> <p>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:</p> <ul style="list-style-type: none"> <li>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</li> <li>1= Software servicing the IWC field in the Invalidation Completion Status register.</li> </ul> |
| 29:0      | 0h<br>RO         | <b>Reserved</b>  |

#### 4.2.25 Invalidation Event Data Register (IEDATA\_REG\_0\_0\_0\_VTD BAR) – 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<br>RW      | <b>Extended Interrupt Message Data (EIMD):</b><br>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<br>RW      | <b>Interrupt Message Data (IMD):</b><br>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<br>RW  | <b>Message Upper Address (MUA):</b><br>Hardware implementations supporting Queued Invalidation and Extended Interrupt Mode are required to implement this register. Hardware implementations not supporting Queued Invalidation 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     | 00000000<br>00000h<br>RW | <b>Interrupt Remapping Table Address (IRTA):</b><br>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.<br>Reads of this field returns value that was last programmed to it.  |
| 11        | 0h<br>RW                 | <b>Extended Interrupt Mode Enable (EIME):</b><br>This field is used by hardware on Intel64 platforms as follows: <ul style="list-style-type: none"> <li>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</li> <li>1= x2APIC mode is active. Hardware interprets all 32-bits of Destination-ID field in the IRTEs</li> </ul> This field is implemented as RsvdZ on implementations reporting Extended Interrupt Mode (EIM) field as Clear in Extended Capability register. |
| 10:4      | 0h<br>RO                 | <b>Reserved</b>   |
| 3:0       | 0h<br>RW                 | <b>S:</b><br>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<br>RO         | <b>Reserved</b>   |
| 18:4      | 0000h<br>RW      | <b>Page Queue Head (PQH):</b><br>Specifies the offset (16-bytes aligned) to the page request queue for the request that will be processed next by software. |
| 3:0       | 0h<br>RO         | <b>Reserved</b>   |

#### 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<br>RO         | <b>Reserved</b>   |
| 18:4      | 0000h<br>RW/V    | <b>Page Queue Tail (PQT):</b><br>Specifies the offset (16-bytes aligned) to the page request queue for the request that will be written next by hardware. |
| 3:0       | 0h<br>RO         | <b>Reserved</b>   |



### 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<br>RO             | <b>Reserved</b>  |
| 45:12     | 00000000<br>0h<br>RW | <b>Page Request Queue Base Address (PQA):</b><br>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<br>RO             | <b>Reserved</b>  |
| 2:0       | 0h<br>RW             | <b>Page Request Queue Size (PQS):</b><br>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<br>RO         | <b>Reserved</b>              |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 0         | 0h<br>RW/1C      | <b>Pending Page Request (PPR):</b><br>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_req_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<br>RW         | <b>Interrupt Mask (IM):</b><br>Interrupt Mask <ul style="list-style-type: none"> <li>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)</li> <li>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.</li> </ul>   |
| 30        | 0h<br>RO/V       | <b>Interrupt Pending (IP):</b><br>Interrupt Pending: Hardware sets the IP field whenever it detects an interrupt condition. Interrupt condition is defined as: <ul style="list-style-type: none"> <li>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</li> <li>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</li> </ul> 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: <ul style="list-style-type: none"> <li>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</li> <li>Software servicing the PPR field in the Page Request Event Status register.</li> </ul> |
| 29:0      | 0h<br>RO         | <b>Reserved</b>  |



#### 4.2.34 Page Request Event Data Register (PEDATA\_REG\_0\_0\_0\_VTD BAR) – 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<br>RW      | <b>Extended Interrupt Message Data (EIMD):</b><br>Extended Interrupt Message Data  |
| 15:0      | 0000h<br>RW      | <b>Interrupt Message Data (IMD):</b><br>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\_VTD BAR) – 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<br>RW  | <b>Message Address (MA):</b><br>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<br>RO         | <b>Reserved</b>  |

### 4.2.36 Page Request Event Upper Address Register (PEUADDR\_REG\_0\_0\_0\_VTD BAR) – 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<br>RW  | <b>Message Upper Address (MUA):</b><br>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\_VTD BAR) – 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<br>RO         | <b>Reserved</b>   |
| 10        | 0h<br>RO         | <b>Write Combining (WC):</b> <ul style="list-style-type: none"> <li>0 = Write-combining (WC) memory type is not supported.</li> <li>1 = Write-combining (WC) memory type is supported. Indicates whether the Write Combining memory type is supported.</li> </ul> |
| 9         | 0h<br>RO         | <b>Reserved</b>   |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 8         | 0h<br>RO         | <b>Fixed Range MTRRs Supported (FIX):</b> <ul style="list-style-type: none"> <li>0 = No fixed range MTRRs are supported</li> <li>1 = Fixed range MTRRs (MTRR_FIX64K_00000 through MTRR_FIX4K_0F8000) are supported</li> </ul> |
| 7:0       | 00h<br>RO        | <b>Variable MTRR Count (VCNT):</b><br>Indicates number of variable range MTRRs are supported.   |

### 4.2.38 MTRR Default Type Register (MTRRDEFAULT\_0\_0\_0\_VTD BAR) – 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<br>RO         | <b>Reserved</b>   |
| 11        | 0h<br>RO         | <b>MTRR Enable (E):</b> <ul style="list-style-type: none"> <li>0 = Disable MTRRs; UC memory type is applied. FE field has no effect.</li> <li>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</li> </ul>  |
| 10        | 0h<br>RO         | <b>Fixed Range MTRR Enable (FE):</b> <ul style="list-style-type: none"> <li>0 = Disable fixed range MTRRs.</li> <li>1 = Enable fixed range MTRRs.</li> </ul> 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<br>RO         | <b>Reserved</b>   |
| 7:0       | 00h<br>RO        | <b>Default Memory Type (MEMTYPE):</b><br>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<br>RO        | <b>R7:</b><br>Register Field 7 |
| 55:48     | 00h<br>RO        | <b>R6:</b><br>Register Field 6 |
| 47:40     | 00h<br>RO        | <b>R5:</b><br>Register Field 5 |
| 39:32     | 00h<br>RO        | <b>R4:</b><br>Register Field 4 |
| 31:24     | 00h<br>RO        | <b>R3:</b><br>Register Field 3 |
| 23:16     | 00h<br>RO        | <b>R2:</b><br>Register Field 2 |
| 15:8      | 00h<br>RO        | <b>R1:</b><br>Register Field 1 |
| 7:0       | 00h<br>RO        | <b>R0:</b><br>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<br>RO         | <b>Reserved</b>   |
| 38:12     | 0000000h<br>RO   | <b>Physical Base (PHYSBASE):</b><br>Base Address for variable memory type range 0 |
| 11:8      | 0h<br>RO         | <b>Reserved</b>   |



| Bit Range | Default & Access | Field Name (ID): Description                                    |
|-----------|------------------|---|
| 7:0       | 00h<br>RO        | <b>MEMTYPE:</b><br>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<br>RO         | <b>Reserved</b>   |
| 38:12     | 0000000h<br>RO   | <b>Physical Mask (PHYSMASK):</b><br>Address mask for variable memory type range 0 |
| 11        | 0h<br>RO         | <b>VALID:</b><br>Valid bit for variable range 0 mask                              |
| 10:0      | 0h<br>RO         | <b>Reserved</b>   |

#### 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<br>RO         | <b>Reserved</b>              |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 38:12     | 0000000h<br>RO   | <b>Physical Base (PHYSBASE):</b><br>Base Address for variable memory type range 1 |
| 11:8      | 0h<br>RO         | <b>Reserved</b>   |
| 7:0       | 00h<br>RO        | <b>MEMTYPE:</b><br>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<br>RO         | <b>Reserved</b>   |
| 38:12     | 0000000h<br>RO   | <b>Physical Mask (PHYSMASK):</b><br>Address mask for variable memory type range 1 |
| 11        | 0h<br>RO         | <b>VALID:</b><br>Valid bit for variable range 1 mask                              |
| 10:0      | 0h<br>RO         | <b>Reserved</b>   |

#### 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<br>RO         | <b>Reserved</b>   |
| 38:12     | 0000000h<br>RO   | <b>Physical Base (PHYSBASE):</b><br>Base Address for variable memory type range 2 |
| 11:8      | 0h<br>RO         | <b>Reserved</b>   |
| 7:0       | 00h<br>RO        | <b>MEMTYPE:</b><br>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<br>RO         | <b>Reserved</b>   |
| 38:12     | 0000000h<br>RO   | <b>Physical Mask (PHYSMASK):</b><br>Address mask for variable memory type range 2 |
| 11        | 0h<br>RO         | <b>VALID:</b><br>Valid bit for variable range 2 mask                              |
| 10:0      | 0h<br>RO         | <b>Reserved</b>   |

#### 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<br>RO         | <b>Reserved</b>   |
| 38:12     | 0000000h<br>RO   | <b>Physical Base (PHYSBASE):</b><br>Base Address for variable memory type range 3 |
| 11:8      | 0h<br>RO         | <b>Reserved</b>   |
| 7:0       | 00h<br>RO        | <b>MEMTYPE:</b><br>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<br>RO         | <b>Reserved</b>   |
| 38:12     | 0000000h<br>RO   | <b>Physical Mask (PHYSMASK):</b><br>Address mask for variable memory type range 3 |
| 11        | 0h<br>RO         | <b>VALID:</b><br>Valid bit for variable range 3 mask                              |
| 10:0      | 0h<br>RO         | <b>Reserved</b>   |

#### 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<br>RO         | <b>Reserved</b>   |
| 38:12     | 0000000h<br>RO   | <b>Physical Base (PHYSBASE):</b><br>Base Address for variable memory type range 4 |
| 11:8      | 0h<br>RO         | <b>Reserved</b>   |
| 7:0       | 00h<br>RO        | <b>MEMTYPE:</b><br>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<br>RO         | <b>Reserved</b>   |
| 38:12     | 0000000h<br>RO   | <b>Physical Mask (PHYSMASK):</b><br>Address mask for variable memory type range 4 |
| 11        | 0h<br>RO         | <b>VALID:</b><br>Valid bit for variable range 4 mask                              |
| 10:0      | 0h<br>RO         | <b>Reserved</b>   |

#### 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<br>RO         | <b>Reserved</b>   |
| 38:12     | 0000000h<br>RO   | <b>Physical Base (PHYSBASE):</b><br>Base Address for variable memory type range 5 |
| 11:8      | 0h<br>RO         | <b>Reserved</b>   |
| 7:0       | 00h<br>RO        | <b>MEMTYPE:</b><br>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<br>RO         | <b>Reserved</b>   |
| 38:12     | 0000000h<br>RO   | <b>Physical Mask (PHYSMASK):</b><br>Address mask for variable memory type range 5 |
| 11        | 0h<br>RO         | <b>VALID:</b><br>Valid bit for variable range 5 mask                              |
| 10:0      | 0h<br>RO         | <b>Reserved</b>   |

#### 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<br>RO         | <b>Reserved</b>   |
| 38:12     | 0000000h<br>RO   | <b>Physical Base (PHYSBASE):</b><br>Base Address for variable memory type range 6 |
| 11:8      | 0h<br>RO         | <b>Reserved</b>   |
| 7:0       | 00h<br>RO        | <b>MEMTYPE:</b><br>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<br>RO         | <b>Reserved</b>   |
| 38:12     | 0000000h<br>RO   | <b>Physical Mask (PHYSMASK):</b><br>Address mask for variable memory type range 6 |
| 11        | 0h<br>RO         | <b>VALID:</b><br>Valid bit for variable range 6 mask                              |
| 10:0      | 0h<br>RO         | <b>Reserved</b>   |

#### 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<br>RO         | <b>Reserved</b>   |
| 38:12     | 0000000h<br>RO   | <b>Physical Base (PHYSBASE):</b><br>Base Address for variable memory type range 7 |
| 11:8      | 0h<br>RO         | <b>Reserved</b>   |
| 7:0       | 00h<br>RO        | <b>MEMTYPE:</b><br>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<br>RO         | <b>Reserved</b>   |
| 38:12     | 0000000h<br>RO   | <b>Physical Mask (PHYSMASK):</b><br>Address mask for variable memory type range 7 |
| 11        | 0h<br>RO         | <b>VALID:</b><br>Valid bit for variable range 7 mask                              |
| 10:0      | 0h<br>RO         | <b>Reserved</b>   |

#### 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<br>RO         | <b>Reserved</b>   |
| 38:12     | 0000000h<br>RO   | <b>Physical Base (PHYSBASE):</b><br>Base Address for variable memory type range 8 |
| 11:8      | 0h<br>RO         | <b>Reserved</b>   |
| 7:0       | 00h<br>RO        | <b>MEMTYPE:</b><br>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<br>RO         | <b>Reserved</b>   |
| 38:12     | 0000000h<br>RO   | <b>Physical Mask (PHYSMASK):</b><br>Address mask for variable memory type range 8 |
| 11        | 0h<br>RO         | <b>VALID:</b><br>Valid bit for variable range 8 mask                              |
| 10:0      | 0h<br>RO         | <b>Reserved</b>   |

#### 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<br>RO         | <b>Reserved</b>   |
| 38:12     | 0000000h<br>RO   | <b>Physical Base (PHYSBASE):</b><br>Base Address for variable memory type range 9 |
| 11:8      | 0h<br>RO         | <b>Reserved</b>   |
| 7:0       | 00h<br>RO        | <b>MEMTYPE:</b><br>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<br>RO         | <b>Reserved</b>   |
| 38:12     | 0000000h<br>RO   | <b>Physical Mask (PHYSMASK):</b><br>Address mask for variable memory type range 9 |
| 11        | 0h<br>RO         | <b>VALID:</b><br>Valid bit for variable range 9 mask                              |
| 10:0      | 0h<br>RO         | <b>Reserved</b>   |



#### 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<br>00000h<br>RO/V | <p><b>Fault Info (FI):</b><br/>When the Fault Reason (FR) field indicates one of the address translation fault conditions, bits 63:12 of this field contains the page address in the faulted request. When PASID Present field is 0 (i.e, faulted request is a request without PASID), hardware treat bits 63:N as reserved (0), where N is the maximum guest address width (MGAW) supported. For requests-with PASID (PASID Present field = 1), hardware treats bits 63:N as reserved (0), where N corresponds to the largest AGAW value supported by hardware.</p> <p>When the Fault Reason (FR) field indicates interrupt-remapping fault conditions other than Fault Reason 25h, bits 63:48 of this field indicate the interrupt_index computed for the faulted interrupt request, and bits 47:12 are cleared. When the Fault Reason (FR) field indicates interrupt-remapping fault condition of blocked Compatibility mode interrupt (Fault Reason 25h), contents of this field is undefined.</p> <p>This field is relevant only when the F field is Set.</p> |
| 11:0      | 0h<br>RO                   | <b>Reserved</b>  |

#### 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<br>RW/1C      | <p><b>F:</b><br/>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.</p>  |
| 62        | 0h<br>RO/V       | <p><b>T:</b><br/>Type of the faulted request:</p> <ul style="list-style-type: none"> <li>0=0: Write request or Page (PRS) Request</li> <li>1=1: Read request or AtomicOp request</li> </ul> <p>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.</p>  |
| 61:60     | 0h<br>RO/V       | <p><b>Address Type (AT):</b><br/>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.</p>  |
| 59:40     | 00000h<br>RO/V   | <p><b>PASID Value (PV):</b><br/>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.</p>   |
| 39:32     | 00h<br>RO/V      | <p><b>Fault Reason (FR):</b><br/>Reason for the fault. This field is relevant only when the F field is set.</p>  |
| 31        | 0h<br>RO/V       | <p><b>PASID Present (PP):</b><br/>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.</p> |
| 30        | 0h<br>RO/V       | <p><b>Execute Permission Requested (EXE):</b><br/>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.</p>   |
| 29        | 0h<br>RO/V       | <p><b>Privilege Mode Requested (PRIV):</b><br/>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.</p>   |
| 28:16     | 0h<br>RO         | <b>Reserved</b>  |



| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 15:0      | 0000h<br>RO/V    | <b>Source Identifier (SID):</b><br>Requester-id associated with the fault condition<br>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     | 00000000<br>000000h<br>RW | <b>ADDR:</b><br>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.<br>A value returned on a read of this field is undefined<br>A value returned on a read of this field is undefined  |
| 11:7      | 0h<br>RO                  | <b>Reserved</b>  |
| 6         | 0h<br>RW                  | <b>Invalidation Hint (IH):</b><br>The field provides hint to hardware about preserving or flushing the non-leaf (page-directory) entries that may be cached in hardware: <ul style="list-style-type: none"> <li>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.</li> <li>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.</li> </ul> A value returned on a read of this field is undefined |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 5:0       | 00h<br>RW        | <p><b>Address Mask (AM):</b><br/>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</p> <p>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.</p> |

### 4.2.73 IOTLB Invalidate Register (IOTLB\_REG\_0\_0\_0\_VTD BAR) – 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<br>RW/V       | <p><b>Invalidate IOTLB (IVT):</b><br/>Software requests IOTLB invalidation by setting this field. Software must also set the requested invalidation granularity by programming the IIRG field<br/>Hardware clears the IVT field to indicate the invalidation request is complete.<br/>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<br/>Software must not submit IOTLB invalidation requests when there is a context-cache invalidation request pending at this remapping hardware unit.<br/>Hardware implementations reporting write-buffer flushing requirement (RWBF=1 in Capability register) must implicitly perform a write buffer flushing before invalidating the IOTLB.</p> |
| 62        | 0h<br>RO         | <b>Reserved</b>  |



| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 61:60     | 0h<br>RW         | <p><b>IOTLB Invalidation Request Granularity (IIRG):</b><br/>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</p> <ul style="list-style-type: none"> <li>• 00 = Reserved</li> <li>• 01 = Global invalidation request</li> <li>• 10 = Domain-selective invalidation request. The target domain-id must be specified in the DID field</li> <li>• 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</li> </ul> <p>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</p>  |
| 59        | 0h<br>RO         | <b>Reserved</b>   |
| 58:57     | 1h<br>RO/V       | <p><b>IOTLB Actual Invalidation Granularity (IAIG):</b><br/>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</p> <ul style="list-style-type: none"> <li>• 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</li> <li>• 01 = Global Invalidation performed. This could be in response to a global, domain-selective, or page-selective invalidation request</li> <li>• 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</li> <li>• 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.</li> </ul> |
| 56:50     | 0h<br>RO         | <b>Reserved</b>   |
| 49        | 0h<br>RW         | <p><b>Drain Reads (DR):</b><br/>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:</p> <ul style="list-style-type: none"> <li>• 0 = Hardware may complete the IOTLB invalidation without draining any translated DMA read requests</li> <li>• 1 = Hardware must drain DMA read requests.</li> </ul>  |
| 48        | 0h<br>RW         | <p><b>Drain Writes (DW):</b><br/>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:</p> <ul style="list-style-type: none"> <li>• 0 = Hardware may complete the IOTLB invalidation without draining DMA write requests</li> <li>• 1 = Hardware must drain relevant translated DMA write requests.</li> </ul>  |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 47:32     | 0000h<br>RW      | <p><b>DID:</b><br/>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.</p> <p>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.</p> |
| 31:0      | 0h<br>RO         | <b>Reserved</b>  |

## 5 PCI Express\* Controller Registers (D1:F0-2, D6:F0)

This chapter documents the registers of the processor PCIe Gen4 Controller devices. The processor contains multiple PCIe controller devices:

- Bus: 0, Device: 1, Function: 0 (PCIe0 x16)
- Bus: 0, Device: 1, Function: 1 (PCIe1 x8)
- Bus: 0, Device: 1, Function: 2 (PCIe2 x4)
- Bus: 0, Device: 6, Function: 0 (PCIe3 x4)

**Note:** Register default values are taken from device PCIe0 only. Consult Volume 1 of this document for Device IDs

**Table 5-1. Summary of Bus: 0, Device: 1, 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     |
| 50h    | 2            | Link Control (LCTL)                              | 0000h         |
| 52h    | 2            | Link Status (LSTS)                               | 1011h         |

| Offset | Size (Bytes) | Register Name (Register Symbol)                   | Default Value |
|--------|--------------|---|---------------|
| 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)                 | 00000410h     |
| 158h   | 4            | PTM Control Register (PTMCTLR)                    | 00000000h     |
| 200h   | 4            | L1 Sub-States Extended Capability Header (L1SECH) | 00000000h     |

| Offset | Size (Bytes) | Register Name (Register Symbol)   | Default Value |
|--------|--------------|---|---------------|
| 204h   | 4            | L1 Sub-States Capabilities (L1SCAP)   | 0028281Fh     |
| 208h   | 4            | L1 Sub-States Control 1 (L1SCTL1)   | 00000000h     |
| 20Ch   | 4            | L1 Sub-States Control 2 (L1SCTL2)   | 00000028h     |
| 220h   | 4            | ACS Extended Capability Header (ACSECH)   | 00000000h     |
| 224h   | 2            | ACS Capability Register (ACSCAPR)   | 001Fh         |
| 226h   | 2            | ACS Control Register (ACSCCLR)  | 0000h         |
| 284h   | 4            | Port VC Capability Register 1 (PVCCR1)  | 00000000h     |
| A00h   | 4            | DPC Extended Capability Header (DPCECH)   | 00000000h     |
| A04h   | 2            | DPC Capability Register (DPCCAPR)   | 14E0h         |
| A06h   | 2            | DPC Control Register (DPCCLR)   | 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     |
| A90h   | 4            | Data Link Feature Extended Capability Header (DLFECH)                           | 00000000h     |
| A94h   | 4            | Data Link Feature Capabilities Register (DLFCAP)                                | 80000000h     |
| A98h   | 4            | Data Link Feature Status Register (DLFSTS)                                      | 00000000h     |
| A9Ch   | 4            | Physical Layer 16.0 GT/s Extended Capability Header (PL16GECH)                  | 00000000h     |
| AA0h   | 4            | Physical Layer 16.0 GT/s Capability Register (PL16CAP)                          | 00000000h     |
| AA4h   | 4            | Physical Layer 16.0 GT/s Control Register (PL16CTL)                             | 00000000h     |
| AA8h   | 4            | Physical Layer 16.0 GT/s Status Register (PL16S)                                | 00000000h     |
| AACh   | 4            | Physical Layer 16.0 GT/s Local Data Parity Mismatch Status Register (PL16LDPMS) | 00000000h     |

| Offset | Size (Bytes) | Register Name (Register Symbol)   | Default Value |
|--------|--------------|---|---------------|
| AB0h   | 4            | Physical Layer 16.0 GT/s First Retimer Data Parity Mismatch Status Register (PL16FRDPMS)  | 00000000h     |
| AB4h   | 4            | Physical Layer 16.0 GT/s Second Retimer Data Parity Mismatch Status Register (PL16SRDPMS) | 00000000h     |
| AB8h   | 4            | Physical Layer 16.0 GT/s Extra Status Register (PL16ES)                                   | 00000000h     |
| ABCh   | 2            | Physical Layer 16.0 GT/s Lane 01 Equalization Control Register (PL16L01EC)                | FFFFh         |
| ABEh   | 2            | Physical Layer 16.0 GT/s Lane 23 Equalization Control Register (PL16L23EC)                | FFFFh         |
| AC0h   | 2            | Physical Layer 16.0 GT/s Lane 45 Equalization Control Register (PL16L45EC)                | FFFFh         |
| AC2h   | 2            | Physical Layer 16.0 GT/s Lane 67 Equalization Control Register (PL16L67EC)                | FFFFh         |
| AC4h   | 2            | Physical Layer 16.0 GT/s Lane 89 Equalization Control Register (PL16L89EC)                | FFFFh         |
| AC6h   | 2            | Physical Layer 16.0 GT/s Lane 1011 Equalization Control Register (PL16L1011EC)            | FFFFh         |
| AC8h   | 2            | Physical Layer 16.0 GT/s Lane 1213 Equalization Control Register (PL16L1213EC)            | FFFFh         |
| ACAh   | 2            | Physical Layer 16.0 GT/s Lane 1415 Equalization Control Register (PL16L1415EC)            | FFFFh         |
| EDCh   | 4            | Physical Layer 16.0 GT/s Margining Extended Capability Header (PL16MECH)                  | 00010027h     |
| EE0h   | 4            | Physical Layer 16.0 GT/s Margining Port Capabilities and Port Status (PL16MPGPS)          | 00000000h     |
| EE4h   | 4            | Physical Layer 16.0 GT/s Lane0 Margin Control and Status Register (PL16L0MCS)             | 00009C38h     |
| EE8h   | 4            | Physical Layer 16.0 GT/s Lane1 Margin Control and Status Register (PL16L1MCS)             | 00009C38h     |
| EECh   | 4            | Physical Layer 16.0 GT/s Lane2 Margin Control and Status Register (PL16L2MCS)             | 00009C38h     |
| EF0h   | 4            | Physical Layer 16.0 GT/s Lane3 Margin Control and Status Register (PL16L3MCS)             | 00009C38h     |
| EF4h   | 4            | Physical Layer 16.0 GT/s Lane4 Margin Control and Status Register (PL16L4MCS)             | 00009C38h     |
| EF8h   | 4            | Physical Layer 16.0 GT/s Lane5 Margin Control and Status Register (PL16L5MCS)             | 00009C38h     |
| EFCh   | 4            | Physical Layer 16.0 GT/s Lane6 Margin Control and Status Register (PL16L6MCS)             | 00009C38h     |
| F00h   | 4            | Physical Layer 16.0 GT/s Lane7 Margin Control and Status Register (PL16L7MCS)             | 00009C38h     |
| F04h   | 4            | Physical Layer 16.0 GT/s Lane8 Margin Control and Status Register (PL16L8MCS)             | 00009C38h     |
| F08h   | 4            | Physical Layer 16.0 GT/s Lane9 Margin Control and Status Register (PL16L9MCS)             | 00009C38h     |
| F0Ch   | 4            | Physical Layer 16.0 GT/s Lane10 Margin Control and Status Register (PL16L10MCS)           | 00009C38h     |
| F10h   | 4            | Physical Layer 16.0 GT/s Lane11 Margin Control and Status Register (PL16L11MCS)           | 00009C38h     |
| F14h   | 4            | Physical Layer 16.0 GT/s Lane12 Margin Control and Status Register (PL16L12MCS)           | 00009C38h     |

| Offset | Size (Bytes) | Register Name (Register Symbol)   | Default Value |
|--------|--------------|---|---------------|
| F18h   | 4            | Physical Layer 16.0 GT/s Lane13 Margin Control and Status Register (PL16L13MCS) | 00009C38h     |
| F1Ch   | 4            | Physical Layer 16.0 GT/s Lane14 Margin Control and Status Register (PL16L14MCS) | 00009C38h     |
| F20h   | 4            | Physical Layer 16.0 GT/s Lane15 Margin Control and Status Register (PL16L15MCS) | 00009C38h     |

## 5.1 Device Identifiers (ID) – Offset 0h

Device ID and Vendor ID

| Type | Size   | Offset               | Default   |
|------|--------|----------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, 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<br>RO/V    | <b>Device Identification (DID):</b><br>See the Device ID table in the first volume of this document. |
| 15:0      | 8086h<br>RO      | <b>Vendor Identification (VID):</b><br>Indicates Intel.  |

## 5.2 Device Command (CMD) – Offset 4h

Device Command

| Type | Size   | Offset               | Default |
|------|--------|----------------------|---------|
| PCI  | 16 bit | [B:0, D:1, 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<br>RO         | <b>Reserved</b>              |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 10        | 0h<br>RW/V2      | <p><b>Interrupt Disable (ID):</b><br/>This disables pin-based INTx# interrupts on enabled hot plug and power management events.<br/>This bit has no effect on MSI operation.<br/>When set, internal INTx# messages will not be generated.<br/>When cleared, internal INTx# messages are generated if there is an interrupt for hot plug or power management and MSI is not enabled.<br/>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.<br/>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.</p> |
| 9         | 0h<br>RO         | <p><b>Fast Back to Back Enable (FBE):</b><br/>This field is reserved per PCI-Express spec.</p>   |
| 8         | 0h<br>RW         | <p><b>SERR# Enable (SEE):</b><br/>When set, enables the root port to generate an SERR# message when PSTS.SSE is set.</p>   |
| 7         | 0h<br>RO         | <p><b>Wait Cycle Control (WCC):</b><br/>This field is reserved per PCI-Express spec.</p>   |
| 6         | 0h<br>RW         | <p><b>Parity Error Response Enable (PERE):</b><br/>Indicates that the device is capable of reporting parity errors as a master on the backbone.</p>  |
| 5         | 0h<br>RO         | <p><b>VGA Palette Snoop (VGA_PSE):</b><br/>This field is reserved per PCI-Express spec.</p>  |
| 4         | 0h<br>RO         | <p><b>Memory Write and Invalidate Enable (MWIE):</b><br/>This field is reserved per PCI-Express spec.</p>  |
| 3         | 0h<br>RO         | <p><b>Special Cycle Enable (SCE):</b><br/>This field is reserved per PCI-Express and PCI bridge spec.</p>  |
| 2         | 0h<br>RW         | <p><b>Bus Master Enable (BME):</b><br/>When set, allows the root port to forward Memory and I/O Read/Write cycles onto the backbone from a PCI-Express device.<br/>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.<br/>The forwarding of Requests other than Memory or I/O requests is not controlled by this bit.</p>   |
| 1         | 0h<br>RW         | <p><b>Memory Space Enable (MSE):</b><br/>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.</p>   |
| 0         | 0h<br>RW         | <p><b>I/O Space Enable (IOSE):</b><br/>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.</p>  |

## 5.3 Primary Status (PSTS) – Offset 6h

Primary Status



| Type | Size   | Offset               | Default |
|------|--------|----------------------|---------|
| PCI  | 16 bit | [B:0, D:1, 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<br>RW/1C/V    | <b>Detected Parity Error (DPE):</b><br>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<br>RW/1C/V    | <b>Signaled System Error (SSE):</b><br>Set when the root port signals a system error to the internal SERR# logic.  |
| 13        | 0h<br>RW/1C/V    | <b>Received Master Abort (RMA):</b><br>Set when the root port receives a completion with unsupported request status from the backbone.   |
| 12        | 0h<br>RW/1C/V    | <b>Received Target Abort (RTA):</b><br>Set when the root port receives a completion with completer abort from the backbone.  |
| 11        | 0h<br>RW/1C/V    | <b>Signaled Target Abort (STA):</b><br>Set whenever the root port forwards a target abort received from the downstream device onto the backbone.   |
| 10:9      | 0h<br>RO         | <b>Primary DEVSEL# Timing Status (PDTS):</b><br>This field is reserved per PCI-Express spec  |
| 8         | 0h<br>RW/1C/V    | <b>Master Data Parity Error Detected (DPD):</b><br>Set when the root port receives a completion with a data parity error on the backbone and PCMD.PERE is set.   |
| 7         | 0h<br>RO         | <b>Primary Fast Back to Back Capable (PFBC):</b><br>This field is reserved per PCI-Express spec.   |
| 6         | 0h<br>RO         | <b>Reserved</b>  |
| 5         | 0h<br>RO         | <b>Primary 66 MHz Capable (PC66):</b><br>This field is reserved per PCI-Express spec.  |
| 4         | 1h<br>RO         | <b>Capabilities List (CLIST):</b><br>Indicates the presence of a capabilities list.  |
| 3         | 0h<br>RO/V       | <b>Interrupt Status (IS):</b><br>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<br>RO         | <b>Reserved</b>  |

## 5.4 Revision ID (RID\_CC) – Offset 8h

Revision ID



| Type | Size   | Offset               | Default   |
|------|--------|----------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, 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<br>RO        | <b>Base Class Code (BCC):</b><br>Indicates the device is a bridge device.  |
| 23:16     | 04h<br>RO/V      | <b>Sub-Class Code (SCC):</b><br>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<br>RO/V      | <b>Programming Interface (PI):</b><br>PCI-to-PCI bridge.   |
| 7:0       | F0h<br>RO/V      | <b>Revision ID (RID):</b><br>Indicates the revision of the bridge.   |

## 5.5 Cache Line Size (CLS) – Offset Ch

Cache Line Size

| Type | Size  | Offset               | Default |
|------|-------|----------------------|---------|
| PCI  | 8 bit | [B:0, D:1, 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<br>RW        | <b>Line Size (LS):</b><br>This is read/write but contains no functionality, per PCI-Express spec |

## 5.6 Primary Latency Timer (PLT) – Offset Dh

Primary Latency Timer

| Type | Size  | Offset               | Default |
|------|-------|----------------------|---------|
| PCI  | 8 bit | [B:0, D:1, 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<br>RO        | <b>Latency Count (CT):</b><br>This field is reserved per PCI-Express spec |
| 2:0       | 0h<br>RO         | <b>Reserved</b>   |

## 5.7 Header Type (HTYPE) – Offset Eh

Header Type

| Type | Size  | Offset               | Default |
|------|-------|----------------------|---------|
| PCI  | 8 bit | [B:0, D:1, 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<br>RO         | <b>Multi-function Device (MFD):</b><br>This bit is 1 to indicate a multi-function device.  |
| 6:0       | 01h<br>RO/V      | <b>Header Type (HTYPE):</b><br>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. |

## 5.8 Bus Numbers (BNUM\_SLT) – Offset 18h

Bus Numbers

| Type | Size   | Offset                | Default   |
|------|--------|-----------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, 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<br>RW/V2     | <b>Secondary Latency Timer (SLT):</b><br>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.<br>This register does not affect the behavior of any HW logic. |
| 23:16     | 00h<br>RW        | <b>Subordinate Bus Number (SBBN):</b><br>Indicates the highest PCI bus number below the bridge.   |
| 15:8      | 00h<br>RW        | <b>Secondary Bus Number (SCBN):</b><br>Indicates the bus number the port.   |
| 7:0       | 00h<br>RW        | <b>Primary Bus Number (PBN):</b><br>Indicates the bus number of the backbone.   |

## 5.9 I/O Base And Limit (IOBL) – Offset 1Ch

I/O Base And Limit

| Type | Size   | Offset                | Default |
|------|--------|-----------------------|---------|
| PCI  | 16 bit | [B:0, D:1, 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<br>RW         | <b>I/O Address Limit (IOLA):</b><br>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<br>RO         | <b>I/O Limit Address Capability (IOLC):</b><br>Indicates that the bridge does not support 32-bit I/O addressing.                                      |
| 7:4       | 0h<br>RW         | <b>I/O Base Address (IOBA):</b><br>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<br>RO         | <b>I/O Base Address Capability (IOBC):</b><br>Indicates that the bridge does not support 32-bit I/O addressing.                                       |

## 5.10 Secondary Status (SSTS) – Offset 1Eh

Secondary Status

| Type | Size   | Offset                | Default |
|------|--------|-----------------------|---------|
| PCI  | 16 bit | [B:0, D:1, 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<br>RW/1C/V    | <b>Detected Parity Error (DPE):</b><br>Set when the port receives a poisoned TLP.  |
| 14        | 0h<br>RW/1C/V    | <b>Received System Error (RSE):</b><br>Set when the port receives an ERR_FATAL or ERR_NONFATAL message from the device.  |
| 13        | 0h<br>RW/1C/V    | <b>Received Master Abort (RMA):</b><br>Set when the port receives a completion with 'Unsupported Request' status from the device.  |
| 12        | 0h<br>RW/1C/V    | <b>Received Target Abort (RTA):</b><br>Set when the port receives a completion with 'Completion Abort' status from the device.   |
| 11        | 0h<br>RW/1C/V    | <b>Signaled Target Abort (STA):</b><br>Set when the port generates a completion with 'Completion Abort' status to the device.  |
| 10:9      | 0h<br>RO/V       | <b>Secondary DEVSEL# Timing Status (SDTS):</b><br>This field is reserved per PCI-Express spec<br>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<br>RW/1C/V    | <b>Data Parity Error Detected (DPD):</b><br>Set when the BCTRL.PERE, and either of the following two conditions occurs:<br>Port receives completion marked poisoned.<br>Port poisons a write request to the secondary side.  |
| 7         | 0h<br>RO/V       | <b>Secondary Fast Back to Back Capable (SFBC):</b><br>This field is reserved per PCI Express spec<br>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<br>RO         | <b>Reserved</b>  |
| 5         | 0h<br>RO         | <b>Secondary 66 MHz Capable (SC66):</b><br>This field is reserved per PCI Express spec   |
| 4:0       | 0h<br>RO         | <b>Reserved</b>  |

## 5.11 Memory Base And Limit (MBL) – Offset 20h

Memory Base And Limit



| Type | Size   | Offset                | Default   |
|------|--------|-----------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, 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<br>RW       | <b>Memory Limit (ML):</b><br>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<br>RO         | <b>Reserved</b>   |
| 15:4      | 000h<br>RW       | <b>Memory Base (MB):</b><br>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<br>RO         | <b>Reserved</b>   |

## 5.12 Prefetchable Memory Base And Limit (PMBL) — Offset 24h

Prefetchable Memory Base And Limit

| Type | Size   | Offset                | Default   |
|------|--------|-----------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, 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<br>RW       | <b>Prefetchable Memory Limit (PML):</b><br>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<br>RO         | <b>64-bit Indicator (I64L):</b><br>Indicates support for 64-bit addressing.   |
| 15:4      | 000h<br>RW       | <b>Prefetchable Memory Base (PMB):</b><br>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<br>RO         | <b>64-bit Indicator (I64B):</b><br>Indicates support for 64-bit addressing.   |

## 5.13 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:1, 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<br>RW  | <b>Prefetchable Memory Base Upper Portion (PMBU):</b><br>Upper 32-bits of the prefetchable address base. |

## 5.14 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:1, 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<br>RW  | <b>Prefetchable Memory Limit Upper Portion (PMLU):</b><br>Upper 32-bits of the prefetchable address limit. |

## 5.15 Capabilities List Pointer (CAPP) – Offset 34h

Capabilities List Pointer



| Type | Size  | Offset                | Default |
|------|-------|-----------------------|---------|
| PCI  | 8 bit | [B:0, D:1, 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<br>RW/O      | <p><b>Capabilities Pointer (PTR):</b><br/>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.</p> <p><b>Capability Linked List (Default Settings)</b><br/>Offset   Capability   Next Pointer<br/>40h   PCI Express   80h<br/>80h   Message Signaled Interrupt (MSI)   90h<br/>90h   Subsystem Vendor   A0h<br/>A0h   PCI Power Management   00h</p> <p><b>Extended PCIe Capability Linked List</b><br/>Offset   Capability   Next Pointer<br/>100h   Advanced Error Reporting   000h<br/>140h   Access Control Services   000h<br/>200h   L1 Sub-states   000h<br/>220h   Secondary PCI Express Capability   000h</p> |

## 5.16 Interrupt Information (INTR) – Offset 3Ch

Interrupt Information



| Type | Size   | Offset                | Default |
|------|--------|-----------------------|---------|
| PCI  | 16 bit | [B:0, D:1, 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<br>RO/V      | <p><b>Interrupt Pin (IPIN):</b><br/>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:<br/>Port Bits[15:12] Bits[11:08]<br/>1 0h STRPFUSECFG.P1IP<br/>2 0h STRPFUSECFG.P2IP<br/>3 0h STRPFUSECFG.P3IP<br/>...<br/>X 0h STRPFUSECFG.PxIP<br/>The value that is programmed into STRPFUSECFG.PxIP is always reflected in this register.<br/>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.<br/>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.</p> |
| 7:0       | 00h<br>RW        | <p><b>Interrupt Line (ILINE):</b><br/>Software written value to indicate which interrupt line (vector) the interrupt is connected to. No hardware action is taken on this register.</p>   |

## 5.17 Bridge Control (BCTRL) – Offset 3Eh

Bridge Control

| Type | Size   | Offset                | Default |
|------|--------|-----------------------|---------|
| PCI  | 16 bit | [B:0, D:1, 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<br>RO         | <b>Reserved</b>   |
| 11        | 0h<br>RW/V2      | <p><b>Discard Timer SERR# Enable (DTSE):</b><br/>This field is reserved per PCI-Express spec.<br/>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.</p> |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 10        | 0h<br>RO         | <b>Discard Timer Status (DTS):</b><br>This field is reserved per PCI-Express spec.<br>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<br>RW/V2      | <b>Secondary Discard Timer (SDT):</b><br>This field is reserved per PCI-Express spec.<br>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<br>RW/V2      | <b>Primary Discard Timer (PDT):</b><br>This field is reserved per PCI-Express spec.<br>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<br>RO         | <b>Fast Back to Back Enable (FBE):</b><br>This field is reserved per PCI-Express spec.   |
| 6         | 0h<br>RW         | <b>Secondary Bus Reset (SBR):</b><br>Triggers a Hot Reset on the PCI-Express port.   |
| 5         | 0h<br>RW/V2      | <b>Master Abort Mode (MAM):</b><br>This field is reserved per PCI-Express spec.<br>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<br>RW         | <b>VGA 16-Bit Decode (V16):</b><br>When set, indicates that the I/O aliases of the VGA range (see BCTRL:VE definition below), are not enabled.<br>0: Execute 10-bit address decode on VGA I/O accesses.<br>1: Execute 16-bit address decode on VGA I/O accesses.   |
| 3         | 0h<br>RW         | <b>VGA Enable (VE):</b><br>When set, the following ranges will be claimed off the backbone by the root port:<br>Memory ranges A0000h-BFFFFh<br>I/O ranges 3B0h - 3BBh and 3C0h - 3DFh, and all aliases of bits 15:10 in any combination of 1's   |
| 2         | 0h<br>RW         | <b>ISA Enable (IE):</b><br>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<br>RW         | <b>SERR# Enable (SE):</b><br>When set, ERR_COR, ERR_NONFATAL, and ERR_FATAL messages received are forwarded to the backbone. When cleared, they are not.   |
| 0         | 0h<br>RW         | <b>Parity Error Response Enable (PERE):</b><br>When set, poisoned write TLPs and completions indicating poisoned TLPs will set the SSTS.DPD.   |

## 5.18 Capabilities List (CLIST) – Offset 40h

### Capabilities List

| Type | Size   | Offset                | Default |
|------|--------|-----------------------|---------|
| PCI  | 16 bit | [B:0, D:1, 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<br>RW/O      | <b>Next Capability (NEXT):</b><br>Indicates the location of the next capability.<br>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.<br>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<br>RO        | <b>Capability ID (CID):</b><br>Indicates this is a PCI Express capability   |

## 5.19 PCI Express Capabilities (XCAP) – Offset 42h

PCI Express Capabilities

| Type | Size   | Offset                | Default |
|------|--------|-----------------------|---------|
| PCI  | 16 bit | [B:0, D:1, 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<br>RO         | <b>Reserved</b>  |
| 13:9      | 00h<br>RO        | <b>Interrupt Message Number (IMN):</b><br>The Root Port does not have multiple MSI interrupt numbers.  |
| 8         | 0h<br>RW/O       | <b>Slot Implemented (SI):</b><br>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<br>RO         | <b>Device / Port Type (DT):</b><br>Indicates this is a PCI-Express root port   |
| 3:0       | 2h<br>RO         | <b>Capability Version (CV):</b><br>Version 2.0 indicates devices compliant to the PCI Express 2.0 and 3.0 specification which incorporates the Register Expansion ECN.                             |



## 5.20 Device Capabilities (DCAP) – Offset 44h

Device Capabilities

| Type | Size   | Offset                | Default   |
|------|--------|-----------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, 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<br>RO         | <b>Reserved</b>   |
| 28        | 0h<br>RO         | <b>Function Level Reset Capable (FLRC):</b><br>Not supported in Root Ports  |
| 27:26     | 0h<br>RO         | <b>Captured Slot Power Limit Scale (CSPS):</b><br>Not supported.  |
| 25:18     | 00h<br>RO        | <b>Captured Slot Power Limit Value (CSPV):</b><br>Not supported.  |
| 17:16     | 0h<br>RO         | <b>Reserved</b>   |
| 15        | 1h<br>RO         | <b>Role Based Error Reporting (RBER):</b><br>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<br>RO         | <b>Reserved</b>   |
| 11:9      | 0h<br>RO         | <b>Endpoint L1 Acceptable Latency (E1AL):</b><br>This field is reserved for root ports.   |
| 8:6       | 0h<br>RO         | <b>Endpoint L0s Acceptable Latency (E0AL):</b><br>This field is reserved for Root port.   |
| 5         | 0h<br>RW/O       | <b>Extended Tag Field Supported (ETFS):</b><br>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<br>RO         | <b>Phantom Functions Supported (PFS):</b><br>No phantom functions supported   |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 2:0       | 1h<br>RW/O       | <p><b>Max Payload Size Supported (MPS):</b><br/>           BIOS should write to this field during system initialization.<br/>           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.</p> <p>000b: 128 bytes max payload size.<br/>           001b: 256 bytes max payload size.<br/>           010b: 512 bytes max payload size.<br/>           011b: 1024 bytes max payload size.<br/>           100b: 2048 bytes max payload size.<br/>           101b: 4096 bytes max payload size.<br/>           110b: Reserved.<br/>           111b: Reserved.</p> <p>This field applies only to the PCIe link interface.</p> |

## 5.21 Device Control (DCTL) – Offset 48h

Device Control

| Type | Size   | Offset                | Default |
|------|--------|-----------------------|---------|
| PCI  | 16 bit | [B:0, D:1, 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<br>RO         | <b>Reserved</b>  |
| 14:12     | 0h<br>RO         | <p><b>Max Read Request Size (MRRS):</b><br/>           Hardwired to 0.<br/>           This field applies only to the PCIe link interface.</p>  |
| 11        | 0h<br>RO         | <p><b>Enable No Snoop (ENS):</b><br/>           Not supported. The root port will never issue non-snoop requests.</p>  |
| 10        | 0h<br>RW/P       | <p><b>Aux Power PM Enable (APME):</b><br/>           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.</p> |
| 9         | 0h<br>RO         | <p><b>Phantom Functions Enable (PFE):</b><br/>           Not supported</p>   |
| 8         | 0h<br>RO         | <p><b>Extended Tag Field Enable (ETFE):</b><br/>           Not supported</p>   |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 7:5       | 1h<br>RW         | <p><b>Max Payload Size (MPS):</b><br/>           The root port supports up to 256B max payload.<br/>           Programming this field to any values greater than DCAP.MPS will result in aliasing to 128B max payload size.<br/>           000b: 128 bytes max payload size.<br/>           001b: 256 bytes max payload size.<br/>           010b: 512 bytes max payload size.<br/>           011b: 1024 bytes max payload size.<br/>           100b: 2048 bytes max payload size.<br/>           101b: 4096 bytes max payload size.<br/>           110b: Reserved.<br/>           111b: Reserved.<br/>           This field applies only to the PCIe link interface.<br/>           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.</p> |
| 4         | 0h<br>RO         | <p><b>Enable Relaxed Ordering (ERO):</b><br/>           Not supported</p>  |
| 3         | 0h<br>RW         | <p><b>Unsupported Request Reporting Enable (URE):</b><br/>           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.</p>   |
| 2         | 0h<br>RW         | <p><b>Fatal Error Reporting Enable (FEE):</b><br/>           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.</p>  |
| 1         | 0h<br>RW         | <p><b>Non-Fatal Error Reporting Enable (NFE):</b><br/>           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.</p>   |
| 0         | 0h<br>RW         | <p><b>Correctable Error Reporting Enable (CEE):</b><br/>           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.</p>   |

## 5.22 Device Status (DSTS) – Offset 4Ah

Device Status

| Type | Size   | Offset                | Default |
|------|--------|-----------------------|---------|
| PCI  | 16 bit | [B:0, D:1, 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<br>RO         | <b>Reserved</b>   |
| 5         | 0h<br>RO         | <b>Transactions Pending (TDP):</b><br>This bit has no meaning for the root port since it never initiates a non-posted request with its own Requester ID.  |
| 4         | 1h<br>RO         | <b>AUX Power Detected (APD):</b><br>The root port contains AUX power for wakeup   |
| 3         | 0h<br>RW/1C/V    | <b>Unsupported Request Detected (URD):</b><br>Indicates an unsupported request was detected.  |
| 2         | 0h<br>RW/1C/V    | <b>Fatal Error Detected (FED):</b><br>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<br>RW/1C/V    | <b>Non-Fatal Error Detected (NFED):</b><br>Indicates a non-fatal error was detected. Set when an received a non-fatal error occurred from a poisoned TLP, unexpected completions, unsupported requests, completer abort, or completer timeout         |
| 0         | 0h<br>RW/1C/V    | <b>Correctable Error Detected (CED):</b><br>Indicates a correctable error was detected.<br>Set when received an internal correctable error from receiver errors / framing errors, TLP CRC error, DLLP CRC error, replay num rollover, replay timeout. |

## 5.23 Link Capabilities (LCAP) – Offset 4Ch

Link Capabilities



| Type | Size   | Offset                | Default   |
|------|--------|-----------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, 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<br>RO/V      | <p><b>Port Number (PN):</b><br/>Indicates the port number for the root port. This value is different for each implemented port:<br/>Port # Value of PN field<br/>1 01h<br/>2 02h<br/>3 03h<br/>:<br/>:<br/>X 0Xh<br/>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.</p>   |
| 23        | 0h<br>RO         | <b>Reserved</b>   |
| 22        | 1h<br>RW/O       | <p><b>ASPM Optionality Compliance (ASPMOC):</b><br/>This bit must be set to 1b for PCIe 3.0 compliant port.<br/>Components implemented against certain earlier versions of this specification will have this bit set to 0b.<br/>Software is permitted to use the value of this bit to help determine whether to enable ASPM or whether to run ASPM compliance tests.</p>  |
| 21        | 1h<br>RO         | <p><b>Link Bandwidth Notification Capability (LBNC):</b><br/>This port supports Link Bandwidth Notification status and interrupt mechanisms.</p>  |
| 20        | 1h<br>RO         | <p><b>Link Active Reporting Capable (LARC):</b><br/>This port supports the optional capability of reporting the DL_Active state of the Data Link Control and Management State Machine.</p>  |
| 19        | 0h<br>RO         | <p><b>Surprise Down Error Reporting Capable (SDERC):</b><br/>Set to 0 to indicate the Root Port does not support Surprise Down Error Reporting</p>  |
| 18        | 0h<br>RO         | <p><b>Clock Power Management (CPM):</b><br/>0' Indicates that root ports do not support the CLKREQ# mechanism.</p>  |
| 17:15     | 2h<br>RW/O       | <p><b>L1 Exit Latency (EL1):</b><br/>Indicates an exit latency of 2us to 4us.<br/>000b: Less than 1 us<br/>001b: 1 us to less than 2 us<br/>010b: 2 us to less than 4 us<br/>011b: 4 us to less than 8 us<br/>100b: 8 us to less than 16 us<br/>101b: 16 us to less than 32 us<br/>110b: 32 us to 64 us<br/>111b: More than 64 us<br/>Note: If power management (e.g PLL shutdown) is enabled, BIOS should program this latency to comprehend PLL lock latency.</p> |



| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 14:12     | 4h<br>RO/V       | <b>L0s Exit Latency (ELO):</b><br>Indicates an exit latency based upon common-clock configuration:<br>LCTL.CCC Value<br>0 MPC.UCEL<br>1 MPC.CCEL  |
| 11:10     | 3h<br>RW/O       | <b>Active State Link PM Support (APMS):</b><br>Indicates the level of active state power management on this link<br>Bits Definition<br>00b: No ASPM Support<br>01b: L0s Supported<br>10b: L1 Supported<br>11b: L0s and L1 Supported   |
| 9:4       | 01h<br>RO/V      | <b>Maximum Link Width (MLW):</b><br>Indicates the maximum link width of the link<br>0x1: x1 Link Width<br>0x2: x2 Link Width<br>0x4: x4 Link Width<br>0x8: x8 Link Width<br>0x10: x16 Link Width  |
| 3:0       | 0h<br>RO/V       | <b>Max Link Speed (MLS):</b><br>This field indicates the maximum Link speed of the associated Port.<br>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.<br>Defined encodings are:<br>0001b: Supported Link Speeds Vector field bit 0.<br>0010b: Supported Link Speeds Vector field bit 1.<br>0011b: Supported Link Speeds Vector field bit 2.<br>0100b: Supported Link Speeds Vector field bit 3.<br>0101b: Supported Link Speeds Vector field bit 4.<br>0110b: Supported Link Speeds Vector field bit 5.<br>0111b: Supported Link Speeds Vector field bit 6.<br>All other encodings are reserved.<br>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.<br>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.<br>Otherwise, this field reports a value of 0011b. |

## 5.24 Link Control (LCTL) – Offset 50h

### Link Control



| Type | Size   | Offset                | Default |
|------|--------|-----------------------|---------|
| PCI  | 16 bit | [B:0, D:1, 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<br>RO         | <b>Reserved</b>  |
| 11        | 0h<br>RW         | <b>Link Autonomous Bandwidth Interrupt Enable (LABIE):</b><br>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<br>RW         | <b>Link Bandwidth Management Interrupt Enable (LBMIE):</b><br>When Set, this bit enables the generation of an interrupt to indicate that the Link Bandwidth Management Status bit has been Set.<br>This bit is not applicable and is reserved for Endpoints, PCI Express-to-PCI/PCI-X bridges, and Upstream Ports of Switches.<br>Functions that do not implement the Link Bandwidth Notification Capability must hardwire this bit to 0b.<br>Default value of this bit is 0b.   |
| 9         | 0h<br>RW         | <b>Hardware Autonomous Width Disable (HAWD):</b><br>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.<br>Note: When operating as PCI Express, this bit defines the value of the Link Upconfigure Capability in TS2 Ordered Sets.<br>Default value of this bit is 0b.  |
| 8         | 0h<br>RO         | <b>Enable Clock Power Management (ECPM):</b><br>Not supported on Root Ports.   |
| 7         | 0h<br>RW         | <b>Extended Sync (ES):</b><br>When set, forces extended transmission of FTS ordered sets in FTS and extra TS2 at exit from L1 prior to entering L0.  |
| 6         | 0h<br>RW         | <b>Common Clock Configuration (CCC):</b><br>When set, indicates that the Root Port and device are operating with a distributed common reference clock.   |
| 5         | 0h<br>WO         | <b>Retrain Link (RL):</b><br>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.<br>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<br>RW         | <b>Link Disable (LD):</b><br>When set, the root port will disable the link by directing the LTSSM to the Disabled state.   |
| 3         | 0h<br>RW/O       | <b>Read Completion Boundary Control (RCBC):</b><br>Indicates the read completion boundary is 64 bytes.   |
| 2         | 0h<br>RO         | <b>Reserved</b>  |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 1:0       | 0h<br>RW         | <p><b>Active State Link PM Control (ASPM):</b><br/>Indicates whether the root port should enter L0s or L1 or both.</p> <p>Bits Definition</p> <p>00 Disabled</p> <p>01 L0s Entry Enabled</p> <p>10 L1 Entry Enabled</p> <p>11 L0s and L1 Entry Enabled</p> <p>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.</p> <p>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.</p> |

## 5.25 Link Status (LSTS) – Offset 52h

Link Status

| Type | Size   | Offset                | Default |
|------|--------|-----------------------|---------|
| PCI  | 16 bit | [B:0, D:1, 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<br>RW/1C/V    | <p><b>Link Autonomous Bandwidth Status (LABS):</b><br/>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.</p> <p>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.</p> <p>The default value of this bit is 0b.</p>  |
| 14        | 0h<br>RW/1C/V    | <p><b>Link Bandwidth Management Status (LBMS):</b><br/>This bit is Set by hardware to indicate that either of the following has occurred without the Port transitioning through DL_Down status:</p> <p>A Link retraining has completed following a write of 1b to the Retrain Link bit</p> <p>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.</p> <p>Hardware has changed Link speed or width to attempt to correct unreliable Link operation, either through an LTSSM timeout or a higher level process</p> <p>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.</p> <p>The default value of this bit is 0b.</p> |
| 13        | 0h<br>RO/V       | <p><b>Link Active (LA):</b><br/>Set to 1b when the Data Link Control and Management State Machine is in the DL_Active state, 0b otherwise.</p>   |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 12        | 1h<br>RO/V       | <p><b>Slot Clock Configuration (SCC):</b><br/>In normal mode, Root Port uses the same reference clock as on the platform and does not generate its own clock.<br/>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.</p>  |
| 11        | 0h<br>RO/V       | <p><b>Link Training (LT):</b><br/>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.</p>   |
| 10        | 0h<br>RO         | <b>Reserved</b>  |
| 9:4       | 01h<br>RO/V      | <p><b>Negotiated Link Width (NLW):</b><br/>Negotiated link width.<br/>0x1: x1 Link Width<br/>0x2: x2 Link Width<br/>0x4: x4 Link Width<br/>0x8: x8 Link Width<br/>0x10: x16 Link Width<br/>The value of this register is undefined if the link has not successfully trained.</p>   |
| 3:0       | 1h<br>RO/V       | <p><b>Current Link Speed (CLS):</b><br/>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.<br/>Defined encodings are:<br/>0001b: Supported Link Speeds Vector field bit 0.<br/>0010b: Supported Link Speeds Vector field bit 1.<br/>0011b: Supported Link Speeds Vector field bit 2.<br/>0100b: Supported Link Speeds Vector field bit 3.<br/>0101b: Supported Link Speeds Vector field bit 4.<br/>0110b: Supported Link Speeds Vector field bit 5.<br/>0111b: Supported Link Speeds Vector field bit 6.<br/>All other encodings are reserved.<br/>The value of this field is undefined if the link is not up.</p> |

## 5.26 Slot Capabilities (SLCAP) – Offset 54h

### Slot Capabilities

| Type | Size   | Offset                | Default   |
|------|--------|-----------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, 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<br>RW/O    | <b>Physical Slot Number (PSN):</b><br>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<br>RO         | <b>No Command Completed Support (NCCS):</b><br>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<br>RO         | <b>Electromechanical Interlock Present (EMIP):</b><br>Set to 0 to indicate that no electro-mechanical interlock is implemented.  |
| 16:15     | 0h<br>RW/O       | <b>Slot Power Limit Scale (SLS):</b><br>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<br>RW/O      | <b>Slot Power Limit Value (SLV):</b><br>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<br>RW/O       | <b>Hot Plug Capable (HPC):</b><br>When set, Indicates that hot plug is supported.  |
| 5         | 1h<br>RW/O       | <b>Hot Plug Surprise (HPS):</b><br>When set, indicates the device may be removed from the slot without prior notification.   |
| 4         | 0h<br>RO         | <b>Power Indicator Present (PIP):</b><br>Indicates that a power indicator LED is not present for this slot.  |
| 3         | 0h<br>RO         | <b>Attention Indicator Present (AIP):</b><br>Indicates that an attention indicator LED is not present for this slot.   |
| 2         | 0h<br>RO         | <b>MRL Sensor Present (MSP):</b><br>Indicates that an MRL sensor is not present  |
| 1         | 0h<br>RO         | <b>Power Controller Present (PCP):</b><br>Indicates that a power controller is not implemented for this slot   |
| 0         | 0h<br>RO         | <b>Attention Button Present (ABP):</b><br>Indicates that an attention button is not implemented for this slot.   |

## 5.27 Slot Control (SLCTL) – Offset 58h

Slot Control



| Type | Size   | Offset                | Default |
|------|--------|-----------------------|---------|
| PCI  | 16 bit | [B:0, D:1, 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<br>RO         | <b>Reserved</b>   |
| 13        | 0h<br>RW         | <b>Auto Slot Power Limit Disable (ASPLD):</b><br>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<br>RW         | <b>Data Link Layer State Changed Enable (DLLSCE):</b><br>When set, this field enables generation of a hot plug interrupt when the Data Link Layer Link Active field is changed.                 |
| 11        | 0h<br>RO         | <b>Electromechanical Interlock Control (EMIC):</b><br>This port does not support an Electromechanical Interlock.  |
| 10        | 0h<br>RO         | <b>Power Controller Control (PCC):</b><br>This bit has no meaning for module based hot plug.  |
| 9:8       | 0h<br>RO         | <b>Power Indicator Control (PIC):</b><br>This register is RO as this port does not implement a Hot Plug Controller.   |
| 7:6       | 0h<br>RO         | <b>Attention Indicator Control (AIC):</b><br>This register is RO as this port does not implement a Hot Plug Controller.   |
| 5         | 0h<br>RW         | <b>Hot Plug Interrupt Enable (HPE):</b><br>When set, enables generation of a hot plug interrupt on enabled hot plug events.   |
| 4         | 0h<br>RO         | <b>Command Completed Interrupt Enable (CCE):</b><br>This register is RO as this port does not implement a Hot Plug Controller.  |
| 3         | 0h<br>RW         | <b>Presence Detect Changed Enable (PDE):</b><br>When set, enables the generation of a hot plug interrupt or wake message when the presence detect logic changes state.                          |
| 2         | 0h<br>RO         | <b>MRL Sensor Changed Enable (MSE):</b><br>This register is RO as this port does not implement a Hot Plug Controller.   |
| 1         | 0h<br>RO         | <b>Power Fault Detected Enable (PFE):</b><br>This register is RO as this port does not implement a Hot Plug Controller.   |
| 0         | 0h<br>RO         | <b>Attention Button Pressed Enable (ABE):</b><br>This register is RO as this port does not implement a Hot Plug Controller.   |

## 5.28 Slot Status (SLSTS) – Offset 5Ah

Slot Status

| Type | Size   | Offset                | Default |
|------|--------|-----------------------|---------|
| PCI  | 16 bit | [B:0, D:1, 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<br>RO         | <b>Reserved</b>   |
| 8         | 0h<br>RW/1C/V    | <b>Data Link Layer State Changed (DLLSC):</b><br>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<br>RO         | <b>Electromechanical Interlock Status (EMIS):</b><br>This port does not support and electromechanical interlock.  |
| 6         | 0h<br>RO/V       | <b>Presence Detect State (PDS):</b><br>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<br>RO         | <b>MRL Sensor State (MS):</b><br>MRL sensor is not implemented.   |
| 4         | 0h<br>RO         | <b>Command Completed (CC):</b><br>This register is RO as this port does not implement a Hot Plug Controller.  |
| 3         | 0h<br>RW/1C/V    | <b>Presence Detect Changed (PDC):</b><br>This bit is set by the root port when the PD bit changes state.  |
| 2         | 0h<br>RO         | <b>MRL Sensor Changed (MSC):</b><br>MRL sensor is not implemented.  |
| 1         | 0h<br>RO         | <b>Power Fault Detected (PFD):</b><br>Power controller is not implemented.  |
| 0         | 0h<br>RO         | <b>Attention Button Pressed (ABP):</b><br>This register is RO as this port does not implement an attention button.  |

## 5.29 Root Control (RCTL) – Offset 5Ch

Root Control

| Type | Size   | Offset                | Default |
|------|--------|-----------------------|---------|
| PCI  | 16 bit | [B:0, D:1, 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<br>RO         | <b>Reserved</b>  |
| 3         | 0h<br>RW         | <b>PME Interrupt Enable (PIE):</b><br>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<br>RW         | <b>System Error on Fatal Error Enable (SFE):</b><br>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<br>RW         | <b>System Error on Non-Fatal Error Enable (SNE):</b><br>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<br>RW         | <b>System Error on Correctable Error Enable (SCE):</b><br>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. |

## 5.30 Root Status (RSTS) – Offset 60h

Root Status

| Type | Size   | Offset                | Default   |
|------|--------|-----------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, 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<br>RO         | <b>Reserved</b>  |
| 17        | 0h<br>RO/V       | <b>PME Pending (PP):</b><br>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 requester ID will be updated, and this bit will be cleared. Root Ports have a one deep PME pending queue. |



| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 16        | 0h<br>RW/1C/V    | <b>PME Status (PS):</b><br>Indicates that PME was asserted by the requester ID in RID. Subsequent PMEs are kept pending until this bit is cleared.   |
| 15:0      | 0000h<br>RO/V    | <b>PME Requester ID (RID):</b><br>Indicates the PCI requester ID of the last PME requester. 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. |

## 5.31 Device Capabilities 2 (DCAP2) – Offset 64h

Device Capabilities 2

| Type | Size   | Offset                | Default   |
|------|--------|-----------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, 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<br>RO         | <b>Reserved</b>  |
| 19:18     | 2h<br>RW/O       | <b>Optimized Buffer Flush/Fill Supported (OBFFS):</b><br>00b: OBFF is not supported.<br>01b: OBFF is supported using Message signaling only.<br>10b: OBFF is supported using WAKE# signaling only.<br>11b: OBFF is supported using WAKE# and Message signaling.<br>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.<br>Note: OBFF is not supported. BIOS should program this field to 00b. |
| 17        | 0h<br>RW/O       | <b>10-Bit Tag Requester Supported (PX10BTRS):</b><br>If this bit is Set, the Function supports 10-Bit Tag Requester capability - otherwise, the Function does not. This bit must not be Set if the 10-Bit Tag Completer Supported bit is Clear.  |
| 16        | 0h<br>RW/O       | <b>10-Bit Tag Completer Supported (PX10BTCS):</b><br>If this bit is Set, the Function supports 10-Bit Tag Completer capability - otherwise, the Function does not.   |
| 15:12     | 0h<br>RO         | <b>Reserved</b>  |
| 11        | 1h<br>RW/O       | <b>LTR Mechanism Supported (LTRMS):</b><br>A value of 1b indicates support for the optional Latency Tolerance Reporting (LTR) mechanism capability.<br>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<br>RO         | <b>Reserved</b>  |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 9         | 0h<br>RW/O       | <b>CAS Completer 128-bit Supported (AC128BS):</b><br>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.   |
| 8         | 0h<br>RW/O       | <b>AtomicOp Completer 64-bit Supported (AC64BS):</b><br>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<br>RW/O       | <b>AtomicOp Completer 32-bit Supported (AC32BS):</b><br>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<br>RW/O       | <b>Atomic Routing Supported (ARS):</b><br>This bit must be set to 1b if the Port supports this optional capability  |
| 5         | 1h<br>RO         | <b>ARI Forwarding Supported (AFS):</b><br>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.<br>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<br>RO         | <b>Completion Timeout Disable Supported (CTDS):</b><br>A value of 1b indicates support for the Completion Timeout Disable mechanism.  |
| 3:0       | 7h<br>RO         | <b>Completion Timeout Ranges Supported (CTRS):</b><br>This field indicates device support for the optional Completion Timeout programmability mechanism. This mechanism allows system software to modify the Completion Timeout value.<br>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.<br>For all other devices this field is reserved and must be hardwired to 0000b.<br>Four time value ranges are defined:<br>Range A: 50us to 10ms<br>Range B: 10ms to 250ms<br>Range C: 250ms to 4s<br>Range D: 4s to 64s<br>Bits are set according to the table below to show timeout value ranges supported.<br>0000b Completion Timeout programming not supported.<br>0001b Range A<br>0010b Range B<br>0011b Ranges A & B<br>0110b Ranges B & C<br>0111b Ranges A, B & C <-- This is what Root Port supports<br>1110b Ranges B, C & D<br>1111b Ranges A, B, C & D<br>All other values are reserved. |

## 5.32 Device Control 2 (DCTL2) – Offset 68h

Device Control 2

| Type | Size   | Offset                | Default |
|------|--------|-----------------------|---------|
| PCI  | 16 bit | [B:0, D:1, 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<br>RO         | <b>Reserved</b>  |
| 14:13     | 0h<br>RW         | <p><b>Optimized Buffer Flush/Fill Enable (OBFEN):</b><br/>           Optimized Buffer Flush/Fill Enable (OBFEN):<br/>           00b Disable OBFF mechanism.<br/>           01b Enable OBFF mechanism using Message signaling (Variation A).<br/>           10b Enable OBFF mechanism using Message signaling (Variation B).<br/>           11b Enable OBFF using WAKE# signaling.<br/>           Note: Only encoding 00b and 11b are supported. The encoding of 01b or 10b would be aliased to 00b.<br/>           If DCAP2.OBFFS is clear, programming this field to any non-zero values will have no effect.</p> |
| 12        | 0h<br>RW/V2      | <p><b>10-Bit Tag Requester Enable (PX10BTRE):</b><br/>           This bit, in combination with the Extended Tag Field Enable bit in the Device Control register, determines how many Tag field bits a Requester is permitted to use. When the 10-Bit Tag Requester Enable bit is Set, the Requester is permitted to use 10-Bit Tags.<br/>           Software should not change the value of this bit while the Function has outstanding Non-Posted Requests - otherwise, the result is undefined.<br/>           Functions that do not implement 10-Bit Tag Requester capability must hardwire this bit to 0b.</p> |
| 11        | 0h<br>RO         | <b>Reserved</b>  |
| 10        | 0h<br>RW         | <p><b>LTR Mechanism Enable (LTREN):</b><br/>           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.<br/>           If DCAP2.LTRMS is clear, programming this field to any non-zero values will have no effect.</p>  |
| 9:8       | 0h<br>RO         | <b>Reserved</b>  |
| 7         | 0h<br>RW         | <p><b>AtomicOp Egress Blocking (AEB):</b><br/>           Applicable and mandatory for Switch Upstream Ports, Switch Downstream Ports, and Root Ports that implement AtomicOp routing capability - otherwise must be hardwired to 0b.<br/>           When this bit is Set, AtomicOp Requests that target going out this Egress Port must be blocked.</p>  |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 6         | 0h<br>RW         | <p><b>AtomicOp Requester Enable (ARE):</b><br/>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.<br/>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.<br/>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.</p>   |
| 5         | 0h<br>RW         | <p><b>ARI Forwarding Enable (AFE):</b><br/>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.</p>  |
| 4         | 0h<br>RW         | <p><b>Completion Timeout Disable (CTD):</b><br/>When set to 1b, this bit disables the Completion Timeout mechanism.<br/>This field is required for all devices that support the Completion Timeout Disable Capability.<br/>Software is permitted to set or clear this bit at any time. When set, the Completion Timeout detection mechanism is disabled.<br/>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.</p>  |
| 3:0       | 0h<br>RW         | <p><b>Completion Timeout Value (CTV):</b><br/>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.<br/>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.<br/>The Root Port targeted configurable ranges are listed below, along with the range allowed by the PCI Express 2.0 specification.<br/>Defined encodings:<br/>0000b Default range: 40-50ms (spec range 50us to 50ms)<br/>Values available if Range A (50us to 10 ms) programmability range is supported:<br/>0001b 90-100us (spec range is 50us to 100us)<br/>0010b 9-10ms (spec range is 1ms to 10 ms)<br/>Values available if Range B (10ms to 250ms) programmability range is supported:<br/>0101b 40-50ms (spec range is 16ms to 55ms)<br/>0110b 160-170ms (spec range is 65ms to 210ms)<br/>Values available if Range C (250ms to 4s) programmability range is supported:<br/>1001b 400-500ms (spec range is 260ms to 900ms)<br/>1010b 1.6-1.7s (spec range is 1s to 3.5s)<br/>Values not defined above are Reserved.<br/>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.</p> |

## 5.33 Device Status 2 (DSTS2) – Offset 6Ah

Device Status 2

| Type | Size   | Offset                | Default |
|------|--------|-----------------------|---------|
| PCI  | 16 bit | [B:0, D:1, 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<br>RO         | <b>Reserved</b>              |

## 5.34 Link Capabilities 2 (LCAP2) – Offset 6Ch

Link Capabilities 2

| Type | Size   | Offset                | Default  |
|------|--------|-----------------------|----------|
| PCI  | 32 bit | [B:0, D:1, F:0] + 6Ch | 000000Eh |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 31:25     | 0h<br>RO         | <b>Reserved</b>  |
| 24        | 0h<br>RW/O       | <p><b>Two Retimers Presence Detect Supported (TRPDS):</b><br/>When set to 1b, this bit indicates that the associated Port supports detection and reporting of two Retimers presence.</p> <p>This bit must be set to 1b in a Downstream Port when the Supported Link Speeds Vector of the Link Capabilities 2 register indicates support for a Link speed of 16.0 GT/s or higher. It is permitted to be set to 1b regardless of the supported Link speeds, and in Upstream Ports, if the Retimer Presence Detect Supported bit is also set to 1b.</p> |
| 23        | 0h<br>RW/O       | <p><b>Retimer Presence Detect Supported (RPDS):</b><br/>When set to 1b, this bit indicates that the associated Port supports detection and reporting of Retimer presence.</p> <p>This bit must be set to 1b in a Downstream Port when the Supported Link Speeds Vector of the Link Capabilities 2 register indicates support for a Link speed of 16.0 GT/s or higher. It is permitted to be set to 1b regardless of the supported Link speeds and in Upstream Ports.</p>   |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 22:16     | 00h<br>RW/O      | <p><b>Lower SKP OS Reception Supported Speeds Vector (LSOSRSS):</b><br/>           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.<br/>           Bit definitions within this field are:<br/>           Bit 0 2.5 GT/s<br/>           Bit 1 5.0 GT/s<br/>           Bit 2 8.0 GT/s<br/>           Bit 3 16.0 GT/s<br/>           Bits 6:4 RsvdP<br/>           Behavior is undefined if a bit is set in this field and the corresponding bit is not set in the Supported Link Speeds Vector.<br/>           This register is Read-Only if LPCR.SRL field is set.<br/> <b>Locked by:</b> LPCR.SRL</p>   |
| 15:9      | 00h<br>RW/O      | <p><b>Lower SKP OS Generation Supported Speeds Vector (LSOSGSSV):</b><br/>           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.<br/>           Bit definitions within this field are:<br/>           Bit 0 2.5 GT/s<br/>           Bit 1 5.0 GT/s<br/>           Bit 2 8.0 GT/s<br/>           Bit 3 16.0GT/s<br/>           Bits 6:4 RsvdP<br/>           Behavior is undefined if a bit is set in this field and the corresponding bit is not set in the Supported Link Speeds Vector.<br/>           This register is Read-Only if LPCR.SRL field is set.<br/> <b>Locked by:</b> LPCR.SRL</p> |
| 8         | 0h<br>RO         | <p><b>Crosslink Supported (CS):</b><br/>           No support for Crosslink.</p>  |
| 7:1       | 07h<br>RO/V      | <p><b>Supported Link Speeds Vector (SLSV):</b><br/>           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.<br/>           Bit definitions within this field for PCI Express are:<br/>           Bit 0: 2.5 GT/s.<br/>           Bit 1: 5.0 GT/s.<br/>           Bit 2: 8.0 GT/s.<br/>           Bit 3: 16.0 GT/s<br/>           Bits 6:4: Reserved.</p>   |
| 0         | 0h<br>RO         | <b>Reserved</b>   |

## 5.35 Link Control 2 (LCTL2) – Offset 70h

Link Control 2

| Type | Size   | Offset                | Default |
|------|--------|-----------------------|---------|
| PCI  | 16 bit | [B:0, D:1, 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<br>RW/P       | <p><b>Compliance Preset/De-emphasis (CD):</b><br/>           For 8.0 GT/s and higher 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.<br/>           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.<br/>           Encodings:<br/>           0001b -3.5 dB<br/>           0000b -6 dB<br/>           When the Link is operating at 2.5 GT/s, the setting of this field has no effect.<br/>           The default value of this field is 0000b.<br/>           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.</p> |
| 11        | 0h<br>RW/P       | <p><b>Compliance SOS (CSOS):</b><br/>           When set to 1b, the LTSSM is required to send SKP Ordered Sets periodically in between the (modified) compliance patterns.<br/>           The default value of this bit is 0b.<br/>           This bit is applicable when the Link is operating at 2.5 GT/s or 5.0 GT/s data rates only.</p>   |
| 10        | 0h<br>RW/P       | <p><b>Enter Modified Compliance (EMC):</b><br/>           When this bit is set to 1b, the device transmits Modified Compliance Pattern if the LTSSM enters Polling.Compliance substate.<br/>           Default value of this bit is 0b.<br/>           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.</p>  |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 9:7       | 0h<br>RW/P       | <p><b>Transmit Margin (TM):</b><br/>This field controls the value of the non-deemphasized 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).<br/>Encodings:<br/>000b Normal operating range<br/>001b 800-1200 mV for full swing and 400-700 mV for half-swing<br/>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<br/>n - 111b reserved<br/>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.<br/>Default value of this field is 000b.<br/>Components that support only the 2.5 GT/s speed are permitted to hardwire this bit to 000b.<br/>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.</p> |
| 6         | 0h<br>RW/P       | <p><b>Selectable De-emphasis (SD):</b><br/>When the Link is operating at 5.0 GT/s speed, this bit selects the level of de-emphasis for an Upstream component.<br/>Encodings:<br/>1b -3.5 dB<br/>0b -6 dB<br/>When the Link is not operating at 5.0 GT/s speed, the setting of this bit has no effect.</p>   |
| 5         | 0h<br>RO         | <b>Reserved</b>   |
| 4         | 0h<br>RW/P       | <p><b>Enter Compliance (EC):</b><br/>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.<br/>Default value of this bit following Fundamental Reset is 0b.<br/>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.</p>  |
| 3:0       | 1h<br>RW/V/P     | <p><b>Target Link Speed (TLS):</b><br/>This field sets an upper limit on Link operational speed by restricting the values advertised by the upstream component in its training sequences.<br/>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.<br/>Defined encodings are:<br/>0001b: Supported Link Speeds Vector field bit 0.<br/>0010b: Supported Link Speeds Vector field bit 1.<br/>0011b: Supported Link Speeds Vector field bit 2.<br/>0100b: Supported Link Speeds Vector field bit 3.<br/>0101b: Supported Link Speeds Vector field bit 4.<br/>0110b: Supported Link Speeds Vector field bit 5.<br/>0111b: Supported Link Speeds Vector field bit 6.<br/>All other encodings are reserved.<br/>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.<br/>The default value of this field is GEN1.<br/>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.</p>   |



## 5.36 Link Status 2 (LSTS2) – Offset 72h

### Link Status 2

| Type | Size   | Offset                | Default |
|------|--------|-----------------------|---------|
| PCI  | 16 bit | [B:0, D:1, F:0] + 72h | 0000h   |

#### Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 15:8      | 0h<br>RO         | <b>Reserved</b>   |
| 7         | 0h<br>RO/V/P     | <b>Two Retimers Presence Detected (PX2RPD):</b><br>When set to 1b, this bit indicates that two Retimers were present during the most recent Link negotiation.<br>The default value of this bit is 0b.<br>This bit is required for Ports that have the Two Retimers Presence Detect Supported bit of the Link Capabilities 2 register set to 1b.<br>Ports that have the Two Retimers Presence Detect Supported bit set to 0b are permitted to hardwire this bit to 0b. |
| 6         | 0h<br>RO/V/P     | <b>Retimer Presence Detected (RPD):</b><br>When set to 1b, this bit indicates that a Retimer was present during the most recent Link negotiation.<br>The default value of this bit is 0b.<br>This bit is required for Ports that have the Retimer Presence Detect Supported bit Set.<br>Ports that have the Retimer Presence Detect Supported bit of the Link Capabilities 2 register set to 0b are permitted to hardwire this bit to 0b.                             |
| 5         | 0h<br>RW/1C/V/P  | <b>Link Equalization Request (LER):</b><br>This bit is set by hardware to request the 8.0 GT/s Link equalization process to be performed on the Link.   |
| 4         | 0h<br>RO/V/P     | <b>Equalization Phase 3 Successful (EQP3S):</b><br>When set to 1, this bit indicates that Phase 3 of the 8.0 GT/s Transmitter Equalization procedure has successfully completed.  |
| 3         | 0h<br>RO/V/P     | <b>Equalization Phase 2 Successful (EQP2S):</b><br>When set to 1, this bit indicates that Phase 2 of the 8.0 GT/s Transmitter Equalization procedure has successfully completed.  |
| 2         | 0h<br>RO/V/P     | <b>Equalization Phase 1 Successful (EQP1S):</b><br>When set to 1, this bit indicates that Phase 1 of the 8.0 GT/s Transmitter Equalization procedure has successfully completed.  |
| 1         | 0h<br>RO/V/P     | <b>Equalization Complete (EQC):</b><br>When set to 1, this bit indicates that the Transmitter Equalization procedure at the 8.0GT/s data rate has completed.  |
| 0         | 0h<br>RO/V       | <b>Current De-emphasis Level (CDL):</b><br>When the Link is operating at 5.0 GT/s speed, this bit reflects the level of de-emphasis.<br>Encodings:<br>1b -3.5 dB<br>0b -6 dB<br>The value in this bit is undefined when the Link is not operating at 5.0 GT/s speed.  |



## 5.37 Slot Capabilities 2 (SLCAP2) – Offset 74h

Slot Capabilities 2

**Note:** Bit definitions are the same as DSTS2, offset 6Ah.

## 5.38 Slot Control 2 (SLCTL2) – Offset 78h

Slot Control 2

**Note:** Bit definitions are the same as DSTS2, offset 6Ah.

## 5.39 Slot Status 2 (SLSTS2) – Offset 7Ah

Slot Status 2

**Note:** Bit definitions are the same as DSTS2, offset 6Ah.

## 5.40 Message Signaled Interrupt Identifiers (MID) – Offset 80h

Message Signaled Interrupt Identifiers

| Type | Size   | Offset                | Default |
|------|--------|-----------------------|---------|
| PCI  | 16 bit | [B:0, D:1, 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<br>RW/O      | <b>Next Pointer (NEXT):</b><br>Indicates the location of the next capability in the list.<br>The default value of this register is 90h which points to the Subsystem Vendor capability structure.<br>BIOS can determine which capabilities will be exposed by including or removing them from the capability linked list.<br>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       | 05h<br>RO        | <b>Capability ID (CID):</b><br>Capabilities ID indicates MSI.  |

## 5.41 Message Signaled Interrupt Message (MC) – Offset 82h

Message Signaled Interrupt Message

| Type | Size   | Offset                | Default |
|------|--------|-----------------------|---------|
| PCI  | 16 bit | [B:0, D:1, 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<br>RO         | <b>Reserved</b>   |
| 7         | 0h<br>RO         | <b>64 Bit Address Capable (C64):</b><br>Capable of generating a 32-bit message only.  |
| 6:4       | 0h<br>RW         | <b>Multiple Message Enable (MME):</b><br>These bits are RW for software compatibility, but only one message is ever sent by the root port.  |
| 3:1       | 0h<br>RO         | <b>Multiple Message Capable (MMC):</b><br>Only one message is required.   |
| 0         | 0h<br>RW         | <b>MSI Enable (MSIE):</b><br>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. |

## 5.42 Message Signaled Interrupt Message Address (MA) – Offset 84h

Message Signaled Interrupt Message Address

| Type | Size   | Offset                | Default   |
|------|--------|-----------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, 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<br>RW  | <b>ADDR:</b><br>Lower 32 bits of the system specified message address, always DW aligned. |

| Bit Range | Default & Access | Field Name (ID): Description |
|-----------|------------------|------------------------------|
| 1:0       | 0h<br>RO         | <b>Reserved</b>              |

## 5.43 Message Signaled Interrupt Message Data (MD) – Offset 88h

Message Signaled Interrupt Message Data

| Type | Size   | Offset                | Default |
|------|--------|-----------------------|---------|
| PCI  | 16 bit | [B:0, D:1, 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<br>RW      | <b>DATA:</b><br>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. |

## 5.44 Subsystem Vendor Capability (SVCAP) – Offset 90h

Subsystem Vendor Capability

| Type | Size   | Offset                | Default |
|------|--------|-----------------------|---------|
| PCI  | 16 bit | [B:0, D:1, 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<br>RW/O      | <b>Next Capability (NEXT):</b><br>Indicates the location of the next capability in the list.<br>The default value of this register is A0h which points to the PCI Power Management capability structure.<br>BIOS can determine which capabilities will be exposed by including or removing them from the capability linked list.<br>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<br>RO        | <b>Capability Identifier (CID):</b><br>Value of 0Dh indicates this is a PCI bridge subsystem vendor capability.   |

## 5.45 Subsystem Vendor IDs (SVID) – Offset 94h

Subsystem Vendor IDs

| Type | Size   | Offset                | Default   |
|------|--------|-----------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, 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<br>RW/O    | <b>Subsystem Identifier (SID):</b><br>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<br>RW/O    | <b>Subsystem Vendor Identifier (SVID):</b><br>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). |

## 5.46 Power Management Capability (PMCAP) – Offset A0h

Power Management Capability



| Type | Size   | Offset                | Default |
|------|--------|-----------------------|---------|
| PCI  | 16 bit | [B:0, D:1, 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<br>RO        | <b>Next Capability (NEXT):</b><br>Indicates this is the last item in the list.                           |
| 7:0       | 01h<br>RO        | <b>Capability Identifier (CID):</b><br>Value of 01h indicates this is a PCI power management capability. |

## 5.47 PCI Power Management Capabilities (PMC) – Offset A2h

PCI Power Management Capabilities

| Type | Size   | Offset                | Default |
|------|--------|-----------------------|---------|
| PCI  | 16 bit | [B:0, D:1, 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<br>RO        | <b>PMES:</b><br>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<br>RO         | <b>D2S:</b><br>The D2 state is not supported.  |
| 9         | 0h<br>RO         | <b>D1S:</b><br>The D1 state is not supported.  |
| 8:6       | 0h<br>RO         | <b>AC:</b><br>Reports 375mA maximum suspend well current required when in the D3COLD state.  |
| 5         | 0h<br>RO         | <b>Device Specific Initialization (DSI):</b><br>Indicates that no device-specific initialization is required.  |
| 4         | 0h<br>RO         | <b>Reserved</b>  |
| 3         | 0h<br>RO         | <b>PME Clock (PMEC):</b><br>Indicates that PCI clock is not required to generate PME#.   |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 2:0       | 3h<br>RO         | <b>VS:</b><br>Indicates support for Revision 1.2 of the PCI Power Management Specification. |

## 5.48 PCI Power Management Control (PMCS) – Offset A4h

PCI Power Management Control

| Type | Size   | Offset                | Default   |
|------|--------|-----------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, 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<br>RO        | <b>DTA:</b><br>Reserved   |
| 23        | 0h<br>RO         | <b>Bus Power / Clock Control Enable (BPCE):</b><br>This field is reserved per PCI Express specification   |
| 22        | 0h<br>RO         | <b>B2/B3 Support (B23S):</b><br>This field is reserved per PCI Express specification.   |
| 21:16     | 0h<br>RO         | <b>Reserved</b>   |
| 15        | 0h<br>RO         | <b>PME Status (PMES):</b><br>Indicates a PME was received on the downstream link.   |
| 14:13     | 0h<br>RO         | <b>Data Scale (DSC):</b><br>Reserved  |
| 12:9      | 0h<br>RO         | <b>Data Select (DSEL):</b><br>Reserved  |
| 8         | 0h<br>RW/P       | <b>PME Enable (PMEE):</b><br>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<br>RO         | <b>Reserved</b>   |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 3         | 1h<br>RW/O       | <p><b>No Soft Reset (NSR):</b><br/>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.</p> <p>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.</p> <p>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.</p> |
| 2         | 0h<br>RO         | <b>Reserved</b>  |
| 1:0       | 0h<br>RW         | <p><b>Power State (PS):</b><br/>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:<br/>00: D0 state<br/>11: D3HOT state</p> <p>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.</p> <p>If software attempts to write a 10 or 01 to these bits, the write will be ignored.</p>  |

## 5.49 Advanced Error Extended (AECH) – Offset 100h

Advanced Error Extended

| Type | Size   | Offset                 | Default   |
|------|--------|------------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, 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<br>RW/O     | <p><b>Next Capability Offset (NCO):</b><br/>Points to the next capability.</p>  |
| 19:16     | 0h<br>RW/O       | <p><b>Capability Version (CV):</b><br/>For systems that support AER, BIOS should write a 1h to this register else it should write 0</p> |
| 15:0      | 0000h<br>RW/O    | <p><b>Capability ID (CID):</b><br/>For systems that support AER, BIOS should write a 0001h to this register else it should write 0</p>  |



## 5.50 Uncorrectable Error Status (UES) – Offset 104h

Uncorrectable Error Status

| Type | Size   | Offset                 | Default   |
|------|--------|------------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, 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<br>RO            | <b>Reserved</b>  |
| 26        | 0h<br>RW/1C/V/<br>P | <b>Poisoned TLP Egress Blocked Status (PTLPEBS):</b><br>Indicates that poisoned TLP Egress Blocked error has occurred.<br>Note: This bit can only be set if DPCCAPR.PTLPEBS = 1 and DPCCTLR.PTLPEBE = 1.                           |
| 25        | 0h<br>RO            | <b>Reserved</b>  |
| 24        | 0h<br>RW/1C/V/<br>P | <b>AtomicOp Egress Blocked Status (AEBS):</b><br>AtomicOp Egress Blocked Status  |
| 23:22     | 0h<br>RO            | <b>Reserved</b>  |
| 21        | 0h<br>RW/1C/V/<br>P | <b>ACS Violation Status (AVS):</b><br>Indicates an ACS Violation is logged.  |
| 20        | 0h<br>RW/1C/V/<br>P | <b>Unsupported Request Error Status (URE):</b><br>Indicates an unsupported request was received.   |
| 19        | 0h<br>RO            | <b>ECRC Error Status (EE):</b><br>ECRC is not supported.   |
| 18        | 0h<br>RW/1C/V/<br>P | <b>Malformed TLP Status (MT):</b><br>Indicates a malformed TLP was received.   |
| 17        | 0h<br>RW/1C/V/<br>P | <b>Receiver Overflow Status (RO):</b><br>Indicates a receiver overflow occurred.   |
| 16        | 0h<br>RW/1C/V/<br>P | <b>Unexpected Completion Status (UC):</b><br>Indicates an unexpected completion was received.  |
| 15        | 0h<br>RW/1C/V/<br>P | <b>Completer Abort Status (CA):</b><br>Indicates a completer abort was received  |
| 14        | 0h<br>RW/1C/V/<br>P | <b>Completion Timeout Status (CT):</b><br>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<br>RO            | <b>Flow Control Protocol Error Status (FCPE):</b><br>Not supported.  |



| Bit Range | Default & Access    | Field Name (ID): Description   |
|-----------|---------------------|--|
| 12        | 0h<br>RW/1C/V/<br>P | <b>Poisoned TLP Status (PT):</b><br>Indicates a poisoned TLP was received.                       |
| 11:6      | 0h<br>RO            | <b>Reserved</b>  |
| 5         | 0h<br>RO            | <b>Surprise Down Error Status (SDE):</b><br>Surprise Down is not supported.                      |
| 4         | 0h<br>RW/1C/V/<br>P | <b>Data Link Protocol Error Status (DLPE):</b><br>Indicates a data link protocol error occurred. |
| 3:1       | 0h<br>RO            | <b>Reserved</b>  |
| 0         | 0h<br>RO            | <b>Training Error Status (TE):</b><br>Not supported.   |

## 5.51 Uncorrectable Error Mask (UEM) – Offset 108h

Uncorrectable Error Mask

| Type | Size   | Offset                 | Default   |
|------|--------|------------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, 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<br>RO         | <b>Reserved</b>   |
| 26        | 0h<br>RW/P       | <b>Poisoned TLP Egress Blocked Mask (PTLPEBM):</b><br>Mask for Poisoned TLP Egress Blocked error. |
| 25        | 0h<br>RO         | <b>Reserved</b>   |
| 24        | 0h<br>RW/P       | <b>AtomicOp Egress Blocked Mask (AEBM):</b><br>Mask for AtomicOp Egress Blocked                   |
| 23:22     | 0h<br>RO         | <b>Reserved</b>   |
| 21        | 0h<br>RW/P       | <b>ACS Violation Mask (AVM):</b><br>Mask for ACS Violation errors.                                |
| 20        | 0h<br>RW/P       | <b>Unsupported Request Error Mask (URE):</b><br>Mask for uncorrectable errors.                    |
| 19        | 0h<br>RO         | <b>ECRC Error Mask (EE):</b><br>ECRC is not supported.  |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 18        | 0h<br>RW/P       | <b>Malformed TLP Mask (MT):</b><br>Mask for malformed TLPs                          |
| 17        | 0h<br>RW/P       | <b>Receiver Overflow Mask (RO):</b><br>Mask for receiver overflows.                 |
| 16        | 0h<br>RW/P       | <b>Unexpected Completion Mask (UC):</b><br>Mask for unexpected completions.         |
| 15        | 0h<br>RW/P       | <b>Completer Abort Mask (CM):</b><br>Mask for completer abort.                      |
| 14        | 0h<br>RW/P       | <b>Completion Timeout Mask (CT):</b><br>Mask for completion timeouts.               |
| 13        | 0h<br>RO         | <b>Flow Control Protocol Error Mask (FCPE):</b><br>Not supported.                   |
| 12        | 0h<br>RW/P       | <b>Poisoned TLP Mask (PT):</b><br>Mask for poisoned TLPs.                           |
| 11:6      | 0h<br>RO         | <b>Reserved</b>   |
| 5         | 0h<br>RO         | <b>Surprise Down Error Mask (SDE):</b><br>Surprise Down is not supported.           |
| 4         | 0h<br>RW/P       | <b>Data Link Protocol Error Mask (DLPE):</b><br>Mask for data link protocol errors. |
| 3:1       | 0h<br>RO         | <b>Reserved</b>   |
| 0         | 0h<br>RO         | <b>Training Error Mask (TE):</b><br>Not supported.                                  |

## 5.52 Uncorrectable Error Severity (UEV) – Offset 10Ch

Uncorrectable Error Severity

| Type | Size   | Offset                 | Default   |
|------|--------|------------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, 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<br>RO         | <b>Reserved</b>   |
| 26        | 0h<br>RW/P       | <b>Poisoned TLP Egress Blocked Severity (PTLPEBS):</b><br>Severity for Poisoned TLP Egress Blocked error. |
| 25        | 0h<br>RO         | <b>Reserved</b>   |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 24        | 0h<br>RW/P       | <b>AtomicOp Egress Blocked Severity (AEBS):</b><br>AtomicOp Egress Blocked Severity             |
| 23:22     | 0h<br>RO         | <b>Reserved</b>   |
| 21        | 0h<br>RW/P       | <b>ACS Violation Severity (AVS):</b><br>Severity for ACS Violation.                             |
| 20        | 0h<br>RW/P       | <b>Unsupported Request Error Severity (URE):</b><br>Severity for unsupported request reception. |
| 19        | 0h<br>RO         | <b>ECRC Error Severity (EE):</b><br>ECRC is not supported.                                      |
| 18        | 1h<br>RW/P       | <b>Malformed TLP Severity (MT):</b><br>Severity for malformed TLP reception.                    |
| 17        | 1h<br>RW/P       | <b>Receiver Overflow Severity (RO):</b><br>Severity for receiver overflow occurrences.          |
| 16        | 0h<br>RW/P       | <b>Unexpected Completion Severity (UC):</b><br>Severity for unexpected completion reception.    |
| 15        | 0h<br>RW/P       | <b>Completer Abort Severity (CA):</b><br>Severity for completer abort.                          |
| 14        | 0h<br>RW/P       | <b>Completion Timeout Severity (CT):</b><br>Severity for completion timeout.                    |
| 13        | 0h<br>RO         | <b>Flow Control Protocol Error Severity (FCPE):</b><br>Not supported.                           |
| 12        | 0h<br>RW/P       | <b>Poisoned TLP Severity (PT):</b><br>Severity for poisoned TLP reception.                      |
| 11:6      | 0h<br>RO         | <b>Reserved</b>   |
| 5         | 0h<br>RO         | <b>Surprise Down Error Severity (SDE):</b><br>Surprise Down is not supported.                   |
| 4         | 1h<br>RW/P       | <b>Data Link Protocol Error Severity (DLPE):</b><br>Severity for data link protocol errors.     |
| 3:1       | 0h<br>RO         | <b>Reserved</b>   |
| 0         | 0h<br>RO         | <b>Training Error Severity (TE):</b><br>TE not supported.                                       |

## 5.53 Correctable Error Status (CES) – Offset 110h

Correctable Error Status

| Type | Size   | Offset                 | Default   |
|------|--------|------------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, 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<br>RO            | <b>Reserved</b>   |
| 13        | 0h<br>RW/1C/V/<br>P | <b>Advisory Non-Fatal Error Status (ANFES):</b><br>When set, indicates that an Advisory Non-Fatal Error occurred. |
| 12        | 0h<br>RW/1C/V/<br>P | <b>Replay Timer Timeout Status (RTT):</b><br>Indicates the replay timer timed out.                                |
| 11:9      | 0h<br>RO            | <b>Reserved</b>   |
| 8         | 0h<br>RW/1C/V/<br>P | <b>Replay Number Rollover Status (RNR):</b><br>Indicates the replay number rolled over.                           |
| 7         | 0h<br>RW/1C/V/<br>P | <b>Bad DLLP Status (BD):</b><br>Indicates a bad DLLP was received.  |
| 6         | 0h<br>RW/1C/V/<br>P | <b>Bad TLP Status (BT):</b><br>Indicates a bad TLP was received.  |
| 5:1       | 0h<br>RO            | <b>Reserved</b>   |
| 0         | 0h<br>RW/1C/V/<br>P | <b>Receiver Error Status (RE):</b><br>Indicates a receiver error occurred.  |

## 5.54 Correctable Error Mask (CEM) – Offset 114h

Correctable Error Mask

| Type | Size   | Offset                 | Default   |
|------|--------|------------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, 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<br>RO         | <b>Reserved</b>   |
| 13        | 1h<br>RW/P       | <b>Advisory Non-Fatal Error Mask (ANFEM):</b><br>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<br>RW/P       | <b>Replay Timer Timeout Mask (RTT):</b><br>Mask for replay timer timeout.   |
| 11:9      | 0h<br>RO         | <b>Reserved</b>   |
| 8         | 0h<br>RW/P       | <b>Replay Number Rollover Mask (RNR):</b><br>Mask for replay number rollover.   |
| 7         | 0h<br>RW/P       | <b>Bad DLLP Mask (BD):</b><br>Mask for bad DLLP reception.  |
| 6         | 0h<br>RW/P       | <b>Bad TLP Mask (BT):</b><br>Mask for bad TLP reception.  |
| 5:1       | 0h<br>RO         | <b>Reserved</b>   |
| 0         | 0h<br>RW/P       | <b>Receiver Error Mask (RE):</b><br>Mask for receiver errors.   |

## 5.55 Advanced Error Capabilities And Control (AECC) — Offset 118h

Advanced Error Capabilities And Control

| Type | Size   | Offset                 | Default   |
|------|--------|------------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, 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<br>RO         | <b>Reserved</b>   |
| 12        | 0h<br>RO         | <b>Completion Timeout Prefix/Header Log Capable (CTPHLC):</b><br>If set, this bit indicates that port records the prefix/header of Request TLPs that experience a Completion Timeout error.<br>Note: BIOS should program this bit before enable the Completion Timeout mechanism. |
| 11:9      | 0h<br>RO         | <b>Reserved</b>   |
| 8         | 0h<br>RO         | <b>ECRC Check Enable (ECE):</b><br>ECRC is not supported.   |
| 7         | 0h<br>RO         | <b>ECRC Check Capable (ECC):</b><br>ECRC is not supported.  |
| 6         | 0h<br>RO         | <b>ECRC Generation Enable (EGE):</b><br>ECRC is not supported.  |
| 5         | 0h<br>RO         | <b>ECRC Generation capable (EGC):</b><br>ECRC is not supported.   |
| 4:0       | 00h<br>RO/V/P    | <b>First Error Pointer (FEP):</b><br>Identifies the bit position of the first error reported in the Uncorrectable Error Status Register.  |

## 5.56 Header Log (HL\_DW1) – Offset 11Ch

Header Log

| Type | Size   | Offset                 | Default   |
|------|--------|------------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, 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<br>RO/V/P | <b>1st DWORD of TLP (DW1):</b><br>Byte0 && Byte1 && Byte2 && Byte3 |



## 5.57 Header Log (HL\_DW2) – Offset 120h

Header Log

| Type | Size   | Offset                 | Default   |
|------|--------|------------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, 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<br>RO/V/P | <b>2nd DWORD of TLP (DW2):</b><br>Byte4 && Byte5 && Byte6 && Byte7 |

## 5.58 Header Log (HL\_DW3) – Offset 124h

Header Log

| Type | Size   | Offset                 | Default   |
|------|--------|------------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, 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<br>RO/V/P | <b>3rd DWORD of TLP (DW3):</b><br>Byte8 && Byte9 && Byte10 && Byte11 |

## 5.59 Header Log (HL\_DW4) – Offset 128h

Header Log



| Type | Size   | Offset                 | Default   |
|------|--------|------------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, 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<br>RO/V/P | <b>4th DWORD of TLP (DW4):</b><br>Byte12 && Byte13 && Byte14 && Byte15 |

## 5.60 Root Error Command (REC) – Offset 12Ch

Root Error Command

| Type | Size   | Offset                 | Default   |
|------|--------|------------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, 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<br>RO         | <b>Reserved</b>  |
| 2         | 0h<br>RW         | <b>Fatal Error Reporting Enable (FERE):</b><br>When set, the root port will generate an interrupt when a fatal error is reported by the attached device.             |
| 1         | 0h<br>RW         | <b>Non-fatal Error Reporting Enable (NERE):</b><br>When set, the root port will generate an interrupt when a non-fatal error is reported by the attached device.     |
| 0         | 0h<br>RW         | <b>Correctable Error Reporting Enable (CERE):</b><br>When set, the root port will generate an interrupt when a correctable error is reported by the attached device. |

## 5.61 Root Error Status (RES) – Offset 130h

Root Error Status



| Type | Size   | Offset                 | Default   |
|------|--------|------------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, 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<br>RO           | <b>Advanced Error Interrupt Message Number (AEMN):</b><br>Reserved  |
| 26:7      | 0h<br>RO            | <b>Reserved</b>   |
| 6         | 0h<br>RW/1C/V/<br>P | <b>Fatal Error Messages Received (FEMR):</b><br>Set when one or more Fatal Uncorrectable Error Messages have been received.                     |
| 5         | 0h<br>RW/1C/V/<br>P | <b>Non-Fatal Error Messages Received (NFEMR):</b><br>Set when one or more Non-Fatal Uncorrectable error messages have been received             |
| 4         | 0h<br>RW/1C/V/<br>P | <b>First Uncorrectable Fatal (FUF):</b><br>Set when the first Uncorrectable Error message received is for a fatal error.                        |
| 3         | 0h<br>RW/1C/V/<br>P | <b>Multiple ERR_FATAL/NONFATAL Received (MENR):</b><br>Set when either a fatal or a non-fatal error is received and the ENR bit is already set. |
| 2         | 0h<br>RW/1C/V/<br>P | <b>ERR_FATAL/NONFATAL Received (ENR):</b><br>Set when either a fatal or a non-fatal error message is received.                                  |
| 1         | 0h<br>RW/1C/V/<br>P | <b>Multiple ERR_COR Received (MCR):</b><br>Set when a correctable error message is received and the CR bit is already set.                      |
| 0         | 0h<br>RW/1C/V/<br>P | <b>ERR_COR Received (CR):</b><br>Set when a correctable error message is received.  |

## 5.62 Error Source Identification (ESID) – Offset 134h

Error Source Identification

| Type | Size   | Offset                 | Default   |
|------|--------|------------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, 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<br>RO/V/P  | <b>ERR_FATAL/NONFATAL Source Identification (EFNFSID):</b><br>Loaded with the requester ID indicated in the received ERR_FATAL or ERR_NONFATAL message when RES.ENR is first set, or the internal requester ID if an internally detected error. |
| 15:0      | 0000h<br>RO/V/P  | <b>ERR_COR Source Identification (ECSID):</b><br>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.                                 |

## 5.63 PTM Extended Capability Header (PTMECH) – Offset 150h

PTM Extended Capability Header

| Type | Size   | Offset                 | Default   |
|------|--------|------------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, 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<br>RW/O     | <b>Next Capability Offset (NCO):</b><br>Points to the next capability.   |
| 19:16     | 0h<br>RW/O       | <b>Capability Version (CV):</b><br>For systems that support PTM Extended Capability, BIOS should write a 1h to this register else it should write 0. |
| 15:0      | 0000h<br>RW/O    | <b>Capability ID (CID):</b><br>For systems that support PTM Extended Capability, BIOS should write a 001Fh to this register else it should write 0.  |

## 5.64 PTM Capability Register (PTMCAPR) – Offset 154h

PTM Capability Register



| Type | Size   | Offset                 | Default   |
|------|--------|------------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, F:0] + 154h | 00000410h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 31:16     | 0h<br>RO         | <b>Reserved</b>  |
| 15:8      | 04h<br>RW/O      | <p><b>Local Clock Granularity (LCG):</b><br/>           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.<br/>           0000 0001b - 1111 1110b: Indicates the period of this Time Source's local clock in ns.<br/>           1111 1111b: Indicates the period of this Time Source's local clock is greater than 254 ns.</p> <p>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.</p> |
| 7:5       | 0h<br>RO         | <b>Reserved</b>  |
| 4         | 1h<br>RO         | <p><b>PTM Propagation Delay Adaptation Capable (PTMPDAC):</b><br/>           When Set, this field indicates the Port supports the PTM Propagation Delay Adaptation Capability.</p>   |
| 3         | 0h<br>RO         | <b>Reserved</b>  |
| 2         | 0h<br>RW/O       | <p><b>PTM Root Capable (PTMRC):</b><br/>           Root Ports must set this bit to 1b.</p>   |
| 1         | 0h<br>RW/O       | <p><b>PTM Responder Capable (PTMRSPC):</b><br/>           Root Ports are permitted to set this bit to 1b to indicate that they implement the PTM Responder role.</p>   |
| 0         | 0h<br>RO         | <p><b>PTM Requester Capable (PTMREQC):</b><br/>           PTM Requester Role is not supported by Root Port.</p>  |

## 5.65 PTM Control Register (PTMCTLR) – Offset 158h

PTM Control Register

| Type | Size   | Offset                 | Default   |
|------|--------|------------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, 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<br>RO         | <b>Reserved</b>   |
| 15:8      | 00h<br>RO        | <b>Effective Granularity (EG):</b><br>Root Port does not support PTM Requester role.  |
| 7:3       | 0h<br>RO         | <b>Reserved</b>   |
| 2         | 0h<br>RW         | <b>PTM Propagation Delay Adaptation Interpretation B (PTMPDAIB):</b><br>If PTM Propagation Delay Adaptation Capable is Set, then this bit when Set selects interpretation B of the Propagation Delay[31:0] field in the PTM ResponseD Message<br>For a Switch, if a specific Port is permanently attached such that this control is not required, it is permitted for that Port for this bit to be RsvdP.<br>Default value is 0b. |
| 1         | 0h<br>RW         | <b>Root Select (RS):</b><br>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<br>RW         | <b>PTM Enable (PTME):</b><br>When Set, this Function is permitted to participate in the PTM mechanism according to its selected role.<br>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.                                    |

## 5.66 L1 Sub-States Extended Capability Header (L1SECH) – Offset 200h

L1 Sub-States Extended Capability Header



| Type | Size   | Offset                 | Default   |
|------|--------|------------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, F:0] + 200h | 00000000h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 31:20     | 000h<br>RW/O     | <p><b>Next Capability Offset (NCO):</b><br/>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.<br/>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.<br/>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.</p> |
| 19:16     | 0h<br>RW/O       | <p><b>Capability Version (CV):</b><br/>This field is a PCI-SIG defined version number that indicates the version of the Capability structure present.<br/>Must be 1h for this version of the specification.<br/>For systems that support L1 Sub-State Extended Capability, BIOS should set this field to 1h.</p>   |
| 15:0      | 0000h<br>RW/O    | <p><b>PCI Express Extended Capability ID (PCIIEC):</b><br/>This field is a PCI-SIG defined ID number that indicates the nature and format of the Extended Capability.<br/>For systems that support L1 Sub-State Extended Capability, BIOS should set this field to 001Eh.</p>  |

## 5.67 L1 Sub-States Capabilities (L1SCAP) – Offset 204h

L1 Sub-States Capabilities

| Type | Size   | Offset                 | Default   |
|------|--------|------------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, F:0] + 204h | 0028281Fh |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description |
|-----------|------------------|------------------------------|
| 31:24     | 0h<br>RO         | <b>Reserved</b>              |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 23:19     | 05h<br>RW/O      | <p><b>Port Tpower_on Value (PTV):</b><br/>           Along with the Port Tpower_on Scale field in the L1 Sub-states Capabilities register sets the time (in us) that this Port requires the port on the opposite side of Link to wait in L1.OFF_EXIT after sampling CLKREQ# asserted before actively driving the interface.<br/>           Port Tpower_on is calculated by multiplying the value in this field by the value in the Port Tpower_on scale field in the L1 Sub-States Capabilities register.<br/>           Required for all Ports that support L1.OFF.</p> |
| 18        | 0h<br>RO         | <b>Reserved</b>  |
| 17:16     | 0h<br>RW/O       | <p><b>Port Tpower_on Scale (PTPOS):</b><br/>           Specifies the scale used for Tpower_on value field in the L1 Sub-states Capabilities register.<br/>           00b: 2 us<br/>           01b: 10 us<br/>           10b: 100 us<br/>           11b: Reserved<br/>           Required for all Ports that support L1.OFF.</p>  |
| 15:8      | 28h<br>RW/O      | <p><b>Port Common Mode Restore Time (PCMRT):</b><br/>           This is the time (in us) required for this Port to re-establish common mode.<br/>           Required for all ports that support L1.OFF.</p>  |
| 7         | 0h<br>RO         | <b>Reserved</b>  |
| 6         | 0h<br>RW/1C/V    | <p><b>CLKREQ# Acceleration Interrupt Status (L1SSEIS):</b><br/>           For a Downstream Port that has both the CLKREQ# Acceleration Supported and CLKREQ# Acceleration Interrupt Enable bits Set, when set this bit indicates that the Port has completed the CLKREQ# Acceleration Link Activation process, and that the Link has reached L0. Software must then clear this bit by writing a 1b to this bit.<br/>           Must be hardwired to 0b for Upstream Ports.<br/>           Default value is 0b.</p>   |
| 5         | 0h<br>RW/O       | <p><b>CLKREQ# Acceleration Supported (L1SSES):</b><br/>           When set this bit indicates that this Port supports CLKREQ# acceleration</p>   |
| 4         | 1h<br>RW/O       | <p><b>L1 PM Sub-states Supported (L1PSS):</b><br/>           When Set this bit indicates that this Port supports L1 PM Sub-states.<br/>           For compatibility with possible future extensions, software must not enable L1 PM Sub-states unless this bit is set.<br/>           This RWO field must be programmed prior to enabling ASPM.<br/>           Required for both Upstream and Downstream Ports.</p>  |
| 3         | 1h<br>RW/O       | <p><b>ASPM L1.1 Supported (AL11S):</b><br/>           When set, this bit indicates ASPM L1.SNOOZ is supported.<br/>           Required for both Upstream and Downstream ports.<br/>           This RWO field must be programmed prior to enabling ASPM.</p>  |
| 2         | 1h<br>RW/O       | <p><b>ASPM L1.2 Supported (AL12S):</b><br/>           When set, this bit indicates that ASPM L1.OFF is supported.<br/>           Required for both Upstream and Downstream ports.<br/>           This RWO field must be programmed prior to enabling ASPM.</p>   |
| 1         | 1h<br>RW/O       | <p><b>PCI-PM L1.1 Supported (PPL11S):</b><br/>           When set, this bit indicates that PCI-PM L1.SNOOZ is supported and this bit must be set by all ports implementing L1 Sub-States. A port that supports L1.OFF must support L1.SNOOZ.<br/>           Required for both upstream and downstream ports.<br/>           This RWO field must be programmed prior to enabling ASPM.</p>  |



| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 0         | 1h<br>RW/O       | <b>PCI-PM L1.2 Supported (PPL12S):</b><br>When set, this bit indicates that PCI-PM L1.OFF is supported.<br>Required for both upstream and downstream ports.<br>This RWO field must be programmed prior to enabling ASPM. |

## 5.68 L1 Sub-States Control 1 (L1SCTL1) – Offset 208h

L1 Sub-States Control 1

| Type | Size   | Offset                 | Default   |
|------|--------|------------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, F:0] + 208h | 00000000h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 31:29     | 0h<br>RW         | <b>L1.2 LTR Threshold Latency Scale Value (L12LTRLV):</b><br>This field contains the L1.OFF LTR Threshold Latency Scale Value for this particular Root Port. The value in this field, together with L12LTRLV is compared against both the snoop and non-snoop LTR values of the device.<br>000: L12LTRLV times 1 ns<br>001: L12LTRLV times 32 ns<br>010: L12LTRLV times 1024 ns<br>011: L12LTRLV times 32768 ns<br>100: L12LTRLV times 1048576 ns<br>101: L12LTRLV times 33554432 ns<br>Others: Not Permitted.<br>This field must be programmed prior to enabling L1.OFF. |
| 28:26     | 0h<br>RO         | <b>Reserved</b>   |
| 25:16     | 000h<br>RW       | <b>L1.2 LTR Threshold Latency Value (L12LTRLV):</b><br>This field contains the L1.2 LTR Threshold Latency Value for this particular Root Port. The value in this field, together with L12LTRLV is compared against both the snoop and non-snoop LTR values of the device.<br>This field must be programmed prior to enabling L1.OFF.  |
| 15:8      | 00h<br>RW        | <b>Common Mode Restore Time (CMRT):</b><br>This is the Tcommon_mode time(in us) the Root Port needs to continue sending TS1 and refrain from sending TS2 in Recovery state to allow the TX common mode to be established prior to sending TS2. The timer starts from the time when the first TS1 has been sent and the receiver has detected un-squelch. The value in this field defines the time in micro-seconds.<br>This field must be programmed prior to enabling L1.OFF.  |
| 7:6       | 0h<br>RO         | <b>Reserved</b>   |



| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 5         | 0h<br>RW         | <b>L1 Substate Exit Control (L1SSEC):</b><br>L1.Substate the Port must initiate the CLKREQ# Acceleration Link Activation process. Apart from that, once the Link reaches L0, the Port must continue to attempt to maintain the Link in L0 for as long as this bit remains Set. However if the Upstream Port request for L1 entry, the Downstream Port will proceed to allow L1 entry but will not re-enter L1.1 or L1.2.  |
| 4         | 0h<br>RW         | <b>CLKREQ# Acceleration Interrupt Enable (L1SSEIE):</b><br>When set this bit enables the generation of an interrupt to indicate the completion of the CLKREQ# acceleration Link Activation process  |
| 3         | 0h<br>RW         | <b>ASPM L1.1 Enable (AL11E):</b><br>When set, this bit indicates that ASPM L1.SNOOZ Sub-states are enabled. Required for both upstream and downstream ports.<br>Note: If STRPFUSECFG.mPHYIOPMDIS is 1, hardware will always see 0 as an output from this register. BIOS reading this register should always return the correct value.   |
| 2         | 0h<br>RW         | <b>ASPM L1.2 Enable (AL12E):</b><br>When set, this bit indicates that ASPM L1.OFF Sub-states are enabled. Required for both upstream and downstream ports.<br>Note: If STRPFUSECFG.mPHYIOPMDIS is 1, hardware will always see 0 as an output from this register. BIOS reading this register should always return the correct value.   |
| 1         | 0h<br>RW         | <b>PCI-PM L1.1 Enable (PPL11E):</b><br>When set, this bit indicates that PCI-PM L1.SNOOZ power management feature is enabled. If L1.OFF is enabled, L1.SNOOZ must also be enabled.<br>This field must be programmed prior to enabling ASPM L1.<br>Note: If STRPFUSECFG.mPHYIOPMDIS is 1, hardware will always see 0 as an output from this register. BIOS reading this register should always return the correct value.   |
| 0         | 0h<br>RW         | <b>PCI-PM L1.2 Enabled (PPL12E):</b><br>When set, this bit indicates that PCI-PM L1.OFF power management feature is enabled. L1.OFF can only be enabled if the platform supports bi-directional CLKREQPLUS#.<br>This field must be programmed prior to enabling ASPM L1.<br>Ports that support L1.OFF shall support Latency Tolerance Reporting.<br>Note: If STRPFUSECFG.mPHYIOPMDIS is 1, hardware will always see 0 as an output from this register. BIOS reading this register should always return the correct value. |

## 5.69 L1 Sub-States Control 2 (L1SCTL2) – Offset 20Ch

L1 Sub-States Control 2

| Type | Size   | Offset                 | Default   |
|------|--------|------------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, F:0] + 20Ch | 00000028h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description |
|-----------|------------------|------------------------------|
| 31:8      | 0h<br>RO         | <b>Reserved</b>              |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 7:3       | 05h<br>RW        | <b>Power On Wait Time (POWT):</b><br>Along with the Tpower_on Scale sets the minimum amount of time (in us) that the Port must wait in L1.OFF EXIT after sampling CLKREQPLUS# asserted before actively driving the interface. The timer starts counting when CLKREQPLUS# is sampled asserted in L1.OFF state.<br>Tpower_on value is calculated by multiplying the value in this field by the value in the TPOS field.<br>This field must be programmed prior to enabling L1.OFF. |
| 2         | 0h<br>RO         | <b>Reserved</b>  |
| 1:0       | 0h<br>RW         | <b>Tpower_on Scale (TPOS):</b><br>Specifies the scale used for Tpower_on value.<br>00b: 2 us<br>01b: 10 us<br>10b: 100us<br>11b: Reserved.<br>Required for all Ports that support L1.OFF.  |

## 5.70 ACS Extended Capability Header (ACSECH) — Offset 220h

ACS Extended Capability Header

| Type | Size   | Offset                 | Default   |
|------|--------|------------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, 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<br>RW/O     | <b>Next Capability Offset (NCO):</b><br>Points to the next capability.   |
| 19:16     | 0h<br>RW/O       | <b>Capability Version (CV):</b><br>For systems that support ACS Extended Capability, BIOS should write a 1h to this register else it should write 0. |
| 15:0      | 0000h<br>RW/O    | <b>Capability ID (CID):</b><br>For systems that support ACS Extended Capability, BIOS should write a 000Dh to this register else it should write 0.  |

## 5.71 ACS Capability Register (ACSCAPR) — Offset 224h

ACS Capability Register

| Type | Size   | Offset                 | Default |
|------|--------|------------------------|---------|
| PCI  | 16 bit | [B:0, D:1, F:0] + 224h | 001Fh   |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 15:7      | 0h<br>RO         | <b>Reserved</b>  |
| 6         | 0h<br>RO         | <b>ACS Direct Translated P2P (T):</b><br>ACS Direct Translated P2P is not supported.   |
| 5         | 0h<br>RO         | <b>ACS P2P Egress Control (E):</b><br>ACS P2P Egress Control is not supported.   |
| 4         | 1h<br>RW/O       | <b>ACS Upstream Forwarding (U):</b><br>ACS Upstream Forwarding.  |
| 3         | 1h<br>RW/O       | <b>ACS P2P Completion Redirect (C):</b><br>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.   |
| 2         | 1h<br>RW/O       | <b>ACS P2P Request Redirect (R):</b><br>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<br>RW/O       | <b>ACS Translation Blocking (B):</b><br>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<br>RW/O       | <b>ACS Source Validation (V):</b><br>Required for Root Ports and Switch Downstream Ports - must be hardwired to 0b otherwise. If 1b, indicates that the component implements ACS Source Validation.  |

## 5.72 ACS Control Register (ACSCTLR) – Offset 226h

ACS Control Register

| Type | Size   | Offset                 | Default |
|------|--------|------------------------|---------|
| PCI  | 16 bit | [B:0, D:1, 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<br>RO         | <b>Reserved</b>   |
| 6         | 0h<br>RO         | <b>ACS Direct Translated P2P Enable (TE):</b><br>ACS Direct Translated P2P is not supported.  |
| 5         | 0h<br>RO         | <b>ACS P2P Egress Control Enable (EE):</b><br>ACS P2P Egress Control is not supported.  |
| 4         | 0h<br>RW         | <b>ACS Upstream Forwarding Enable (UE):</b><br>ACS Upstream Forwarding.   |
| 3         | 0h<br>RW         | <b>ACS P2P Completion Redirect Enable (CE):</b><br>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<br>RW         | <b>ACS P2P Request Redirect Enable (RE):</b><br>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.                    |
| 1         | 0h<br>RW         | <b>ACS Translation Blocking Enable (BE):</b><br>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<br>RW         | <b>ACS Source Validation Enable (VE):</b><br>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.      |

## 5.73 Port VC Capability Register 1 (PVCCR1) – Offset 284h

Port VC Capability Register 1

| Type | Size   | Offset                 | Default   |
|------|--------|------------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, F:0] + 284h | 00000000h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 31:12     | 0h<br>RO         | <b>Reserved</b>   |
| 11:10     | 0h<br>RO         | <b>Function Arbitration Table Entry Size (FARES):</b><br>Indicates the size (in bits) of Function Arbitration table entry in the device.<br>Defined encodings are:<br>00b Size of Function Arbitration table entry is 1 bit<br>01b Size of Function Arbitration table entry is 2 bits<br>10b Size of Function Arbitration table entry is 4 bits<br>11b Size of Function Arbitration table entry is 8 bits |
| 9:8       | 0h<br>RO         | <b>Reference Clock (RC):</b><br>Indicates the reference clock for Virtual Channels that support time-based WRR Function Arbitration.<br>Defined encodings are:<br>00b 100 ns reference clock<br>01b 11b Reserved  |
| 7         | 0h<br>RO         | <b>Reserved</b>   |
| 6:4       | 0h<br>RO         | <b>Low Priority Extended VC Count (LPEVCC):</b><br>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 minimum value of this field is 000b and the maximum value is Extended VC Count.                               |
| 3         | 0h<br>RO         | <b>Reserved</b>   |
| 2:0       | 0h<br>RW/O       | <b>Extended VC Count (EVCC):</b><br>Indicates the number of (extended) Virtual Channels in addition to the default VC supported by the device.<br>The minimum value of this field is zero (for devices that only support the default VC).<br>The maximum value is seven.  |

## 5.74 DPC Extended Capability Header (DPCECH) – Offset A00h

DPC Extended Capability Header



| Type | Size   | Offset                 | Default   |
|------|--------|------------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, 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<br>RW/O     | <b>Next Capability Offset (NCO):</b><br>Points to the next capability.   |
| 19:16     | 0h<br>RW/O       | <b>Capability Version (CV):</b><br>For systems that support DPC Extended Capability, BIOS should write a 1h to this register else it should write 0. |
| 15:0      | 0000h<br>RW/O    | <b>Capability ID (CID):</b><br>For systems that support DPC Extended Capability, BIOS should write a 001Dh to this register else it should write 0.  |

## 5.75 DPC Capability Register (DPCCAPR) – Offset A04h

DPC Capability Register

| Type | Size   | Offset                 | Default |
|------|--------|------------------------|---------|
| PCI  | 16 bit | [B:0, D:1, 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<br>RO         | <b>Reserved</b>  |
| 12        | 1h<br>RW/O       | <b>DL_Active ERR_COR Signaling Supported (DLAECSS):</b><br>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<br>RW/O       | <b>RP PIO Log Size (RPPIOLS):</b><br>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<br>RW/O       | <b>DPC Software Triggering Supported (DPCSTS):</b><br>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.   |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 6         | 1h<br>RW/O       | <b>Poisoned TLP Egress Blocking Supported (PTLPEBS):</b><br>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<br>RW/O       | <b>RP Extensions For DPC (RPEFDPC):</b><br>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<br>RW/O      | <b>DPC Interrupt Message Number (DPCIMN):</b><br>This field indicates which MSI/MSI-X vector is used for the interrupt message generated in association with the DPC Capability structure.<br>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.<br>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.<br>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.<br>Note: BIOS is expected to update this field with the right value before enabling DPC interrupt. |

## 5.76 DPC Control Register (DPCCTLR) – Offset A06h

DPC Control Register

| Type | Size   | Offset                 | Default |
|------|--------|------------------------|---------|
| PCI  | 16 bit | [B:0, D:1, 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<br>RO         | <b>Reserved</b>   |
| 7         | 0h<br>RW         | <b>DL_Active ERR_COR Enable (DLAECE):</b><br>This bit when set, enables the downstream port to signal ERR_COR when the link transitions to the DL_Active state. |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 6         | 0h<br>RW/1S/V    | <b>DPC Software Trigger (DPCST):</b><br>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.<br>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.<br>*Note: This bit always return 0b when read. |
| 5         | 0h<br>RW         | <b>Poisoned TLP Egress Blocking Enable (PTLPEBE):</b><br>This bit, when set, enables the associated Egress Port to block the transmission of poisoned TLP.  |
| 4         | 0h<br>RW         | <b>DPC ERR_COR Enable (DPCECE):</b><br>When set, this bit enables the generation of an interrupt to indicate that DPC has been triggered.   |
| 3         | 0h<br>RW         | <b>DPC Interrupt Enable (DPCIE):</b><br>When set, this bit enables the generation of an interrupt to indicate that DPC has been triggered.  |
| 2         | 0h<br>RW         | <b>DPC Completion Control (DPCCC):</b><br>This bit controls the Completion Status for completions formed during DPC.<br>0b: Completer Abort (CA) Completion Status.<br>1b: Unsupported Request (UR) Completion Status.  |
| 1:0       | 0h<br>RW         | <b>DPC Trigger Enable (DPCTE):</b><br>This field enables DPC and controls the conditions that cause DPC to be triggered.<br>00b: DPC is disabled.<br>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.<br>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.<br>11b: Reserved.   |

## 5.77 DPC Status Register (DPCSR) – Offset A08h

DPC Status Register

| Type | Size   | Offset                 | Default |
|------|--------|------------------------|---------|
| PCI  | 16 bit | [B:0, D:1, 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<br>RO         | <b>Reserved</b>              |



| Bit Range | Default & Access    | Field Name (ID): Description  |
|-----------|---------------------|---|
| 12:8      | 1Fh<br>RO/V/P       | <p><b>RP PIO First Error Pointer (RPPIOFEP):</b><br/>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.<br/>This field is applicable only for Root Ports that support RP Extensions for DPC, and is otherwise reserved.<br/>If this field is not reserved, the default value is 11111b.</p>   |
| 7         | 0h<br>RO            | <b>Reserved</b>   |
| 6:5       | 0h<br>RO/V/P        | <p><b>DPC Trigger Extension (DPCTE):</b><br/>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.<br/>00b: DPC was triggered due to RP PIO error.<br/>01b: DPC was triggered due to DPC Software Trigger bit.<br/>10b: Reserved.<br/>11b: Reserved.<br/>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.</p>   |
| 4         | 0h<br>RO/V          | <p><b>DPC RP Busy (DPCRPB):</b><br/>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.<br/>This field is valid only when the DPC Trigger Status bit is Set - otherwise the value of this field is undefined.<br/>This bit is applicable only for Root Ports that support RP Extensions for DPC, and is Reserved otherwise.</p>                             |
| 3         | 0h<br>RW/1C/V/<br>P | <p><b>DPC Interrupt Status (DPCIS):</b><br/>This bit is set if DPC is triggered while the DPC Interrupt Enable bit is set.</p>  |
| 2:1       | 0h<br>RO/V/P        | <p><b>DPC Trigger Reason (DPCTR):</b><br/>This field indicates why DPC has been triggered.<br/>00b: DPC was triggered due to an unmasked uncorrectable error.<br/>01b: DPC was triggered due to receiving an ERR_NONFATAL.<br/>10b: DPC was triggered due to receiving an ERR_FATAL.<br/>11b: DPC was triggered due to a reason that is indicated by the DPC Trigger Reason Extension field.<br/>Note: This field is only valid when DPC Trigger Status bit is set - otherwise the value of this field is undefined.</p>  |
| 0         | 0h<br>RW/1C/V/<br>P | <p><b>DPC Trigger Status (DPCTS):</b><br/>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.<br/>Refer to PCIe Base specification 3.0 for more timing requirements pertaining to this bit.</p> |

## 5.78 DPC Error Source ID Register (DPCESIDR) — Offset A0Ah

DPC Error Source ID Register



| Type | Size   | Offset                 | Default |
|------|--------|------------------------|---------|
| PCI  | 16 bit | [B:0, D:1, 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<br>RO/V/P  | <b>DPC Error Source ID (DPCESID):</b><br>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. |

## 5.79 RP PIO Status Register (RPPIOSR) – Offset A0Ch

RP PIO Status Register

| Type | Size   | Offset                 | Default   |
|------|--------|------------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, 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<br>RO            | <b>Reserved</b>   |
| 18        | 0h<br>RW/1C/V/<br>P | <b>Memory Completion Timeout Status (MCTS):</b><br>Non-posted memory request completion times out.                |
| 17        | 0h<br>RW/1C/V/<br>P | <b>Memory Completer Abort Completion Status (MCACS):</b><br>Non-posted memory request received CA completion.     |
| 16        | 0h<br>RW/1C/V/<br>P | <b>Memory Unsupported Request Completion Status (MURCS):</b><br>Non-posted Memory request received UR completion. |
| 15:11     | 0h<br>RO            | <b>Reserved</b>   |
| 10        | 0h<br>RW/1C/V/<br>P | <b>I/O Completion Timeout Status (IOCTS):</b><br>I/O request completion times out.                                |
| 9         | 0h<br>RW/1C/V/<br>P | <b>I/O Completer Abort Completion Status (IOCACS):</b><br>I/O request received CA completion.                     |

| Bit Range | Default & Access    | Field Name (ID): Description   |
|-----------|---------------------|--|
| 8         | 0h<br>RW/1C/V/<br>P | <b>I/O Unsupported Request Completion Status (IOURCS):</b><br>I/O request received UR completion.                    |
| 7:3       | 0h<br>RO            | <b>Reserved</b>  |
| 2         | 0h<br>RW/1C/V/<br>P | <b>Configuration Completion Timeout Status (CCTS):</b><br>Configuration request completion times out.                |
| 1         | 0h<br>RW/1C/V/<br>P | <b>Configuration Completer Abort Completion Status (CCACS):</b><br>Configuration request received CA completion.     |
| 0         | 0h<br>RW/1C/V/<br>P | <b>Configuration Unsupported Request Completion Status (CURCS):</b><br>Configuration request received UR completion. |

## 5.80 RP PIO Mask Register (RPPIOMR) – Offset A10h

RP PIO Mask Register

| Type | Size   | Offset                 | Default  |
|------|--------|------------------------|----------|
| PCI  | 32 bit | [B:0, D:1, F:0] + A10h | 0007070h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 31:19     | 0h<br>RO         | <b>Reserved</b>  |
| 18        | 1h<br>RW/P       | <b>Memory Completion Timeout Mask (MCTM):</b><br>Mask bit for Memory Completion Timeout Status.                          |
| 17        | 1h<br>RW/P       | <b>Memory Completer Abort Completion Mask (MCACM):</b><br>Mask bit for Memory Completer Abort Completion Status.         |
| 16        | 1h<br>RW/P       | <b>Memory Unsupported Request Completion Mask (MURCM):</b><br>Mask bit for Memory Unsupported Request Completion Status. |
| 15:11     | 0h<br>RO         | <b>Reserved</b>  |
| 10        | 1h<br>RW/P       | <b>I/O Completion Timeout Mask (IOCTM):</b><br>Mask bit for I/O Completion Timeout Status.                               |
| 9         | 1h<br>RW/P       | <b>I/O Completer Abort Completion Mask (IOCACM):</b><br>Mask bit for I/O Completer Abort Completion Status.              |
| 8         | 1h<br>RW/P       | <b>I/O Unsupported Request Completion Mask (IOURCM):</b><br>Mask bit for I/O Unsupported Request Completion Status.      |
| 7:3       | 0h<br>RO         | <b>Reserved</b>  |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 2         | 1h<br>RW/P       | <b>Configuration Completion Timeout Mask (CCTM):</b><br>Mask bit for Configuration Completion Timeout Status.                          |
| 1         | 1h<br>RW/P       | <b>Configuration Completer Abort Completion Mask (CCACM):</b><br>Mask bit for Configuration Completer Abort Status.                    |
| 0         | 1h<br>RW/P       | <b>Configuration Unsupported Request Completion Mask (CURCM):</b><br>Mask bit for Configuration Unsupported Request Completion Status. |

## 5.81 RP PIO Severity Register (RPPIOVR) – Offset A14h

RP PIO Severity Register

| Type | Size   | Offset                 | Default   |
|------|--------|------------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, 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<br>RO         | <b>Reserved</b>   |
| 18        | 0h<br>RW/P       | <b>Memory Completion Timeout Severity (MCTSV):</b><br>Severity bit for Memory Completion Timeout Status.                          |
| 17        | 0h<br>RW/P       | <b>Memory Completer Abort Completion Severity (MCACSV):</b><br>Severity bit for Memory Completer Abort Completion Status.         |
| 16        | 0h<br>RW/P       | <b>Memory Unsupported Request Completion Severity (MURCSV):</b><br>Severity bit for Memory Unsupported Request Completion Status. |
| 15:11     | 0h<br>RO         | <b>Reserved</b>   |
| 10        | 0h<br>RW/P       | <b>I/O Completion Timeout Severity (IOCTSV):</b><br>Severity bit for I/O Completion Timeout Status.                               |
| 9         | 0h<br>RW/P       | <b>I/O Completer Abort Completion Severity (IOACSV):</b><br>Severity bit for I/O Completer Abort Completion Status.               |
| 8         | 0h<br>RW/P       | <b>I/O Unsupported Request Completion Severity (IOURCSV):</b><br>Severity bit for I/O Unsupported Request Completion Status.      |
| 7:3       | 0h<br>RO         | <b>Reserved</b>   |
| 2         | 0h<br>RW/P       | <b>Configuration Completion Timeout Severity (CCTSV):</b><br>Severity bit for Configuration Completion Timeout Status.            |
| 1         | 0h<br>RW/P       | <b>Configuration Completer Abort Completion Severity (CCACSV):</b><br>Severity bit for Configuration Completer Abort Status.      |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 0         | 0h<br>RW/P       | <b>Configuration Unsupported Request Completion Severity (CURCSV):</b><br>Severity bit for Configuration Unsupported Request Completion Status. |

## 5.82 RP PIO SysError Register (RPPIOSER) – Offset A18h

RP PIO SysError Register

| Type | Size   | Offset                 | Default   |
|------|--------|------------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, 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<br>RO         | <b>Reserved</b>   |
| 18        | 0h<br>RW/P       | <b>Memory Completion Timeout SysErr (MCTSE):</b><br>SysErr bit for Memory Completion Timeout Status.  |
| 17        | 0h<br>RW/P       | <b>Memory Completer Abort Completion SysErr (MCACSE):</b><br>SysErr bit for Memory Completer Abort Completion Status.                       |
| 16        | 0h<br>RW/P       | <b>Memory Unsupported Request Completion SysErr (MURCSE):</b><br>SysErr bit for Memory Unsupported Request Completion Status.               |
| 15:11     | 0h<br>RO         | <b>Reserved</b>   |
| 10        | 0h<br>RW/P       | <b>I/O Completion Timeout SysErr (IOCTSE):</b><br>SysErr bit for I/O Completion Timeout Status.   |
| 9         | 0h<br>RW/P       | <b>I/O Completer Abort Completion SysErr (IOACSE):</b><br>SysErr bit for I/O Completer Abort Completion Status.                             |
| 8         | 0h<br>RW/P       | <b>I/O Unsupported Request Completion SysErr (IOURCSE):</b><br>SysErr bit for I/O Unsupported Request Completion Status.                    |
| 7:3       | 0h<br>RO         | <b>Reserved</b>   |
| 2         | 0h<br>RW/P       | <b>Configuration Completion Timeout SysErr (CCTSE):</b><br>SysErr bit for Configuration Completion Timeout Status.                          |
| 1         | 0h<br>RW/P       | <b>Configuration Completer Abort Completion SysErr (CCACSE):</b><br>SysErr bit for Configuration Completer Abort Status.                    |
| 0         | 0h<br>RW/P       | <b>Configuration Unsupported Request Completion SysErr (CURCSE):</b><br>SysErr bit for Configuration Unsupported Request Completion Status. |



## 5.83 RP PIO Exception Register (RPPIOER) – Offset A1Ch

RP PIO Exception Register

| Type | Size   | Offset                 | Default  |
|------|--------|------------------------|----------|
| PCI  | 32 bit | [B:0, D:1, F:0] + A1Ch | 0000000h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 31:19     | 0h<br>RO         | <b>Reserved</b>  |
| 18        | 0h<br>RW/P       | <b>Memory Completion Timeout Exception (MCTE):</b><br>Exception bit for Memory Completion Timeout Status.  |
| 17        | 0h<br>RW/P       | <b>Memory Completer Abort Completion Exception (MCACE):</b><br>Exception bit for Memory Completer Abort Completion Status.                       |
| 16        | 0h<br>RW/P       | <b>Memory Unsupported Request Completion Exception (MURCE):</b><br>Exception bit for Memory Unsupported Request Completion Status.               |
| 15:11     | 0h<br>RO         | <b>Reserved</b>  |
| 10        | 0h<br>RW/P       | <b>I/O Completion Timeout Exception (IOCTE):</b><br>Exception bit for I/O Completion Timeout Status.   |
| 9         | 0h<br>RW/P       | <b>I/O Completer Abort Completion Exception (IOACE):</b><br>Exception bit for I/O Completer Abort Completion Status.                             |
| 8         | 0h<br>RW/P       | <b>I/O Unsupported Request Completion Exception (IOURCE):</b><br>Exception bit for I/O Unsupported Request Completion Status.                    |
| 7:3       | 0h<br>RO         | <b>Reserved</b>  |
| 2         | 0h<br>RW/P       | <b>Configuration Completion Timeout Exception (CCTE):</b><br>Exception bit for Configuration Completion Timeout Status.                          |
| 1         | 0h<br>RW/P       | <b>Configuration Completer Abort Completion Exception (CCACE):</b><br>Exception bit for Configuration Completer Abort Status.                    |
| 0         | 0h<br>RW/P       | <b>Configuration Unsupported Request Completion Exception (CURCE):</b><br>Exception bit for Configuration Unsupported Request Completion Status. |

## 5.84 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:1, 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<br>RO/V/P | <b>1st DWORD of TLP (DW1):</b><br>Byte0 AND Byte1 AND Byte2 AND Byte3. |

## 5.85 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:1, 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<br>RO/V/P | <b>2nd DWORD of TLP (DW2):</b><br>Byte4 AND Byte5 AND Byte6 AND Byte7. |

## 5.86 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:1, 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<br>RO/V/P | <b>3rd DWORD of TLP (DW3):</b><br>Byte8 AND Byte9 AND Byte10 AND Byte11. |

## 5.87 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:1, 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<br>RO/V/P | <b>4th DWORD of TLP (DW4):</b><br>Byte12 AND Byte13 AND Byte14 AND Byte15. |

## 5.88 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:1, 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<br>RW/O     | <p><b>Next Capability Offset (NCO):</b><br/>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.<br/>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.<br/>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.</p> |
| 19:16     | 0h<br>RW/O       | <p><b>Capability Version (CV):</b><br/>This field is a PCI-SIG defined version number that indicates the version of the Capability structure present.<br/>For systems that support Secondary PCI Express Extended Capability, BIOS should write a 1h to this register else it should write 0.</p>  |
| 15:0      | 0000h<br>RW/O    | <p><b>PCI Express Extended Capability ID (PCIECID):</b><br/>This field is a PCI-SIG defined ID number that indicates the nature and format of the Extended Capability.<br/>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.</p>   |

## 5.89 Link Control 3 (LCTL3) – Offset A34h

Link Control 3

| Type | Size   | Offset                 | Default   |
|------|--------|------------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, 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<br>RO         | <b>Reserved</b>              |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 15:9      | 00h<br>RW        | <b>Enable Lower SKP OS Generation Vector (ELSOSGV):</b><br>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.<br>Bit definitions within this field are:<br>Bit 0 2.5 GT/s<br>Bit 1 5.0 GT/s<br>Bit 2 8.0 GT/s<br>Bit 3 16.0 GT/s<br>Bits 6:4 Rsvd<br>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<br>RO         | <b>Reserved</b>  |
| 1         | 0h<br>RW/P       | <b>Link Equalization Request Interrupt Enable (LERIE):</b><br>When set, this bit enables the generation of an interrupt to indicate that the Link Equalization Request bit has been set.   |
| 0         | 0h<br>RW/1S/V    | <b>Perform Equalization (PE):</b><br>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.<br>This bit is cleared by Root Port upon entry to Link Equalization Phase 1.  |

## 5.90 Lane Error Status (LES) – Offset A38h

Lane Error Status

| Type | Size   | Offset                 | Default   |
|------|--------|------------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, 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<br>RO            | <b>Reserved</b>  |
| 15        | 0h<br>RW/1C/V/<br>P | <b>Lane 15 Error Status (L15ES):</b><br>Lane 15 detected a Lane-based error. |
| 14        | 0h<br>RW/1C/V/<br>P | <b>Lane 14 Error Status (L14ES):</b><br>Lane 14 detected a Lane-based error. |
| 13        | 0h<br>RW/1C/V/<br>P | <b>Lane 13 Error Status (L13ES):</b><br>Lane 13 detected a Lane-based error. |
| 12        | 0h<br>RW/1C/V/<br>P | <b>Lane 12 Error Status (L12ES):</b><br>Lane 12 detected a Lane-based error. |

| Bit Range | Default & Access    | Field Name (ID): Description   |
|-----------|---------------------|--|
| 11        | 0h<br>RW/1C/V/<br>P | <b>Lane 11 Error Status (L11ES):</b><br>Lane 11 detected a Lane-based error. |
| 10        | 0h<br>RW/1C/V/<br>P | <b>Lane 10 Error Status (L10ES):</b><br>Lane 10 detected a Lane-based error. |
| 9         | 0h<br>RW/1C/V/<br>P | <b>Lane 9 Error Status (L9ES):</b><br>Lane 9 detected a Lane-based error.    |
| 8         | 0h<br>RW/1C/V/<br>P | <b>Lane 8 Error Status (L8ES):</b><br>Lane 8 detected a Lane-based error.    |
| 7         | 0h<br>RW/1C/V/<br>P | <b>Lane 7 Error Status (L7ES):</b><br>Lane 7 detected a Lane-based error.    |
| 6         | 0h<br>RW/1C/V/<br>P | <b>Lane 6 Error Status (L6ES):</b><br>Lane 6 detected a Lane-based error.    |
| 5         | 0h<br>RW/1C/V/<br>P | <b>Lane 5 Error Status (L5ES):</b><br>Lane 5 detected a Lane-based error.    |
| 4         | 0h<br>RW/1C/V/<br>P | <b>Lane 4 Error Status (L4ES):</b><br>Lane 4 detected a Lane-based error.    |
| 3         | 0h<br>RW/1C/V/<br>P | <b>Lane 3 Error Status (L3ES):</b><br>Lane 3 detected a Lane-based error.    |
| 2         | 0h<br>RW/1C/V/<br>P | <b>Lane 2 Error Status (L2ES):</b><br>Lane 2 detected a Lane-based error.    |
| 1         | 0h<br>RW/1C/V/<br>P | <b>Lane 1 Error Status (L1ES):</b><br>Lane 1 detected a Lane-based error.    |
| 0         | 0h<br>RW/1C/V/<br>P | <b>Lane 0 Error Status (L0ES):</b><br>Lane 0 detected a Lane-based error.    |

## 5.91 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:1, F:0] + A3Ch | 7F7F7F7h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 31        | 0h<br>RO         | <b>Reserved</b>   |
| 30:28     | 7h<br>RW         | <b>Upstream Port Lane 1 Receiver Preset Hint (UPL1RPH):</b><br>Field contains the Receiver Preset Hint value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 27:24     | Fh<br>RW         | <b>Upstream Port Lane 1 Transmitter Preset (UPL1TP):</b><br>Field contains the Transmitter Preset value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ.      |
| 23        | 0h<br>RO         | <b>Reserved</b>   |
| 22:20     | 7h<br>RW         | <b>Downstream Port Lane 1 Receiver Preset Hint (DPL1RPH):</b><br>Receiver Preset Hint may be used as a hint for 8 GT/s receiver equalization by this Port when the Port is operating as a Downstream Port.  |
| 19:16     | Fh<br>RW         | <b>Downstream Port Lane 1 Transmitter Preset (DPL1TP):</b><br>Transmitter Preset used for 8 GT/s 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<br>RO         | <b>Reserved</b>   |
| 14:12     | 7h<br>RW         | <b>Upstream Port Lane 0 Receiver Preset Hint (UPL0RPH):</b><br>Field contains the Receiver Preset Hint value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 11:8      | Fh<br>RW         | <b>Upstream Port Lane 0 Transmitter Preset (UPL0TP):</b><br>Field contains the Transmitter Preset value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ.      |
| 7         | 0h<br>RO         | <b>Reserved</b>   |
| 6:4       | 7h<br>RW         | <b>Downstream Port Lane 0 Receiver Preset Hint (DPL0RPH):</b><br>Receiver Preset Hint may be used as a hint for 8 GT/s 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<br>RW         | <b>Downstream Port Lane 0 Transmitter Preset (DPL0TP):</b><br>Transmitter Preset used for 8 GT/s 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. |

## 5.92 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:1, F:0] + A40h | 7F7F7F7h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 31        | 0h<br>RO         | <b>Reserved</b>   |
| 30:28     | 7h<br>RW         | <b>Upstream Port Lane 3 Receiver Preset Hint (UPL3RPH):</b><br>Field contains the Receiver Preset Hint value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 27:24     | Fh<br>RW         | <b>Upstream Port Lane 3 Transmitter Preset Hint (UPL3TP):</b><br>Field contains the Transmitter Preset value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 23        | 0h<br>RO         | <b>Reserved</b>   |
| 22:20     | 7h<br>RW         | <b>Downstream Port Lane 3 Receiver Preset Hint (DPL3RPH):</b><br>Receiver Preset Hint may be used as a hint for 8 GT/s receiver equalization by this Port when the Port is operating as a Downstream Port.  |
| 19:16     | Fh<br>RW         | <b>Downstream Port Lane 3 Transmitter Preset (DPL3TP):</b><br>Transmitter Preset used for 8 GT/s 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<br>RO         | <b>Reserved</b>   |



| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 14:12     | 7h<br>RW         | <b>Upstream Port Lane 2 Receiver Preset Hint (UPL2RPH):</b><br>Field contains the Receiver Preset Hint value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 11:8      | Fh<br>RW         | <b>Upstream Port Lane 2 Transmitter Preset (UPL2TP):</b><br>Field contains the Transmitter Preset value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ.      |
| 7         | 0h<br>RO         | <b>Reserved</b>   |
| 6:4       | 7h<br>RW         | <b>Downstream Port Lane 2 Receiver Preset Hint (DPL2RPH):</b><br>Receiver Preset Hint may be used as a hint for 8 GT/s receiver equalization by this Port when the Port is operating as a Downstream Port.  |
| 3:0       | Fh<br>RW         | <b>Downstream Port Lane 2 Transmitter Preset (DPL2TP):</b><br>Transmitter Preset used for 8 GT/s 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.   |

## 5.93 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:1, F:0] + A44h | 7F7F7F7h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 31        | 0h<br>RO         | <b>Reserved</b>   |
| 30:28     | 7h<br>RW         | <b>Upstream Port Lane 5 Receiver Preset Hint (UPL5RPH):</b><br>Field contains the Receiver Preset Hint value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 27:24     | Fh<br>RW         | <b>Upstream Port Lane 5 Transmitter Preset (UPL5TP):</b><br>Field contains the Transmitter Preset value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ.      |
| 23        | 0h<br>RO         | <b>Reserved</b>   |
| 22:20     | 7h<br>RW         | <b>Downstream Port Lane 5 Receiver Preset Hint (DPL5RPH):</b><br>Receiver Preset Hint may be used as a hint for 8 GT/s receiver equalization by this Port when the Port is operating as a Downstream Port.  |
| 19:16     | Fh<br>RW         | <b>Downstream Port Lane 5 Transmitter Preset (DPL5TP):</b><br>Transmitter Preset used for 8 GT/s 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<br>RO         | <b>Reserved</b>   |
| 14:12     | 7h<br>RW         | <b>Upstream Port Lane 4 Receiver Preset Hint (UPL4RPH):</b><br>Field contains the Receiver Preset Hint value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 11:8      | Fh<br>RW         | <b>Upstream Port Lane 4 Transmitter Preset (UPL4TP):</b><br>Field contains the Transmitter Preset value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ.      |
| 7         | 0h<br>RO         | <b>Reserved</b>   |
| 6:4       | 7h<br>RW         | <b>Downstream Port Lane 4 Receiver Preset Hint (DPL4RPH):</b><br>Receiver Preset Hint may be used as a hint for 8 GT/s receiver equalization by this Port when the Port is operating as a Downstream Port.  |
| 3:0       | Fh<br>RW         | <b>Downstream Port Lane 4 Transmitter Preset (DPL4TP):</b><br>Transmitter Preset used for 8 GT/s 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.   |

## 5.94 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:1, F:0] + A48h | 7F7F7F7h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 31        | 0h<br>RO         | <b>Reserved</b>   |
| 30:28     | 7h<br>RW         | <b>Upstream Port Lane 7 Receiver Preset Hint (UPL7RPH):</b><br>Field contains the Receiver Preset Hint value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 27:24     | Fh<br>RW         | <b>Upstream Port Lane 7 Transmitter Preset (UPL7TP):</b><br>Field contains the Transmitter Preset value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ.      |
| 23        | 0h<br>RO         | <b>Reserved</b>   |
| 22:20     | 7h<br>RW         | <b>Downstream Port Lane 7 Receiver Preset Hint (DPL7RPH):</b><br>Receiver Preset Hint may be used as a hint for 8 GT/s receiver equalization by this Port when the Port is operating as a Downstream Port.  |
| 19:16     | Fh<br>RW         | <b>Downstream Port Lane 7 Transmitter Preset (DPL7TP):</b><br>Transmitter Preset used for 8 GT/s 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<br>RO         | <b>Reserved</b>   |
| 14:12     | 7h<br>RW         | <b>Upstream Port Lane 6 Receiver Preset Hint (UPL6RPH):</b><br>Field contains the Receiver Preset Hint value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 11:8      | Fh<br>RW         | <b>Upstream Port Lane 6 Transmitter Preset (UPL6TP):</b><br>Field contains the Transmitter Preset value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ.      |
| 7         | 0h<br>RO         | <b>Reserved</b>   |
| 6:4       | 7h<br>RW         | <b>Downstream Port Lane 6 Receiver Preset Hint (DPL6RPH):</b><br>Receiver Preset Hint may be used as a hint for 8 GT/s 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<br>RW         | <b>Downstream Port Lane 6 Transmitter Preset (DPL6TP):</b><br>Transmitter Preset used for 8 GT/s 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. |

## 5.95 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:1, 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<br>RO         | <b>Reserved</b>   |
| 30:28     | 7h<br>RW         | <b>Upstream Port Lane 9 Receiver Preset Hint (UPL9RPH):</b><br>Field contains the Receiver Preset Hint value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 27:24     | Fh<br>RW         | <b>Upstream Port Lane 9 Transmitter Preset (UPL9TP):</b><br>Field contains the Transmitter Preset value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ.      |
| 23        | 0h<br>RO         | <b>Reserved</b>   |
| 22:20     | 7h<br>RW         | <b>Downstream Port Lane 9 Receiver Preset Hint (DPL9RPH):</b><br>Receiver Preset Hint may be used as a hint for 8 GT/s receiver equalization by this Port when the Port is operating as a Downstream Port.  |
| 19:16     | Fh<br>RW         | <b>Downstream Port Lane 9 Transmitter Preset (DPL9TP):</b><br>Transmitter Preset used for 8 GT/s 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<br>RO         | <b>Reserved</b>   |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 14:12     | 7h<br>RW         | <b>Upstream Port Lane 8 Receiver Preset Hint (UPL8RPH):</b><br>Field contains the Receiver Preset Hint value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 11:8      | Fh<br>RW         | <b>Upstream Port Lane 8 Transmitter Preset (UPL8TP):</b><br>Field contains the Transmitter Preset value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ.      |
| 7         | 0h<br>RO         | <b>Reserved</b>   |
| 6:4       | 7h<br>RW         | <b>Downstream Port Lane 8 Receiver Preset Hint (DPL8RPH):</b><br>Receiver Preset Hint may be used as a hint for 8 GT/s receiver equalization by this Port when the Port is operating as a Downstream Port.  |
| 3:0       | Fh<br>RW         | <b>Downstream Port Lane 8 Transmitter Preset (DPL8TP):</b><br>Transmitter Preset used for 8 GT/s 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.   |

## 5.96 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:1, F:0] + A50h | 7F7F7F7h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 31        | 0h<br>RO         | <b>Reserved</b>   |
| 30:28     | 7h<br>RW         | <b>Upstream Port Lane 11 Receiver Preset Hint (UPL11RPH):</b><br>Field contains the Receiver Preset Hint value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 27:24     | Fh<br>RW         | <b>Upstream Port Lane 11 Transmitter Preset (UPL11TP):</b><br>Field contains the Transmitter Preset value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ.      |
| 23        | 0h<br>RO         | <b>Reserved</b>   |
| 22:20     | 7h<br>RW         | <b>Downstream Port Lane 11 Receiver Preset Hint (DPL11RPH):</b><br>Receiver Preset Hint may be used as a hint for 8 GT/s receiver equalization by this Port when the Port is operating as a Downstream Port.  |
| 19:16     | Fh<br>RW         | <b>Downstream Port Lane 11 Transmitter Preset (DPL11TP):</b><br>Transmitter Preset used for 8 GT/s 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<br>RO         | <b>Reserved</b>   |
| 14:12     | 7h<br>RW         | <b>Upstream Port Lane 10 Receiver Preset Hint (UPL10RPH):</b><br>Field contains the Receiver Preset Hint value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 11:8      | Fh<br>RW         | <b>Upstream Port Lane 10 Transmitter Preset (UPL10TP):</b><br>Field contains the Transmitter Preset value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ.      |
| 7         | 0h<br>RO         | <b>Reserved</b>   |
| 6:4       | 7h<br>RW         | <b>Downstream Port Lane 10 Receiver Preset Hint (DPL10RPH):</b><br>Receiver Preset Hint may be used as a hint for 8 GT/s receiver equalization by this Port when the Port is operating as a Downstream Port.  |
| 3:0       | Fh<br>RW         | <b>Downstream Port Lane 10 Transmitter Preset (DPL10TP):</b><br>Transmitter Preset used for 8 GT/s 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.   |

## 5.97 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:1, F:0] + A54h | 7F7F7F7h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 31        | 0h<br>RO         | <b>Reserved</b>   |
| 30:28     | 7h<br>RW         | <b>Upstream Port Lane 13 Receiver Preset Hint (UPL13RPH):</b><br>Field contains the Receiver Preset Hint value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 27:24     | Fh<br>RW         | <b>Upstream Port Lane 13 Transmitter Preset (UPL13TP):</b><br>Field contains the Transmitter Preset value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ.      |
| 23        | 0h<br>RO         | <b>Reserved</b>   |
| 22:20     | 7h<br>RW         | <b>Downstream Port Lane 13 Receiver Preset Hint (DPL13RPH):</b><br>Receiver Preset Hint may be used as a hint for 8 GT/s receiver equalization by this Port when the Port is operating as a Downstream Port.  |
| 19:16     | Fh<br>RW         | <b>Downstream Port Lane 13 Transmitter Preset (DPL13TP):</b><br>Transmitter Preset used for 8 GT/s 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<br>RO         | <b>Reserved</b>   |
| 14:12     | 7h<br>RW         | <b>Upstream Port Lane 12 Receiver Preset Hint (UPL12RPH):</b><br>Field contains the Receiver Preset Hint value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 11:8      | Fh<br>RW         | <b>Upstream Port Lane 12 Transmitter Preset (UPL12TP):</b><br>Field contains the Transmitter Preset value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ.      |
| 7         | 0h<br>RO         | <b>Reserved</b>   |
| 6:4       | 7h<br>RW         | <b>Downstream Port Lane 12 Receiver Preset Hint (DPL12RPH):</b><br>Receiver Preset Hint may be used as a hint for 8 GT/s 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<br>RW         | <b>Downstream Port Lane 12 Transmitter Preset (DPL12TP):</b><br>Transmitter Preset used for 8 GT/s 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. |

## 5.98 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:1, F:0] + A58h | 7F7F7F7h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 31        | 0h<br>RO         | <b>Reserved</b>   |
| 30:28     | 7h<br>RW         | <b>Upstream Port Lane 15 Receiver Preset Hint (UPL15RPH):</b><br>Field contains the Receiver Preset Hint value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 27:24     | Fh<br>RW         | <b>Upstream Port Lane 15 Transmitter Preset (UPL15TP):</b><br>Field contains the Transmitter Preset value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ.      |
| 23        | 0h<br>RO         | <b>Reserved</b>   |
| 22:20     | 7h<br>RW         | <b>Downstream Port Lane 15 Receiver Preset Hint (DPL15RPH):</b><br>Receiver Preset Hint may be used as a hint for 8 GT/s receiver equalization by this Port when the Port is operating as a Downstream Port.  |
| 19:16     | Fh<br>RW         | <b>Downstream Port Lane 15 Transmitter Preset (DPL15TP):</b><br>Transmitter Preset used for 8 GT/s 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<br>RO         | <b>Reserved</b>   |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 14:12     | 7h<br>RW         | <b>Upstream Port Lane 14 Receiver Preset Hint (UPL14RPH):</b><br>Field contains the Receiver Preset Hint value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 11:8      | Fh<br>RW         | <b>Upstream Port Lane 14 Transmitter Preset (UPL14TP):</b><br>Field contains the Transmitter Preset value sent or received during Port 8 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ.      |
| 7         | 0h<br>RO         | <b>Reserved</b>   |
| 6:4       | 7h<br>RW         | <b>Downstream Port Lane 14 Receiver Preset Hint (DPL14RPH):</b><br>Receiver Preset Hint may be used as a hint for 8 GT/s receiver equalization by this Port when the Port is operating as a Downstream Port.  |
| 3:0       | Fh<br>RW         | <b>Downstream Port Lane 14 Transmitter Preset (DPL14TP):</b><br>Transmitter Preset used for 8 GT/s 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.   |

## 5.99 Data Link Feature Extended Capability Header (DLFECH) – Offset A90h

Data Link Feature Extended Capability Header

| Type | Size   | Offset                 | Default   |
|------|--------|------------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, F:0] + A90h | 00000000h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 31:20     | 000h<br>RW/O     | <b>Next Capability Offset (NCO):</b><br>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.<br>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.<br>The bottom 2 bits of this offset are Reserved and must be implemented as 00b although software must mask them to allow for future uses of these bits. |
| 19:16     | 0h<br>RW/O       | <b>Capability Version (CV):</b><br>This field is a PCI-SIG defined version number that indicates the version of the Capability structure present.   |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 15:0      | 0000h<br>RW/O    | <b>PCI Express Extended Capability ID (PCIECID):</b><br>This field is a PCI-SIG defined ID number that indicates the nature and format of the Extended Capability. |

## 5.100 Data Link Feature Capabilities Register (DLFCAP) – Offset A94h

Data Link Feature Capabilities Register

| Type | Size   | Offset                 | Default   |
|------|--------|------------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, F:0] + A94h | 80000000h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 31        | 1h<br>RW/O       | <b>Data Link Feature Exchange Enable (DLFEE):</b><br>If set, this bit indicates that this Port will enter the DL_Feature negotiation state. Default is 1b.   |
| 30:23     | 0h<br>RO         | <b>Reserved</b>  |
| 22:1      | 000000h<br>RW/O  | <b>Local Feature Supported (LFS):</b><br>These bits indicate that the Downstream Port supports the associated Data Link Feature. For this version of this specification, this field is hardwired to 0. |
| 0         | 0h<br>RW/O       | <b>Local Scaled Flow Control Supported (LSFCS):</b><br>This bit indicates that the Port supports the Scaled Flow Control Feature.  |

## 5.101 Data Link Feature Status Register (DLFSTS) – Offset A98h

Data Link Feature Status Register



| Type | Size   | Offset                 | Default   |
|------|--------|------------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, F:0] + A98h | 00000000h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| R           | R          | R         |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 31        | 0h<br>RO/V       | <b>Data Link Feature Status Valid (DLFSV):</b><br>This bit indicates that the Downstream Port has received a Data Link Feature DLLP after the Link entered L0.<br>When this bit is 1b, bits 23:0 are frozen. Software must clear this bit to re-enable capturing information. This bit is cleared on DL_Down. |
| 30:23     | 0h<br>RO         | <b>Reserved</b>   |
| 22:1      | 000000h<br>RO/V  | <b>Remote Feature Supported (RFS):</b><br>These bits indicate that the Remote Port supports the corresponding Data Link Feature. These bits capture all information from the Data Link Feature DLLP even when this Port does not support the corresponding feature.   |
| 0         | 0h<br>RO/V       | <b>Remote Scaled Flow Control Supported (RSFCS):</b><br>This bit indicates that the Remote Port indicated it supports the Scaled Flow Control Feature   |

## 5.102 Physical Layer 16.0 GT/s Extended Capability Header (PL16GECH) – Offset A9Ch

Physical Layer 16.0 GT/s Extended Capability Header

| Type | Size   | Offset                 | Default   |
|------|--------|------------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, F:0] + A9Ch | 00000000h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 31:20     | 000h<br>RW/O     | <b>Next Capability Offset (NCO):</b><br>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.<br>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. |
| 19:16     | 0h<br>RW/O       | <b>Capability Version (CV):</b><br>This field is a PCI-SIG defined version number that indicates the version of the Capability structure present.  |



| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 15:0      | 0000h<br>RW/O    | <b>PCI Express Extended Capability ID (PCIECID):</b><br>This field is a PCI-SIG defined ID number that indicates the nature and format of the Extended Capability.<br>Extended Capability ID for the Physical Layer 16.0 GT/s Capability |

### 5.103 Physical Layer 16.0 GT/s Capability Register (PL16CAP) – Offset AA0h

Physical Layer 16.0 GT/s Capability Register

**Note:** Bit definitions are the same as [DSTS2, offset 6Ah](#).

### 5.104 Physical Layer 16.0 GT/s Control Register (PL16CTL) – Offset AA4h

Physical Layer 16.0 GT/s Control Register

**Note:** Bit definitions are the same as [DSTS2, offset 6Ah](#).

### 5.105 Physical Layer 16.0 GT/s Status Register (PL16S) – Offset AA8h

Physical Layer 16.0 GT/s Status Register

| Type | Size   | Offset                 | Default   |
|------|--------|------------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, F:0] + AA8h | 00000000h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access    | Field Name (ID): Description   |
|-----------|---------------------|--|
| 31:5      | 0h<br>RO            | <b>Reserved</b>  |
| 4         | 0h<br>RW/1C/V/<br>P | <b>Link Equalization Request 16.0 GT/s (LERG4):</b><br>This bit is Set by hardware to request the 16.0 GT/s Link equalization process to be performed on the Link.<br>The default value of this bit is 0b.                             |
| 3         | 0h<br>RO/V/P        | <b>Equalization 16.0 GT/s Phase 3 Successful (EQP3SG4):</b><br>When set to 1b, this bit indicates that Phase 3 of the 16.0 GT/s Transmitter Equalization procedure has successfully completed.<br>The default value of this bit is 0b. |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 2         | 0h<br>RO/V/P     | <b>Equalization 16.0 GT/s Phase 2 Successful (EQP2SG4):</b><br>When set to 1b, this bit indicates that Phase 2 of the 16.0 GT/s Transmitter Equalization procedure has successfully completed.<br>The default value of this bit is 0b. |
| 1         | 0h<br>RO/V/P     | <b>Equalization 16.0 GT/s Phase 1 Successful (EQP1SG4):</b><br>When set to 1b, this bit indicates that Phase 1 of the 16.0 GT/s Transmitter Equalization procedure has successfully completed.<br>The default value of this bit is 0b. |
| 0         | 0h<br>RO/V/P     | <b>Equalization 16.0 GT/s Complete (EQG4):</b><br>When set to 1b, this bit indicates that the Transmitter Equalization procedure at the 16.0 GT/s data rate has completed.<br>The default value of this bit is 0b.                     |

## 5.106 Physical Layer 16.0 GT/s Local Data Parity Mismatch Status Register (PL16LDPMS) – Offset AACH

Physical Layer 16.0 GT/s Local Data Parity Mismatch Status Register

| Type | Size   | Offset                 | Default   |
|------|--------|------------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, F:0] + AACH | 00000000h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access   | Field Name (ID): Description  |
|-----------|--------------------|---|
| 31:16     | 0h<br>RO           | <b>Reserved</b>   |
| 15:0      | 0000h<br>RW/1C/V/P | <b>Local Data Parity Mismatch Status (LDPMS):</b><br>Each bit indicates if the corresponding Lane detected a Data Parity mismatch. A value of 1b indicates that a mismatch was detected on the corresponding Lane Number.<br>The default value of each bit is 0b. |

## 5.107 Physical Layer 16.0 GT/s First Retimer Data Parity Mismatch Status Register (PL16FRDPMS) – Offset AB0h

Physical Layer 16.0 GT/s First Retimer Data Parity Mismatch Status Register

| Type | Size   | Offset                 | Default   |
|------|--------|------------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, F:0] + AB0h | 00000000h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access       | Field Name (ID): Description  |
|-----------|------------------------|---|
| 31:16     | 0h<br>RO               | <b>Reserved</b>   |
| 15:0      | 0000h<br>RW/1C/V/<br>P | <b>First Retimer Data Parity Mismatch Status (FRDPMS):</b><br>Each bit indicates if the corresponding Lane detected a Data Parity mismatch. A value of 1b indicates that a mismatch was detected on the corresponding Lane Number. The default value of each bit is 0b. |

## 5.108 Physical Layer 16.0 GT/s Second Retimer Data Parity Mismatch Status Register (PL16SRDPMS) – Offset AB4h

Physical Layer 16.0 GT/s Second Retimer Data Parity Mismatch Status Register

| Type | Size   | Offset                 | Default   |
|------|--------|------------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, F:0] + AB4h | 00000000h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access       | Field Name (ID): Description   |
|-----------|------------------------|--|
| 31:16     | 0h<br>RO               | <b>Reserved</b>  |
| 15:0      | 0000h<br>RW/1C/V/<br>P | <b>Second Retimer Data Parity Mismatch Status (SRDPMS):</b><br>Each bit indicates if the corresponding Lane detected a Data Parity mismatch. A value of 1b indicates that a mismatch was detected on the corresponding Lane Number. The default value of each bit is 0b. |

## 5.109 Physical Layer 16.0 GT/s Extra Status Register (PL16ES) – Offset AB8h

Physical Layer 16.0 GT/s Extra Status Register

**Note:** Bit definitions are the same as [DSTS2](#), offset 6Ah.



## 5.110 Physical Layer 16.0 GT/s Lane 01 Equalization Control Register (PL16L01EC) – Offset ABCh

Physical Layer 16.0 GT/s Lane 01 Equalization Control Register

| Type | Size   | Offset                 | Default |
|------|--------|------------------------|---------|
| PCI  | 16 bit | [B:0, D:1, F:0] + ABCh | FFFFh   |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 15:12     | Fh<br>RW         | <b>Upstream Port 16 GT/s Port Lane 1 Transmitter Preset (UP16L1TP):</b><br>Field contains the Transmitter Preset value sent or received during Port 16 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 11:8      | Fh<br>RW         | <b>Downstream Port 16 GT/s Lane 1 Transmitter Preset (DP16L1TP):</b><br>Transmitter Preset used for 16 GT/s 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.   |
| 7:4       | Fh<br>RW         | <b>Upstream Port 16 GT/s Port Lane 0 Transmitter Preset (UP16L0TP):</b><br>Field contains the Transmitter Preset value sent or received during Port 16 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 3:0       | Fh<br>RW         | <b>Downstream Port 16 GT/s Lane 0 Transmitter Preset (DP16L0TP):</b><br>Transmitter Preset used for 16 GT/s 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.   |

## 5.111 Physical Layer 16.0 GT/s Lane 23 Equalization Control Register (PL16L23EC) – Offset ABEh

Physical Layer 16.0 GT/s Lane 23 Equalization Control Register

| Type | Size   | Offset                 | Default |
|------|--------|------------------------|---------|
| PCI  | 16 bit | [B:0, D:1, F:0] + ABEh | FFFFh   |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 15:12     | Fh<br>RW         | <b>Upstream Port 16 GT/s Port Lane 3 Transmitter Preset (UP16L3TP):</b><br>Field contains the Transmitter Preset value sent or received during Port 16 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 11:8      | Fh<br>RW         | <b>Downstream Port 16 GT/s Lane 3 Transmitter Preset (DP16L3TP):</b><br>Transmitter Preset used for 16 GT/s 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.   |
| 7:4       | Fh<br>RW         | <b>Upstream Port 16 GT/s Port Lane 2 Transmitter Preset (UP16L2TP):</b><br>Field contains the Transmitter Preset value sent or received during Port 16 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 3:0       | Fh<br>RW         | <b>Downstream Port 16 GT/s Lane 2 Transmitter Preset (DP16L2TP):</b><br>Transmitter Preset used for 16 GT/s 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.   |

## 5.112 Physical Layer 16.0 GT/s Lane 45 Equalization Control Register (PL16L45EC) – Offset AC0h

Physical Layer 16.0 GT/s Lane 45 Equalization Control Register



| Type | Size   | Offset                 | Default |
|------|--------|------------------------|---------|
| PCI  | 16 bit | [B:0, D:1, F:0] + AC0h | FFFFh   |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 15:12     | Fh<br>RW         | <b>Upstream Port 16 GT/s Port Lane 5 Transmitter Preset (UP16L5TP):</b><br>Field contains the Transmitter Preset value sent or received during Port 16 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 11:8      | Fh<br>RW         | <b>Downstream Port 16 GT/s Lane 5 Transmitter Preset (DP16L5TP):</b><br>Transmitter Preset used for 16 GT/s 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.   |
| 7:4       | Fh<br>RW         | <b>Upstream Port 16 GT/s Port Lane 4 Transmitter Preset (UP16L4TP):</b><br>Field contains the Transmitter Preset value sent or received during Port 16 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 3:0       | Fh<br>RW         | <b>Downstream Port 16 GT/s Lane 4 Transmitter Preset (DP16L4TP):</b><br>Transmitter Preset used for 16 GT/s 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.   |

## 5.113 Physical Layer 16.0 GT/s Lane 67 Equalization Control Register (PL16L67EC) – Offset AC2h

Physical Layer 16.0 GT/s Lane 67 Equalization Control Register

| Type | Size   | Offset                 | Default |
|------|--------|------------------------|---------|
| PCI  | 16 bit | [B:0, D:1, F:0] + AC2h | FFFFh   |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 15:12     | Fh<br>RW         | <b>Upstream Port 16 GT/s Port Lane 7 Transmitter Preset (UP16L7TP):</b><br>Field contains the Transmitter Preset value sent or received during Port 16 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 11:8      | Fh<br>RW         | <b>Downstream Port 16 GT/s Lane 7 Transmitter Preset (DP16L7TP):</b><br>Transmitter Preset used for 16 GT/s 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.   |
| 7:4       | Fh<br>RW         | <b>Upstream Port 16 GT/s Port Lane 6 Transmitter Preset (UP16L6TP):</b><br>Field contains the Transmitter Preset value sent or received during Port 16 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 3:0       | Fh<br>RW         | <b>Downstream Port 16 GT/s Lane 6 Transmitter Preset (DP16L6TP):</b><br>Transmitter Preset used for 16 GT/s 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.   |

## 5.114 Physical Layer 16.0 GT/s Lane 89 Equalization Control Register (PL16L89EC) – Offset AC4h

Physical Layer 16.0 GT/s Lane 89 Equalization Control Register



| Type | Size   | Offset                 | Default |
|------|--------|------------------------|---------|
| PCI  | 16 bit | [B:0, D:1, F:0] + AC4h | FFFFh   |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 15:12     | Fh<br>RW         | <b>Upstream Port 16 GT/s Port Lane 9 Transmitter Preset (UP16L9TP):</b><br>Field contains the Transmitter Preset value sent or received during Port 16 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 11:8      | Fh<br>RW         | <b>Downstream Port 16 GT/s Lane 9 Transmitter Preset (DP16L9TP):</b><br>Transmitter Preset used for 16 GT/s 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.   |
| 7:4       | Fh<br>RW         | <b>Upstream Port 16 GT/s Port Lane 8 Transmitter Preset (UP16L8TP):</b><br>Field contains the Transmitter Preset value sent or received during Port 16 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 3:0       | Fh<br>RW         | <b>Downstream Port 16 GT/s Lane 8 Transmitter Preset (DP16L8TP):</b><br>Transmitter Preset used for 16 GT/s 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.   |

## 5.115 Physical Layer 16.0 GT/s Lane 1011 Equalization Control Register (PL16L1011EC) – Offset AC6h

Physical Layer 16.0 GT/s Lane 1011 Equalization Control Register



| Type | Size   | Offset                 | Default |
|------|--------|------------------------|---------|
| PCI  | 16 bit | [B:0, D:1, F:0] + AC6h | FFFFh   |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 15:12     | Fh<br>RW         | <b>Upstream Port 16 GT/s Port Lane 11 Transmitter Preset (UP16L11TP):</b><br>Field contains the Transmitter Preset value sent or received during Port 16 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 11:8      | Fh<br>RW         | <b>Downstream Port 16 GT/s Lane 11 Transmitter Preset (DP16L11TP):</b><br>Transmitter Preset used for 16 GT/s 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.   |
| 7:4       | Fh<br>RW         | <b>Upstream Port 16 GT/s Port Lane 10 Transmitter Preset (UP16L10TP):</b><br>Field contains the Transmitter Preset value sent or received during Port 16 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 3:0       | Fh<br>RW         | <b>Downstream Port 16 GT/s Lane 10 Transmitter Preset (DP16L10TP):</b><br>Transmitter Preset used for 16 GT/s 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.   |

## 5.116 Physical Layer 16.0 GT/s Lane 1213 Equalization Control Register (PL16L1213EC) — Offset AC8h

Physical Layer 16.0 GT/s Lane 1213 Equalization Control Register



| Type | Size   | Offset                 | Default |
|------|--------|------------------------|---------|
| PCI  | 16 bit | [B:0, D:1, F:0] + AC8h | FFFFh   |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 15:12     | Fh<br>RW         | <b>Upstream Port 16 GT/s Port Lane 13 Transmitter Preset (UP16L13TP):</b><br>Field contains the Transmitter Preset value sent or received during Port 16 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 11:8      | Fh<br>RW         | <b>Downstream Port 16 GT/s Lane 13 Transmitter Preset (DP16L13TP):</b><br>Transmitter Preset used for 16 GT/s 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.   |
| 7:4       | Fh<br>RW         | <b>Upstream Port 16 GT/s Port Lane 12 Transmitter Preset (UP16L12TP):</b><br>Field contains the Transmitter Preset value sent or received during Port 16 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 3:0       | Fh<br>RW         | <b>Downstream Port 16 GT/s Lane 12 Transmitter Preset (DP16L12TP):</b><br>Transmitter Preset used for 16 GT/s 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.   |

## 5.117 Physical Layer 16.0 GT/s Lane 1415 Equalization Control Register (PL16L1415EC) – Offset ACAh

Physical Layer 16.0 GT/s Lane 1415 Equalization Control Register

| Type | Size   | Offset                 | Default |
|------|--------|------------------------|---------|
| PCI  | 16 bit | [B:0, D:1, F:0] + ACAh | FFFFh   |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 15:12     | Fh<br>RW         | <b>Upstream Port 16 GT/s Port Lane 15 Transmitter Preset (UP16L15TP):</b><br>Field contains the Transmitter Preset value sent or received during Port 16 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 11:8      | Fh<br>RW         | <b>Downstream Port 16 GT/s Lane 15 Transmitter Preset (DP16L15TP):</b><br>Transmitter Preset used for 16 GT/s 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.   |
| 7:4       | Fh<br>RW         | <b>Upstream Port 16 GT/s Port Lane 14 Transmitter Preset (UP16L14TP):</b><br>Field contains the Transmitter Preset value sent or received during Port 16 GT/s Link Equalization.<br>Port Direction: Downstream Port<br>Crosslink Supported: Any<br>Usage: Contains value sent on the associated Lane during Link EQ. |
| 3:0       | Fh<br>RW         | <b>Downstream Port 16 GT/s Lane 14 Transmitter Preset (DP16L14TP):</b><br>Transmitter Preset used for 16 GT/s 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.   |

## 5.118 Physical Layer 16.0 GT/s Margining Extended Capability Header (PL16MECH) — Offset EDCh

Physical Layer 16.0 GT/s Margining Extended Capability Header

| Type | Size   | Offset                 | Default   |
|------|--------|------------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, F:0] + EDCh | 00010027h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 31:20     | 000h<br>RW/O     | <b>Next Capability Offset (NCO):</b><br>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.<br>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.<br>The bottom 2 bits of this offset are Reserved and must be implemented as 00b although software must mask them to allow for future uses of these bits. |
| 19:16     | 1h<br>RW/O       | <b>Capability Version (CV):</b><br>This field is a PCI-SIG defined version number that indicates the version of the Capability structure present.   |
| 15:0      | 0027h<br>RW/O    | <b>PCI Express Extended Capability ID (PCIECID):</b><br>This field is a PCI-SIG defined ID number that indicates the nature and format of the Extended Capability.<br>Extended Capability ID for the Physical Layer 16.0 GT/s Margining Capability  |

## 5.119 Physical Layer 16.0 GT/s Margining Port Capabilities and Port Status (PL16MPCPS) — Offset EE0h

Physical Layer 16.0 GT/s Margining Port Capabilities and Port Status

| Type | Size   | Offset                 | Default   |
|------|--------|------------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, F:0] + EE0h | 00000000h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 31:18     | 0h<br>RO         | <b>Reserved</b>  |
| 17        | 0h<br>RO/V       | <b>Margining Software Ready (MARGINSWRDY):</b><br>When Margining uses Driver Software is Set, then this bit, when Set, indicates that the required software has performed the required initialization. The value of this bit is Undefined if Margining users Driver Software is Clear. |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 16        | 0h<br>RO/V       | <b>Margining Ready (MARGINRDY):</b><br>Indicates when the Margining feature is ready to accept margining commands. Behavior is undefined if this bit is Clear and, for any Lane, any of the Receiver Number, Margin Type, Usage Model, or Margin Payload fields are written.<br>If Margining uses Driver Software is Set, Margining Ready must be Set no later than 100 ms after the later of Margining Software Ready becoming Set or the link training to 16.0 GT/s.<br>If Margining uses Driver Software is Clear, Margining Ready must be Set no later than 100 ms after the Link trains to 16.0 GT/s. |
| 15:1      | 0h<br>RO         | <b>Reserved</b>  |
| 0         | 0h<br>RW/O       | <b>Margining uses Driver Software (MARGINDRISW):</b><br>If Set, indicates that Margining is partially implemented using Device Driver software. Margining Software Ready indicates when this software is initialized. If Clear, Margining does not require device driver software. In this case the value read from Margining Software Ready is undefined  |

## 5.120 Physical Layer 16.0 GT/s Lane0 Margin Control and Status Register (PL16L0MCS) – Offset EE4h

Physical Layer 16.0 GT/s Lane0 Margin Control and Status Register

| Type | Size   | Offset                 | Default   |
|------|--------|------------------------|-----------|
| PCI  | 32 bit | [B:0, D:1, F:0] + EE4h | 00009C38h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 31:24     | 00h<br>RO/V      | <b>Margin Payload Status (MPSTS):</b><br>This field is only meaningful, when the Margin Type<br>This field must be reset to the default value if the Port goes to DL_Down status.                                     |
| 23        | 0h<br>RO         | <b>Reserved</b>   |
| 22        | 0h<br>RO/V       | <b>Usage Model Status (UMS):</b><br>This field must be reset to the default value if the Port goes to DL_Down status.   |
| 21:19     | 0h<br>RO/V       | <b>Margin Type Status (MTS):</b><br>This field must be reset to the default value if the Port goes to DL_Down status.   |
| 18:16     | 0h<br>RO/V       | <b>Receiver Number Status (RNS):</b><br>This field must be reset to the default value if the Port goes to DL_Down status.   |
| 15:8      | 9Ch<br>RW        | <b>Margin Payload (MP):</b><br>This fields value is used in conjunction with the Margin Type field.<br>The default value is 9Ch.<br>This field must be reset to the default value if the Port goes to DL_Down status. |
| 7         | 0h<br>RO         | <b>Reserved</b>   |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 6         | 0h<br>RW         | <b>Usage Model (UM):</b><br>The default value is 0b.<br>This field must be reset to the default value if the Port goes to DL_Down status.       |
| 5:3       | 7h<br>RW         | <b>Margin Type (MT):</b><br>The default value is 111b.<br>This field must be reset to the default value if the Port goes to DL_Down status.     |
| 2:0       | 0h<br>RW         | <b>Receiver Number (RN):</b><br>The default value is 000b.<br>This field must be reset to the default value if the Port goes to DL_Down status. |

### 5.121 Physical Layer 16.0 GT/s Lane1 Margin Control and Status Register (PL16L1MCS) – Offset EE8h

Physical Layer 16.0 GT/s Lane1 Margin Control and Status Register

**Note:** Bit definitions are the same as [PL16L0MCS](#), offset EE4h.

### 5.122 Physical Layer 16.0 GT/s Lane2 Margin Control and Status Register (PL16L2MCS) – Offset EECh

Physical Layer 16.0 GT/s Lane2 Margin Control and Status Register

**Note:** Bit definitions are the same as [PL16L0MCS](#), offset EE4h.

### 5.123 Physical Layer 16.0 GT/s Lane3 Margin Control and Status Register (PL16L3MCS) – Offset EF0h

Physical Layer 16.0 GT/s Lane3 Margin Control and Status Register

**Note:** Bit definitions are the same as [PL16L0MCS](#), offset EE4h.

### 5.124 Physical Layer 16.0 GT/s Lane4 Margin Control and Status Register (PL16L4MCS) – Offset EF4h

Physical Layer 16.0 GT/s Lane4 Margin Control and Status Register

**Note:** Bit definitions are the same as [PL16L0MCS](#), offset EE4h.

### 5.125 Physical Layer 16.0 GT/s Lane5 Margin Control and Status Register (PL16L5MCS) – Offset EF8h

Physical Layer 16.0 GT/s Lane5 Margin Control and Status Register

**Note:** Bit definitions are the same as [PL16L0MCS](#), offset EE4h.

## 5.126 Physical Layer 16.0 GT/s Lane6 Margin Control and Status Register (PL16L6MCS) – Offset EFCh

Physical Layer 16.0 GT/s Lane6 Margin Control and Status Register

**Note:** Bit definitions are the same as PL16L0MCS, offset EE4h.

## 5.127 Physical Layer 16.0 GT/s Lane7 Margin Control and Status Register (PL16L7MCS) – Offset F00h

Physical Layer 16.0 GT/s Lane7 Margin Control and Status Register

**Note:** Bit definitions are the same as PL16L0MCS, offset EE4h.

## 5.128 Physical Layer 16.0 GT/s Lane8 Margin Control and Status Register (PL16L8MCS) – Offset F04h

Physical Layer 16.0 GT/s Lane8 Margin Control and Status Register

**Note:** Bit definitions are the same as PL16L0MCS, offset EE4h.

## 5.129 Physical Layer 16.0 GT/s Lane9 Margin Control and Status Register (PL16L9MCS) – Offset F08h

Physical Layer 16.0 GT/s Lane9 Margin Control and Status Register

**Note:** Bit definitions are the same as PL16L0MCS, offset EE4h.

## 5.130 Physical Layer 16.0 GT/s Lane10 Margin Control and Status Register (PL16L10MCS) – Offset F0Ch

Physical Layer 16.0 GT/s Lane10 Margin Control and Status Register

**Note:** Bit definitions are the same as PL16L0MCS, offset EE4h.

## 5.131 Physical Layer 16.0 GT/s Lane11 Margin Control and Status Register (PL16L11MCS) – Offset F10h

Physical Layer 16.0 GT/s Lane11 Margin Control and Status Register

**Note:** Bit definitions are the same as PL16L0MCS, offset EE4h.



### **5.132 Physical Layer 16.0 GT/s Lane12 Margin Control and Status Register (PL16L12MCS) — Offset F14h**

Physical Layer 16.0 GT/s Lane12 Margin Control and Status Register

**Note:** Bit definitions are the same as [PL16L0MCS](#), offset EE4h.

### **5.133 Physical Layer 16.0 GT/s Lane13 Margin Control and Status Register (PL16L13MCS) — Offset F18h**

Physical Layer 16.0 GT/s Lane13 Margin Control and Status Register

**Note:** Bit definitions are the same as [PL16L0MCS](#), offset EE4h.

### **5.134 Physical Layer 16.0 GT/s Lane14 Margin Control and Status Register (PL16L14MCS) — Offset F1Ch**

Physical Layer 16.0 GT/s Lane14 Margin Control and Status Register

**Note:** Bit definitions are the same as [PL16L0MCS](#), offset EE4h.

### **5.135 Physical Layer 16.0 GT/s Lane15 Margin Control and Status Register (PL16L15MCS) — Offset F20h**

Physical Layer 16.0 GT/s Lane15 Margin Control and Status Register

**Note:** Bit definitions are the same as [PL16L0MCS](#), offset EE4h.



# 6 Dynamic Tuning Technology Registers (D4:F0)

This chapter documents the registers in Bus: 0, Device 4, Function 0.

**Table 6-1. 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)                         | 4C03h            |
| 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) | 000000000000004h |
| 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)                   | 0000FFFFh        |
| E4h    | 4            | Capabilities A (CAPID0_A_0_4_0_PCI)               | 00000000h        |
| E8h    | 4            | Capabilities B (CAPID0_B_0_4_0_PCI)               | 00000000h        |

## 6.1 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<br>RO      | <b>VID:</b><br>PCI standard identification for Intel. |

## 6.2 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 | 4C03h   |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 15:0      | 4C03h<br>RW/V/L  | <b>DID:</b><br>Identifier assigned to the Thermal Management Controller. |

## 6.3 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<br>RO         | <b>Reserved</b>   |
| 10        | 0h<br>RW         | <b>INTDIS:</b><br>This bit, when set, disables the device from asserting INTA#.   |
| 9         | 0h<br>RO         | <b>FB2B:</b><br>The DTT device does not implement this bit and it is hardwired to a 0.  |
| 8         | 0h<br>RO         | <b>SERRE:</b><br>The DTT device does not implement this bit and it is hardwired to a 0.   |
| 7         | 0h<br>RO         | <b>ADSTEP:</b><br>The DTT device does not implement this bit and it is hardwired to a 0.  |
| 6         | 0h<br>RO         | <b>PERRE:</b><br>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<br>RO         | <b>VGASNOOP:</b><br>The DTT device does not implement this bit and it is hardwired to a 0.  |
| 4         | 0h<br>RO         | <b>MWIE:</b><br>This bit is hardwired to 0.<br>The DTT Device will never issue memory write and invalidate commands, and therefore has no need to implement this bit.   |
| 3         | 0h<br>RO         | <b>SCE:</b><br>The DTT device does not implement this bit and it is hardwired to a 0.   |
| 2         | 0h<br>RW         | <b>BME:</b><br>The DTT Device is enabled to function as a PCI-compliant bus master when this bit is set.<br>If it is not set, bus mastering is disabled.  |
| 1         | 0h<br>RW         | <b>MAE:</b><br>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<br>RO         | <b>IOAE:</b><br>The DTT device does not implement this bit and it is hardwired to a 0.  |

## 6.4 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<br>RO         | <b>DPE:</b><br>The DTT device does not implement this bit and it is hardwired to a 0.  |
| 14        | 0h<br>RO         | <b>SSE:</b><br>This bit is hardwired to zero.<br>The DTT Device never asserts SERR#, and therefore it has no need to implement this bit.   |
| 13        | 0h<br>RO         | <b>RURS:</b><br>The DTT device does not implement this bit and it is hardwired to a 0.   |
| 12        | 0h<br>RO         | <b>RCAS:</b><br>The DTT device does not implement this bit and it is hardwired to a 0.   |
| 11        | 0h<br>RO         | <b>STAS:</b><br>This bit is hardwired to 0.<br>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<br>RO         | <b>DEVT:</b><br>These bits are hardwired to 0.<br>Device 4 does not physically connect to PCI_A.   |
| 8         | 0h<br>RO         | <b>DPD:</b><br>This bit is hardwired to 0.<br>PERR signaling and messaging are not implemented by the DTT Device, and therefore it has no need to implement this bit.  |
| 7         | 1h<br>RO         | <b>FB2B:</b><br>This bit is hardwired to 1.<br>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<br>RO         | <b>Reserved</b>  |
| 5         | 0h<br>RO         | <b>PCI66M:</b><br>The DTT device does not implement this bit and it is hardwired to a 0.   |
| 4         | 1h<br>RO         | <b>CLIST:</b><br>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<br>RW/V/L     | <b>IS:</b><br>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<br>RO         | <b>Reserved</b>  |

## 6.5 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<br>RW/L       | <b>Revision ID Upper Bits (RID_MSB):</b><br>DTT device Revision ID 4 upper bits. |
| 3:0       | 0h<br>RW/L       | <b>Revision ID Lower Bits (RID):</b><br>DTT device Revision ID 4 lower bits.     |

## 6.6 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<br>RO        | <b>PI:</b><br>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. |



## 6.7 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<br>RO        | <b>BCC:</b><br>This is an 8-bit value that indicates the base class code for the DTT Thermal Controller.<br>This code has the value 11h, indicating a device that is used for data acquisition and signal processing. |
| 7:0       | 80h<br>RO        | <b>SUBCC:</b><br>The code is 80h which indicates Other Data Acquisition and Signal Processing Controllers.  |

## 6.8 Cache Line Size Register (CLS\_0\_4\_0\_PCI) – Offset Ch

The DTT Device does not support this register as a PCI subordinate.

| 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<br>RO        | <b>CLS:</b><br>This field is hardwired to 0.<br>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. |

## 6.9 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<br>RO        | <b>MLT:</b><br>This field is hardwired to 0. The DTT Device does not support perform bursts. |

## 6.10 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<br>RO        | <b>HDR:</b><br>This field always returns 0 to indicate that the DTT device is a single function device with standard header layout. |

## 6.11 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<br>RO         | <b>BS:</b><br>This bit is hardwired to zero. The DTT Device does not support BIST. |
| 6:0       | 0h<br>RO         | <b>Reserved</b>  |

## 6.12 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<br>RO         | <b>Reserved</b>  |
| 38:16     | 000000h<br>RW    | <b>TMMBA:</b><br>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.<br>This register ensures that a naturally aligned 64KB space is allocated within total addressable memory space.<br>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<br>RO         | <b>Reserved</b>   |
| 14:4      | 000h<br>RO       | <b>ADM:</b><br>Hardwired to 0s to indicate at least 32KB address range. |
| 3         | 0h<br>RO         | <b>PM:</b><br>Hardwired to 0 to prevent prefetching.                    |
| 2:1       | 2h<br>RO         | <b>MT:</b><br>Hardwired to 10 to indicate 64-bit address.               |
| 0         | 0h<br>RO         | <b>MIOS:</b><br>Hardwired to 0 to indicate memory space.                |

### 6.13 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<br>RW/L    | <b>SUBVID:</b><br>This field should be programmed during boot-up to indicate the vendor of the system board.<br>After it has been written once, it becomes read only.<br><b>Locked by:</b> WRITE_ONCE_LOCK.SUBVID_WOL |

### 6.14 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<br>RW/L    | <b>SUBID:</b><br>This field should be programmed during BIOS initialization. After it has been written once, it becomes read only.<br><b>Locked by:</b> WRITE_ONCE_LOCK.SUBID_WOL |

## 6.15 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<br>RW/V/L    | <b>CAPPV:</b><br>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]. |

## 6.16 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<br>RW        | <b>INTCON:</b><br>Used to communicate interrupt line routing information.<br>BIOS Requirement: POST software writes the routing information into this register as it initializes and configures the system.<br>The value indicates to which input of the system interrupt controller this devices interrupt pin is connected. |

## 6.17 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<br>RO        | <b>INTPIN:</b><br>As a single function device, the DTT device specifies INTA as its interrupt pin. 01h = INTA. |

## 6.18 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<br>RO        | <b>MGV:</b><br>These bits are hardwired to zero. The DTT Device does not burst as a PCI compliant master. |

## 6.19 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<br>RO        | <b>MLV:</b><br>These bits are hardwired to zero. The DTT Device has no specific requirements for how often it needs to access the PCI bus. |

## 6.20 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 | 0000FFFFh |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | R          | R         |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 31:16     | 0h<br>RO         | <b>Reserved</b>  |
| 15        | 1h<br>RW/L       | <b>D8EN:</b><br>0: Bus 0 Device 8 is disabled and not visible.<br>1: Bus 0 Device 8 is enabled and visible.<br>This bit will be set to 0b and remain 0b if Device 8 capability is disabled.<br><b>Locked by:</b> CAPID0_B_0_0_0_PCI.GMM_DIS  |
| 14        | 1h<br>RW/L       | <b>D14FOEN:</b><br>VMD Enable -<br>0: Bus 0 Device 14 Function 0 is disabled and hidden.<br>1: Bus 0 Device 14 Function 0 is enabled and visible.<br><b>Locked by:</b> CAPID0_B_0_0_0_PCI.VMD_DIS  |
| 13        | 1h<br>RW/L       | <b>D6EN:</b><br>0: Bus 0 Device 6 Function 0 is disabled and not visible.<br>1: Bus 0 Device 6 Function 0 is enabled and visible.<br>This bit will be set to 0b and remain 0b if Device 6 Function 0 capability is disabled.<br><b>Locked by:</b> CAPID0_A_0_0_0_PCI.PEG60D                                    |
| 12        | 1h<br>RW/L       | <b>D9EN:</b><br>0: Bus 0 Device 9 is disabled and not visible.<br>1: Bus 0 Device 9 is enabled and visible.<br>This bit will be set to 0b and remain 0b if Device 9 capability is disabled.<br><b>Locked by:</b> CAPID0_B_0_0_0_PCI.NPK_DIS  |
| 11        | 1h<br>RW/L       | <b>D10EN:</b><br>Device10 enable<br>0: Bus 0 Device 10 is disabled and not visible.<br>1: Bus 0 Device 10 is enabled and visible.<br>This bit will be set to 0b and remain 0b if Device 10 capability is disabled.<br><b>Locked by:</b> CAPID0_B_0_0_0_PCI.DEVICE10_DIS  |
| 10        | 1h<br>RW/L       | <b>D5EN:</b><br>0: Bus 0 Device 5 is disabled and not visible.<br>1: Bus 0 Device 5 is enabled and visible.<br>This bit will be set to 0b and remain 0b if Device 5 capability is disabled.<br><b>Locked by:</b> CAPID0_B_0_0_0_PCI.IMGU_DIS   |
| 9         | 1h<br>RW/L       | <b>D11F1EN:</b><br>Device11 function 1 enable<br>0: Bus 0 Device 11 function 1 is disabled and not visible.<br>1: Bus 0 Device 11 function 1 is enabled and visible.<br>This bit will be set to 0b and remain 0b if Device 11F1 capability is disabled.<br><b>Locked by:</b> CAPID0_B_0_0_0_PCI.DEVICE11F1_DIS |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 8         | 1h<br>RW/L       | <b>D11F0EN:</b><br>Device11 function 0 enable<br>0: Bus 0 Device 11 function 0 is disabled and not visible.<br>1: Bus 0 Device 11 function 0 is enabled and visible.<br>This bit will be set to 0b and remain 0b if Device 11F0 capability is disabled.<br><b>Locked by:</b> CAPID0_B_0_0_0_PCI.DEVICE11F0_DIS |
| 7         | 1h<br>RW/L       | <b>D4EN:</b><br>0: Bus 0 Device 4 is disabled and not visible.<br>1: Bus 0 Device 4 is enabled and visible.<br>This bit will be set to 0b and remain 0b if Device 4 capability is disabled.<br><b>Locked by:</b> CAPID0_A_0_0_0_PCI.CDD  |
| 6         | 1h<br>RW/L       | <b>D3F7EN:</b><br>NVMe - Device 3 function 7 enable.<br>0: Bus 0 Device 3 function 7 is disabled and hidden.<br>1: Bus 0 Device 3 function 7 is enabled and visible.<br>This bit will be set to 0b and remain 0b if Device 3 capability is disabled.<br><b>Locked by:</b> CAPID0_A_0_0_0_PCI.NVME_F7D          |
| 5         | 1h<br>RW/L       | <b>D3F0EN:</b><br>NVMe - Device 3 function 0 enable.<br>0: Bus 0 Device 3 function 0 is disabled and hidden.<br>1: Bus 0 Device 3 function 0 is enabled and visible.<br>This bit will be set to 0b and remain 0b if Device 3 capability is disabled.<br><b>Locked by:</b> CAPID0_A_0_0_0_PCI.NVME_F0D          |
| 4         | 1h<br>RW/L       | <b>D2EN:</b><br>0: Bus 0 Device 2 is disabled and hidden<br>1: Bus 0 Device 2 is enabled and visible<br>This bit will be set to 0b and remain 0b if Device 2 capability is disabled.<br><b>Locked by:</b> CAPID0_A_0_0_0_PCI.IGD   |
| 3         | 1h<br>RW/L       | <b>D1F0EN:</b><br>0: Bus 0 Device 1 Function 0 is disabled and hidden.<br>1: Bus 0 Device 1 Function 0 is enabled and visible.<br>This bit will be set to 0b and remain 0b if PEG10 capability is disabled.<br><b>Locked by:</b> CAPID0_A_0_0_0_PCI.PEG10D   |
| 2         | 1h<br>RW/L       | <b>D1F1EN:</b><br>0: Bus 0 Device 1 Function 1 is disabled and hidden.<br>1: Bus 0 Device 1 Function 1 is enabled and visible.<br><b>Locked by:</b> CAPID0_A_0_0_0_PCI.PEG11D  |
| 1         | 1h<br>RW/L       | <b>D1F2EN:</b><br>0: Bus 0 Device 1 Function 2 is disabled and hidden.<br>1: Bus 0 Device 1 Function 2 is enabled and visible.<br><b>Locked by:</b> CAPID0_A_0_0_0_PCI.PEG12D  |
| 0         | 1h<br>RO         | <b>DOEN:</b><br>Bus 0 Device 0 Function 0 may not be disabled and is therefore hardwired to 1.   |

## 6.21 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<br>RW/L       | <b>NVME Device 3 Function 0 Disable (NVME_F0D):</b><br>0: Device 3 Function 0 and associated memory spaces are accessible.<br>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<br>RW/L       | <b>PCIe Device 1 Function 2 Disable (PEG12D):</b><br>0: Device 1 Function 2 and associated memory spaces are accessible.<br>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<br>RW/L       | <b>PCIe Device 1 Function 1 Disable (PEG11D):</b><br>0: Device 1 Function 1 and associated memory spaces are accessible.<br>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<br>RW/L       | <b>PCIe Device 1 Function 0 Disable (PEG10D):</b><br>0: Device 1 Function 0 and associated memory spaces are accessible.<br>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<br>RW/L       | <b>PCIe Link Width Up-config Disable (PELWUD):</b><br>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.<br>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<br>RW/L       | <b>DMI Width (DW):</b><br>0: DMI x4<br>1: DMI x2  |
| 25        | 0h<br>RW/L       | <b>DRAM ECC Disable (ECCDIS):</b><br>0: ECC is supported<br>1: ECC is not supported   |
| 24        | 0h<br>RW/L       | <b>Force DRAM ECC Enable (FDEE):</b><br>0: DRAM ECC optional via software.<br>1: DRAM ECC enabled. MCHBAR COMISCCTL bit [0] and C1MISCCTL bit [0] are forced to 1 and Read-Only.  |
| 23        | 0h<br>RW/L       | <b>VT-d Disable (VTDD):</b><br>0: VT-d is supported<br>1: VT-d is not supported   |
| 22        | 0h<br>RW/L       | <b>DMI GEN2 Disable (DMIG2DIS):</b><br>0: Capable of running DMI in Gen 2 mode<br>1: Not capable of running DMI in Gen 2 mode   |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 21        | 0h<br>RW/L       | <b>PCIe Controller Gen 2 Disable (PEGG2DIS):</b><br>0: Capable of running any of the PEG controllers in Gen 2 mode<br>1: Not capable of running any of the PEG controllers in Gen 2 mode  |
| 20:19     | 0h<br>RW/L       | <b>DRAM Maximum Size per Channel (DDRSZ):</b><br>This field defines the maximum allowed memory size per channel.<br><ul style="list-style-type: none"><li>• 0: Unlimited (64GB per channel)</li><li>• 1: Maximum 8GB per channel</li><li>• 2: Maximum 4GB per channel</li><li>• 3: Maximum 2GB per channel</li></ul>  |
| 18        | 0h<br>RW/L       | <b>PCIe Controller Device 6 Function 0 Disabled (PEG60D):</b><br>PCIe Controller Device 6 Function 0 is disabled<br>0: Device 6 Function 0 is supported<br>1: Device 6 Function 0 is not supported  |
| 17        | 0h<br>RW/L       | <b>DRAM 1N Timing Disable (D1NM):</b><br>0: Part is capable of supporting 1n mode timings on the DDR interface.<br>1: Part is not capable of supporting 1n mode. Only supported timings are 2n or greater.  |
| 16        | 0h<br>RO         | <b>Reserved</b>   |
| 15        | 0h<br>RW/L       | <b>DTT Device Disable (CDD):</b><br>0: DTT Device enabled.<br>1: DTT Device disabled.   |
| 14        | 0h<br>RW/L       | <b>2 DIMMs Per Channel Enable (DDPCD):</b><br>Allows Dual Channel operation but only supports 1 DIMM per channel.<br>0: 2 DIMMs per channel enabled<br>1: 2 DIMMs per channel disabled.<br>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<br>RW/L       | <b>X2APIC Enable (X2APIC_EN):</b><br>Extended Interrupt Mode.<br>0b: Hardware does not support Extended APIC mode.<br>1b: Hardware supports Extended APIC mode.   |
| 12        | 0h<br>RW/L       | <b>Dual Memory Channel Support (PDCD):</b><br>0: Capable of Dual Channel<br>1: Not Capable of Dual Channel - only single channel capable.   |
| 11        | 0h<br>RW/L       | <b>Internal Graphics Disable (IGD):</b><br>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.<br>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. |



| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 10        | 0h<br>RW/L       | <b>DID0 Override Enable (DID0OE):</b><br>0: Disable ability to override DID0 - For production<br>1: Enable ability to override DID - For debug and samples only   |
| 9:8       | 0h<br>RO         | <b>Reserved</b>   |
| 7:4       | 0h<br>RW/L       | <b>Compatibility Revision ID (CRID):</b><br>Compatibility Revision ID   |
| 3         | 0h<br>RW/L       | <b>Memory Overclocking (DDR_OVERCLOCK):</b><br>Memory Overclocking support<br>0: Memory Overclocking is not supported<br>1: Memory Overclocking is supported  |
| 2:1       | 0h<br>RO         | <b>Reserved</b>   |
| 0         | 0h<br>RW/L       | <b>NVME F7D (NVME_F7D):</b><br>0: Device 3 Function 7 and associated memory spaces are accessible.<br>1: Device 3 Function 7 (NVMe F7) and associated memory space are disabled by hardwiring the D3F7EN field, bit 6 of the SoC Device Enable register |

## 6.22 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 | 0000000h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| RW          | RW         | RW        |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 31        | 0h<br>RW/L       | <b>Image Processing Unit (IPU) Disable (IPU_DIS):</b><br>0: Device 5 associated memory spaces are accessible.<br>1: Device 5 associated memory and IO spaces are disabled. |
| 30        | 0h<br>RW/L       | <b>Trace Hub Disable (TRACE_HUB_DIS):</b><br>0: Trace Hub associated memory spaces are accessible.<br>1: Trace Hub associated memory and IO spaces are disabled.           |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 29        | 0h<br>RW/L       | <b>Overclocking Enabled (OC_ENABLED):</b><br>0: Overclocking is Disabled<br>1: Overclocking is Enabled<br>If overclocking is enabled, MSR FLEX_RATIO.OC_BINS contains how many bits of over-clocking are supported.<br>The encoding is as follows:<br>0: Overclocking is Disabled<br>1-6: Turbo ratio limits can be incremented by this amount<br>7: Unlimited<br>If overclocking is disabled, FLEX_RATIO.OC_BINS is meaningless.  |
| 28        | 0h<br>RW/L       | <b>SMT Capability (SMT):</b><br>This setting indicates whether the processor is SMT (HyperThreading) capable.  |
| 27:25     | 0h<br>RW/L       | <b>Cache Size (CACHESZ):</b><br>This setting indicates the supporting cache sizes.   |
| 24        | 0h<br>RW/L       | <b>SVM Disable (SVM_DISABLE):</b><br>0: SVM enabled<br>1: SVM disabled   |
| 23:21     | 0h<br>RW/L       | <b>Memory 100MHz Reference Clock (PLL_REF100_CFG):</b><br>DDR Maximum Frequency Capability with 100MHz memory reference clock (ref_clk).<br>0: 100 MHz memory reference clock is not supported<br>1-6: Reserved<br>7: Unlimited  |
| 20        | 0h<br>RW/L       | <b>PCIe Gen 3 Disable (PEG3_DIS):</b><br>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)<br>1: Not capable of running any of the PCIe controllers in Gen 3 mode   |
| 19        | 0h<br>RW/L       | <b>Processor Package Type (PKGTYP):</b><br>This setting indicates the CPU Package Type.  |
| 18        | 0h<br>RW/L       | <b>Additive Graphics Enabled (ADDGF Xen):</b><br>0: Additive Graphics is disabled<br>1: Additive Graphics is enabled   |
| 17        | 0h<br>RW/L       | <b>Additive Graphics Capability Disable (ADDGFXCAP):</b><br>0: Capable of Additive Graphics<br>1: Not capable of Additive Graphics   |
| 16        | 0h<br>RW/L       | <b>PCIe x16 Disable (PEGX16D):</b><br>0: Capable of x16 PCIe Port<br>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<br>RW/L       | <b>DMI Gen 3 Disable (DMIG3DIS):</b><br>DMI Gen 3 Disable  |
| 14:12     | 0h<br>RW/L       | <b>2 Level Memory Technology Support (LTECH):</b><br>0: 1LM<br>1: EDRAM0<br>3: EDRAM0+1<br>4: 2LM<br>Other values are reserved.  |
| 11        | 0h<br>RW/L       | <b>HDCP Disable (HDCPD):</b><br>0: Capable of HDCP<br>1: HDCP Disabled   |

| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 10        | 0h<br>RW/L       | <b>2 Level Memory Support (2LM_SUPPORTED):</b><br>0: 2 Level Memory (2LM) is not supported.<br>1: 2 Level Memory (2LM) is supported.   |
| 9         | 0h<br>RO         | <b>Reserved</b>  |
| 8         | 0h<br>RW/L       | <b>GNA (GMM) Disable (GNA_DIS):</b><br>0: Device 8 associated memory spaces are accessible.<br>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<br>RW/L       | <b>DDD:</b><br>0: Debug mode<br>1: Production mode   |
| 6:4       | 0h<br>RO         | <b>Reserved</b>  |
| 3         | 0h<br>RW/L       | <b>S/H OPI Enable (SH_OPI_EN):</b><br>Specifies if OPI or DMI are enabled for S/H models.<br>0: DMI is enabled<br>1: OPI is enabled  |
| 2         | 0h<br>RW/L       | <b>VMD Disable (VMD_DIS):</b><br>Indicates if VMD is disabled.   |
| 1         | 0h<br>RW/L       | <b>Global Single PCIe Lane (DPEGFX1):</b><br>This bit has no effect on Device 1 unless Device 1 is configured for at least two ports via PEG0CFGSEL strap.<br>0: All PCIe port widths do not depend on their respective BCTRL[VGAEN].<br>1: Each PCIe port width is limited to x1 operation when its respective BCTRL[VGAEN] is set to 1b. |
| 0         | 0h<br>RW/L       | <b>Single PCIe Lane (SPEGFX1):</b><br>This bit has no effect on Device 1 unless Device 1 is configured for a single port via PEG0CFGSEL strap.<br>0: Device 1 Function 0 width does not depend on its BCTRL[VGAEN].<br>1: Device 1 Function 0 width is limited to x1 operation when its respective BCTRL[VGAEN] is set to 1.               |

# 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.

**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         |
| F0h    | 2            | FLR Capability ID (FLRCAPID)                        | 0013h         |



| Offset | Size (Bytes) | Register Name (Register Symbol)             | Default Value |
|--------|--------------|---|---------------|
| 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<br>RO/V    | <b>Device Identification Number (DID):</b><br>Indicates the device ID assigned to the GNA. |
| 15:0      | 8086h<br>RO      | <b>Vendor Identification Number (VID):</b><br>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<br>RO         | <b>Reserved</b>   |
| 14        | 0h<br>RO         | <b>Unsupported Request Error Reporting Enable (UNSPREQERREN):</b><br>Unsupported Request Error Reporting Enable   |
| 13        | 0h<br>RO         | <b>Poisoned TLP Error Reporting Enable (PTLPERREN):</b><br>Poisoned TLP Error Reporting Enable  |
| 12:11     | 0h<br>RO         | <b>Reserved</b>   |
| 10        | 0h<br>RW         | <b>Interrupt Disable (INTDIS):</b><br>Interrupt Disable:<br>Controls the ability of the function to generate INTx interrupts.<br>0: INTx allowed<br>1: INTx disabled  |
| 9:6       | 0h<br>RO         | <b>Reserved</b>   |
| 5         | 0h<br>RO         | <b>Max Aligned Payload Size (MXAPAYLDSZ):</b><br>Max Aligned Payload Size - Reserved  |
| 4         | 0h<br>RO         | <b>Max Aligned Read Request Size (MXARDREQSZ):</b><br>Max Aligned Read Request Size - Reserved  |
| 3         | 0h<br>RO         | <b>Special Cycle Enable (SCEN):</b><br>Special Cycle Enable - Reserved  |
| 2         | 0h<br>RW         | <b>Bus Master Enable (BME):</b><br>Bus Master Enable:<br>0: Disable (default).<br>1: Enabled. Device may generate bus master transactions depending on its mode of operation.                                 |
| 1         | 0h<br>RW         | <b>Memory Space Enable (MSE):</b><br>Memory Space Enable<br>Controls the GMM devices response to memory space accesses.<br>0: Disabled (default)<br>1: Enabled. Device will respond to memory space accesses. |
| 0         | 0h<br>RO         | <b>IO Space Enable (IOSE):</b><br>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<br>RO         | <b>Detected Parity Error (DPE):</b><br>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.<br>Note: some implementations use this error type as non-fatal error indication<br>This bit is typically RWC. Change to RO as this bit is not in use. |
| 14        | 0h<br>RO         | <b>Signaled System Error (SSE):</b><br>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.<br>Note: some implementations use this error for fatal.<br>When received all operations are aborted.<br>This bit is typically RWC. Change to RO as this bit is not in use  |
| 13        | 0h<br>RW/1C/V    | <b>Received Master Abort (RMA):</b><br>This bit is set when a requester receives a completion with Unsupported Request Completion status.<br>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<br>RW/1C/V    | <b>Received Target Abort (RTA):</b><br>This bit is set when a transaction abort is received to a GMM initiated transaction.  |
| 11        | 0h<br>RW/1C/V    | <b>Signaled Target Abort (STA):</b><br>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<br>RO         | <b>Reserved</b>  |
| 7         | 0h<br>RO         | <b>Fast Back-to-Back (FB2B):</b><br>Fast Back-to-Back<br>(ignored by SW)   |
| 6:5       | 0h<br>RO         | <b>Reserved</b>  |
| 4         | 1h<br>RO         | <b>Capability List (CLIST):</b><br>Capability List<br>0: no capability list<br>1: the GMM contains a linked list of capabilities which is accessed via the CAPPTR register at offset 34h   |
| 3         | 0h<br>RO/V       | <b>Interrupt Status (INTSTS):</b><br>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.<br>This bit is controlled by HW.<br>0: No interrupt pending<br>1: Interrupt pending  |

| Bit Range | Default & Access | Field Name (ID): Description |
|-----------|------------------|------------------------------|
| 2:0       | 0h<br>RO         | <b>Reserved</b>              |

## 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<br>RO        | <b>Base Class Code (BCC):</b><br>Base Class (Generic system Peripherals)            |
| 23:16     | 80h<br>RO        | <b>Sub Class Code (SCC):</b><br>Code for Sub Class                                  |
| 15:8      | 00h<br>RO        | <b>Peripheral Interface (PROGINTERFACE):</b><br>Interface (other system peripheral) |
| 7:0       | 00h<br>RO/V      | <b>Revision ID (RID):</b><br>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<br>RW        | <b>Cache Line Size (CLS):</b><br>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<br>RO         | <b>Multi Function Device (MFD):</b><br>Hardwired to 0 indicating this device is not a multi-function device.    |
| 6:0       | 00h<br>RO        | <b>Header Type (HT):</b><br>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<br>RO         | <b>BIST Capable (BISTCAP):</b><br>BIST Capable. Hardwired to 0 since this device does not implement BIST. |
| 6         | 0h<br>RO         | <b>Start BIST (BISTST):</b><br>Start BIST. Hardwired to 0 since this device does not implement BIST.      |
| 5:4       | 0h<br>RO         | <b>Reserved</b>   |
| 3:0       | 0h<br>RO         | <b>BIST Completion Code (BISTCC):</b><br>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 remaining 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<br>RW     | <b>Memory Base Address Low (BAL):</b><br>Base address of this device's memory mapped IO space. A page of 4KB of address is used. |
| 11:4      | 00h<br>RO        | <b>Address Mask (ADDRMSK):</b><br>Hardwired to 0s to indicate at least 4KB address range   |
| 3         | 0h<br>RO         | <b>Prefetchable Memory (PREF):</b><br>Hardwired to 0 indicating that this range is not prefetchable.                             |



| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 2:1       | 2h<br>RO         | <b>Memory Type (MEMTY):</b><br>Memory Type:<br>00: 32 bit base address<br>01: reserved<br>10: 64-bit base address<br>11: reserved |
| 0         | 0h<br>RO         | <b>Space Type (SPTY):</b><br>Space Type:<br>Memory/IO Space<br>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<br>RW   | <b>Memory Base Address High (Reserved) (BAR):</b><br>These bits must be loaded with zeros.   |
| 6:0       | 00h<br>RW        | <b>Memory Base Address High (BAH):</b><br>Includes the high bits of the base address used by 64-bit OS.<br>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<br>RW/O    | <b>Subsystem Vendor ID (SSVID):</b><br>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<br>RW/O    | <b>Subsystem ID (SSID):</b><br>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<br>RO         | <b>Reserved</b>  |
| 7:0       | 90h<br>RO        | <b>Capability Pointer (CAPP):</b><br>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<br>RW        | <b>Interrupt Connection (INTCON):</b><br>Communicate interrupt line routing information.<br>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<br>RO         | <b>Reserved</b>   |
| 2:0       | 1h<br>RO         | <b>Legacy Interrupt (LEGINT):</b><br>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<br>RO        | <b>Min Latency (MINLAT):</b><br>Reserved |
| 7:0       | 00h<br>RO        | <b>Min Grant (MINGNT):</b><br>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<br>RO         | <b>Reserved</b>  |
| 8         | 0h<br>RW         | <b>Sideband Clock Gating Enable (SBDCGEN):</b><br>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<br>RO         | <b>Reserved</b>  |

## 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<br>RO        | <b>Pointer to Next Capability (NXPTR):</b><br>This contains a pointer to the next item in the capabilities list which is the Power Management Capability |
| 7:0       | 05h<br>RO        | <b>Capability ID (CAPID):</b><br>Capability ID<br>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<br>RO         | <b>Reserved</b>   |
| 8         | 0h<br>RO         | <b>Per-Vector Masking Capable (PVMCAP):</b><br>Per-Vector Masking Capable.<br>0: not supported by GMM.  |
| 7         | 0h<br>RO         | <b>64-bit Address Capable (ADDR64CAP):</b><br>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<br>RW         | <b>Multiple Message Enable (MMEN):</b><br>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<br>RO         | <b>Multiple Message Capable (MMCAP):</b><br>Indicates to SW the number of vectors that the GMM module is requesting for use.<br>Value Number of Messages requested<br>000 1<br>001 2 (reserved)<br>010 4 (reserved)<br>011 8 (reserved)<br>100 16(reserved)<br>101 32(reserved)<br>Other reserved                                     |
| 0         | 0h<br>RW         | <b>MSI Enable (MSIEN):</b><br>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<br>RW  | <b>Message Address (MADDR):</b><br>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<br>RO         | <b>Reserved</b>   |

## 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<br>RO         | <b>Reserved</b>   |
| 15:0      | 0000h<br>RW      | <b>Message Data (MDAT):</b><br>Base message data pattern assigned by system software and used to handle an MSI from the device.<br>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<br>RO        | <b>Pointer to Next Capability (NXTPTR):</b><br>This contains a pointer to the next item in the capabilities list which is the Power Management Capability. |
| 7:0       | 09h<br>RO        | <b>Capability ID (CAPID):</b><br>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<br>RO         | <b>Vendor-Specific Capability ID (VSID):</b><br>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<br>RO         | <b>Vendor Specific Capability Revision (VSREV):</b><br>Reserved   |
| 7:0       | 14h<br>RO        | <b>Vendor Specific Capability Length (VSLLEN):</b><br>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<br>RO       | <b>Vendor Specific Extended Capability Length (VSECLN):</b><br>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<br>RO         | <b>Vendor Specific Extended Capability Revision (VSREV):</b><br>For this revision of DevIdle, this field is 0h.  |
| 15:0      | 0010h<br>RO      | <b>Vendor Specific Extended Capability ID (VSECID):</b><br>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<br>RO   | <b>SW LTR Update MMIO Offset Location (SWLTRLOC):</b><br>The value in this field is ignored as GMM does not support SW LTR. |
| 3:1       | 0h<br>RO         | <b>Base Address Register Number (BARNUM):</b><br>The value in this field is ignored as GMM does not support SW LTR.         |
| 0         | 0h<br>RO         | <b>Valid Indicator (VALID):</b><br>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 | 0000A81h |

Register Level Access:

| BIOS Access | SMM Access | OS Access |
|-------------|------------|-----------|
| R           | R          | R         |

| Bit Range | Default & Access | Field Name (ID): Description  |
|-----------|------------------|---|
| 31:4      | 00000A8h<br>RO   | <b>DevIdle MMIO Offset Location (DEVIDLELOC):</b><br>This location pointer to the DevIdle register in MMIO space, as an offset from the BAR base. |
| 3:1       | 0h<br>RO         | <b>Base Address Register Number (BARNUM):</b><br>The DevIdle is located in BAR0.  |
| 0         | 1h<br>RO         | <b>Valid Indicator (VALID):</b><br>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<br>RO         | <b>Reserved</b>   |
| 12:10     | 2h<br>RO         | <b>Power On Latency Scale (POLS):</b><br>Latency Scale multiplier:<br>010: 1us<br>011: 32us<br>All other settings are reserved.<br>This field is a RO as there is no need for BIOS programming of it. |
| 9:0       | 000h<br>RO       | <b>Power On Latency Value (POLV):</b><br>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 programming 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<br>RO         | <b>Reserved</b>  |
| 5         | 1h<br>RW         | <b>Hardware Autonomous Enable (HAE):</b><br>If set, then the IP may request a PG whenever it is idle.<br>NOTE: If this bit is set, then bits[2:0] must be 000.   |
| 4         | 0h<br>RO         | <b>Reserved</b>  |
| 3         | 1h<br>RW         | <b>Sleep Enable (SE):</b><br>If clear, then IP will never assert Sleep to the retention flops.<br>If set, then IP may assert Sleep during PGing.<br>Note that some platforms may default this bit to 0, others to 1. |
| 2         | 0h<br>RW         | <b>D3-Hot Enable (D3HE):</b><br>If set, then IP will PG when idle and the PMCSR[1:0] register in the IP =11.   |
| 1         | 0h<br>RW         | <b>I3 Enable (I3E):</b><br>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<br>RW         | <b>PMC Request Enable (PMCRE):</b><br>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 (PMCAPIID) — 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<br>RO        | <b>Next Pointer (NXPTR):</b><br>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<br>RO        | <b>Capability Identifier (CAPID):</b><br>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<br>RO        | <b>PME Support (PMES):</b><br>This device does not support PMEB signal.   |
| 10        | 0h<br>RO         | <b>D2 Support (D2S):</b><br>This device does not support D2.  |
| 9         | 0h<br>RO         | <b>D1 Support (D1S):</b><br>This device does not support D1.  |
| 8:6       | 0h<br>RO         | <b>Auxiliary Current (AUXC):</b><br>Reserved  |
| 5         | 0h<br>RO         | <b>Device Specific Initialization (DSI):</b><br>Indicates that this device requires device specific initialization before generic class device driver is to use it. |
| 4         | 0h<br>RO         | <b>Auxiliary Power (AUXP):</b><br>This device does not use Aux power.   |
| 3         | 0h<br>RO         | <b>PME Clock (PMEC):</b><br>Indicate this device does NOT support PMEB generation.  |



| Bit Range | Default & Access | Field Name (ID): Description   |
|-----------|------------------|--|
| 2:0       | 2h<br>RO         | <b>Version for PM (VER):</b><br>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<br>RO         | <b>PME Generation from D3 (cold) (PMEGD3):</b><br>Not supported.   |
| 14:13     | 0h<br>RO         | <b>Data Scale (DATSC):</b><br>No support for Power Management Data register.   |
| 12:9      | 0h<br>RO         | <b>Data Select (DATSEL):</b><br>No support for Power Management Data register.   |
| 8         | 0h<br>RO         | <b>PME Enable (PMEE):</b><br>PMEB is not supported.  |
| 7:2       | 0h<br>RO         | <b>Reserved</b>  |
| 1:0       | 0h<br>RW         | <b>Power State (PS):</b><br>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.<br>00: D0<br>01: D1 (Not supported in this device.)<br>10: D2 (Not supported in this device.)<br>11: D3<br>Write of reserved values is ignored and state will not change.<br>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<br>RO        | <b>Next Pointer (NXTPTR):</b><br>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<br>RO        | <b>Capability Identifier (CAPID):</b><br>A value that indicates FLR (Vendor specific value).<br>0: 09h (FLR in use)<br>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<br>RO         | <b>Reserved</b>   |
| 9         | 1h<br>RO         | <b>FLR Capability (FLRCAP):</b><br>Indicates support for Function Level Reset (FLR).  |
| 8         | 1h<br>RO         | <b>TXP Capability (TXPCAP):</b><br>Indicates that TP bit is supported.  |
| 7:0       | 06h<br>RO        | <b>Capability Length (CAPLEN):</b><br>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<br>RO         | <b>Reserved</b>   |
| 0         | 0h<br>WO         | <b>Initiate FLR (INITFLR):</b><br>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<br>RO         | <b>Reserved</b>  |
| 0         | 0h<br>RO/V       | <b>Transaction Pending (XPEND):</b><br>0: FLR not in progress.<br>1: FLR is in progress (due to internal operation or waiting for the completion of a non-posted transaction). |