BIOS and Kernel Developer's Guide (BKDG) for AMD Family 15h Models 30h-3Fh Processors

Table of Contents

List of Figures

List of Tables

Revision History

KV BKDG Revision 3.06 Changes, Feb 10, 2015; Public release

- 2.15.3 [Error Injection and Simulation]: Updated.
- 2.15.3.1 [DRAM Error Injection]: Updated.
- D18F3x44[NbMcaToMstCpuEn]: Updated.

KV BKDG Revision 3.05 Changes, Jan 21, 2015; Public release

- D0F0xE0 [Link Index Address]: Updated.
- 1.2 [Reference Documents]: Updated.
- 1.3.2 [Arithmetic And Logical Operators]: Updated.
- 1.4 [Definitions]: Updated.
- 1.5.2 [Major Changes]: Updated.
- 2.4.1 [Compute Unit]: Updated.
- 2.4.2.1 [Registers Shared by Cores in a Compute Unit]: Updated.
- 2.4.6.1.1 [Determining Memory Type]: Updated.
- 2.4.9.1.10 [Spurious Interrupts Caused by Timer Tick Interrupt]: Updated.
- 2.4.9.1.15 [State at Reset]: Updated.
- 2.4.9.2.2 [Operating Mode and Default Register Values]: Updated.
- 2.4.9.2.4 [SMM Initial State]: Updated.
- 2.4.9.2.5 [SMM Save State]: Updated.
- 2.5.4.1.3.1 [NB P-state COF and VID Synchronization After Warm Reset]: Updated.
- 2.5.4.1.3.2 [NB P-state Transitions]: Updated.
- 2.8.3 [Memory Scrubbers]: Updated.
- 2.9.10.1.4 [BubbleCnt and CmdStreamLen Programming]: Updated.
- 2.9.14 [DRAM On DIMM Thermal Management and Power Capping]: Updated.
- 2.11.4.3 [Link Configuration and Initialization]: Updated.
- 2.12 [IOMMU]: Updated.
- 2.12.2 [IOMMU Initialization]: Updated.
- 2.14.2 [Frame Buffer (FB)]: Updated.
- 3.1.1 [Northbridge MSRs In Multi-Core Products]: Updated.
- CPUID Fn8000_001B_EAX [Instruction Based Sampling Identifiers]: Updated.
- D0F0x0C[DeviceType]: Updated.
- D0F0x48[DeviceType]: Updated.
- D0F0x98_x02 [ORB PGMEM Control]: Updated.
- D0F0x98_x3A [ORB Source Tag Translation Control 2]: Updated.
- D0F0x98_x3B[IocOutstandingMask]: Updated.
- D0F0xBC_x3F800 [FIRMWARE_FLAGS]: Updated.
- D0F0xBC_xC010_40A0[SviLoadLineOffsetVdd, SviLoadLineOffsetVddNb, SviLoadLineTrimVdd, SviLoadLineTrimVddNb, SviLoadLineVdd, SviLoadLineVddNb]: Updated.
- D0F0xFC_x1[B:0] [IOAPIC BR Interrupt Routing Register]: Updated.
- D0F2x0C[LatencyTimer]: Updated.
- D0F2x2C[SubsystemId, SubsystemVendorId]: Updated.
- D0F2x40[IommuIoTlbsup]: Updated.
- D0F2x50 [IOMMU Miscellaneous Information Register]: Updated.
- D0F2xF4_x0C[FLTCMBPriority]: Updated.
- D0F2xF4_x14 [L2_ITC_CONTROL]: Updated.
- D0F2xF4_x18[PTCA2MMode, PTCAEntries, PTCALRUUpdatePri, PTCAParityEn, PTCAParitySupport, PTCAReplacementSel, PTCASoftInvalidate, PTCAWays]: Updated.
- D0F2xF4_x1C[PTCB2MMode, PTCBBypass, PTCBSoftInvalidate]: Updated.

- D0F2xF4_x22[L2aUpdateFilterBypass, L2aUpdateFilterRdlatency]: Updated.
- D0F2xF4_x30[ERRRuleLock1]: Updated.
- D0F2xF4_x33[CKGateL2ACacheDisable, CKGateL2ADynamicDisable, CKGateL2ARegsDisable]: Updated.
- D0F2xF4_x47: Update.
- D0F2xF4_x48[L2STATUS1]: Updated.
- D0F2xF4_x49 [L2_SB_LOCATION]: Updated.
- D0F2xF4_x50 [L2_PDC_CONTROL]: Updated.
- D0F2xF4_x51[PDCDomainBits]: Updated.
- D0F2xF4_x54[TWPTEOnAddrTransExcl, TWPTEOnUntransExcl, TWPrefetchEn, TWPrefetchOnly4KDis, TWPrefetchRange, TWQueueLimit, TwContWalkPErrDis]: Updated.
- D0F2xF4_x56[CPRdDelay]: Updated.
- D0F2xF4_x6A[IntPPROrderEn]: Updated.
- D0F2xF4_x90[CKGateL2BCacheDisable, CKGateL2BDynamicDisable, CKGateL2BMiscDisable, CKGateL2BRegsDisable]: Updated.
- D0F2xFC_x00_L1i[4:0][L1PerfCountHi0, L1PerfCountHi1, L1PerfEvent0, L1PerfEvent1]: Updated.
- D0F2xFC_x01_L1i[4:0][L1PerfCount0]: Updated.
- D0F2xFC_x02_L1i[4:0][L1PerfCount1]: Updated.
- D0F2xFC_x09_L1i[4:0] [L1_SB_LOCATION]: Updated.
- D0F2xFC_x0D_L1i[4:0][AtsNobufferInsert, L1CacheSelInterleave, L1CacheSelReqid]: Updated.
- D0F2xFC_x11_L1i[4:0][L1cachelinedis0, L1cachelinedis1]: Updated.
- D1F0x04[MasterDataPerr]: Updated.
- D1F0x50[NextPtr]: Updated.
- D1F0x64[AspmOptionalityCompliance, ClockPowerManagement, DlActiveReportingCapable, L0sExitLatency, L1ExitLatency, LinkBWNotificationCap, LinkSpeed, PMSupport, SurpriseDown-ErrReporting]: Updated.
- D1F0x68[SlotClockCfg]: Updated.
- D1F0xA0[NextPtr]: Updated.
- D1F0xA8[MsiMsgAddrHi]: Updated.
- D1F1x04[CapList, MasterDataPerr]: Updated.
- D1F1xA8[MsiMsgAddrHi]: Updated.
- D[4:2]F[5:1]x7C[CplTimeoutDisSupported, CplTimeoutRangeSupported]: Updated.
- D[4:2]F[5:1]xE4_xA2 [LC Link Width Control]: Updated.
- D18F0x1A0 [Link Initialization Status]: Updated.
- D18F0x1DC [Core Enable]: Updated.
- D18F0x68[CPURdRspPassPW]: Updated.
- D18F0x6C[ApplyIsocModeEnNow, RlsIntFullTokCntImm, RlsLnkFullTokCntImm]: Updated.
- D18F0x[E4,C4,A4,84][Addr64BitEn, IsocEn, LinkFail]: Updated.
- D18F0x[F0,D0,B0,90] [Link Base Channel Buffer Count]: Updated.
- D18F0x[F4,D4,B4,94][IsocNpReqCmd, IsocNpReqData, IsocPReq, IsocRspCmd, IsocRspData]: Updated.
- D18F1x10C [DCT Configuration Select]: Updated.
- D18F1x124[31:24]: Updated.
- D18F1x2[4C:40][DctHighAddrOffset[38:27]]: Updated.
- D18F1xF4 [VGA Enable]: Updated.
- D18F1x[1F:1E,D:C][8,0][VE]: Updated.
- D18F1x[2B:1A,B:8][8,0][Lock]: Updated.
- D18F1x[2B:1A,B:8][C,4] [MMIO Limit Low]: Updated.
- D18F2x110[MemClrInit]: Updated.
- D18F2x118 [Memory Controller Configuration Low]: Updated.
- D18F2x11C[DctWrLimit]: Updated.

- D18F2x1B4[DemandAlloWm1, DemandPropWm2, S3SmafId]: Updated.
- D18F2x208_dct[3:0]: Updated..
- D18F2x20C_dct[3:0]_mp[1:0][Tcwl]: Updated.
- D18F2x220_dct[3:0] [DDR3 DRAM Timing 7]: Updated.
- D18F2x228_dct[3:0][Tstag0]: Updated.
- D18F2x22C_dct[3:0]_mp[1:0] [DDR3 DRAM Timing 10]: Updated.
- D18F2x240_dct[3:0]_mp[1:0] [DDR3 DRAM ODT Control]: Updated.
- D18F2x244_dct[3:0][PrtlChPDDynDly]: Updated.
- D18F2x25C_dct[3:0] [DRAM Command 0]: Updated.
- D18F2x25[8,4]_dct[3:0][TgtAddress[9:0]]: Updated.
- D18F2x260_dct[3:0] [DRAM Command 1]: Updated.
- D18F2x264_dct[3:0] [DRAM Status 0]: Updated.
- D18F2x290_dct[3:0] [DRAM Status 3]: Updated.
- D18F2x2E0_dct[3:0][CurMemPstate, FastMstateDis, MxMrsEn]: Updated.
- D18F2x7C_dct[3:0][EnDramInit]: Updated.
- D18F2x90_dct[3:0][IdleCycLowLimit]: Updated.
- D18F2x94_dct[3:0] [DRAM Configuration High]: Updated.
- D18F2xA4 [DRAM Controller Temperature Throttle]: Updated.
- D18F2x[234:230]_dct[3:0] [DDR3 DRAM Read ODT Pattern [High:Low]]: Updated.
- D18F2x[23C:238]_dct[3:0] [DDR3 DRAM Write ODT Pattern [High:Low]]: Updated.
- D18F3x180 [Extended NB MCA Configuration]: Updated.
- D18F3x18C[26, 21]: Deleted.
- D18F3x1A0 [Core Interface Buffer Count]: Updated.
- D18F3x1[54,50,4C,48] [Link to XCS Token Count]: Updated.
- D18F3x40[AtomicRMWEn, CECCEn, CpPktDatEn, McaCpuDatErrEn, MstrAbortEn, NbArrayParEn, NbIntProtEn, SyncPktEn, TgtAbortEn, UECCEn, UsPwDatErrEn, WDTRptEn]: Updated.
- D18F3x44[DramEccEn]: Updated.
- D18F3x48[Syndrome[15:8]]: Update.
- D18F3x64 [Hardware Thermal Control (HTC)]: Updated.
- D18F3x68 [Software P-state Limit]: Updated.
- D18F3x70[UpReqCBC]: Updated.
- D18F3x80[NbGateEnSmafAct0]: Updated.
- D18F3xA4 [Reported Temperature Control]: Updated.
- D18F3xB8 [NB Array Address]: Updated.
- D18F3xBC_x8[EccVector]: Updated.
- D18F3xD4 [Clock Power/Timing Control 0]: Updated.
- D18F3xDC [Clock Power/Timing Control 2]: Updated.
- D18F4x118 [C-state Control 1]: Updated.
- D18F4x13C [SMU P-state Control]: Updated.
- D18F4x15C [Core Performance Boost Control]: Updated.
- D18F4x16C[CstateBoost]: Updated.
- D18F4x1C0[NodeCacLatest]: Updated.
- D18F4x250[NodeTdpLimit]: Updated.
- D18F5x128[27]: Updated.
- D18F5x128[NbFidChgCpuOpEn, PC6Vid[6:0], PllRegTime, 27]: Updated.
- D18F5x12C [Clock Power/Timing Control 4]: Updated.
- D18F5x16[C:0][NbIddDiv, NbIddValue]: Updated.
- D18F5x170[MemPstateDis, NbPstateGnbSlowDis, NbPstateHi, NbPstateHiRes, NbPstateLo, NbPstateLoRes, NbPstateThreshold]: Updated.
- D18F5x174[NbPstateReqBusy, 30:25]: Updated.
- D18F5x178[CstateThreeWayHsEn, SwGfxDis]: Updated.

- D18F5x8C[EnSrqAllocGt31]: Updated.
- Fixed missing space after register name.
- IOMMUx18[GaEn, PprLogEn, SmiFEn, SmiFLogEn]: Updated.
- IOMMUx2020[PprInt, PprRun]: Updated.
- IOMMUx2030[PprHdptr]: Updated.
- IOMMUx2038[PprTailptr]: Updated.
- IOMMUx30[GaSup, PprSup]: Updated.
- IOMMUx38[PprBase[31:12]]: Updated.
- IOMMUx3C[PprBase[51:32], PprLen]: Updated.
- IOMMUx4000 [Counter Configuration]: Updated.
- IOMMUx4[1,0][3:0]28[EventNote[31:0]]: Updated.
- IOMMUx4[1,0][3:0]2C[CERE]: Updated.
- IOMMUx50[HEO]: Updated.
- MSR0000_0411[Syndrome[7:0]]: Updated.
- MSRC000_0105[LwpCoreId]: Updated.
- MSRC001_0060 [BIST Results]: Updated.
- MSRC001_0063[CurPstate]: Updated.
- MSRC001_1002 [CPUID Features for CPUID Fn0000_0007_E[B,A]X_x0]: Updated.
- MSRC001_1003[FeaturesEcx]: Updated.
- MSRC001_1004 [CPUID Features (Features)]: Updated.
- MSRC001_1005 [Extended CPUID Features (ExtFeatures)]: Updated.
- MSRC001_1028 [Floating Point Configuration (FP_CFG)]: Updated.
- NBIOAPICx10_x01[PRQ, Version]: Updated.
- NBIOAPICx10_x[4E:10:step2][DestinationMode, TriggerMode, Vector]: Updated.
- NBIOAPICx20[InputIrq]: Updated.
- NBIOAPICx40[Vector]: Updated.
- SMMFEC0[TF]: Updated.
- SMMFED8[HostEflagsIf]: Updated.

KV BKDG Revision 3.03 Changes, Jun 17, 2014, PUB release

- 1.5 [Changes Between Revisions and Product Variations]: Updated.
- 1.5.1 [Revision Conventions]: Updated.
- 2.4.1 [Compute Unit]: Updated.
- 2.6.1.2 [NB Performance Monitor Counters]: Updated.
- 2.9.1 [Common DCT Definitions]: Updated.
- 2.9.11.1 [Chip Select Interleaving]: Updated.
- 2.10.3.1 [PROCHOT_L and Hardware Thermal Control (HTC)]: Updated.
- 2.11.4.5.2 [Dynamic Link-width Control]: Updated.
- 2.12.2 [IOMMU Initialization]: Updated.
- 2.14.2 [Frame Buffer (FB)]: Updated.
- 2.15.1.9 [Error Diagnosis]: Updated.
- CPUID Fn0000_0001_EAX[BaseFamily, BaseModel, ExtFamily, ExtModel, Stepping]: Updated.
- CPUID Fn8000_001A_EAX[FP256]: Updated.
- D0F0x64_x19: Updated.
- D0F0x64_x1A: Updated.
- D0F0x90: Updated.
- D0F0x98_x02 [ORB PGMEM Control]: Updated.
- D0F0xD4_x0109_14E1 [CC Bif Bx Strap0 Ind]: Updated.
- D0F0xD4_x0109_1507[StrapBifMemApSizePin]: Updated.
- D0F2xF4_x1C[PTCBEntries, PTCBLRUUpdatePri, PTCBParityEn, PTCBParitySupport, PTCBRe-

placementSel, PTCBSoftInvalidate, PTCBWays]: Updated.
- D0F2xF4_x20[FLTCMBCredits, QUEUECredits, QUEUEOverride]: Updated.
- D0F2xF4_x30[ERRRuleLock1]: Updated.
- D0F2xF4_x3B[FsmAddr, P1Select, PGRead, PGWrite, PowerDown, PowerUp, RegAddr]: Updated.
- D0F2xF4_x53[L2bUpdateFilterBypass, L2bUpdateFilterRdlatency]: Updated.
- D0F2xF4_x56[CPFlushOnInv, CPFlushOnWait, CPPrefetchDis]: Updated.
- D0F2xF4_x6A[IntCPOrderEn, IntEventOrderEn, IntPPROrderEn]: Updated.
- D0F2xF4_x70[DTECredits, DTEOverride, FC1Credits, FC1Override, FC2Credits, FC2Override, FC3Credits, FC3Override]: Updated.
- D0F2xF4_x71[CpPrefetchCredits, PDTIECredits, PDTIEOverride, PprMcifCredits, TWELCredits, TWELOverride]: Updated.
- D0F2xF4_x78[MCIFBaseReadCredits, MCIFBaseWriteDataCredits, MCIFBaseWriteHdrCredits, MCIFIsocReadCredits]: Updated.
- D0F2xFC[L1cfgData]: Updated.
- D0F2xFC_x00_L1i[4:0][L1PerfCountHi0, L1PerfCountHi1, L1PerfEvent0, L1PerfEvent1]: Updated.
- D0F2xFC_x01_L1i[4:0][L1PerfCount0]: Updated.
- D0F2xFC_x02_L1i[4:0][L1PerfCount1]: Updated.
- D0F2xFC_x0D_L1i[4:0][AtsNobufferInsert, CacheByPass, L1CacheInvAllEn, L1CacheParityEn, L1CacheSelInterleave, L1CacheSelReqid, L1DTEDis, L1orderEn, PretransNovaFilteren, SndFilterDis, Untrans2mFilteren, VOQPortBits, WqEntrydis, 31:30]: Updated.
- D0F2xFC_x0F_L1i[4:0][AtsTlbinvPulseWidth]: Updated.
- D0F2xFC_x10_L1i[4:0][L1cachebanksel0]: Updated.
- D0F2xFC_x11_L1i[4:0][L1cachelinedis0, L1cachelinedis1]: Updated.
- D0F2xFC_x23_L1i[4:0][InvalidationStatus]: Updated.
- D1F0x00 [Device/Vendor ID]: Updated.
- D1F0x50[D1Support, D2Support]: Updated.
- D1F1x00 [Device/Vendor ID]: Updated.
- D1F1x50[D1Support, D2Support]: Updated.
- D1F1x54 [Power Management Control and Status]: Updated.
- D[4:2]F[5:1]x78[PmeStatus]: Updated.
- D[4:2]F[5:1]x7C[ExtendedFmtFieldSupported]: Updated.
- D[4:2]F[5:1]x88[ComplianceDeemphasis]: Updated.
- D[4:2]F[5:1]xE4_xA4 [LC Link Speed Control]: Updated.
- D18F0x6C[InitDet]: Updated.
- D18F0x[11C,118,114,110][ClumpEn]: Updated.
- D18F2x118[McqMedPriByPassMax]: Updated.
- D18F2x1BC_dct[3:0] [DRAM CKE to CS Map]: Updated.
- D18F2x228_dct[3:0][Tstag0]: Updated.
- D18F2x248_dct[3:0]_mp[1:0][30, 31]: Updated.
- D18F2x90_dct[3:0][UnbuffDimm]: Updated.
- D18F2xA4: Updated.
- D18F2xB64_dct[3:0][DatScrambleKey]: Updated.
- D18F3x1A0 [Core Interface Buffer Count]: Updated.
- D18F3x34: Updated.
- D18F3x34[CapPtr]: Updated.
- D18F3x4C[MiscV]: Updated.
- D18F3xF0 - D18F3xF8: Added.
- D18F3xF4 [DEV Function Register]: Updated.
- D18F3xF8_x4: Added.
- D18F4x118 [C-state Control 1]: Updated.
- D18F4x218: Updated.

- D18F5x240 [ECC Exclusion Base Address Low]: Updated.
- D18F5x[78,68,58,48] [Northbridge Performance Event Counter Low]: Updated.
- D18F5x[7C,6C,5C,4C] [Northbridge Performance Event Counter High]: Updated.
- IOMMUx18[PassPw]: Updated.
- IOMMUx2020[EventLogRun, PprRun]: Updated.
- IOMMUx50[HEO]: Updated.
- IOMMUx[78,70,68,60][SMIDV, SMIDid, SMIFlock]: Updated.
- MSR0000_002A [Cluster ID (EBL_CR_POWERON)]: Updated.
- MSR0000_0411[MiscV]: Updated.MSR0000_0413[CntEn, CntP, ErrCnt, IntType, Locked, LvtOffset, Ovrflw, Valid]: Updated.
- MSRC000_0408[CntEn, CntP, ErrCnt, IntType, Locked, LvtOffset, Ovrflw, Valid]: Updated.
- MSRC001_011A[Alias of SMMFEC4 [Local SMI Status].]: Updated.
- MSRC001_024[7,5,3,1] [Northbridge Performance Event Counter (NB_PERF_CTR[3:0])]: Updated.
- MSRC001_024[7,5,3,1] [Northbridge Performance Event Counter (NB_PERF_CTR[3:0])]: Updated.

KV BKDG Revision 3.02 Changes, Mar 5, 2014, PUB release

- 2.9.1 [Common DCT Definitions]: Updated.
- D0F0x84[7:4]: Updated.
- D0F0x90[22:0]: Updated.
- D0F0xCC_x01_ib[21,1D:19,12:11][15:4]: Updated.
- D0F0xFC_x00[31:5]: Updated.
- D18F2xA4 [DRAM Controller Temperature Throttle]: Updated.
- D18F3xDC[CacheFlushOnHaltCtl]: Updated.
- D18F5x194[Index]: Updated.
- D18F5x194[Index]: Updated.
- MSRC001_0070 [COFVID Control]: Updated.
- MSRC001_102A[L2UpsizeCUCT, L2UpsizeERT]: Updated.

KV BKDG Revision 3.01 Changes, Feb 19, 2014, PUB release

- 1.4 [Definitions]: Updated.
- 1.5.2 [Major Changes]: Updated.
- 2.8.2.1.3.1 [Recommended Buffer Count Settings Overview]: Updated.
- 2.9.1 [Common DCT Definitions]: Updated.
- 2.10.3.1 [PROCHOT_L and Hardware Thermal Control (HTC)]: Updated.
- 2.11.2.1 [IOAPIC Configuration]: Updated.
- 2.11.4.5.2 [Dynamic Link-width Control]: Updated.
- 2.12.2.3 [IOMMU SMI Filtering]: Updated.
- 2.14.2 [Frame Buffer (FB)]: Updated.
- 2.15.1.3.2 [Error Logging During Overflow]: Updated.
- 2.15.1.9.1 [Common Diagnosis Information]: Updated.
- APIC300[DS]: Updated.
- D0F0x60[MiscIndAddr]: Updated.
- D0F0x94[OrbIndAddr]: Updated.
- D0F0xB8[NbSmuIndAddr]: Updated.
- D0F0xBC[NbSmuIndData]: Updated.
- D0F0xCC[NbDevIndData]: Updated.
- D0F0xD0[NbGbifIndAddr]: Updated.
- D0F0xD4[NbGbifIndData]: Updated.
- D0F2x70[NxSupW]: Updated.

- D18F0x[F0,D0,B0,90] [Link Base Channel Buffer Count]: Updated.
- D18F2xB68_dct[3:0]_nbp[3:0]: Corrected.
- D18F3x160 [NB Machine Check Misc (DRAM Thresholding) 0 (MC4_MISC0)]: Updated.
- D18F3x[84:80]: Updated. Fixed Rule.
- D18F5x16[C:0][NbDid]: Updated.
- D18F5x194[Index]: Updated.
- D18F5x198[Data]: Updated.
- IFCM: Updated.
- IOMMU: Updated.
- MSRC001_0070 [COFVID Control]: Updated.
- Table 48: Updated.

KV BKDG Revision 3.00 Changes, Jan 10, 2014, PUB release

1 Overview

This document defines AMD Family 15h Models 30h-3Fh Processors, henceforth referred to as the processor.

- The processor overview is located at 2.1 [Processor Overview].
- The processor is distinguished by the combined ExtFamily and BaseFamily fields of the CPUID instruction (see CPUID Fn8000_0001_EAX in 3.18 [CPUID Instruction Registers]).

1.1 Intended Audience

This document provides the processor behavioral definition and associated design notes. It is intended for platform designers and for programmers involved in the development of low-level BIOS (basic input/output system) functions, drivers, and operating system kernel modules. It assumes prior experience in personal computer platform design, microprocessor programming, and legacy x86 and AMD64 microprocessor architecture. The reader should also have familiarity with various platform technologies, such as DDR DRAM.

1.2 Reference Documents

- Advanced Configuration and Power Interface (ACPI) Specification. www.acpi.info.
- AMD64 Architecture Programmer's Manual Volume 1: Application Programming, #24592.
- AMD64 Architecture Programmer's Manual Volume 2: System Programming, #24593.
- AMD64 Architecture Programmer's Manual Volume 3: Instruction-Set Reference, #24594.
- AMD64 Architecture Programmer's Manual Volume 4: 128-Bit and 256-Bit Media Instructions, #26568.
- AMD64 Architecture Programmer's Manual Volume 5: 64-Bit Media and x87 Floating-Point Instructions, #26569.
- AMD I/O Virtualization Technology™ (IOMMU) Specification, #34434.
- Software Optimization Guide for AMD Family 15h Processors, #47414.
- Revision Guide for AMD Family 15h Models 30h-3Fh Processors, #51603.
- JEDEC standards. www.jedec.org.
- PCI local bus specification. (www.pcisig.org).
- PCI Express® specification. (www.pcisig.org).
- AMD64 Technology Lightweight Profiling Specification, #43724.

1.3 Conventions

1.3.1 Numbering

- **Binary numbers**. Binary numbers are indicated by appending a “b” at the end, e.g., 0110b.
- **Decimal numbers**. Unless specified otherwise, all numbers are decimal. This rule does not apply to the register mnemonics described in 3.1 [Register Descriptions and Mnemonics]; register mnemonics all utilize hexadecimal numbering.
- **Hexadecimal numbers**. hexadecimal numbers are indicated by appending an “h” to the end, e.g., 45f8h.
- **Underscores in numbers**. Underscores are used to break up numbers to make them more readable. They do not imply any operation. E.g., 0110_1100b.

1.3.2 Arithmetic And Logical Operators

In this document, formulas generally follow Verilog conventions for logic equations.

Table 1: Arithmetic and Logical Operators

Operator	Definition
{}	Concatenation. Curly brackets are used to indicate a group of bits that are concatenated together. Each set of bits is separated by a comma. E.g., {Addr[3:2], Xlate[3:0]} represents a 6-bit value; the two MSBs are Addr[3:2] and the four LSBs are Xlate[3:0].
|	Bitwise OR. E.g. (01b | 10b == 11b).
||	Logical OR. E.g. (01b || 10b == 1b); treats multibit operand as 1 if >=1 and produces a 1-bit result.
&	Bitwise AND. E.g. (01b & 10b == 00b).
&&	Logical AND. E.g. (01b && 10b == 1b); bgical treats multibit operand as 1 if >=1 and produces a 1-bit result.
^	Bitwise exclusive-OR. E.g. (01b ^ 10b == 11b). Sometimes used as "raised to the power of" as well, as indicated by the context in which it is used. E.g. (2^2 == 4).
~	Bitwise NOT. (also known as one's complement). E.g. (~10b == 01b).
!	Logical NOT. E.g. (!10b == 0b); treats multibit operand as 1 if >=1 and produces a 1-bit result.
<, <=, >, >=, ==, !=	Relational. Less than, Less than or equal, greater, greater than or equal, equal, and not equal.
+, -, *, /, %	Arithmetic. Addition, subtraction, multiplication, division, and modulus.
<<	Bitwise left shift. Shift left first operand by the number of bits specified by the 2nd operand. E.g. (01b << 01b == 10b).
>>	Bitwise right shift. Shift right first operand by the number of bits specified by the 2nd operand. E.g. (10b >> 01b == 01b).
?:	Ternary conditional. E.g. *condition* ? *value if true* : *value if false*. Equivalent to IF *condition* THEN *value if true* ELSE *value if false*.

Table 2: Functions

Function	Definition
ABS	ABS(integer-expression): Remove sign from signed value.
FLOOR	FLOOR(integer-expression): Rounds real number down to nearest integer.
CEIL	CEIL(real-expression): Rounds real number up to nearest integer.
MIN	MIN(integer-expression-list): Picks minimum integer or real value of comma separated list.
MAX	MAX(integer-expression-list): Picks maximum integer or real value of comma separated list.
COUNT	COUNT(integer-expression): Returns the number of binary 1's in the integer.

Table 2: Functions

Function	Definition
ROUND	ROUND(real-expression): Rounds to the nearest integer; halfway rounds away from zero.
UNIT	UNIT(fieldName UnitOfMeasure): Input operand is a register field name that defines all values with the same unit of measure. Returns the value expressed in the unit of measure for the current value of the register field.
POW	POW(base, exponent): POW(x,y) returns the value x to the power of y.

1.3.3 Operator Precedence and Associativity

This document follows C operator precedence and associativity. The following table lists operator precedence (highest to lowest). Their associativity indicates in what order operators of equal precedence in an expression are applied. Parentheses are also used to group sub-expressions to force a different precedence; such parenthetical expressions can be nested and are evaluated from inner to outer. E.g. “X = A | ~B & C” is the same as “X= A | ((~B) & C)”.

Table 3: Operator Precedence and Associativity

Operator	Description	Associativity
!, ~	Logical negation/bitwise complement	right-to-left
*, /, %	Multiplication/division/modulus	left-to-right
+, -	Addition/subtraction	left-to-right
<<, >>	Bitwise shift left, Bitwise shift right	left-to-right
< , <=, >, >=, ==, !=	Relational operators	left-to-right
&	Bitwise AND	left-to-right
^	Bitwise exclusive OR	left-to-right
|	Bitwise inclusive OR	left-to-right
&&	Logical AND	left-to-right
||	Logical OR	left-to-right
?:	Ternary conditional	right-to-left

1.4 Definitions

Table 4: Definitions

Term	Definition
AP	Application processor. See 2.3 [Processor Initialization].
BAPM	Bidirectional Application Power Management. See 2.5.9.3 [Bidirectional Application Power Management (BAPM)].
Battery-Power	The system is running from a battery power source or otherwise undocked from a continuous power supply. Setting using this definition may be required to change during runtime.
BCS	Base configuration space. See 2.7 [Configuration Space].

Table 4: Definitions

Term	Definition
BERT	Bit error rate tester. A piece of test equipment that generates arbitrary test patterns and checks that a device under test returns them without errors.
BIST	Built-in self-test. Hardware within the processor that generates test patterns and verifies that they are stored correctly (in the case of memories) or received without error (in the case of links).
Boot VID	Boot voltage ID. This is the VDD and VDDNB voltage level that the processor requests from the external voltage regulator during the initial phase of the cold boot sequence. See 2.5.1.2 [Internal VID Registers and Encodings].
BCD	Binary coded decimal number format.
BSC	Boot strap core. Core 0 of the BSP. Specified by MSR0000_001B[BSC].
BSP	Boot strap processor. See 2.3 [Processor Initialization].
CAR	Use of the L2 cache as RAM during boot. See 2.3.3 [Using L2 Cache as General Storage During Boot].
C-states	These are ACPI-defined core power states. C0 is operational. All other C-states are low-power states in which the processor is not executing code. See 2.5.3.2 [Core C-states].
Canonical address	An address in which the state of the most-significant implemented bit is duplicated in all the remaining higher-order bits, up to bit 63.
Channel	See DRAM channel.
Channel interleaved mode	Mode in which DRAM address space is interleaved between DRAM channels. See 2.9.11 [Memory Interleaving Modes].
CMP	Chip multi-processing. Refers to processors that include multiple cores. See 2.1 [Processor Overview].
COF	Current operating frequency of a given clock domain. See 2.5.3 [CPU Power Management].
Cold reset	PWROK is deasserted and RESET_L is asserted. See 2.3 [Processor Initialization].
Compute Unit	Two Cores that share IC, DE, FP and L2 resources. See 2.1 [Processor Overview].
Core	The instruction execution unit of the processor. See 2.1 [Processor Overview].
CPB	Core performance boost. See 2.5.9.1 [Core Performance Boost (CPB)].
CpuCoreNum	Specifies the core number. See 2.4.4 [Processor Cores and Downcoring].
CPUID function X	Refers to the CPUID instruction when EAX is preloaded with X. See 3.18 [CPUID Instruction Registers].
CS	Chip select. See D18F2x[5C:40]_dct[3:0] [DRAM CS Base Address].
DCT	DRAM controller. See 2.9 [DRAM Controllers (DCTs)].
DCQ	DRAM controller queue.
DDR3	DDR3 memory technology. See 2.9 [DRAM Controllers (DCTs)].
DID	Divisor identifier. Specifies the post-PLL divisor used to reduce the COF. See 2.5.3 [CPU Power Management].
Doubleword	A 32-bit value.
Downcoring	Removal of cores. See 2.4.4 [Processor Cores and Downcoring].

Table 4: Definitions

Term	Definition
DRAM channel	The part of the DRAM interface that connects to a DIMM. See 2.9 [DRAM Controllers (DCTs)].
Dual-Plane	Refers to a processor or system board where VDD and VDDNB are separate and may operate at independent voltage levels. Refer to 2.5.1 [Processor Power Planes And Voltage Control].
DW	Doubleword. A 32-bit value.
ECS	Extended configuration space. See 2.7 [Configuration Space].
EDS	Electrical data sheet. See 1.2 [Reference Documents].
EFLAGS	See AMD64 Architecture Programmer's Manual Volume 2: System Programming, #24593, section 3.1.6 RFLAGS register, as the legacy EFLAGS register is identical to the low 32 bits of this register.
FCH	Fusion Controller Hub. The platform device that contains the bridge to the system BIOS.
FDS	Functional data sheet; there is one FDS for each package type.
FID	Frequency identifier. Specifies the PLL frequency multiplier for a given clock domain. See 2.5.3 [CPU Power Management].
FreeRunSampleTimer	An internal free running timer used by many power management features. The timer increments at the rate specified by D18F4x110[CSampleTimer].
GB	Gbyte or Gigabyte; 1,073,741,824 bytes.
#GP	A general-protection exception.
#GP(0)	Notation indicating a general-protection exception (#GP) with error code of 0.
GpuEnabled	GpuEnabled = (D1F0x00!=FFFF_FFFFh).
GT/s	Giga-transfers per second.
HCD	Host Controller Driver. A software component.
HTC	Hardware thermal control. See 2.10.3.1 [PROCHOT_L and Hardware Thermal Control (HTC)].
HTC-active state	Hardware-controlled lower-power, lower-performance state used to reduce temperature. See 2.10.3.1 [PROCHOT_L and Hardware Thermal Control (HTC)].
IBS	Instruction based sampling. See 2.6.2 [Instruction Based Sampling (IBS)].
IFCM	Isochronous flow-control mode, as defined in the link specification.
ILM	Internal loopback mode. Mode in which the link receive lanes are connected directly to the transmit lanes of the same link for testing and characterization. See D18F0x[18C:170] [Link Extended Control].
IO configuration	Access to configuration space through IO ports CF8h and CFCh. See 2.7 [Configuration Space].
IORR	IO range register. See MSRC001_00[18,16] [IO Range Base (IORR_BASE[1:0])].
IOMMU	I/O Memory Management Unit. Also known as AMD Virtualization™ Technology.
KB	Kbyte or Kilobyte; 1024 bytes.
L1 cache	The level 1 caches (instruction cache and the data cache) and the level 2 caches. See 2.1 [Processor Overview].
L2 cache	
Linear (virtual) address	The address generated by a core after the segment is applied.

Table 4: Definitions

Term	Definition
Link	Generic term that refers to a refer to PCIe® link.
LINT	Local interrupt.
Logical address	The address generated by a core before the segment is applied.
LVT	Local vector table. A collection of APIC registers that define interrupts for local events. E.g., APIC[530:500] [Extended Interrupt [3:0] Local Vector Table].
Master abort	This is a PCI-defined term that is applied to transactions on other than PCI buses. It indicates that the transaction is terminated without affecting the intended target; reads return all 1's; writes are discarded; the master abort error code is returned in the response, if applicable; master abort error bits are set if applicable.
MB	Megabyte; 1024 KB.
MCT	Memory controller. See 2.8 [Northbridge (NB)].
MCQ	Memory controller queue. See 2.8 [Northbridge (NB)].
Micro-op	Micro-op. Instructions have variable-length encoding and many perform multiple primitive operations. The processor does not execute these complex instructions directly, but, instead, decodes them internally into simpler fixed-length instructions called macro-ops. Processor schedulers subsequently break down macro-ops into sequences of even simpler instructions called micro-ops, each of which specifies a single primitive operation. See *Software Optimization Guide for AMD Family 15h Processors*.
MEMCLK	Refers to the clock signals, M[B, A][3:0]_CLK, that are driven from the processor to DDR DIMMs.
MMIO	Memory-mapped input-output range. This is physical address space that is mapped to the IO functions such as the IO links or MMIO configuration. The IO link MMIO ranges are specified by D18F1x[2CC:2A0,1CC:180,BC:80] [MMIO Base/Limit].
MMIO configuration	Access to configuration space through memory space. See 2.7 [Configuration Space].
MSR	Model-specific register. The core includes several MSRs for general configuration and control. See 3.19 [MSRs - MSR0000_xxxx] for the beginning of the MSR register definitions.
MTRR	Memory-type range register. The MTRRs specify the type of memory associated with various memory ranges. See MSR0000_00FE, MSR0000_020[F:0], MSR0000_02[6F:68,59:58,50], and MSR0000_02FF.
NB	Northbridge. The transaction routing block of the node. See 2.1 [Processor Overview].
NBC	NBC = (CPUID Fn0000_0001_EBX[LocalApicId[3:0]]==0). Node Base Core. The lowest numbered core in the node.
NBPMC	Performance monitor counter. See 2.6.1.2 [NB Performance Monitor Counters].
NCLK	The main northbridge clock. The NCLK frequency is the NB COF.
Node	See 2.1 [Processor Overview].
Normalized address	Addresses used by DCTs. See 2.8 [Northbridge (NB)].
OW	Octoword. An 128-bit value.
ODM	On-DIMM mirroring. See D18F2x[5C:40]_dct[3:0][OnDimmMirror].
ODT	On-die termination, which is applied DRAM interface signals.
ODTS	DRAM On-die thermal sensor.

Table 4: Definitions

Term	Definition
Operational frequency	The frequency at which the processor operates. See 2.5 [Power Management].
PCIe®	PCI Express®.
PDS	Product data sheet.
Physical address	Addresses used by cores in transactions sent to the NB.
PMC	Performance monitor counter. See 2.6.1.1 [Core Performance Monitor Counters].
PRBS	Pseudo-random bit sequence.
Processor	See 2.1 [Processor Overview].
PSI	Power Status Indicator. See 2.5.1.3.1 [PSIx_L Bit].
P-state	Performance state. See 2.5 [Power Management].
PTE	Page table entry.
QW	Quadword. A 64-bit value.
RAS	Reliability, availability and serviceability (industry term). See 2.15.1 [Machine Check Architecture].
RDQ	Read data queue.
REFCLK	Reference Clock, refers to the clock frequency (100 MHz) or the clock period (10 ns) depending on the context used.
RX	Receiver.
Scrubber	Background memory checking logic. See 2.8.3 [Memory Scrubbers].
Shutdown	A state in which the affected core waits for either INIT, RESET, or NMI. When shutdown state is entered, a shutdown special cycle is sent on the IO links.
Single-Plane	Refers to a processor or system board where VDD and VDDNB are tied together and operate at the same voltage level. Refer to 2.5.1 [Processor Power Planes And Voltage Control].
Slam	Refers to changing the voltage to a new value in one step (as opposed to stepping). See 2.5.1.4.1 [Hardware-Initiated Voltage Transitions].
SMAF	System management action field. This is the code passed from the SMC to the processors in STPCLK assertion messages. The action taken by the processors in response to this message is specified by D18F3x[84:80] [ACPI Power State Control].
SMBus	System management bus. Refers to the protocol on which the serial VID interface (SVI) commands are based. See 2.5.1 [Processor Power Planes And Voltage Control], and 1.2 [Reference Documents].
SMC	System management controller. This is the platform device that communicates system management state information to the processor through an IO link, typically the system IO hub.
SMI	System management interrupt. See 2.4.9.2.1 [SMM Overview].
SMM	System management mode. See 2.4.9.2 [System Management Mode (SMM)].
Speculative event	A performance monitor event counter that counts all occurrences of the event even if the event occurs during speculative code execution.
SVI2	Serial VID 2.0 interface. See 2.5.1.1 [Serial VID Interface].
SVM	Secure virtual machine. See 2.4.10 [Secure Virtual Machine Mode (SVM)].

Table 4: Definitions

Term	Definition
Sync flood	The propagation of continuous sync packets to all links. This is used to quickly stop the transmission of potentially bad data when there are no other means to do so. See the link specification for additional information.
TCC	Temperature calculation circuit. See 2.10 [Thermal Functions].
Tctl	Processor temperature control value. See 2.10.3 [Temperature-Driven Logic].
TDC	Thermal design current. See the AMD Infrastructure Roadmap, #41482.
TDP	Thermal design power. A power consumption parameter that is used in conjunction with thermal specifications to design appropriate cooling solutions for the processor. See 2.5.9.2 [TDP Limiting].
Token	A scheduler entry used in various northbridge queues to track outstanding requests. See D18F3x140 [SRI to XCS Token Count].
TX	Transmitter.
UI	Unit interval. This is the amount of time equal to one half of a clock cycle.
UMI	Unified Media Interface. The link between the processor and the FCH.
VDD	Main power supply to the processor core logic.
VDDNB	Main power supply to the processor NB logic.
VID	Voltage level identifier. See 2.5.1 [Processor Power Planes And Voltage Control].
Virtual CAS	The clock in which CAS is asserted for the burst, N, plus the burst length (in MEMCLKs), minus 1; so the last clock of virtual CAS = N + (BL/2) - 1.
VRM	Voltage regulator module.
W	Word. A 16-bit value.
Warm reset	RESET_L is asserted only (while PWROK stays high). See 2.3 [Processor Initialization].
WDT	Watchdog timer. A timer that detects activity and triggers an error if a specified period of time expires without the activity. For example, see MSRC001_0074 [CPU Watchdog Timer (CpuWdtCfg)] or the NB watchdog timer in D18F3x40 [MCA NB Control].
WDQ	Write data queue.
XBAR	Cross bar; command packet switch. See 2.8 [Northbridge (NB)].

1.5 Changes Between Revisions and Product Variations

Feature support varies by brands and OPNs. To determine the features supported by your processor, contact your customer representative.

1.5.1 Revision Conventions

The processor revision is specified by CPUID Fn0000_0001_EAX [Family, Model, Stepping Identifiers] or CPUID Fn8000_0001_EAX [Family, Model, Stepping Identifiers]. This document uses a revision letter instead of specific model numbers. The following table contains the definitions based on model and stepping used in this document. Where applicable, the processor stepping is indicated after the revision letter. All behavior marked with a revision letter apply to future revisions unless they are superseded by a change in a later revision. See the revision guide for additional information about revision determination. See 1.2 [Reference Documents].

Table 5: Processor revision conventions

Term	Definition
PROC	PROC = {CPUID Fn0000_0001_EAX[ExtFamily], CPUID Fn0000_0001_EAX[ExtModel], CPUID Fn0000_0001_EAX[BaseModel], CPUID Fn0000_0001_EAX[Stepping]}.
KV_A1	KV_A1 = {06h,3h,0h,1h}.

1.5.2 Major Changes

This section describes the major changes relative to Family 15h Models 10h-1Fh Processors.

- CPU core changes:
  - Architectural changes:
    - XSAVEOPT: Added XSAVE optimization. Reported by CPUID Fn0000_000D_EAX_x1[XSAVE-OPT].
    - PTSC: Added "Performance Time Stamp Counter" that is a synchronized value across all cores and the GPU. Used by LWP. See MSRC001_0280. Reported by CPUID Fn8000_0001_ECX[PerfTsc] and CPUID Fn8000_0008_ECX[PerfTscSize].
    - DataBreakpointExtension: Added debug breakpoint address matching enhancement. See CPUID Fn8000_0001_ECX[DataBreakpointExtension], MSRC001_1027[31:12], and MSRC001_101[B:9].
    - LWP: Added LWP support for Global Timestamp Counter and Continuous Wrapping Mode. See CPUID Fn8000_001C_EAX[LwpPTSC, LwpCont], MSRC000_0105[LwpPTSC, LwpCont], CPUID Fn8000_001C_EDX[LwpPTSC, LwpCont].
    - PCID: Added software ASID support. Reported by CPUID Fn0000_0001_ECX[PCID].
    - FSGSBASE: Add ability for user code to write FS and GS segments. This facilitates user mode scheduling of threads. Reported by CPUID Fn0000_0007_EBX_x0[FSGSBASE].
  - IPC changes:
    - Store to load forwarding optimization.
    - Dispatch and retire up to 2 stores per cycle.
    - Improved memfile, from last 3 stores to last 8 stores, and allow tracking of dependent stack operations.
    - Load queue (LDQ) size increased to 48, from 44.
    - Store queue (STQ) size increased to 32, from 24.
    - Increase dispatch bandwidth to 8 INT ops per cycle (4 to each core), from 4 INT ops per cycle (4 to just 1 core). 4 ops per cycle per core remains unchanged.
    - Accelerate SYSCALL/SYSRET.
    - Increased L2 BTB size from 5K to 10K and from 8 to 16 banks.
    - Added L2 BTB extended target array. Provides full physical address when relative address is insufficient.
    - Improved branch prediction.
    - Improved loop prediction.
    - Increase PFB from 8 to 16 entries; the 8 additional entries can be used either for prefetch or as a loop buffer.
    - Increase snoop tag throughput.
    - Change from 4 to 3 FP pipe stages.
  - MSR Changes:
- Cache changes:
  - IC: Increased from 64 KB (2-way) to 96 KB (3-way).
- TLB changes:

- Memory controller changes:
- Links and IO changes:
- RAS-related changes:
  - L2 single bit errors corrected in array; L2 single bit errors corrected previously only corrected/poisoned to requestor, leaving single bit error in array.
- Northbridge changes:
- Power management changes:
  - Dynamic L2 Power Gating. Reduce L2 leakage by reducing the number of L2 ways on C6 exit according to usage.
- Core/NB performance counter changes:
  - Increase Onion Bandwidth. Double to 32Byte width in each direction.
  - Add coherency for FSA. Add FSA 0.85 support.
    - Add second onion bus
    - Support for PCIe® and OpenCL™ atomics:
    - Configuration bit to enable command throttling on onion
  - Add support for GNB DSM
    - Incorporate StopClocks from GNB:
    - Incorporate Cross Triggers from GNB:
    - Incorporate SelfRefresh, HTReceiveDisable from GNB
  - Bandwidth Improvements
    - Local probe responses bypass SRQ -> MCT
    - Send SrcDone based on TgtDone
    - Two commands per clock from MCT/XBR -> SRQ
    - Two commands per clock from SRI -> MCQ; MCQ can sink two responses/clk
    - SRQ/SRA/SRD +16 (see SRQ Changes)
    - MCQ +16
    - LCS/LPS +16
    - Improve write holding register bandwidth
  - Supply DRAM utilization as a frequency sensitivity hint to the OS
  - Memory parking performance counters. Over time shift traffic from all channels to one channel.
  - Add onion bus.
  - Add PCIe® endpoint mode.
  - 2 or 3 core-pairs Add 3 CU support.
  - Buffer size changes
  - SMU Pstate Control

1.5.2.1 Major Changes to Core/NB Performance Counters

Major Changes to Core/NB Performance Counters:

- Core performance counters:
  - PMCx000[7,3]: Changed to reserved; Removed pipe 3.
  - PMCx042 [Data Cache Refills from L2 or System]: Added [4].
  - PMCx060, PMCx061[5:0], PMCx062, PMCx063, PMCx064: Added.
  - PMCx186 [Uops Dispatched From Decoder]: Added.
  - PMCx0D1, PMCx0D5-PMCx0D8, PMCx1D8, PMCx1DD-PMCx1DE: These events count even when dispatch selects the other core of the compute-unit.
  - PMCx1D0 [Retired Fused Branch Instructions]: Added.
  - PMCx1DF [FP Dispatch Contention]: Changed.

2 Functional Description

2.1 Processor Overview

The *processor* is defined as follows:
- The processor is a package that contains one node.
- Supports x86-based instruction sets.
- Packages:
  - FM2r2: Desktop Package.
  - FP3: Notebook Package.
  - See CPUID Fn8000_0001_EBX[PkgType].
- Compute Unit
  - 2 cores per compute unit. Up to 2 compute units.
  - 2 MB L2
  - See 2.4.1 [Compute Unit].
- DRAM:
  - Configurable to two 64-bit DDR3 memory channels (A, B). See Figure 2 [A processor].
  - ECC: Yes.
  - Max speed: 2133 MT/s (1.5V).
  - See 2.9.2 for voltage control affecting DRAM speed.
- Northbridge:
  - One communication packet routing block referred to as the northbridge (NB). The NB routes transactions between the cores, the link, and the DRAM interfaces. It includes the configuration register space for the device.
- Graphics northbridge:
  - Links:
    - PCIe® Gen3 on Gfx link, PCIe® Gen2 on the GPP links and PCIe® Gen2 on the UMI link.
    - Gfx lanes: One x16, GPP lanes: One x4, UMI lanes: One x4.
    - See 2.11.3 [Links].
    - See 2.11.3.1 for voltage control affecting data rate of the Gfx link.
- Power Management:
  - See 2.5 [Power Management].
- RAS:
  - See 2.15 [RAS Features].

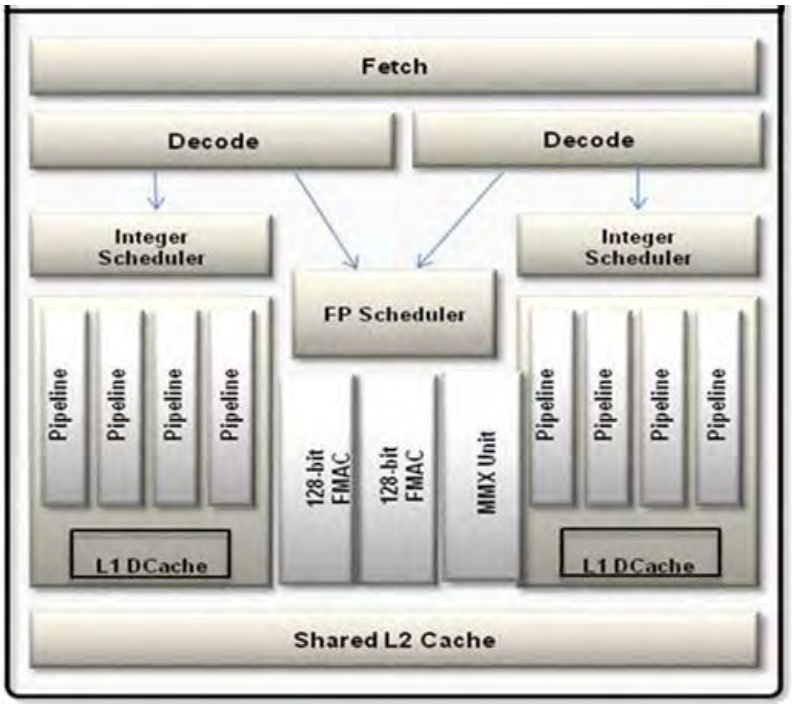

Figure 1: A Compute Unit

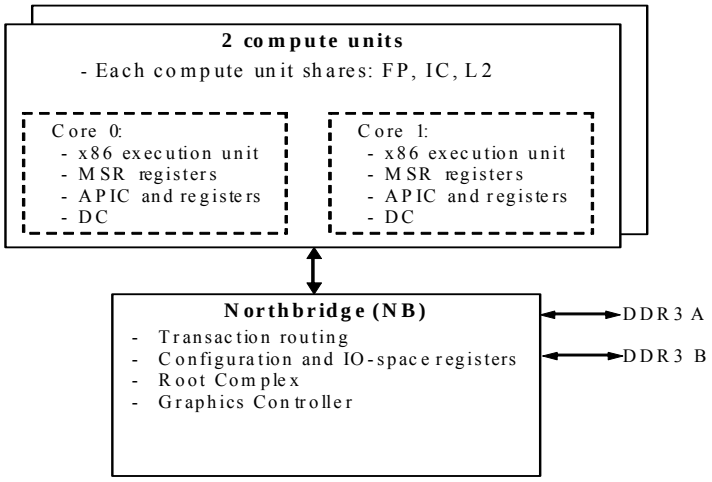

Figure 2: A processor

2.2 System Overview

2.3 Processor Initialization

This section describes the initialization sequence after a cold reset.

Core 0 of the processor, the bootstrap core (BSC), begins executing code from the reset vector. The remaining cores do not fetch code until their enable bits are set (D18F0x1DC[CpuEn]).

2.3.1 BSC Initialization

The BSC must perform the following tasks as part of boot.

- Store BIST information from the EAX register into an unused processor register.
- D18F0x6C[InitDet] may be used by BIOS to differentiate between INIT and cold/warm reset.
- Determine type of startup using D18F0x6C[ColdRstDet].
  - If this is a warm reset then BIOS may check for valid MCA errors and if present save the status for later use. See 2.15.1.6 [Handling Machine Check Exceptions].
- Enable the cache, program the MTRRs for CAR and initialize CAR. See 2.3.3 [Using L2 Cache as General Storage During Boot].
- Setup the SMU.
- Setup of APIC (2.4.9.1.3 [ApicId Enumeration Requirements]).
- Setup the link configuration.
- Setup the root complex and initialize the I/O links.
- If required, reallocate data and flow control buffers of the links (see D18F0x[F0,D0,B0,90] [Link Base Channel Buffer Count] and D18F0x[F4,D4,B4,94] [Link Isochronous Channel Buffer Count]).
- Issue system warm reset.
- Configure the DRAM controllers.
- Configure processor power management. See 2.5 [Power Management].
- Allow other cores to begin fetching instructions by setting D18F0x1DC[CpuEn] in the PCI configuration space of all nodes. See 2.4.4 [Processor Cores and Downcoring].

2.3.2 AP Initialization

All other processor cores other than core 0 begin executing code from the reset vector. They must perform the following tasks as part of boot.

- Store BIST information from the eax register into an unused processor register.
- D18F0x6C[InitDet] may be used by BIOS to differentiate between INIT and cold/warm reset.
- Determine the history of this reset using the D18F0x6C [Link Initialization Control] [ColdRstDet] bit:
  - If this is a warm reset then BIOS may check for valid MCA errors and if present save the status for use later. See 2.15.1.6 [Handling Machine Check Exceptions].
- Set up the local APIC. See 2.4.9.1.3 [ApicId Enumeration Requirements].
- Configure processor power management. See 2.4 [Core].

2.3.3 Using L2 Cache as General Storage During Boot

Prior to initializing the DRAM controller for system memory, BIOS may use the L2 cache of each core as general storage.

The L2 cache as general storage is described as follows:
- Each Compute Unit has its own L2 cache.
- BIOS manages the mapping of the L2 storage such that cacheable accesses do not cause L2 victims.
- The L2 size, L2 associativity, and L2 line size is determined by reading CPUID Fn8000_0006_ECX[L2Size, L2Assoc, L2LineSize]. L2WayNum is defined to be the number of ways indicated by the L2Assoc code.
  - The L2 cache is viewed as (L2Size/L2LineSize) cache lines of storage, organized as L2WayNum ways, each way being (L2Size/L2WayNum) in size.
    - E.g. L2Assoc=8 so L2WayNum=16 (there are 16 ways). If (L2Size=2MB) then there are 16 blocks of cache, each 2MB/16 in size, or 128KB each.
  - For each of the following values of L2Size, the following values are defined:

    - L2Size=1 MB: L2Tag=PhysAddr[39:16], L2WayIndex=PhysAddr[15:6].
    - L2Size=2 MB: L2Tag=PhysAddr[39:17], L2WayIndex=PhysAddr[16:6].
  - PhysAddr[5:0] addresses the L2LineSize number of bytes of storage associated with the cache line.
  - The L2 cache, when allocating a line at L2WayIndex:
    - Picks an invalid way before picking a valid way.
    - Prioritizes the picking of invalid ways such that way L2WayNum-1 is the highest priority and 0 is the lowest priority.
  - It is recommended that BIOS assume a simpler allocation of L2 cache memory, being L2WayNum size-aligned blocks of memory, each being L2Size/L2WayNum bytes.
  - BIOS can rely on a minimum L2Size of 256 KB and can rely on being able to use a minimum of 14 ways for general storage. See CPUID Fn8000_0006_ECX[L2Size]. See initialization requirements below for MSRC001_1023[L2WayLock, L2FirstLockedWay].

The following memory types are supported:

  - WP-IO: BIOS ROM may be assigned the write-protect IO memory type and may be accessed read-only as data and fetched as instructions.
    - WP-IO accesses, both read and write, do not get evicted to the L2 and therefore do not need to be considered for allocation into the L2.
  - WB-DRAM: General storage may be assigned the write-back DRAM memory type and may be accessed as read-write data, but not accessed by instruction fetch.
    - BIOS initializes an L2LineSize sized and aligned location in the L2 cache, mapped as write-back DRAM, with 1 read to at least 1 byte of the L2LineSize sized and aligned WB-DRAM address. BIOS may store to a line only after it has been allocated by a load.
    - Fills, sent to the disabled memory controller, return undefined data.
  - All of memory space that is not accessed as WP-IO or WB-DRAM space must be marked as UC memory type.

- In order to prevent victimizing L2 data, no more than L2WayNum cache lines accessed as WB-DRAM may have the same L2WayIndex.
  - Software does not need to know which ways the L2WayNum lines are allocated to for any given value of L2WayIndex, only that invalid ways will be selected for allocation before valid ways will be selected for allocation.
  - Software is not allowed to deallocate a line in the L2 by using CLFLUSH.

Performance monitor event PMCx07F[1], titled “L2 Writebacks to system“, can be used to indicate whether L2 dirty data was lost by being victimized and sent to the disabled memory controller.

The following requirements must be satisfied prior to using the cache as general storage:

  - Paging must be disabled.
  - MSRC001_0015[INVDWBINVD]=0.
  - MSRC001_1020[DisSS]=1.
  - MSRC001_1021[DisSpecTlbRld]=1. Disable speculative ITLB reloads.
  - MSRC001_1022[DisSpecTlbRld]=1. Disable speculative DTLB reloads.
  - MSRC001_1022[DisHwPf]=1.
  - MSRC001_102B[CombineCr0Cd]=0. See MSRC001_102B[CombineCr0Cd].
  - CLFLUSH, INVD, and WBINVD must not be used during CAR but may be used when tearing down CAR for all compute units on a node.
  - The BIOS must not use SSE, or MMX™ instructions, with the exception of the following list: MOVD, MOVQ, MOVDQA, MOVQ2DQ, MOVDQ2Q.
  - The BIOS must not enable exceptions, page-faults, and other interrupts.
  - BIOS must not use software prefetches.

- UC-DRAM: All of DRAM that is not accessed as WB-DRAM space must be marked as UC memory type.
- If (MSRC001_1023[L2WayLock]==1) then:
  - Only the ways 0 through (MSRC001_1023[L2FirstLockedWay]-1) may be used for general storage.
  - BIOS can rely on MSRC001_1023[L2FirstLockedWay] to have a minimum value of Eh.
- If (MSRC001_1023[L2WayLock]==0) then:
  - Set MSRC001_1023[L2WayLock]=1.
  - Set MSRC001_1023[L2FirstLockedWay]=Fh.

When BIOS has completed using the cache for general storage the following steps are followed:

1. An INVD instruction is executed on each core that used cache as general storage; an INVD is issued when all cores on all nodes have completed using the cache for general storage.
2. If DRAM is initialized and there is data in the cache that needs to get moved to main memory, CLFLUSH or WBINVD may be used instead of INVD, but software must ensure that needed data in main memory is not overwritten.
3. Program the following configuration state (Order is unimportant):
   - MSRC001_0015[INVDWBINVD]=1.
   - MSRC001_1020[DisSS]=0.
   - MSRC001_1021[DisSpecTlbRld]=0.
   - MSRC001_1022[DisSpecTlbRld]=0.
   - MSRC001_1022[DisHwPf]=0.
   - If ((MSRC001_1023[L2WayLock]==1) & (MSRC001_1023[L2FirstLockedWay]==Fh)), program MSRC001_1023[L2WayLock]=0.

2.4 Core

The majority of the behavioral definition of the core is specified in the AMD64 Architecture Programmer's Manual. See 1.2 [Reference Documents].

2.4.1 Compute Unit

A *compute unit* includes 2 cores each having an x86 instruction execution logic and first-level (L1) data cache. The FP unit, second level (L2) general-purpose cache, and first-level instruction cache, are shared between both cores of the compute unit.

There is a set of MSRs and APIC registers associated with each core. Processors that include multiple cores are said to incorporate *chip multi-processing* or CMP. Unless otherwise specified the processor configuration interface hides the Compute Unit implementation and presents software with homogenous cores, each independent of the other.

Software may use D18F5x80[Enabled, DualCore] in order to associate a core with a Compute Unit. This information can be useful because some configuration settings are determined based on active Compute Units and core performance may vary based on resource sharing within a Compute Unit.

Table 6: Compute Unit Definitions

Term	Definition
NumOfCompUnits	The number of Compute Units for which at least 1 core is enabled. NumOfCompUnits = COUNT(D18F5x80[Enabled]).
DualCoreEnabled	Both cores of a compute unit are enabled. DualCoreEnabled = (D18F5x80[DualCore[0]]==1). 0=Core 0 enabled, Core 1 disabled.

2.4.2 Caches and TLBs

Cache and TLBstorage available to a core is reported by:
- CPUID Fn8000_0005_EAX-CPUID Fn8000_0006_EDX.
- CPUID Fn8000_0019_EAX-CPUID Fn8000_0019_E[D,C]X.
- CPUID Fn8000_001D_EAX_x0-CPUID Fn8000_001E_EDX.

Cache and TLB storage available to a core is summarized as follows:
- L1 and L2 Caches:
  - DC: 16 KB, 4-way, write-through, per-core.
  - IC: 96 KB, 2-way, shared between cores of a compute unit.
  - L2: 1 MB or 2MB (Product-specific), 16-way associative, shared between both cores of a compute unit.
- TLBs:
  - D, L1TLB:
    - 4 KB: 32 entries, fully associative.
    - 2 MB: 32 entries, fully associative.
    - 1 GB: 32 entries, fully associative.
  - D, L2TLB:
    - None. Full size of unified TLB reported as L2 DTLB.
  - I, L1TLB:
    - 4 KB: 48 entries, fully associative.
    - 2 MB, 1 GB: 24 entries, fully associative. 2M and 1G entries share the same L1TLB bank.
  - I, L2TLB:
    - 4 KB: 512 entries, 4-way associative. (Same as Fam10h)
    - 2 MB: None. Full size of unified TLB reported as L2 ITLB.
    - 1 GB: None. Full size of unified TLB reported as L2 ITLB.
  - Unified TLB:
    - 1024 entries, 8-way associative, any entry can cache:
      - D: 4K, 2M, 4M, or 1G translation.
      - I: 2M, 4M, or 1G translation. Not 4K ITLB translations.
      - Notes: Unified TLB natively stores 4M translations. An entry allocated by one core is not visible to the other core of a compute unit.

2.4.2.1 Registers Shared by Cores in a Compute Unit

Some registers are implemented one instance per Compute Unit instead of per core; these registers are designated as Per-compute-unit. The absence of Per-compute-unit implies the normal per-core instance programming model.
Some Per-compute-unit MSRs are implemented as registers that when read the contents are saved in the L1 data cache and are not coherent between cores; these registers are called SharedNC or “shared non-coherent”.

Programing rules for Per-compute-unit registers:
- Software must ensure that a shared MSR written by one core on a Compute Unit will not cause a problem for software that is running on the other core of the Compute Unit.
- Not SharedNC: A write to a MSR does not have to be written to the other core of the compute unit in order for the other core to see the updated value.
- SharedNC: A write to a SharedNC MSR has to be written to both cores of the compute unit in order for both cores to see the updated value.
  - If software can know that the other core has not read the SharedNC MSR since the last warm reset, then a write is not needed to the SharedNC MSR on the other core.
  - Software may not rely on the other core maintaining the previous value of the SharedNC MSR.

- The SharedNC MSRs are: MSRC001_00[35:30], MSRC001_0054.
- A read-modify-write of a shared MSR register is not atomic. Software must ensure atomicity between the cores that could simultaneously read-modify-write the shared register.

2.4.3 Virtual Address Space

The processor supports 48 address bits of virtual memory space (256 TB) as indicated by CPUID Fn8000_0008_EAX.

2.4.4 Processor Cores and Downcoring

Each node supports downcoring as follows:
- The number of cores supported is specified by D18F5x84[CmpCap].
- The cores of a compute unit may be software downcored by D18F3x190[DisCore] if (DualCoreEnabled==1). If (DualCoreEnabled==0) then the cores of a compute unit may not be software downcored. See 2.4.4.1 [Software Downcoring using D18F3x190[DisCore]].
  - All cores of a compute unit must be downcored if either core needs to be downcored.
  - Clocks are turned off and power is gated to downcored Compute Units. The power savings is the same as CC6.
  - There must be at least 1 Compute Unit enabled.
  - D18F3x190[DisCore] affects the value of CPUID Fn0000_0001_EBX[LogicalProcessorCount], CPUID Fn0000_0001_EDX[HTT], CPUID Fn8000_0001_ECX[CmpLegacy], CPUID Fn8000_0008_ECX[NC], D18F5x80[Enabled, DualCore]. D18F3x190[DisCore] does not affect the value of D18F5x84[CmpCap].
- An implemented (physical) core that is downcored is not visible to software. Cores that are not downcored are numbered logically in a contiguous manner.
- D18F5x80 [Compute Unit Status 1] reports core topology information to software.
- The number of cores specified in CPUID Fn8000_0008_ECX[NC] must be the same as the number of cores enabled in D18F0x1DC[CpuEn].
- The core number, *CpuCoreNum*, is provided to SW running on each core through CPUID Fn0000_0001_EBX[LocalApicId] and APIC20[ApicId]; CpuCoreNum also affects D18F0x1DC[CpuEn]. CpuCoreNum, varies as the lowest integers from 0 to D18F5x84[CmpCap], based on the number of enabled cores; e.g., a 4-core node with 1 core disabled results in cores reporting CpuCoreNum values of 0, 1, and 2 regardless of which core is disabled. The boot core is always the core reporting CpuCoreNum=0.

Some legacy operating systems do not support processors with a non-power-of-2 number of cores. The BIOS is recommended to support a user configurable option to disable cores down to a power-of-2 number of cores for legacy operating system support.

2.4.4.1 Software Downcoring using D18F3x190[DisCore]

Cores may be downcored by D18F3x190[DisCore].

Software is required to use D18F3x190[DisCore] as follows:
- Setting bits corresponding to cores that are not present results in undefined behavior.
- Once a core has been removed by D18F3x190[DisCore]=1, it cannot be added back without a cold reset. E.g. Software may only set DisCore bits, never clear them.
- Software may remove cores only once. If software removes cores by setting D18F3x190[DisCore]=1, then software is not allowed to disable additional cores after the next warm reset.
- The most significant bit N is (the number of cores)-1 at cold reset; the number of cores at cold reset is (CPUID Fn8000_0008_ECX[NC]+1).

- The most significant bit N and the core ID significance of DisCore is not affected by the value of DisCore followed by a warm-reset.
  - E.g. If core 2 is disabled by DisCore[3:0]=0100b followed by a warm reset, then the new core 2 is the old core 3. If the new core 2 needs to then be disabled then DisCore[3:0]=1100b followed by a warm reset.
- All bits greater than bit N are reserved.
- If D18F3x190[DisCore] is changed, then the following need to be updated:
  - D18F0x60[CpuCnt[4:0]].
  - D18F5x170[NbPstateThreshold].
  - MSRC001_102A[ThrottleNbInterface].

2.4.5 Physical Address Space

The processor supports a 40 bit physical address space, even though the core indicates support for a 48 bit physical address space. See CPUID Fn8000_0008_EAX [Long Mode Address Size Identifiers].

The processor master aborts the following upper-address transactions (to address PhysAddr):
- Link or core requests with non-zero PhysAddr[63:40].

2.4.6 System Address Map

The processor defines a reserved memory address region starting at 0000_00FD_0000_0000h and extending up to 0000_0100_0000_0000h. System software must not map memory into this region. Downstream host accesses to the reserved address region results in a page fault. Upstream system device accesses to the reserved address region results in an undefined operation.

2.4.6.1 Memory Access to the Physical Address Space

All memory accesses to the physical address space from a core are sent to its associated northbridge (NB). All memory accesses from a link are routed through the NB. An IO link access to physical address space indicates to the NB the cache attribute (Coherent or Non-coherent, based on bit[0] of the Sized Read and Write commands).

A core access to physical address space has two important attributes that must be determined before issuing the access to the NB: the memory type (e.g., WB, WC, UC; as described in the MTRRs) and the access destination (DRAM or MMIO).

This mechanism is managed by the BIOS and does not require any setup or changes by system software.

2.4.6.1.1 Determining Memory Type

The memory type for a core access is determined by the highest priority of the following ranges that the access falls in: 1==Lowest priority.

1. The memory type as determined by architectural mechanisms.
   - See the APM2 chapter titled “Memory System”, sections “Memory-Type Range Registers” and “Page-Attribute Table Mechanism”.
   - See the APM2 chapter titled “Nested Paging”, section “Combining Memory Types, MTRRs”.
   - See MSR0000_02FF [MTRR Default Memory Type (MTRRdefType)], MSR0000_020[F:0] [Variable-Size MTRRs Base/Mask], MSR0000_02[6F:68,59:58,50] [Fixed-Size MTRRs].
2. TSeg & ASeg SMM mechanism. (see MSRC001_0112 and MSRC001_0113)
3. CR0[CD]: If (CR0[CD]==1) then MemType=CD.
4. MMIO configuration space, APIC space.

- MMIO APIC space and MMIO config space must not overlap.
- MemType=UC.
- See 2.4.9.1.2 [APIC Register Space] and 2.7 [Configuration Space].

5. If ("In SMM Mode" && ~((MSRC001_0113[AValid] && "The address falls within the ASeg region") || (MSRC001_0113[TValid] && "The address falls within the TSeg region"))) then MemType=CD.

2.4.6.1.2 Determining The Access Destination for Core Accesses

The access destination, DRAM or MMIO, is based on the highest priority of the following ranges that the access falls in: 1==Lowest priority.

1. RdDram/WrDram as determined by MSRC001_001A [Top Of Memory (TOP_MEM)] and MSRC001_001D [Top Of Memory 2 (TOM2)].
2. The IORRs. (see MSRC001_00[18,16] and MSRC001_00[19,17]).
3. The fixed MTRRs. (see MSR0000_02[6F:68,59:58,50] [Fixed-Size MTRRs])
4. TSeg & ASeg SMM mechanism. (see MSRC001_0112 and MSRC001_0113)
5. MMIO config space, APIC space.
   - MMIO APIC space and MMIO config space must not overlap.
   - RdDram=IO, WrDram=IO.
   - See 2.4.9.1.2 [APIC Register Space] and 2.7 [Configuration Space].
6. NB address space routing. See 2.8.2.1.1 [DRAM and MMIO Memory Space].

2.4.7 Timers

Each core includes the following timers. These timers do not vary in frequency regardless of the current P-state or C-state.

- MSR0000_0010 [Time Stamp Counter (TSC)]; the TSC increments at the rate specified by the P0 P-state.
  - See 2.5.3.1.1.1 [Software P-state Numbering].
  - See MSRC001_00[6B:64] [P-state [7:0]].
- The APIC timer (APIC380 and APIC390), which increments at the rate of 2xCLKIN; the APIC timer may increment in units of between 1 and 8.

2.4.8 Implicit Conditions for TLB Invalidation

The following family specific conditions will cause all TLBs for both cores of the compute unit to be invalidated; except MSR0000_0277 which will only clear the TLBs for the core that did the MSR write. The architectural conditions that cause TLB invalidation are documented by the APM2 section titled "Translation-Lookaside Buffer (TLB)"; see "Implicit Invalidations".

- MSR0000_020[F:0] [Variable-Size MTRRs Base/Mask].
- MSR0000_02[6F:68,59:58,50] [Fixed-Size MTRRs].
- MSR0000_0277 [Page Attribute Table (PAT)] (TLBs not cleared for the other core).
- MSR0000_02FF [MTRR Default Memory Type (MTRRdefType)].
- MSRC001_0010 [System Configuration (SYS_CFG)] write.
- MSRC001_00[18,16] [IO Range Base (IORR_BASE[1:0])] write.
- MSRC001_00[19,17] [IO Range Mask (IORR_MASK[1:0])] write.
- MSRC001_001A [Top Of Memory (TOP_MEM)] write.
- MSRC001_001D [Top Of Memory 2 (TOM2)] write.
- MSRC001_1023 [Combined Unit Configuration (CU_CFG)] write.
- MSRC001_102A [Combined Unit Configuration 2 (CU_CFG2)] write.
- MSRC001_102B [Combined Unit Configuration 3 (CU_CFG3)] write.

2.4.9 Interrupts

2.4.9.1 Local APIC

The local APIC contains logic to receive interrupts from a variety of sources and to send interrupts to other local APICs, as well as registers to control its behavior and report status. Interrupts can be received from:

- IO devices including the IO hub (IO APICs).
- Other local APICs (inter-processor interrupts).
- APIC timer.
- Thermal events.
- Performance counters.
- Legacy local interrupts from the IO hub (INTR and NMI).
- APIC internal errors.

The APIC timer, thermal events, performance counters, local interrupts, and internal errors are all considered local interrupt sources, and their routing is controlled by local vector table entries. These entries assign a message type and vector to each interrupt, allow them to be masked, and track the status of the interrupt.

IO and inter-processor interrupts have their message type and vector assigned at the source and are unaltered by the local APIC. They carry a destination field and a mode bit that together determine which local APIC(s) accepts them. The destination mode (DM) bit specifies if the interrupt request packet should be handled in physical or logical destination mode. If the destination field matches the broadcast value specified by D18F0x68[ApicExtBrdCst], then the interrupt is a broadcast interrupt and is accepted by all local APICs regardless of destination mode.

2.4.9.1.1 Detecting and Enabling

APIC is detected and enabled via CPUID Fn0000_0001_EDX[APIC].

The local APIC is enabled via MSR0000_001B[ApicEn]. Reset forces APIC disabled.

2.4.9.1.2 APIC Register Space

MMIO APIC space:

- Memory mapped to a 4 KB range. The memory type of this space is the UC memory type. The base address of this range is specified by {MSR0000_001B[ApicBar[47:12]], 000h}.
- The mnemonic is defined to be APICXX; XX is the byte address offset from the base address.
- MMIO APIC registers in xAPIC mode is defined by the register from APIC20 to APIC[530:500].
- Treated as normal memory space when APIC is disabled, as specified by MSR0000_001B[ApicEn].

2.4.9.1.3 ApicId Enumeration Requirements

System hardware and BIOS must ensure that the number of cores per processor (NC) exposed to the operating system by all tables, registers, and instructions across all cores in the processor is identical. See 2.4.11.1 [Multi-Core Support] to derive NC.

Operating systems are expected to use CPUID Fn8000_0008_ECX[ApicIdCoreIdSize], the number of least significant bits in the Initial APIC ID that indicate core ID within a processor, in constructing per-core CPUID masks. (ApicIdCoreIdSize[3:0] determines the maximum number of cores (MNC) that the processor could theoretically support, not the actual number of cores that are actually implemented or enabled on the processor, as indicated by CPUID Fn8000_0008_ECX[NC].) MNC = (2 ^ CPUID Fn8000_0008_ECX[ApicIdCoreIdSize]).

BIOS must use the ApicId MNC rule when assigning APIC20[ApicId] values as described below.

ApicId MNC rule: The ApicId of core j on processor i must be enumerated/assigned as:
- ApicId[proc=i, core=j] = (OFFSET_IDX + i) * MNC + j
- Where OFFSET_IDX is an integer offset (0 to N) used to shift up the core ApicId values to allow room for IOAPIC devices.

It is recommended that BIOS use the following APIC ID assignments for the broadest operating system support. Given N = (Number_Of_Processors * MNC) and M = Number_Of_IOAPICs:
- If (N+M) < 16, then assign the local (core) ApicIds first from 0 to N-1, and the IOAPIC IDs from N to N+(M-1). APIC ID 15 is reserved for broadcast when APIC410[ExtApicIdEn]==0.
- If (N+M) >= 16, then assign the IOAPIC IDs first from 0 to M-1, and the local (core) ApicIds from K to K+(N-1), where K is an integer multiple of MNC greater than M-1.

2.4.9.1.4 Physical Destination Mode

The interrupt is only accepted by the local APIC whose APIC20[ApicId] matches the destination field of the interrupt. Physical mode allows up to 255 APICs to be addressed individually.

2.4.9.1.5 Logical Destination Mode

A local APIC accepts interrupts selected by APICD0 [Logical Destination (LDR)] and the destination field of the interrupt using either cluster or flat format as configured by APICE0[Format].

If flat destinations are in use, bits [7:0] of APICD0[Destination] are checked against bits [7:0] of the arriving interrupt's destination field. If any bit position is set in both fields, the local APIC is a valid destination. Flat format allows up to 8 APICs to be addressed individually.

If cluster destinations are in use, bits [7:4] of APICD0[Destination] are checked against bits [7:4] of the arriving interrupt's destination field to identify the cluster. If all of bits [7:4] match, then bits [3:0] of APICD0[Destination] and the interrupt destination are checked for any bit positions that are set in both fields to identify processors within the cluster. If both conditions are met, the local APIC is a valid destination. Cluster format allows 15 clusters of 4 APICs each to be addressed.

2.4.9.1.6 Interrupt Delivery

SMI, NMI, INIT, Startup, and External interrupts are classified as non-vectored interrupts.

When an APIC accepts a non-vectored interrupt, it is handled directly by the processor instead of being queued in the APIC. When an APIC accepts a fixed or lowest-priority interrupt, it sets the bit in APIC[270:200] [Interrupt Request (IRR)] corresponding to the vector in the interrupt. For local interrupt sources, this comes from the vector field in that interrupt's local vector table entry. The corresponding bit in APIC[1F0:180] [Trigger Mode (TMR)] is set if the interrupt is level-triggered and cleared if edge-triggered. If a subsequent interrupt with the same vector arrives when the corresponding bit in APIC[270:200][RequestBits] is already set, the two interrupts are collapsed into one. Vectors 15-0 are reserved.

2.4.9.1.7 Vectored Interrupt Handling

APIC80 [Task Priority (TPR)] and APICA0 [Processor Priority (PPR)] each contain an 8-bit priority divided into a main priority (bits [7:4]) and a priority sub-class (bits [3:0]). The task priority is assigned by software to set a threshold priority at which the processor is interrupted.

The processor priority is calculated by comparing the main priority (bits [7:4]) of APIC80[Priority] to bits [7:4] of the 8-bit encoded value of the highest bit set in APIC[170:100] [In-Service (ISR)]. The processor priority is the higher of the two main priorities.

The processor priority is used to determine if any accepted interrupts (indicated by APIC[270:200][RequestBits]) are high enough priority to be serviced by the processor. When the processor is ready to service an interrupt, the highest bit in APIC[270:200][RequestBits] is cleared, and the corresponding bit is set in APIC[170:100][InServiceBits].

When the processor has completed service for an interrupt, it performs a write to APICB0 [End of Interrupt], clearing the highest bit in APIC[170:100][InServiceBits] and causing the next-highest interrupt to be serviced. If the corresponding bit in APIC[1F0:180][TriggerModeBits] is set, a write to APICB0 is performed on all APICs to complete service of the interrupt at the source.

2.4.9.1.8 Interrupt Masking

Interrupt masking is controlled by the APIC410 [Extended APIC Control]. If APIC410[IerEn] is set, APIC[4F0:480] [Interrupt Enable] are used to mask interrupts. Any bit in APIC[4F0:480][InterruptEnableBits] that is clear indicates the corresponding interrupt is masked. A masked interrupt is not serviced and the corresponding bit in APIC[270:200][RequestBits] remains set.

2.4.9.1.9 Spurious Interrupts

In the event that the task priority is set to or above the level of the interrupt to be serviced, the local APIC delivers a spurious interrupt vector to the processor, as specified by APICF0 [Spurious-Interrupt Vector (SVR)]. APIC[170:100] is not changed and no write to APICB0 occurs.

2.4.9.1.10 Spurious Interrupts Caused by Timer Tick Interrupt

A typical interrupt is asserted until it is serviced. An interrupt is deasserted when software clears the interrupt status bit within the interrupt service routine. Timer tick interrupt is an exception, since it is deasserted regardless of whether it is serviced or not.

The processor is not always able to service interrupts immediately (i.e. when interrupts are masked by clearing EFLAGS.IM).

If the processor is not able to service the timer tick interrupt for an extended period of time, the INTR caused by the first timer tick interrupt asserted during that time is delivered to the local APIC in ExtInt mode and latched, and the subsequent timer tick interrupts are lost. The following cases are possible when the processor is ready to service interrupts:

- An ExtInt interrupt is pending, and INTR is asserted. This results in timer tick interrupt servicing. This occurs 50 percent of the time.
- An ExtInt interrupt is pending, and INTR is deasserted. The processor sends the interrupt acknowledge cycle, but when the PIC receives it, INTR is deasserted, and the PIC sends a spurious interrupt vector. This occurs 50 percent of the time.

There is a 50 percent probability of spurious interrupts to the processor.

2.4.9.1.11 Lowest-Priority Interrupt Arbitration

Fixed, remote read, and non-vectored interrupts are accepted by their destination APICs without arbitration.

Delivery of lowest-priority interrupts requires all APICs to arbitrate to determine which one accepts the interrupt. If APICF0[FocusDisable] is clear, then the focus processor for an interrupt always accepts the interrupt. A processor is the focus of an interrupt if it is already servicing that interrupt (corresponding bit in APIC[170:100][InServiceBits] is set) or if it already has a pending request for that interrupt (corresponding bit in APIC[270:200][RequestBits] is set). If APIC410[IerEn] is set the interrupt must also be enabled in APIC[4F0:480][InterruptEnableBits] for a processor to be the focus processor. If there is no focus processor for an interrupt, or focus processor checking is disabled, then each APIC calculates an arbitration priority value, stored in APIC90 [Arbitration Priority (APR)], and the one with the lowest result accepts the interrupt.

The arbitration priority value is calculated by comparing APIC80[Priority] with the 8-bit encoded value of the highest bit set in APIC[270:200][RequestBits] (IRRVec) and the 8-bit encoded value of the highest bit set APIC[170:100][InServiceBits] (ISRVec). If APIC410[IerEn] is set the IRRVec and ISRVec are based off the highest enabled interrupt. The main priority bits [7:4] are compared as follows:

```
IF ((APIC80[Priority[7:4]] >= IRRVec[7:4]) && (APIC80[Priority[7:4]] > ISRVec[7:4])) THEN
    APIC90[Priority] = APIC80[Priority]
ELSEIF (IRRVec[7:4] > ISRVec[7:4]) THEN
    APIC90[Priority] = {IRRVec[7:4],0h}
ELSE
    APIC90[Priority] = {ISRVect[7:4],0h}
ENDIF.
```

2.4.9.1.12 Inter-Processor Interrupts

APIC300 [Interrupt Command Low (ICR Low)] and APIC310 [Interrupt Command High (ICR High)] provide a mechanism for generating interrupts in order to redirect an interrupt to another processor, originate an interrupt to another processor, or allow a processor to interrupt itself. A write to register APIC300 causes an interrupt to be generated with the properties specified by the APIC300 and APIC310 fields.

2.4.9.1.13 APIC Timer Operation

The local APIC contains a 32-bit timer, controlled by APIC320 [LVT Timer], APIC380 [Timer Initial Count], and APIC3E0 [Timer Divide Configuration]. The processor bus clock is divided by the value in APIC3E0[Div] to obtain a time base for the timer. When APIC380[Count] is written, the value is copied into APIC390 [Timer Current Count]. APIC390[Count] is decremented at the rate of the divided clock. When the count reaches 0, a timer interrupt is generated with the vector specified in APIC320[Vector]. If APIC320[Mode] specifies periodic operation, APIC390[Count] is reloaded with the APIC380[Count] value, and it continues to decrement at the rate of the divided clock. If APIC320[Mask] is set, timer interrupts are not generated.

2.4.9.1.14 Generalized Local Vector Table

All LVTs (APIC330 to APIC3[60:50], and APIC[530:500]) support a generalized message type as follows:

- 000b=Fixed
- 010b=SMI
- 100b=NMI
- 111b=ExtINT
- All other messages types are reserved.

2.4.9.1.15 State at Reset

At power-up or reset, the APIC is hardware disabled (MSR0000_001B[ApicEn]==0) so only SMI, NMI, INIT, and ExtInt interrupts may be accepted.

The APIC can be software disabled through APICF0[APICSWEn]. The software disable has no effect when the APIC is hardware disabled.

When a processor accepts an INIT interrupt, the APIC is reset as at power-up, with the exception that:
- APIC20[ApicId] is unaffected.
- Pending APIC register writes complete.

2.4.9.2 System Management Mode (SMM)

System management mode (SMM) is typically used for system control activities such as power management. These activities are typically transparent to the operating system.

2.4.9.2.1 SMM Overview

SMM is entered by a core on the next instruction boundary after a system management interrupt (SMI) is received and recognized. A core may be programmed to broadcast a special cycle to the system, indicating that it is entering SMM mode. The core then saves its state into the SMM memory state save area and jumps to the SMI service routine (or SMI handler). The pointer to the SMI handler is specified by MSRs. The code and data for the SMI handler are stored in the SMM memory area, which may be isolated from the main memory accesses.

The core returns from SMM by executing the RSM instruction from the SMI handler. The core restores its state from the SMM state save area and resumes execution of the instruction following the point where it entered SMM. The core may be programmed to broadcast a special bus cycle to the system, indicating that it is exiting SMM mode.

2.4.9.2.2 Operating Mode and Default Register Values

The software environment after entering SMM has the following characteristics:
- Addressing and operation is in Real mode.
  - A far jump, call or return in the SMI handler can only address the lower 1M of memory, unless the SMI handler first switches to protected mode.
  - If (MSRC001_0111[SmmBase]>=0010_0000h) then:
    - The value of the CS selector is undefined upon SMM entry.
    - The undefined CS selector value should not be used as the target of a far jump, call, or return.
- 4-Gbyte segment limits.
- Default 16-bit operand, address, and stack sizes (instruction prefixes can override these defaults).
- Control transfers that do not override the default operand size truncate the EIP to 16 bits.
- Far jumps or calls cannot transfer control to a segment with a base address requiring more than 20 bits, as in Real mode segment-base addressing, unless a change is made into protected mode.
- A20M# is disabled. A20M# assertion or deassertion have no affect during SMM.
- Interrupt vectors use the Real mode interrupt vector table.
- The IF flag in EFLAGS is cleared (INTR is not recognized).
- The TF flag in EFLAGS is cleared.
- The NMI and INIT interrupts are masked.
- Debug register DR7 is cleared (debug traps are disabled).

The SMM base address is specified by MSRC001_0111[SmmBase]. Important offsets to the base address pointer are:
- MSRC001_0111[SmmBase] + 8000h: SMI handler entry point.
- MSRC001_0111[SmmBase] + FE00h - FFFFh: SMM state save area.

2.4.9.2.3 SMI Sources And Delivery

The processor accepts SMIs as link-defined interrupt messages only. The core/node destination of these SMIs is a function of the destination field of these messages. However, the expectation is that all such SMI messages are specified to be delivered globally (to all cores of all nodes).

There are also several local events that can trigger SMIs. However, these local events do not generate SMIs directly. Each of them triggers a programmable IO cycle that is expected to target the SMI command port in the IO hub and trigger a global SMI interrupt message back to the coherent fabric.

Local sources of SMI events that generate the IO cycle specified in MSRC001_0056 [SMI Trigger IO Cycle] are:

- In the core, as specified by:
  - MSRC001_0022 [Machine Check Exception Redirection].
  - MSRC001_00[53:50] [IO Trap (SMI_ON_IO_TRAP_[3:0])].
- All local APIC LVT registers programmed to generate SMIs.

The status for these is stored in SMMFEC4.

2.4.9.2.4 SMM Initial State

After storing the save state, execution starts at MSRC001_0111[SmmBase] + 08000h. The SMM initial state is specified in the following table.

Table 7: SMM Initial State

Register	SMM Initial State
CS	SmmBase[19:4]
DS	0000h
ES	0000h
FS	0000h
GS	0000h
SS	0000h
General-Purpose Registers	Unmodified
EFLAGS	0000_0002h
RIP	0000_0000_0000_8000h
CR0	Bits 0, 2, 3, and 31 cleared (PE, EM, TS, and PG); remainder is unmodified
CR4	0000_0000_0000_0000h
GDTR	Unmodified
LDTR	Unmodified
IDTR	Unmodified
TR	Unmodified
DR6	Unmodified
DR7	0000_0000_0000_0400h
EFER	All bits are cleared except bit 12 (SVME) which is unmodified.

2.4.9.2.5 SMM Save State

In the following table, the offset field provides the offset from the SMM base address specified by MSRC001_0111 [SMM Base Address (SMM_BASE)].

Table 8: SMM Save State

Offset	Size	Contents		Access
FE00h	Word	ES	Selector	Read-only
FE02h	6 Bytes		Reserved	
FE08h	Quadword		Descriptor in memory format	
FE10h	Word	CS	Selector	Read-only
FE12h	6 Bytes		Reserved	
FE18h	Quadword		Descriptor in memory format	
FE20h	Word	SS	Selector	Read-only
FE22h	6 Bytes		Reserved	
FE28h	Quadword		Descriptor in memory format	
FE30h	Word	DS	Selector	Read-only
FE32h	6 Bytes		Reserved	
FE38h	Quadword		Descriptor in memory format	
FE40h	Word	FS	Selector	Read-only
FE42h	2 Bytes		Reserved	
FE44h	Doubleword		FS Base {16'b[47], 47:32}[1]	
FE48h	Quadword		Descriptor in memory format	
FE50h	Word	GS	Selector	Read-only
FE52h	2 Bytes		Reserved	
FE54h	Doubleword		GS Base {16'b[47], 47:32}[1]	
FE58h	Quadword		Descriptor in memory format	
FE60h	4 Bytes	GDTR	Reserved	Read-only
FE64h	Word		Limit	
FE66h	2 Bytes		Reserved	
FE68h	Quadword		Descriptor in memory format	
FE70h	Word	LDTR	Selector	Read-only
FE72h	Word		Attributes	
FE74h	Doubleword		Limit	
FE78h	Quadword		Base	
FE80h	4 Bytes	IDTR	Reserved	Read-only
FE84h	Word		Limit	
FEB6h	2 Bytes		Reserved	
FE88h	Quadword		Base	

Table 8: SMM Save State

Offset	Size	Contents		Access
FE90h	Word	TR	Selector	Read-only
FE92h	Word		Attributes	
FE94h	Doubleword		Limit	
FE98h	Quadword		Base	
FEA0h	Quadword	IO_RESTART_RIP		Read-only
FEA8h	Quadword	IO_RESTART_RCX		
FEB0h	Quadword	IO_RESTART_RSI		
FEB8h	Quadword	IO_RESTART_RDI		
FEC0h	Doubleword	SMMFEC0 [SMM IO Trap Offset]		Read-only
FEC4	Doubleword	SMMFEC4 [Local SMI Status]		Read-only
FEC8h	Byte	SMMFEC8 [SMM IO Restart Byte]		Read-write
FEC9h	Byte	SMMFEC9 [Auto Halt Restart Offset]		Read-write
FECAh	Byte	SMMFECA [NMI Mask]		Read-write
FECBh	5 Bytes	Reserved		
FED0h	Quadword	EFER		Read-only
FED8h	Quadword	SMMFED8 [SMM SVM State]		Read-only
FEE0h	Quadword	Guest VMCB physical address		Read-only
FEE8h	Quadword	SVM Virtual Interrupt Control		Read-only
FEF0h	16 Bytes	Reserved		
FEFCh	Doubleword	SMMFEFC [SMM-Revision Identifier]		Read-only
FF00h	Doubleword	SMMFF00 [SMM Base Address (SMM_BASE)]		Read-write
FF04h	28 Bytes	Reserved		
FF20h	Quadword	Guest PAT		Read-only
FF28h	Quadword	Host EFER[2]		
FF30h	Quadword	Host CR4[2]		
FF38h	Quadword	Nested CR3[2]		
FF40h	Quadword	Host CR0[2]		
FF48h	Quadword	CR4		
FF50h	Quadword	CR3		
FF58h	Quadword	CR0		
FF60h	Quadword	DR7		Read-only
FF68h	Quadword	DR6		
FF70h	Quadword	RFLAGS R		ead-write

Table 8: SMM Save State

Offset	Size	Contents	Access
FF78h	Quadword	RIP	Read-write
FF80h	Quadword	R15	
FF88h	Quadword	R14	
FF90h	Quadword	R13	
FF98h	Quadword	R12	
FFA0h	Quadword	R11	
FFA8h	Quadword	R10	
FFB0h	Quadword	R9	
FFB8h	Quadword	R8	
FFC0h	Quadword	RDI	Read-write
FFC8h	Quadword	RSI	
FFD0h	Quadword	RBP	
FFD8h	Quadword	RSP	
FFE0h	Quadword	RBX	
FFE8h	Quadword	RDX	
FFF0h	Quadword	RCX	
FFF8h	Quadword	RAX	

Notes:
1. This notation specifies that bit[47] is replicated in each of the 16 MSBs of the DW (sometimes called *sign extended*). The 16 LSBs contain bits[47:32].
2. Only used for an SMI in guest mode with nested paging enabled.

The SMI save state includes most of the integer execution unit. Not included in the save state are: the floating point state, MSRs, and CR2. In order to be used by the SMI handler, these must be saved and restored. The save state is the same, regardless of the operating mode (32-bit or 64-bit).

The following are some offsets in the SMM save state area. The mnemonic for each offset is in the form SMMxxxx, where xxxx is the offset in the save state.

SMMFEC0 SMM IO Trap Offset

If the assertion of SMI is recognized on the boundary of an IO instruction, SMMFEC0 [SMM IO Trap Offset] contains information about that IO instruction. For example, if an IO access targets an unavailable device, the system can assert SMI and trap the IO instruction. SMMFEC0 then provides the SMI handler with information about the IO instruction that caused the trap. After the SMI handler takes the appropriate action, it can reconstruct and then re-execute the IO instruction from SMM. Or, more likely, it can use SMMFEC8 [SMM IO Restart Byte], to cause the core to re-execute the IO instruction immediately after resuming from SMM.

Bits	Description
31:16	**Port: trapped IO port address**. Read-only. This provides the address of the IO instruction.
15:12	**BPR: IO breakpoint match**. Read-only.
11	**TF:** EFLAGS TF value. Read-only.

10:7	Reserved.
6	**SZ32: size 32 bits**. Read-only. 1=Port access was 32 bits.
5	**SZ16: size 16 bits**. Read-only. 1= Port access was 16 bits.
4	**SZ8: size 8 bits**. Read-only. 1=Port access was 8 bits.
3	**REP: repeated port access**. Read-only.
2	**STR: string-based port access**. Read-only.
1	**V: IO trap word valid**. Read-only. 1=The core entered SMM on an IO instruction boundary; all information in this offset is valid. 0=The other fields of this offset are not valid.
0	**RW: port access type**. Read-only. 0=IO write (OUT instruction). 1=IO read (IN instruction).

SMMFEC4 Local SMI Status

This offset stores status bits associated with SMI sources local to the core. For each of these bits, 1=The associated mechanism generated an SMI.

Bits	Description
31:20	Reserved.
19	**SmiSrcThrCntHt: SMI source link thresholding**. Read-only. This bit is associated with the SMI source specified in the link thresholding register (see MSR0000_0403 [MC0 Machine Check Miscellaneous (MC0_MISC)]).
18	**SmiSrcThrCntDram: SMI source DRAM thresholding**. Read-only. This bit is associated with the SMI source specified in the DRAM thresholding register (see D18F3x160 [NB Machine Check Misc (DRAM Thresholding) 0 (MC4_MISC0)]).
17	**SmiSrcLvtExt: SMI source LVT extended entry**. Read-only. This bit is associated with the SMI sources specified in APIC[530:500] [Extended Interrupt [3:0] Local Vector Table].
16	**SmiSrcLvtLcy: SMI source LVT legacy entry**. Read-only. This bit is associated with the SMI sources specified by the non-extended LVT entries of the APIC.
15:11	Reserved.
10	**IntPendSmiSts: interrupt pending SMI status**. Read-only. This bit is associated with the SMI source specified when (MSRC001_0055[IntPndMsg]==1).
9	Reserved.
8	**MceRedirSts: machine check exception redirection status**. Read-only. This bit is associated with the SMI source specified in MSRC001_0022[RedirSmiEn].
7:4	Reserved.
3:0	**IoTrapSts: IO trap status**. Read-only. Each of these bits is associated with each of the respective SMI sources specified in MSRC001_00[53:50] [IO Trap (SMI_ON_IO_TRAP_[3:0])].

SMMFEC8 SMM IO Restart Byte

00h on entry into SMM.

If the core entered SMM on an IO instruction boundary, the SMI handler may write this to FFh. This causes the core to re-execute the trapped IO instruction immediately after resuming from SMM. The SMI handler should only write to this byte if SMMFEC0 field V==1; otherwise, the behavior is undefined.

If a second SMI is asserted while a valid IO instruction is trapped by the first SMI handler, the core services the second SMI prior to re-executing the trapped IO instruction. SMMFEC0 field V==0 during the second entry into SMM, and the second SMI handler must not rewrite this byte.

If there is a simultaneous SMI IO instruction trap and debug breakpoint trap, the processor first responds to the SMI and postpones recognizing the debug exception until after resuming from SMM. If debug registers other than DR6 and DR7 are used while in SMM, they must be saved and restored by the SMI handler. If SMMFEC8 [SMM IO Restart Byte], is set to FFh when the RSM instruction is executed, the debug trap does not occur until after the IO instruction is re-executed.

Bits	Description
7:0	**RST: SMM IO Restart Byte**. Read-write.

SMMFEC9 Auto Halt Restart Offset

Bits	Description
7:1	Reserved.
0	**HLT: halt restart**. Read-write. Upon SMM entry, this bit indicates whether SMM was entered from the Halt state. 0=Entered SMM on a normal x86 instruction boundary. 1=Entered SMM from the Halt state. Before returning from SMM, this bit can be written by the SMI handler to specify whether the return from SMM should take the processor back to the Halt state or to the instruction-execution state specified by the SMM state save area (normally, the instruction after the halt). 0=Return to the instruction specified in the SMM save state. 1=Return to the halt state. If the return from SMM takes the processor back to the Halt state, the HLT instruction is not refetched and re-executed. However, the Halt special bus cycle is broadcast and the processor enters the Halt state.

SMMFECA NMI Mask

Bits	Description
7:1	Reserved.
0	**NmiMask**. Read-write. Specifies whether NMI was masked upon entry to SMM. 0=NMI not masked. 1=NMI masked.

SMMFED8 SMM SVM State

Read-only. This offset stores the SVM state of the processor upon entry into SMM.

Bits	Description
63:4	Reserved.

3	**HostEflagsIf: host** EFLAGS IF.
2:0	**SvmState**. Bits — Definition 000b — SMM entered from a non-guest state. 001b — Reserved. 010b — SMM entered from a guest state. 101b-011b — Reserved. 110b — SMM entered from a guest state with nested paging enabled. 111b — Reserved.

SMMFEFC SMM-Revision Identifier

SMM entry state: 0003_0064h.

Bits	Description
31:18	Reserved.
17	**BRL**. Read-only. Base relocation supported.
16	**IOTrap**. Read-only. IO trap supported.
15:0	**Revision**. Read-only.

SMMFF00 SMM Base Address (SMM_BASE)

Bits	Description
31:0	See: MSRC001_0111[SmmBase].

2.4.9.2.6 Exceptions and Interrupts in SMM

When SMM is entered, the core masks INTR, NMI, SMI, INIT, and A20M interrupts. The core clears the IF flag to disable INTR interrupts. To enable INTR interrupts within SMM, the SMM handler must set the IF flag to 1. A20M is disabled so that address bit [20] is never masked when in SMM.

Generating an INTR interrupt can be used for unmasking NMI interrupts in SMM. The core recognizes the assertion of NMI within SMM immediately after the completion of an IRET instruction. Once NMI is recognized within SMM, NMI recognition remains enabled until SMM is exited, at which point NMI masking is restored to the state it was in before entering SMM.

While in SMM, the core responds to the DBREQ and STPCLK interrupts, as well as to all exceptions that may be caused by the SMI handler.

2.4.9.2.7 The Protected ASeg and TSeg Areas

These ranges are controlled by MSRC001_0112 and MSRC001_0113; see those registers for details.

2.4.9.2.8 SMM Special Cycles

Special cycles can be initiated on entry and exit from SMM to acknowledge to the system that these transitions are occurring. These are controlled by MSRC001_0015[RsmSpCycDis, SmiSpCycDis].

2.4.9.2.9 Locking SMM

The SMM registers (MSRC001_0112 and MSRC001_0113) can be locked from being altered by setting MSRC001_0015[SmmLock]. SBIOS must lock the SMM registers after initialization to prevent unexpected changes to these registers.

2.4.9.2.10 Synchronizing SMM Entry (Spring-Boarding)

The BIOS must take special care to ensure that all cores have entered SMM prior to accessing shared IO resources and all core SMI interrupt status bits are synchronized. This generally requires that BIOS waits for all cores to enter SMM.

The following conditions can cause one or more cores to enter SMM without all cores entering SMM:

- More than one IO device in the system is enabled to signal an SMI without hardware synchronization (e.g. using an end of SMI gate).
- A single device may signal multiple SMI messages without hardware synchronization (e.g. using an end of SMI gate).
- An SMI is received while one or more AP coresare in the INIT state. This may occur either during BIOS or secure boot.
- A hardware error prevents a core from entering SMM.

The act of synchronizing cores into SMM is called spring-boarding. Because not all of the above conditions can be avoided, it is recommended that all systems support spring-boarding.

An ACPI-compliant IO hub is required for spring-boarding. Depending on the IO hub design, BIOS may have to set additional end-of-SMI bits to trigger an SMI from within SMM.

The software requirements for the suggested spring-boarding implementation are listed as follows.

- A binary semaphore located in SMRAM, accessible by all cores. For the purpose of this discussion, the semaphore is called CheckSpringBoard. CheckSpringBoard is initialized to zero.
- Two semaphores located in SMRAM, accessible by all cores. For the purpose of this discussion, the semaphores are called NotInSMM and WaitInSMM. NotInSMM and WaitInSMM are initialized to a value equal to the number of cores in the system (NumCPUs).

The following BIOS algorithm describes spring-boarding and is optimized to reduce unnecessary SMI activity. This algorithm must be made part of the SMM instruction sequence for each core in the system.

1. Attempt to obtain ownership of the CheckSpringBoard semaphore with a read-modify-write instruction. If ownership was obtained then do the following, else proceed to step 2:
   - Check all enabled SMI status bits in the IO hub.
     Let Status=enable1&status1 | enable2&status2 | enable3&status3 … enable n & status n.
   - If (Status==0) then perform the following sub-actions.
     - Trigger an SMI broadcast assertion from the IO hub by writing to the software SMI command port.
     - Resume from SMM with the RSM instruction.

     //Example:

```
InLineASM{
   BTS CheckSpringBoard,0; Try to obtain ownership of semaphore
   JC Step_2:
   CALL CheckIOHUB_SMIEVT; proc returns ZF=1 for no events
   JNZ Step_2:
   CALL Do_SpringBoard;Trigger SMI and then RSM
```

```
Step_2:
}
```

2. Decrement the NotInSMM variable. Wait for (NotInSMM==0). See Note 1.
3. Execute the core-local event SMI handler. Using a third semaphore (not described here), synchronize core execution at the end of the task. After all cores have executed, proceed to step 4. The following is a brief description of the task for each core:
   - Check all enabled core-local SMI status bits in the core's private or MSR address space. Handle the event if possible, or pass information necessary to handle the event to a mailbox for the BSC to handle.
   - An exclusive mailbox must exist for each core for each core local event.
   - Wait for all cores to complete this task at least once.
4. If the current core executing instructions is not the BSC then jump to step 5. If the core executing instructions is the BSC then jump to the modified main SMI handler task, described below.
   - Check all enabled SMI status bits in the IO hub. Check mailboxes for event status.
   - For each event, handle the event and clear the corresponding status bit.
   - Repeat until all enabled SMI status bits are clear and no mailbox events remain.
   - Set NotInSMM=NumCPUs. (Jump to step 5.)
5. Decrement the WaitInSMM variable. Wait for WaitInSMM=0. See Note 2.
6. Increment the WaitInSMM variable. Wait for WaitInSMM=NumCPUs.
7. If the current processor core executing instructions is the BSC then reset CheckSpringBoard to zero.
8. Resume from SMM with the RSM instruction.

Notes:
1. To support a secure startup by the secure loader the BIOS must provide a timeout escape from the otherwise endless loop. The timeout value should be large enough to account for the latency of all cores entering SMM. The maximum SMM entrance latency is defined by the platform's IO sub-system, not the processor. A value of twice the watchdog timer count is recommended. See D18F3x44 [MCA NB Configuration] for more information on the watchdog time-out value. If a time-out occurs in the wait loop, the BIOS (the last core to decrement NotInSMM) should record the number of cores that have not entered SMM and all cores must fall out of the loop.
2. If a time-out occurs in the wait loop in step 2, the BIOS must not wait for WaitInSMM=0. Instead it must wait for WaitInSMM=(the number of cores recorded in step 2).
3. If BIOS places APs in the INIT state during any part of the boot process when SMIs may be generated, or may generate SMIs before taking all APs out of their initial microcode reset loop (i.e., before D18F0x1DC[CpuEn] is set), then it is recommended that BIOS keep a record of how many APs are in these two states and exclude these cores from the wait loops. SMIs are not recognized by a processor in these states. AMD does not recommend enabling SMI sources prior to bringing all APs out of these states.

2.4.10 Secure Virtual Machine Mode (SVM)

Support for SVM mode is indicated by CPUID Fn8000_0001_ECX[SVM].

2.4.10.1 BIOS support for SVM Disable

The BIOS should include the following user setup options to enable and disable AMD Virtualization™ technology.

- Enable AMD Virtualization™:
  - MSRC001_0114[SvmeDisable] = 0.
  - MSRC001_0114[Lock] = 1.
  - MSRC001_0118[SvmLockKey] = 0000_0000_0000_0000h.
- Disable AMD Virtualization™:

- MSRC001_0114[SvmeDisable]=1.
- MSRC001_0114[Lock]=1.
- MSRC001_0118[SvmLockKey] = 0000_0000_0000_0000h.

The BIOS may also include the following user setup options to disable AMD Virtualization™ technology.

- Disable AMD Virtualization™, with a user supplied key:
  - MSRC001_0114[SvmeDisable]=1.
  - MSRC001_0114[Lock]=1.
  - MSRC001_0118[SvmLockKey] programmed with value supplied by user. This value should be stored in NVRAM.

2.4.11 CPUID Instruction

The CPUID instruction provides data about the features supported by the processor. See 3.18 [CPUID Instruction Registers].

2.4.11.1 Multi-Core Support

There are two methods for determining multi-core support. A recommended mechanism is provided and a legacy method is also available for existing operating systems. System software should use the correct architectural mechanism to detect the number of physical cores by observing CPUID Fn8000_0008_ECX[NC]. The legacy method utilizes the CPUID Fn0000_0001_EBX[LogicalProcessorCount].

2.5 Power Management

The processor supports many power management features in a variety of systems. Table 9 provides a summary of ACPI states and power management features and indicates whether they are supported.

Table 9: Power Management Support

ACPI/Power Management State	Supported	Description
G0/S0/C0: Working	Yes	
G0/S0/C0: Core P-state transitions	Yes	2.5.3.1 [Core P-states]
G0/S0/C0: NB P-state transitions	Yes	2.5.4.1 [NB P-states]
G0/S0/C0: Hardware thermal control (HTC)	Yes	2.10.3.1 [PROCHOT_L and Hardware Thermal Control (HTC)]
G0/S0/Per-core IO-based C-states	Yes	2.5.3.2 [Core C-states] and 2.5.1.3.2 [Low Power Voltages]
G0/S0/C1: Halt	Yes	
G0/S0/CC6: Per-compute unit Power gating	Yes	2.5.3.2 [Core C-states]
G0/S0/CC6: L2 power gating	Yes	2.5.3.2 [Core C-states]
G0/S0/PC6: 0V support (VDD power plane).	Yes	2.5.3.2 [Core C-states] and 2.5.1.3.2 [Low Power Voltages]
G0/S0/Cx: Cache flushing support	Yes	2.5.3.2.3.1 [C-state Probes and Cache Flushing]
G0/S0: Northbridge C-states	Yes	2.5.4.2 [NB C-states]
G1/S1: Stand By (Powered On Suspend)	No	
G1/S3: Stand By (Suspend to RAM)	Yes	2.5.8.1 [S-states]
G1/S4: Hibernate (Suspend to Disk)	Yes	
G1/S5: Shut Down (Soft Off)	Yes	
G3 Mechanical Off	Yes	
Parallel VID Interface	No	2.5.1 [Processor Power Planes And Voltage Control]
Serial VID Interface 1	No	
Serial VID Interface 2	Yes	
Single-plane systems	No	
Number of voltage planes	2	2.5.1 [Processor Power Planes And Voltage Control]
APM: Application Power Management	Yes	2.5.9 [Application Power Management (APM)]

2.5.1 Processor Power Planes And Voltage Control

Refer to the *Electrical Data Sheet* for power plane definitions. See 1.2 [Reference Documents].

2.5.1.1 Serial VID Interface

The processor includes an interface to control external voltage regulators, called the serial VID interface (SVI). Only SVI2 is supported. The frequency of SVC for SVI2 is controlled by D18F3xA0[Svi2HighFreqSel]. See the *AMD Serial VID Interface 2.0 (SVI2) Specification* for additional details.

2.5.1.1.1 SVI2 Features

The processor supports the following SVI2 features:

- Voltage offsets:
  - VDD: D18F5x12C[CoreOffsetTrim].
  - VDDNB: D18F5x188[NbOffsetTrim].

- Load line trim:
  - VDD: D18F5x12C[CoreLoadLineTrim].
  - VDDNB: D18F5x188[NbLoadLineTrim].

2.5.1.2 Internal VID Registers and Encodings

All VID register fields within the processor are 8-bits wide. The VID encodings to voltage translation for all VID codes are defined by the SVI mode. See the *AMD Serial VID Interface 2.0 (SVI2) Specification* for additional details.

The boot VID is 1.0 volts.

2.5.1.2.1 MinVid and MaxVid Check

Hardware limits the minimum and maximum VID code that is sent to the voltage regulator. The allowed limits are specified in D18F5x17C[MinVid, MaxVid]. Prior to generating VID-change commands to SVI, the processor filters the InputVid value to the OutputVid as follows (higher VID codes correspond to lower voltages and lower VID codes correspond to higher voltages):

- If InputVid < MaxVid, OutputVid=MaxVid.
  - Else if (InputVid > MinVid) & (MinVid!=00h), OutputVid=MinVid.
  - Else OutputVid=InputVid.

This filtering is applied regardless of the source of the VID-change command.

2.5.1.3 Low Power Features

2.5.1.3.1 PSIx_L Bit

The processor can indicate whether or not it's in a low-voltage state via the PSIx_L bit. This indicator may be used by the voltage regulator to place itself into a more power efficient mode. PSIx_L is controlled independently for VDD and VDDNB.

- The processor supports the PSI0_L and the PSI1_L bits in the data fields of the SVI2 command.
  - PSI0_L: PSI0_L for VDD and VDDNB is enabled using D18F3xA0[PsiVidEn] and D18F5x17C[NbPsi0VidEn], respectively. Once enabled, the state of PSI0_L is controlled by D18F3xA0[PsiVid[7:0]] and D18F5x17C[NbPsi0Vid]. Changes to the state of PSI0_L can only occur on VID changes.
  - PSI1_L: The PSI1_L bit for VDD and VDDNB is specified by D18F5x12C[CorePsi1En] and D0F0xBC_x3F9EC[EnableNbPsi1], respectively. See also D18F5x188[NbPsi1]. Changes to the state of PSI1_L can occur at any time.

2.5.1.3.1.1 BIOS Requirements for PSI0_L

Enabling PSI0_L for the VDD and VDDNB planes depends on support from the voltage regulator and is therefore system specific. The voltage regulator must be able to supply the current required for the processor to operate at the VID code specified in D18F3xA0[PsiVid[7:0]] and D18F5x17C[NbPsi0Vid[7:0]]. Depending on the regulator used, AMD recommends one of the following methods:

- PSI0_L disabled:

- VDD: To set PSI0_L for the VDD plane, program D18F3xA0[PsiVidEn]=0.
- VDDNB: To set PSI0_L for the VDDNB plane, program D18F5x17C[NbPsi0VidEn]=0.

- PSI0_L set/clear based on current requirements:
  - VDD: The following algorithm describes how to program PSI0_L on VDD:

```
PSI_vrm_current = current at which the regulator allows PSI0_L.
previous_voltage = FFh

for (each P-state from P0 to D18F3xDC[HwPstateMaxVal]) {
  pstate_current = ProcIddMax for the current P-state,
                   see 2.5.3.1.7 [Processor-Systemboard Power Delivery Compatibility Check];
  pstate_voltage = MSRC001_00[6B:64][CpuVid] of the current P-state;

  if (current P-state == D18F3xDC[HwPstateMaxVal]) {
    next_pstate_current = 0;
  } else {
    next_pstate_current = ProcIddMax for the next P-state,
                   see 2.5.3.1.7 [Processor-Systemboard Power Delivery Compatibility Check];
  }

  if ((pstate_current <= PSI_vrm_current) &&
      (next_pstate_current <= PSI_vrm_current) &&
      (pstate_voltage != previous_voltage)) {
    Program D18F3xA0[PsiVid] = pstate_voltage;
    Program D18F3xA0[PsiVidEn] = 1;
    break;
  }
  previous_voltage = pstate_voltage;
}
```

  - VDDNB: The following algorithm describes how to program PSI0_L on VDDNB:

NbIddMax = D18F5x16[C:0][NbIddDiv] current.

```
PSI_vrm_current = current at which the VDDNB regulator allows PSI0_L.
previous_voltage = FFh

for (each valid NB P-state starting with NBP0) {
  pstate_current = NbIddMax of the current NB P-state;
  pstate_voltage = D18F5x16[C:0][NbVid] of the current NB P-state;

  if (current P-state is the last valid P-state) {
    next_pstate_current = 0;
  } else {
    next_pstate_current = NbIddMax for the next P-state;
  }

  if ((pstate_current <= PSI_vrm_current) &&
      (next_pstate_current <= PSI_vrm_current) &&
      (pstate_voltage != previous_voltage)) {
    Program D18F5x17C[NbPsi0Vid] = pstate_voltage;
    Program D18F5x17C[NbPsi0VidEn] = 1;
    break;
  }
  previous_voltage = pstate_voltage;
}
```

2.5.1.3.2 Low Power Voltages

In order to save power, voltages lower than those normally needed for operation may be applied to the VDD power plane while the processor is in a C-state or S-state. The lower voltage is defined as follows:

- PC6Vid: D18F5x128[PC6Vid] specifies a voltage that does not retain the CPU caches or the core microarchitectural state. PC6Vid does not allow execution and is only applied to the cores. See 2.5.3.2.3.4 [Package C6 (PC6) State].

2.5.1.4 Voltage Transitions

The processor supports dynamic voltage transitions on the VDD and VDDNB planes. These transitions are requested by either hardware or software during state changes such as reset, P-state changes, and C-state changes. In all cases the VID code passed to the voltage regulator changes from the old value to the new value without stepping through intermediate values. The voltage regulator ramps the voltage directly from the starting voltage to the final voltage, no stepping occurs. See the *AMD Serial VID Interface 2.0 (SVI2) Specification* for additional details.

- If a voltage increase is requested , the processor waits the amount of time specified by D18F5x12C[WaitVidCompDis] before sending any additional voltage change requests to the voltage regulator or before beginning a frequency transition.
- If a voltage decrease is requested, the processor waits the amount of time specified by D18F5x128[FastSlamTimeDown] before sending any additional voltage change requests to the voltage regulator. For voltage decreases, the processor does not wait any time before beginning frequency changes.

The processor continues code execution during voltage changes when in the C0 state.

2.5.1.4.1 Hardware-Initiated Voltage Transitions

When software requests any of the following state changes, or hardware determines that any of the following state changes are necessary, hardware coordinates the necessary voltage changes:

- VDD:
  - Core P-state transition. See 2.5.3.1 [Core P-states].
  - Package C-state transition. D18F5x128[PC6Vid] specifies a voltage that does not retain the CPU caches or the core microarchitectural state. PC6Vid does not allow execution and is only applied to the cores. See 2.5.3.2.3.4 [Package C6 (PC6) State].
  - S-state transition. See 2.5.8.1 [S-states].

- VDDNB:
  - NB P-state transition. See 2.5.4.1 [NB P-states].
  - S-state transition. See 2.5.8.1 [S-states].

2.5.1.4.2 Software-Initiated Voltage Transitions

2.5.1.4.2.1 Software-Initiated NB Voltage Transitions

Software can request voltage changes on the VDDNB power plane using the BIOSSMC_MSG_VDDNB_REQUEST software interrupt. To make a voltage change request, software uses the sequence described in 2.13.1 [Software Interrupts] with Service Index 3Ah.

Software voltage requests are considered by hardware when taking voltage plane dependencies into account (see 2.5.2.2 [Dependencies Between Subcomponents on VDDNB]).

2.5.2 Frequency and Voltage Domain Dependencies

2.5.2.1 Dependencies Between Cores

Whenever a P-state or C-state is requested on a core (see 2.5.3.1 [Core P-states] and 2.5.3.2 [Core C-states]), hardware must take the following frequency and voltage domain dependencies into account when deciding whether to make the requested change:

- Cores within a compute unit share a common frequency and voltage domain.
- Compute units within a processor share a common voltage domain, but have independent frequency domains. The voltage is determined by the highest-performance P-state requested on any core.

As a result, the P-state and C-state change requests have the following results:

- If different compute units request different voltages, the VDD voltage is determined by the highest voltage (lowest VID) requested.
- If the cores within a compute unit request different P-states while in C0, frequency and voltage are determined by the highest-performance P-state requested.
- If one core within a compute unit requests a CC6 while the other core is in C0, the frequency and voltage of the compute unit is determined by the core in C0.

2.5.2.2 Dependencies Between Subcomponents on VDDNB

Many subcomponents of the processor reside on the VDDNB power plane. Hardware must take voltage domain dependencies into account when determining whether to make a voltage change requested by one of the subcomponents. Whenever a state transition occurs that causes a voltage change request (see 2.5.1.4.1 [Hardware-Initiated Voltage Transitions]), or software makes a voltage change request (see 2.5.1.4.2 [Software-Initiated Voltage Transitions]), the VDDNB voltage requested by the processor is determined by the highest voltage (lowest VID) request made by any of the subcomponents or by software.

2.5.2.3 BIOS Requirements for Power Plane Initialization

- Ensure the following fields are configured to their BIOS recommendations:
  - D18F3xA0[Svi2HighFreqSel].
  - D18F3xD8[VSRampSlamTime].
- Optionally configure PSIx_L. Refer to 2.5.1.3.1 [PSIx_L Bit] for additional details.

2.5.3 CPU Power Management

2.5.3.1 Core P-states

Core P-states are operational performance states characterized by a unique combination of core frequency and voltage. The processor supports up to 8 core P-states (P0 through P7), specified in MSRC001_00[6B:64]. Out of cold reset, the voltage and frequency of the compute units is specified by MSRC001_0071[StartupPstate].

Support for dynamic core P-state changes is indicated by more than one enabled selection in MSRC001_00[6B:64][PstateEn]. At least one enabled P-state (P0) is specified for all processors.

Software requests core P-state changes for each core independently using the hardware P-state control mechanism (a.k.a. fire and forget). Support for hardware P-state control is indicated by CPUID Fn8000_0007_EDX[HwPstate]==1b. Software may not request any P-state transitions using the hardware P-

state control mechanism until the P-state initialization requirements defined in 2.5.3.1.6 [BIOS Requirements for Core P-state Initialization and Transitions] are complete.

The processor supports independently-controllable frequency planes for each compute unit and the NB; and independently-controllable voltage planes. See 2.5.1 [Processor Power Planes And Voltage Control] for voltage plane definitions.
The following terms may be applied to each of these planes:

- FID: frequency ID. Specifies the PLL frequency multiplier, relative to the reference clock, for a given domain.
- DID: divisor ID. Specifies the post-PLL power-of-two divisor that can be used to reduce the operating frequency.
- COF: current operating frequency. Specifies the operating frequency as a function of the FID and DID. Refer to CoreCOF for the CPU COF formula and NBCOF for the NB COF formula.
- VID: voltage ID. Specifies the voltage level for a given domain. Refer to 2.5.1.2.1 [MinVid and MaxVid Check] for encodings.

All FID and DID parameters for software P-states must be programmed to equivalent values for all cores and NBs in the coherent fabric. See 2.5.3.1.1.1 [Software P-state Numbering]. Refer to MSRC001_00[6B:64] and D18F5x16[C:0] for further details on programming requirements.

2.5.3.1.1 Core P-state Naming and Numbering

Since the number of boosted P-states may vary from product to product, the mapping between MSRC001_00[6B:64] and the indices used to request P-state changes or status also varies. In order to clarify this, two different numbering schemes are used.

2.5.3.1.1.1 Software P-state Numbering

When referring to software P-state numbering, the following naming convention is used:

- Non-boosted P-states are referred to as P0, P1, etc.
  - P0 is the highest power, highest performance, non-boosted P-state.
  - Each ascending P-state number represents a lower-power, lower performance non-boosted P-state than the prior P-state number.
- Boosted P-states are referred to as Pb0, Pb1, etc.
  - Pb0 is the highest-performance, highest-power boosted P-state.
  - Each higher numbered boosted P-state represents a lower-power, lower-performance boosted P-state.

For example, if D18F4x15C[NumBoostStates] contains the values shown below, then the P-states would be named as follows:

Table 10: Software P-state Naming

D18F4x15C[NumBoost-States]=1		D18F4x15C[NumBoost-States]=3	
P-state Name	**Corresponding MSR Address**	**P-state Name**	**Corresponding MSR Address**
Pb0	MSRC001_0064	Pb0	MSRC001_0064
P0	MSRC001_0065	Pb1	MSRC001_0065
P1	MSRC001_0066	Pb2	MSRC001_0066
P2	MSRC001_0067	P0	MSRC001_0067
P3	MSRC001_0068	P1	MSRC001_0068
P4	MSRC001_0069	P2	MSRC001_0069
P5	MSRC001_006A	P3	MSRC001_006A
P6	MSRC001_006B	P4	MSRC001_006B

All sections and register definitions use software P-state numbering unless otherwise specified.

2.5.3.1.1.2 Hardware P-state Numbering

When referring to hardware P-state numbering, the following naming convention is used:

- All P-states are referred to as P0, P1, etc.
  - P0 is the highest power, highest-performance P-state, regardless of whether it is a boosted P-state or a non-boosted P-state.
  - Each ascending P-state number represents a lower-power, lower-performance P-state, regardless of whether it is a boosted P-state or not.

2.5.3.1.2 Core P-state Control

Core P-states are dynamically controlled by software and are exposed through ACPI objects (refer to 2.5.3.1.8.3 [ACPI Processor P-state Objects]). Software requests a core P-state change by writing a 3-bit index corresponding to the desired P-state number to MSRC001_0062[PstateCmd] of the appropriate core. For example, to request P3 for core 0 software would write 011b to core 0's MSRC001_0062[PstateCmd].

Boosted P-states may not be directly requested by software. Whenever software requests the P0 state on a processor that supports APM (i.e. writes 000b to MSRC001_0062[PstateCmd]), hardware dynamically places the core into the highest-performance P-state possible as determined by APM. See 2.5.9 [Application Power Management (APM)].

Hardware sequences the frequency and voltage changes necessary to complete a P-state transition as specified by 2.5.3.1.5 [Core P-state Transition Behavior] with no additional software interaction required. Hardware also coordinates frequency and voltage changes when differing P-state requests are made on cores that share a frequency or voltage plane. See 2.5.2 [Frequency and Voltage Domain Dependencies] for details about hardware coordination.

Table 11: Software P-state Control

D18F4x15C[NumBoostStates]=1			D18F4x15C[NumBoostStates]=3		
P-state Name	**Index Used for Requests/Status**	**Corresponding MSR Address**	**P-state Name**	**Index Used for Requests/Status**	**Corresponding MSR Address**
Pb0	n/a	MSRC001_0064	Pb0	n/a	MSRC001_0064
P0	0	MSRC001_0065	Pb1	n/a	MSRC001_0065
P1	1	MSRC001_0066	Pb2	n/a	MSRC001_0066
P2	2	MSRC001_0067	P0	0	MSRC001_0067
P3	3	MSRC001_0068	P1	1	MSRC001_0068
P4	4	MSRC001_0069	P2	2	MSRC001_0069
P5	5	MSRC001_006A	P3	3	MSRC001_006A
P6	6	MSRC001_006B	P4	4	MSRC001_006B

Hardware controls the VID for each voltage domain according to the highest requirement of the frequency domain(s) on each plane. For example, the VID for a 4 compute unit dual-plane system must be maintained at the highest level required for all 4 frequency domains. The number of frequency domains in a voltage domain is package/platform specific. Refer to 2.5.3.1.5 [Core P-state Transition Behavior] for details on hardware P-state voltage control. 2.5.2.3 [BIOS Requirements for Power Plane Initialization] specifies the processor initialization requirements for voltage plane control.

2.5.3.1.3 Core P-state Visibility

MSRC001_0063[CurPstate] reflects the current non-boosted P-state number for each compute unit. For example, if MSRC001_0063[CurPstate]==010b on compute unit 1, then compute unit 1 is in the P2 state. If a compute unit is in a boosted P-state, MSRC001_0063[CurPstate] reads back as 0.

The voltage on a compute unit may not correspond to the VID code specified by the current P-state of the compute unit due to voltage plane dependencies. See 2.5.2 [Frequency and Voltage Domain Dependencies]. If a compute unit is in the P0 state (i.e. if MSRC001_0063[CurPstate]==0), the frequency of the compute unit could be the frequency specified by P0 or any boosted P-state. To determine the frequency of a compute unit, see 2.5.3.3 [Effective Frequency].

2.5.3.1.4 Core P-state Limits

Core P-states may be limited to lower-performance values under certain conditions, including:

- HTC. See D18F3x64[HtcPstateLimit].
- Software. See D18F3x68[SwPstateLimit].
- Core Performance Boost. See 2.5.9 [Application Power Management (APM)].
- PROCHOT_L assertion. See 2.10.3.1 [PROCHOT_L and Hardware Thermal Control (HTC)].
- SMU. See D18F4x13C[SmuPstateLimit].

P-state limits are applied to all cores on the processor. The current P-state limit is provided in MSRC001_0061[CurPstateLimit]. Changes to the MSRC001_0061[CurPstateLimit] can be programmed to trigger interrupts through D18F3x64[PslApicLoEn, PslApicHiEn]. In addition, the maximum P-state value, regardless of the source, is limited as specified in MSRC001_0061[PstateMaxVal].

2.5.3.1.5 Core P-state Transition Behavior

The following rules specify how P-states changes function and interact with other system or processor states:

- If the P-state number is increasing (the compute unit is moving to a lower-performance state), then the COF is changed first, followed by the VID change. If the P-state number is decreasing, then the VID is changed first followed by the COF.
- When the processor initiates a VID change that increases voltage for a voltage domain, no new voltage or frequency changes occur until D18F3xD8[VSRampSlamTime] has expired, regardless of whether any new requests are received. When the processor initiates a VID change that decreases voltage for a voltage domain, new voltage or frequency changes are allowed to occur immediately.
  - This is true regardless of whether the frequency or voltages changes occur as a result of P-state or C-state changes.
- If multiple commands are issued that affect the P-state of a domain prior to when the processor initiates the change of the P-state of that domain, then the processor operates on the last one issued.
- Once a P-state change starts, the P-state state machine (PSSM) continues through completion unless interrupted by a PWROK deassertion. If multiple P-state changes are requested concurrently, the PSSM may group the associated VID changes separately from the associated COF changes.
- Behavior during RESET_L assertions:
  - All cores are transitioned to C0.
  - VDD VID is transitioned to HWP0 VID. See MSRC001_0064[CpuVid].
  - If there is no P-state transition activity, then the compute units and NB remain in the current P-state.
  - If a RESET_L assertion interrupts a P-state transition, then the COF remains in it's current state at the time RESET_L is asserted (either the value of the old or the new P-state). BIOS is required to transition to valid COF and VID settings after a warm reset according to the sequence defined in 2.5.3.1.8 [BIOS COF and VID Requirements After Warm Reset].
  - After a warm reset MSRC001_0063 [P-state Status] is consistent with MSRC001_0071[CurPstate]. MSRC001_0062 [P-state Control] may not be consistent with MSRC001_0071[CurPstate].
- The OS controls the P-state through MSRC001_0062 [P-state Control], independent of P-state limits described in D18F3x64[HtcPstateLimit], D18F3x68[SwPstateLimit]. P-state limits interact with OS-directed P-state transitions as follows:
  - Of all the active P-state limits, the one that represents the lowest-performance P-state number, at any given time, is treated as an upper limit on performance.
  - As the limit becomes active or inactive, or if it changes, the P-state for each compute unit is placed in either the last OS-requested P-state or the new limit P-state, whichever is a lower performance P-state number.
    - If the resulting P-state number exceedsMSRC001_0061[PstateMaxVal], regardless of whether it isa limit or OS-requested, then the PstateMaxVal is used instead.

2.5.3.1.6 BIOS Requirements for Core P-state Initialization and Transitions

1. Check that CPUID Fn8000_0007_EDX[HwPstate]=1. If not, P-states are not supported, no P-state related ACPI objects should be generated, and BIOS must skip the rest of these steps.
2. Complete the 2.5.2.3 [BIOS Requirements for Power Plane Initialization].
3. Ensure the following fields are configured to their BIOS recommendations:
   - D18F3xA0[PllLockTime].
   - D18F3xD4[PowerStepUp, PowerStepDown].
4. Transition all cores to the minimum performance P-state using the algorithm detailed in 2.5.3.1.8.2 [Core Minimum P-state Transition Sequence After Warm Reset].
5. Complete the 2.5.4.1.3.1 [NB P-state COF and VID Synchronization After Warm Reset]. All cores on a processor must be in the minimum performance P-state prior to executing this sequence.

6. Complete the 2.5.3.1.7 [Processor-Systemboard Power Delivery Compatibility Check].
7. Perform the following steps in any order:
   A. Enable 2.5.9 [Application Power Management (APM)] as follows:
      - Ensure the following fields are configured to their BIOS recommendations:
        - D18F4x110[CSampleTimer].
        - D18F4x15C[ApmMasterEn].
        - D18F5xE0[RunAvgRange].
      - See your AMD representative for details on how to enable the GPU aspects of 2.5.9 [Application Power Management (APM)].
      - If D18F4x15C[NumBoostStates]!=0, program D18F4x15C[BoostSrc]=1.
   B. Transition all cores to themaximum performance P-state by writing 0 to MSRC001_0062[PstateCmd].
   C. Create ACPI objects if neccessary:
      - Determine the valid set of P-states as indicated by MSRC001_00[6B:64][PstateEn].
      - If P-states are not supported, as indicated by only one enabled selection in MSRC001_00[6B:64][PstateEn], then BIOS must not generate ACPI-defined P-state objects described in 2.5.3.1.8.3 [ACPI Processor P-state Objects]. Otherwise, the ACPI objects should be generated to enable P-state support.
   D. Configure the COF and VID for each processor appropriately based on the sequence described in 2.5.4.1.3 [BIOS NB P-state Configuration].
8. Configure PSIx_L. Refer to 2.5.1.3.1 [PSIx_L Bit] for additional details.

2.5.3.1.7 Processor-Systemboard Power Delivery Compatibility Check

BIOS must disable processor P-states that require higher power delivery than the systemboard can support. This power delivery compatibility check is designed to prevent system failures caused by exceeding the power delivery capability of the systemboard for the power plane(s) that contain the core(s). Refer to 2.5.1 [Processor Power Planes And Voltage Control] for power plane definitions and configuration information. BIOS can optionally notify the user if P-states are detected that exceed the systemboard power delivery capability. Modifications to MSRC001_00[6B:64] [P-state [7:0]] must be applied equally to all cores on the same node. This check does not ensure functionality for all package/socket compatible processor/systemboard combinations.

MSRC001_00[6B:64][PstateEn] must be set to 0 for any P-state MSR where PstateEn=1 and the processor current requirement (ProcIddMax), defined by the following equation, is greater than the systemboard current delivery capability.

ProcIddMax = MSRC001_00[6B:64][IddValue] current * 1/10^MSRC001_00[6B:64][IddDiv] * (D18F5x84[CmpCap]+1)

The power delivery check should be applied starting with hardware P0 and continue with increasing P-state indexes (1, 2, 3, and 4) for all enabled P-states. Once a compatible P-state is found using the ProcIddMax equation the check is complete. All processor P-states with higher indexes are defined to be lower power and performance, and are therefore compatible with the systemboard.

Example:
- MSRC001_0065[IddValue] = 32d
- MSRC001_0065[IddDiv] = 0d
- D18F5x84[CmpCap] = 1d
- ProcIddMax = 32 * 1 * 2 = 64A per plane

The systemboard must be able to supply >= 64A for the unified core power plane in order to support P1 for this

processor. If the systemboard current delivery capability is < 64A per plane then BIOS must set MSRC001_0065[PstateEn]=0 for all cores on this node, and continue by checking P2 in the same fashion.

If no P-states are disabled while performing the power delivery compatibility check then BIOS does not need to take any action.

If at least one P-state is disabled by performing the power delivery compatibility check and at least one P-state remains enabled, then BIOS must perform the following steps:

1. If the P-state pointed to by MSRC001_0063[CurPstate] is disabled by the power delivery compatibility check, then BIOS must request a transition to an enabled P-state using MSRC001_0062[PstateCmd] and wait for MSRC001_0063[CurPstate] to reflect the new value.
2. Copy the contents of the enabled P-state MSRs (MSRC001_00[6B:64]) to the highest performance P-state locations. E.g. if P0 and P1 are disabled by the power delivery compatibility check and P2 - P4 remain enabled, then the contents of P2 - P4 should be copied to P0 - P2 and P3 and P4 should be disabled (PstateEn==0). This step uses software P-state numbering. See 2.5.3.1.1.1 [Software P-state Numbering].
3. Request a P-state transition to the P-state MSR containing the COF/VID values currently applied. E.g. If MSRC001_0063[CurPstate]==100b and P4 P-state MSR information is copied to P2 in step 2, then BIOS should write 010b to MSRC001_0062[PstateCmd] and wait for MSRC001_0063[CurPstate] to reflect the new value.
4. If a subset of boosted P-states are disabled, then copy the contents of the P-state MSR pointed to by the highest performance boosted P-state that is enabled to the P-state MSRs pointed to by the boosted P-states that are disabled.
5. If all boosted P-states are disabled, then program D18F4x15C[BoostSrc]==0.
6. Adjust the following P-state parameters affected by the P-state MSR copy by subtracting the number of software P-states that are disabled by the power delivery compatibility check. This calculation should not wrap, but saturate at 0. E.g. if P0 and P1 are disabled, then each of the following register fields should have 2 subtracted from them:
   - D18F3x64[HtcPstateLimit]
   - D18F3x68[SwPstateLimit]
   - D18F3xDC[HwPstateMaxVal]

If any node has all P-states disabled after performing the power delivery compatibility check, then BIOS must perform the following steps. This does not ensure operation and BIOS should notify the user of the incompatibility between the processor and systemboard if possible.

1. If MSRC001_0063[CurPstate]!=MSRC001_0061[PstateMaxVal], then write MSRC001_0061[PstateMaxVal] to MSRC001_0062[PstateCmd] and wait for MSRC001_0063[CurPstate] to reflect the new value.
2. If MSRC001_0061[PstateMaxVal]!=000b copy the contents of the P-state MSR pointed to by MSRC001_0061[PstateMaxVal] to MSRC001_0064 and set MSRC001_0064[PstateEn]; Write 000b to MSRC001_0062[PstateCmd] and wait for MSRC001_0063[CurPstate] to reflect the new value. This step uses software P-state numbering. See 2.5.3.1.1.1 [Software P-state Numbering].
3. Adjust the following fields to 000b.
   - D18F3x64[HtcPstateLimit]
   - D18F3x68[SwPstateLimit]
   - D18F3xDC[HwPstateMaxVal]
4. Program D18F4x15C[BoostSrc]=0.

2.5.3.1.8 BIOS COF and VID Requirements After Warm Reset

Warm reset is asynchronous and can interrupt P-state transitions leaving the processor in a VID state that does not correspond to MSRC001_0063[CurPstate] on any core. The processor frequency after warm reset

corresponds to MSRC001_0063[CurPstate]. See 2.5.3.1.5 [Core P-state Transition Behavior] for P-state transition behavior when RESET_L is asserted. BIOS is required to transition the processor to valid COF and VID settings corresponding to an enabled P-state following warm reset. The cores may be transitioned to either the maximum or minimum P-state COF and VID settings using the sequences defined in 2.5.3.1.8.1 [Core Maximum P-state Transition Sequence After Warm Reset] and 2.5.3.1.8.2 [Core Minimum P-state Transition Sequence After Warm Reset]. Transitioning to the minimum P-state after warm reset is recommended to prevent undesired system behavior if a warm reset occurs before the 2.5.3.1.7 [Processor-Systemboard Power Delivery Compatibility Check] is complete. BIOS is not required to manipulate NB COF and VID settings following warm reset if the warm reset was issued by BIOS to update D18F5x16[C:0][NbFid[5:0]].

2.5.3.1.8.1 Core Maximum P-state Transition Sequence After Warm Reset

1. If MSRC001_0071[CurPstate] == D18F3xDC[HwPstateMaxVal], then skip step 3 for that core.
2. Write MSRC001_0061[PstateMaxVal] to MSRC001_0062[PstateCmd] on all cores in the processor.
3. Wait for MSRC001_0071[CurCpuFid, CurCpuDid] == [CpuFid[5:0], CpuDid] from MSRC001_00[6B:64] indexed by D18F3xDC[HwPstateMaxVal].
4. Wait for MSRC001_0071[CurCpuVid] == [CurCpuVid] from MSRC001_00[6B:64] indexed by D18F3xDC[HwPstateMaxVal].
5. All previous steps must be completed on all cores prior to continuing the sequence since a compute unit transitions to the highest performance P-state requested on either core.
6. Write 0 to MSRC001_0062[PstateCmd] on all cores in the processor.
7. Wait for MSRC001_0071[CurCpuFid, CurCpuDid] == [CpuFid[5:0], CpuDid] from MSRC001_00[6B:64] indexed by MSRC001_0071[CurPstateLimit].
8. If MSRC001_0071[CurPstateLimit] != D18F3xDC[HwPstateMaxVal], wait for MSRC001_0071[CurCpuVid] == [CpuVid] from MSRC001_00[6B:64] indexed by MSRC001_0071[CurPstateLimit].
9. Wait for MSRC001_0063[CurPstate] == MSRC001_0061[CurPstateLimit].

2.5.3.1.8.2 Core Minimum P-state Transition Sequence After Warm Reset

1. If MSRC001_0071[CurPstate] == MSRC001_0071[CurPstateLimit], then skip step 3 for that core.
2. Write 0 to MSRC001_0062[PstateCmd] on all cores in the processor.
3. Wait for MSRC001_0071[CurCpuFid, CurCpuDid] == [CpuFid[5:0], CpuDid] from MSRC001_00[6B:64] indexed by MSRC001_0071[CurPstateLimit].
4. Write MSRC001_0061[PstateMaxVal] to MSRC001_0062[PstateCmd] on all cores in the processor.
5. Wait for MSRC001_0071[CurCpuFid, CurCpuDid] == [CpuFid[5:0], CpuDid] from MSRC001_00[6B:64] indexed by D18F3xDC[HwPstateMaxVal].
6. If MSRC001_0071[CurPstateLimit] != MSRC001_0071[CurPstate], wait for MSRC001_0071[CurCpuVid] == [CpuVid] from MSRC001_00[6B:64] indexed by D18F3xDC[HwPstateMaxVal].
7. Wait for MSRC001_0063[CurPstate] == MSRC001_0062[PstateCmd].

2.5.3.1.8.3 ACPI Processor P-state Objects

Processor performance control is implemented through the _PCT, _PSS and _PSD objects in ACPI 2.0 and later revisions. The presence of these objects indicates to the OS that the platform and processor are capable of supporting multiple performance states. Processor performance states are not supported with ACPI 1.0b. BIOS must provide the _PCT, _PSS, and _PSD objects, and define other ACPI parameters to support operating systems that provide native support for processor P-state transitions.

The following rules apply to BIOS generated ACPI objects in multi-core systems. Refer to the appropriate

ACPI specification for additional details:

- All cores must expose the same number of performance states to the OS.
- The respective performance states displayed to the OS for each core must have identical performance and power-consumption parameters (e.g. P0 on core 0 must have the same performance and power-consumptions parameters as P0 on core 1, P1 on core 0 must have the same parameters as P1 on core 1, however P0 can be different than P1).
- Performance state objects must be present under each processor object in the system.

2.5.3.1.8.3.1 _PCT (Performance Control)

BIOS must declare the performance control object parameters as functional fixed hardware. This definition indicates the processor driver understands the architectural definition of the P-state interface associated with CPUID Fn8000_0007_EDX[HwPstate]=1.

- Perf_Ctrl_Register = Functional Fixed Hardware
- Perf_Status_Register = Functional Fixed Hardware

2.5.3.1.8.3.2 _PSS (Performance Supported States)

A unique _PSS entry is created for each non-boosted P-state. The value contained in the _PSS Control field is written to MSRC001_0062 [P-state Control] to request a P-state change to the CoreFreq of the associated _PSS object. The value contained in MSRC001_0063 [P-state Status] can be used to identify the _PSS object of the current P-state request by equating MSRC001_0063[CurPstate] to the value of the Status field. See 2.5.3.1 [Core P-states].

BIOS loops through each of MSRC001_00[6B:64] applying the following formulas to create the fields for the _PSS object for for each valid P-state (see MSRC001_00[6B:64][PstateEn]). BIOS skips over any P-state MSRs that specify boost P-states (see D18F4x15C[NumBoostStates]).

- CoreFreq (MHz) = Calculated using the formula for CoreCOF.
- Power (mW) = MSRC001_00[6B:64][CpuVid] voltage * MSRC001_00[6B:64][IddValue] current * 1000.
- TransitionLatency (us) and BusMasterLatency (us):
  - If MSRC001_00[6B:64][CpuFid[5:0]] is the same for all enabled P-states (see MSRC001_00[6B:64][PstateEn]) and all boosted P-states:
    - TransitionLatency = BusMasterLatency = (15 steps * D18F3xD4[PowerStepDown] time * 1000 us/ns) + (15 steps * D18F3xD4[PowerStepUp] time * 1000 us/ns)
  - Else if MSRC001_00[6B:64][CpuFid[5:0]] is different for any enabled (see MSRC001_00[6B:64][PstateEn]) or boost P-states:
    - TransitionLatency = BusMasterLatency = (15 steps * D18F3xD4[PowerStepDown] time * 1000 us/ns) + D18F3xA0[PllLockTime] time + (15 steps * D18F3xD4[PowerStepUp] time * 1000 us/ns)
  - Example:
    - MSRC001_00[6B:64][CpuFid[5:0]] is not the same for all P-states
    - D18F3xD4[PowerStepDown] = D18F3xD4[PowerStepUp] = 8h (50 ns/step)
    - D18F3xA0[PllLockTime] = 001b (2 us)
    - TransitionLatency = BusMasterLatency = (15 steps * 50 ns/step / 1000 us/ns) + 2us + (15 steps * 50 ns/step / 1000 us/ns) = 3.5 us (round up to 4 us)
- Control/Status:
  - The highest performance non-boosted P-state must have the _PSS control and status fields programmed to 0.
  - Any lower performance non-boosted P-states must have the _PSS control and status fields programmed

in ascending order.

2.5.3.1.8.3.3 _PPC (Performance Present Capabilities)

The _PPC object is optional. Refer to the ACPI specification for details on use and content.

2.5.3.1.8.3.4 _PSD (P-state Dependency)

AMD recommends the ACPI 3.0 _PSD object be generated for each core as follows to cause the cores to transition between P-states independently:

- NumberOfEntries = 5.
- Revision = 0.
- Domain = CPUID Fn0000_0001_EBX[LocalApicId[7:2]].
- CoordType = FEh. (HW_ALL)
- NumProcessors = 2.

A vendor may choose to generate _PSD object to allow cores to transition between P-states together as follows:

- NumberOfEntries = 5.
- Revision = 0.
- Domain = 0.
- CoordType = FCh. (SW_ALL)
- NumProcessors = CPUID Fn8000_0008_ECX[NC] + 1.

BIOS provides an option to choose between either _PSD definition.

2.5.3.1.8.4 Fixed ACPI Description Table (FADT) Entries

Declare the following FADT entries:

- PSTATE_CNT = 00h.
- DUTY_WIDTH = 00h.

2.5.3.1.8.5 XPSS (Microsoft® Extended PSS) Object

Some Microsoft® operating systems require an XPSS object to make P-state changes function properly. A BIOS that implements an XPSS object has special requirements for the _PCT object. See the Microsoft *Extended PSS ACPI Method Specification* for the detailed requirements to implement these objects.

2.5.3.2 Core C-states

C-states are processor power states. C0 is the operational state in which instructions are executed. All other C-states are low-power states in which instructions are not executed. When coming out of warm and cold reset, the processor is transitioned to the C0 state.

2.5.3.2.1 C-state Names and Numbers

C-states are often referred to by an alphanumeric naming convention, C1, C2, C3, etc. The mapping between ACPI defined C-states and AMD specified C-states is not direct. AMD specified C-states are referred to as IO-based C-states. Up to three IO-based C-states are supported, IO-based C-state 0, 1, and 2. The IO-based C-state index corresponds to the offset added to MSRC001_0073[CstateAddr] to initiate a C-state request. See

2.5.3.2.2 [C-state Request Interface]. The actions taken by the processor when entering a low-power C-state are configured by software. See 2.5.3.2.3 [C-state Actions] for information about AMD specific actions.

2.5.3.2.2 C-state Request Interface

C-states are dynamically requested by software and are exposed through ACPI objects (see 2.5.3.2.6 [ACPI Processor C-state Objects]). C-states can be requested on a per-core basis. Software requests a C-state change in one of two ways:

- Reading from an IO address: The IO address must be the address specified by MSRC001_0073[CstateAddr] plus an offset of 0 through 7. The processor always returns 0 for this IO read. Offsets 2 through 7 result in an offset of 2.
- Executing the HLT instruction. This is equivalent to reading from the IO address specified by D18F4x128[HaltCstateIndex].

When software requests a C-state transition, hardware evaluates any frequency and voltage domain dependencies and determines which C-state actions to execute. See 2.5.2 [Frequency and Voltage Domain Dependencies] and 2.5.3.2.3 [C-state Actions].

2.5.3.2.3 C-state Actions

A core takes one of several different possible actions based upon a C-state change request from software. The C-state action fields are defined in D18F4x11[C:8].

2.5.3.2.3.1 C-state Probes and Cache Flushing

If probes occur after a core enters a non-C0 state, and the caches are not flushed by hardware, the core clock may be ramped back up to the C0 frequency to service the probes, as specified by D18F4x118/D18F4x11C[CpuPrbEn].
If a core enters a non-C0 state and cache flush is enabled (see D18F3xDC[CacheFlushOnHaltCtl] and D18F4x118/D18F4x11C[CacheFlushEn]), a timer counts down for a programmable period of time as specified by D18F3xDC[CacheFlushOnHaltTmr] or D18F4x118/D18F4x11C[CacheFlushTmrSel]. When the timer expires, the core flushes its L1 and L2 caches to DRAM and the core clocks are ramped down to a divisor specified by D18F3xDC[CacheFlushOnHaltCtl]. The timer is reset if the core exits the C-state for any reason. See 2.5.3.2.4.2 [Cache Flush On Halt Saturation Counter].
Once a core flushes its caches, probes are no longer sent to that core. This improves probing performance for cores that are in C0.

2.5.3.2.3.2 Core C1 (CC1) State

When a core enters the CC1 state, its clock ramps down to the frequency specified by D18F4x118/D18F4x11C[ClkDivisorCstAct].

2.5.3.2.3.3 Core C6 (CC6) State

A core can gate off power to its internal logic when it enters any non-C0 state. This power gated state is known as CC6. In order to enter CC6, hardware first enters CC1 and then flushes the caches (see 2.5.3.2.3.1 [C-state Probes and Cache Flushing]) before checking D18F4x118/D18F4x11C[PwrGateEnCstAct]. Power gating reduces the amount of power consumed by the core. VDD voltage is not reduced when a core is in CC6. The following sequence occurs when a core enters the CC6 state:

1. If MSRC001_0071[CurPstate] < D18F3xA8[PopDownPstate], transition the core P-state to

D18F3xA8[PopDownPstate].
2. L1 and L2 caches are flushed to DRAM. See 2.5.3.2.3.1 [C-state Probes and Cache Flushing].
3. Internal core state is saved to DRAM.
4. Power is removed from the core and the core PLL/voltage regulator is powered down as specified by D18F5x128[CC6PwrDwnRegEn].

All of the following must be true in order for a core to be placed into CC6:
- D18F4x118/D18F4x11C[CacheFlushEn]=1 for the corresponding C-state action field.
- D18F4x118/D18F4x11C[CacheFlushTmrSel] != 11b for the corresponding C-state action field.
- D18F4x118/D18F4x11C[PwrGateEnCstAct]=1 for the corresponding C-state action field.
- D18F2x118[CC6SaveEn]=1.
- D18F2x118[LockDramCfg]=1 .
- The CC6 storage area in DRAM is configured. See 2.9.13 [DRAM CC6/PC6 Storage].

The events which cause a core to exit the CC6 state are specified in 2.5.3.2.5 [Exiting C-states].

If a warm reset occurs while a core is in CC6, all MCA registers in the core shown in Table 47 are cleared to 0. See 2.15.1 [Machine Check Architecture].

The time required to enter and exit CC6 is directly proportional to the core P-state frequency. Slower core frequencies require longer entry and exit times. Latency issues may occur with core P-state frequencies less than 800MHz.

2.5.3.2.3.4 Package C6 (PC6) State

When all cores enter a non-C0 state, VDD can be reduced to a non-operational voltage that does not retain core state. This state is known as PC6 and reduces the amount of static and dynamic power consumed by all cores. The following actions are taken by hardware prior to PC6 entry:
1. If MSRC001_0071[CurPstate] < D18F3xA8[PopDownPstate], transition the core P-state to D18F3xA8[PopDownPstate].
2. For all cores not in CC6, L1 and L2 caches are flushed to DRAM. See 2.5.3.2.3.1 [C-state Probes and Cache Flushing].
3. For all cores not in CC6, internal core state is saved to DRAM.
4. VDD is transitioned to the VID specified by D18F5x128[PC6Vid].
5. If the core PLLs are not powered down during CC6 entry (see 2.5.3.2.3.3 [Core C6 (CC6) State]), then they are powered down as specified by D18F5x128[PC6PwrDwnRegEn].

All of the following must be true on all cores in order for a package to be placed into PC6:
- D18F4x118/D18F4x11C[CacheFlushEn]=1 for the corresponding C-state action field
- D18F4x118/D18F4x11C[CacheFlushTmrSel] != 11b for the corresponding C-state action field.
- D18F4x118/D18F4x11C[PwrOffEnCstAct]=1 for the corresponding C-state action field.
- D18F2x118[CC6SaveEn]=1.
- D18F2x118[LockDramCfg]=1.
- MSRC001_0015[HltXSpCycEn]=1.

2.5.3.2.4 C-state Request Monitors

Deeper C-states have higher entry and exit latencies but provide greater power savings than shallower C-states. To help balance the performance and power needs of the system, the processor can limit access to specific C-states in certain scenarios.

2.5.3.2.4.1 FCH Messaging

The FCH can be notified when the processor transitions package C-states. See the following:

- D18F4x128[CstateMsgDis].
- D18F5x178[CstateFusionDis].
- MSRC001_0015[HltXSpCycEn].

2.5.3.2.4.2 Cache Flush On Halt Saturation Counter

A cache flush success monitor tracks the success rate of cache flush timer expirations relative to the core exiting a C-state. Based on the success rate, caches may be flushed immediately without waiting for the cache flush timer to expire. See D18F4x128[CacheFlushSucMonThreshold]. When the core resumes normal execution, the caches refill as normal.

2.5.3.2.5 Exiting C-states

The following events may cause the processor to exit a non-C0 C-state and return to C0:

- INTR
- NMI
- SMI
- INIT
- RESET_L assertion

If an INTR is received while a core is in a non-C0 C-state, the state of EFLAGS[IF] and the mechanism used to enter the non-C0 C-state determine the actions taken by the processor.

- Entry via HLT, EFLAGS[IF]==0: The interrupt does not wake up the core.
- Entry via HLT, EFLAGS[IF]==1: The interrupt wakes the core and the core begins execution at the interrupt service routine.
- Entry via IO read, EFLAGS[IF]==0: The interrupt wakes the core and the core begins execution at the instruction after the IN instruction that was used to enter the non-C0 C-state.
- Entry via IO read, EFLAGS[IF]==1: The interrupt wakes the core and the core begins execution at the interrupt service routine.

2.5.3.2.6 ACPI Processor C-state Objects

Processor power control is implemented through the _CST object in ACPI 2.0 and later revisions. The presence of the _CST object indicates to the OS that the platform and processor are capable of supporting multiple power states. BIOS must provide the _CST object and define other ACPI parameters to support operating systems that provide native support for processor C-state transitions. See 2.5.3.2.6.1 [_CST]. See 2.5.3.2.6.2 [_CSD].

The _CST object is not supported with ACPI 1.0b. BIOS should provide FADT entries to support operating systems that are not compatible with ACPI 2.0 and later revisions. See 2.5.3.2.6.3 [_CRS].

2.5.3.2.6.1 _CST

The _CST object should be generated for each core as follows:

- Count = 1.
- Register = MSRC001_0073[CstateAddr] + 1.
- Type = 2
- Latency = 400.

- Power = 0

2.5.3.2.6.2 _CSD

The _CSD object should be generated for each core as follows:
- NumberOfEntries = 6.
- Revision = 0.
- Domain = CPUID Fn0000_0001_EBX[LocalApicId[7:1]].
- CoordType = FEh. (HW_ALL)
- NumProcessors = 2.
- Index = 0.

2.5.3.2.6.3 _CRS

BIOS must declare in the root host bridge _CRS object that the IO address range from MSRC001_0073[CstateAddr] to MSRC001_0073[CstateAddr]+7 is consumed by the host bridge.

2.5.3.2.6.4 Fixed ACPI Description Table (FADT) Entries

Declare the following FADT entries:
- P_LVL2_LAT = 100.
- P_LVL3_LAT = 1001.
- FLAGS.PROC_C1 = 1.
- FLAGS.P_LVL2_UP = 1.

Declare the following P_BLK entries:
- P_LVL2 =MSRC001_0073[CstateAddr] + 1.
- P_LVL3 = 0.

BIOS must declare the PSTATE_CNT entry as 00h.

2.5.3.2.7 BIOS Requirements for Initialization

1. Initialize MSRC001_0073[CstateAddr] with an available IO address. See 2.5.3.2.6.3 [_CRS].
2. Initialize D18F4x11[C:8].
3. Generate ACPI objects as described in 2.5.3.2.6 [ACPI Processor C-state Objects].

2.5.3.3 Effective Frequency

The effective frequency interface allows software to discern the average, or effective, frequency of a given core over a configurable window of time. This provides software a measure of actual performance rather than forcing software to assume the current frequency of the core is the frequency of the last P-state requested. This can be useful when the P-state is limited by:
- HTC
- D18F3x68[SwPstateLimit]
- SBI
- CPB

The following procedure calculates effective frequency using MSR0000_00E7 [Max Performance Frequency Clock Count (MPERF)] and MSR0000_00E8 [Actual Performance Frequency Clock Count (APERF)]:

1. At some point in time, write 0 to both MSRs.

2. At some later point in time, read both MSRs.
3. Effective frequency = (value read from MSR0000_00E8 / value read from MSR0000_00E7) * P0 frequency using software P-state numbering.

Additional notes:
- The amount of time that elapses between steps 1 and 2 is determined by software.
- It is software's responsibility to disable interrupts or any other events that may occur in between the write of MSR0000_00E7 and the write of MSR0000_00E8 in step 1 or between the read of MSR0000_00E7 and the read of MSR0000_00E8 in step 2.
- The behavior of MSR0000_00E7 and MSR0000_00E8 may be modified by MSRC001_0015[EffFreqCntMwait].
- The effective frequency interface provides +/- 50MHz accuracy if the following constraints are met:
- Effective frequency is read at most one time per millisecond.
- When reading or writing MSR0000_00E7 and MSR0000_00E8 software executes only MOV instructions, and no more than 3 MOV instructions, between the two RDMSR or WRMSR instructions.
- MSR0000_00E7 and MSR0000_00E8 are invalid if an overflow occurs.

2.5.4 NB Power Management

2.5.4.1 NB P-states

The processor supports up to four NB P-states (NBP0 through NBP3), specified in D18F5x16[C:0]. Each NB P-state consists of the following:

- Enable: D18F5x16[C:0][NbPstateEn].
- NCLK frequency: D18F5x16[C:0][NbFid[5:0], NbDid].
- VDDNB voltage: D18F5x16[C:0][NbVid].
- Memory P-state: D18F5x16[C:0][MemPstate]. See 2.5.7.1 [Memory P-states].

Out of cold reset, the NB P-state is specified by D18F5x174[StartupNbPstate] and D18F3xA0[CofVidProg]. The current NB P-state is specified by D18F5x174[CurNbFid[5:0], CurNbDid, {CurNbVid[7], CurNbVid[6:0]}].

Although four NB P-states are defined, only two NB P-states are used at any given time, specified by D18F5x170[NbPstateHi, NbPstateLo].

2.5.4.1.1 Northbridge Dynamic Power Management (NB DPM)

Northbridge Dynamic Power Management (NB DPM) dynamically changes which two of the four NB P-states are in use based on GPU activity as follows:

- When the GPU is active :
  - The high NB P-state is specified by D0F0xBC_x3F9E8[DpmXNbPsHi].
  - The low NB P-state is specified by D0F0xBC_x3F9E8[DpmXNbPsLo].

- When the GPU is idle and the timer timer specified by D0F0xBC_x3F9EC[Hysteresis] has expired:
  - The high NB P-state is specified by D0F0xBC_x3F9E8[Dpm0PgNbPsHi].
  - The low NB P-state is specified by D0F0xBC_x3F9E8[Dpm0PgNbPsLo].

In addition, hardware forces the NB P-state to the active high or low NB P-state based on the GPU activity level.

2.5.4.1.2 NB P-state Transitions

Hardware selects whether to use the high or low NB P-state based on several criteria as follows:

- Core P-state:
  - MSRC001_00[6B:64][NbPstate].
  - D18F5x170[NbPstateThreshold].
- GPU activity:
  - The GPU driver selects levels of GPU activity that force the NB P-state to either the high or low state or allow either NB P-state.
- Hysteresis timer:
  - D18F5x170[NbPstateHiRes, NbPstateLoRes].
- The following configuration registers:
  - D18F5x170[SwNbPstateLoDis, NbPstateDisOnP0].
  - MSRC001_0071[NbPstateDis].

Once the NB determines that an NB P-state transition is necessary, the NB executes the following sequence:

1. If transitioning from the low NB P-state to the high NB P-state, transition VDDNB voltage.
2. If the GPU is enabled as specified by D18F5x178[SwGfxDis], wait for display buffer to fill.
3. Quiesce all active cores.
4. If the internal GPU is enabled as specified by D18F5x178[SwGfxDis], wait for display buffer to fill.
5. Stop memory traffic and place DRAM into self-refresh.
6. Transition NCLK frequency.
7. Update NB P-state specific DRAM settings within hardware, see D18F2x210_dct[3:0]_nbp[3:0].
8. Take DRAM out of self-refresh and allow memory traffic.
9. Wake up cores.
10. If transitioning from the high NB P-state to the low NB P-state, transition VDDNB voltage.

2.5.4.1.3 BIOS NB P-state Configuration

2.5.4.1.3.1 NB P-state COF and VID Synchronization After Warm Reset

BIOS performs the following sequence on one core. This is done after any warm reset and before 2.9.9 [DCT/DRAM Initialization and Resume].

1. Temp1=D18F5x170[SwNbPstateLoDis].
2. Temp2=D18F5x170[NbPstateDisOnP0].
3. Temp3=D18F5x170[NbPstateThreshold].
4. Temp4=D18F5x170[NbPstateGnbSlowDis].
5. If MSRC001_0070[NbPstate]==0, go to step 6. If MSRC001_0070[NbPstate]==1, go to step 11.
6. Write 1 to D18F5x170[NbPstateGnbSlowDis].
7. Write 0 to D18F5x170[SwNbPstateLoDis, NbPstateDisOnP0, NbPstateThreshold].
8. Wait for (D18F5x174[NbPstateReqBusy]==0 && D18F5x174[CurNbPstateLo]==1) and D18F5x174[CurNbFid, CurNbDid]=[NbFid, NbDid] from D18F5x16[C:0] indexed by D18F5x170[NbPstateLo].
9. Set D18F5x170[SwNbPstateLoDis]=1.
10. Wait for (D18F5x174[NbPstateReqBusy]==0 && D18F5x174[CurNbPstateLo]==0) and D18F5x174[CurNbFid, CurNbDid]==[NbFid, NbDid] from D18F5x16[C:0] indexed by D18F5x170[NbPstateHi]. Go to step 15.
11. Write 1 to D18F5x170[SwNbPstateLoDis].

12. Wait for (D18F5x174[NbPstateReqBusy]==0 && D18F5x174[CurNbPstateLo]==0) and D18F5x174[CurNbFid, CurNbDid]==[NbFid, NbDid] from D18F5x16[C:0] indexed by D18F5x170[NbPstateHi].
13. Write 0 to D18F5x170[SwNbPstateLoDis, NbPstateDisOnP0, NbPstateThreshold].
14. Wait for (D18F5x174[NbPstateReqBusy]==0 && D18F5x174[CurNbPstateLo]==1) and D18F5x174[CurNbFid, CurNbDid]==[NbFid, NbDid] from D18F5x16[C:0] indexed by D18F5x170[NbPstateLo].
15. Set D18F5x170[SwNbPstateLoDis]=Temp1, D18F5x170[NbPstateDisOnP0]=Temp2, and D18F5x170[NbPstateThreshold]=Temp3, and D18F5x170[NbPstateGnbSlowDis]=Temp4.

2.5.4.1.3.2 NB P-state Transitions

During boot when D18F5x174[NbPstateDis]=0, BIOS forces the processor to the desired NB P-states using the following steps:

1. Save the values in D18F5x170 for later restoration to unforce the NB P-state.
2. Force transitions if needed:
    a. If modifying NbPstateHi, force transition to NbPstateLo first (ensure D18F5x174[CurNbPstateLo]==1 && D18F5x174[NbPstateReqBusy]==0). To force, look at step 4.
    b. If modifying NbPstateLo, force transition to NbPstateHi first (ensure D18F5x174[CurNbPstateLo]==0&& D18F5x174[NbPstateReqBusy]==0). To Force, look at step 4.
3. Set the desired NB P-state pointers, D18F5x170[NbPstateHi, NbPstateLo].
4. Transition to the desired state as follows:
    - In order to transition to D18F5x170[NbPstateHi], program D18F5x170 as follows:
        - SwNbPstateLoDis = 1.
        - Wait for D18F5x174[CurNbPstateLo]==0 && D18F5x174[NbPstateReqBusy]==0.
    - In order to transition to D18F5x170[NbPstateLo], program D18F5x170 as follows:
        - SwNbPstateLoDis = NbPstateDisOnP0 = NbPstateThreshold = 0.
        - Wait for D18F5x174[CurNbPstateLo]==1 && D18F5x174[NbPstateReqBusy]==0.

2.5.4.1.3.3 NB P-state Configuration for Runtime

Please see your AMD representative for details.

2.5.4.2 NB C-states

NB C-states are package-level actions that occur only when all cores enter a non-C0 state (see 2.5.3.2 [Core C-states]). The NB C-state actions are:

- DRAM self-refresh (see 2.5.7.2 [DRAM Self-Refresh]):
    - Enable bit: D18F4x118/D18F4x11C[SelfRefr].
    - Entry requirements:
        - No outstanding GPU traffic or traffic from a link.
    - Exit conditions (any of the following must be true):
        - The local APIC timer expires. See 2.4.9.1 [Local APIC].
        - New GPU traffic or traffic from a link.
        - A P-state limit update (see 2.5.3.1.4 [Core P-state Limits]) causes the most restrictive P-state limit to become a higher number than the current P-state for any core in CC1.

- NB clock gating:
    - Enable bit: D18F4x118/D18F4x11C[NbClkGate].

- Entry requirements:
  - No outstanding GPU traffic or traffic from a link.
- Exit conditions (any of the following must be true):
  - The local APIC timer expires. See 2.4.9.1 [Local APIC].
  - New GPU traffic or traffic from a link.
  - A P-state limit update (see 2.5.3.1.4 [Core P-state Limits]) causes the most restrictive P-state limit to become a higher number than the current P-state for any core in CC1.

NOTE: For SERVER system solutions, NB power gating should be disabled by setting D18F4x118/D18F4x11C[NbPwrGate] = 0 in the BIOS. BIOSsetting of D18F4x118/D18F4x11C[NbPwrGate] = 1 should be set for client systems.

- NB power gating:
  - Enable bit: D18F4x118/D18F4x11C[NbPwrGate].
  - Entry requirements (all of the following must be true):
    - No outstanding GPU traffic or traffic from a link.
    - All cores are in CC6.
    - DRAM is either in or entering self-refresh.
  - Exit conditions (any of the following must be true):
    - The local APIC timer expires. See 2.4.9.1 [Local APIC].
    - New GPU traffic or traffic from a link.
    - A P-state limit update (see 2.5.3.1.4 [Core P-state Limits]) causes the most restrictive P-state limit to become a higher number than the current P-state for any core in CC1.

When entering NB C-states, the actions are taken in the following order:
1. DRAM self-refresh.
2. NB clock gating.
3. NB power gating.

When exiting NB C-states, the actions are taken in the following order:
1. NB power gating.
2. NB clock gating.
3. DRAM self-refresh.

2.5.4.3 Fuse Power Gating

Fuse controller can gate off power to its internal logic when no fuse activity is detected for a period of time. Fuse controller exits power gated state when it detects an event that requires access to the fuses.

2.5.5 Bandwidth Requirements

- The frequency relationship of (core COF / NB COF) <= 6 must be maintained for all supported P-state combinations. E.g., a core P0 COF of 4.0 GHz could not be combined with a NB P0 COF of 0.6 GHz; the NB P0 COF would have to be 0.8 GHz or greater; if the NB P0 COF is 1.2 GHz, then the NB P1 COF of 0.6 GHz may only be supported if the corresponding core P-state specify a COF of 3.0 GHz or less.
- All core P-states are required to be defined such that (NB COF/core COF) <= 32, for all NB/core P-state combinations. E.g., if the NB COF is 4.8 GHz then the core COF must be no less than 150 MHz.
- All core P-states must be defined such that CoreCOF >= 500 MHz.
- All core P-states must be defined such that MSRC001_00[6B:64][CpuFid[5:0]] <= 22h.
- All NB P-states must be defined such that D18F5x16[C:0][NbFid[5:0]] <= 2Eh.
- NBCOF >= MEMCLK frequency.
- NBCOF >= 700MHz.

- NBCOF < 2.4GHz.

2.5.6 GPU and Root Complex Power Management

2.5.6.1 Dynamic Power Management (DPM)

The processor supports dynamic GPU frequency changes along with VDDNB voltage change requests, known as Dynamic Power Management (DPM). Once initialized, hardware dynamically monitors processor utilization and adjusts the frequencies and voltage based on that utilization. For DPM, higher numbered states represent higher performance and lower numbered states represent lower performance.

2.5.6.1.1 Activity Monitors

The processor contains activity monitors which track the usage level of different processor subcomponents. A binary signal from each subcomponent is used to determine whether that subcomponent is busy. On each clock cycle, the activity monitor samples the signal from each unmasked subcomponent.

See D0F0xBC_xC020_0110 for LCLK DPM activity monitor.

The output of the activity monitor is then used to determine whether the DPM state should be changed.

2.5.6.1.2 SCLK DPM

SCLK DPM consists of up to 8 states. Any number of states up through 8 may be used and there is no requirement that the states be contiguous.

2.5.6.1.3 LCLK DPM

LCLK DPM consists of up to 8 states. Any number of states up through 8 may be used and there is no requirement that the states be contiguous.Each state is made up of the following parameters.

- Valid bit: D0F0xBC_x3FD[8C:00:step14][StateValid].
- Voltage change hysteresis threshold: D0F0xBC_x3FD[8C:00:step14][LowVoltageReqThreshold].
- Divisor: D0F0xBC_x3FD[8C:00:step14][LclkDivider].
- VID: D0F0xBC_x3FD[8C:00:step14][VID].
  - See 2.5.2.2 [Dependencies Between Subcomponents on VDDNB].
- State change hysteresis thresholds: D0F0xBC_x3FD[94:08:step14][HysteresisUp, HysteresisDown].
- Activity thresholds: D0F0xBC_x3FD[9C:10:step14][ActivityThreshold].
- Residency counter: See D0F0xBC_x3FD[94:08:step14][ResidencyCounter].

LCLK DPM is enabled by setting D0F0xBC_x3FDC8[LclkDpmEn]. LCLK DPM voltage changes are enabled using D0F0xBC_x3FDC8[VoltageChgEn]. When LCLK DPM is first enabled, the DPM state is transitioned to D0F0xBC_x3FDC8[LclkDpmBootState].

2.5.6.2 GPU and Root Complex Power Gating

Several subcomponents of the GPU and root complex can be power gated when not in use.

- **GPU:** GPU power gating is initialized and enabled by software (see GpuEnabled and D0F0x7C[ForceIntGfxDisable]). Once initialized and enabled, the GPU is power gated by hardware when inactive and is ungated by hardware when needed. When internal GPU is disabled by BIOS, BIOS is responsible for power gating the GPU.

- **UVD:** UVD is power gated by software when not in use and is ungated by software when needed. UVD's internal state is not saved and UVD goes through an internal reset when power is restored.

- **GMC:** GMC power gating is initialized and enabled by software. Once initialized and enabled, GMC is power gated by hardware when inactive and is ungated by hardware when needed. GMC's state is saved internally. If the internal GPU is disabled, either by hardware (fusing) or by software, software is repsonsible for power gating GMC.

- **VCE:** VCE is power gated by software when not in use and is ungated by software when needed. VCE's internal state is not saved and VCE goes through an internal reset when power is restored.

- **DCE:** DCE is power gated by software when there is no display connected. DCE's internal state is not saved and DCE goes through an internal reset when power is restored.

- **PCIe:** Any core that does not contain the UMI link can be power gated when it is not in use. In addition, the individual phys on the TX and RX sides of each link can be power gated when the links are not connected. During POST and runtime, several software components inform the SMU whether the link core or the link phys are in use. SMU power gates or ungates the link core and the link phys as needed.

2.5.7 DRAM Power Management

2.5.7.1 Memory P-states

The processor supports up to 2 memory P-states, M0 and M1. Each memory P-state consists of the following:

- MEMCLK frequency
- A set of frequency dependent DRAM timing and configuration registers

See 2.9 [DRAM Controllers (DCTs)] for DRAM technology specific information and requirements.

All valid memory P-states are associated with a specific NB P-state, as specified by D18F5x16[C:0][MemPstate]. When hardware transitionsto a new NB P-state, the memory P-state is transitioned to that specified by the new NB P-state.

Out of cold reset the current memory P-state is M0. The P-state value specified by D18F5x16[C:0][MemPstate] of the NB P-state indexed by D18F5x174[StartupNbPstate] is invalid. Support for dynamic memory P-state changes is indicated by D18F3xE8[MemPstateCap]=1 and one or more D18F5x16[C:0][MemPstate]=1; otherwise M0 is used by hardware for configuration purposes.

During boot, and if D18F5x170[MemPstateDis]=0, the BIOS can disable memory P-states using the following steps:

1. Program D18F5x170[MemPstateDis]=1.
2. Program D18F5x16[C:0][MemPstate]=0.

2.5.7.2 DRAM Self-Refresh

DRAM is placed into self-refresh on S3 entry (see 2.5.8.1.1 [ACPI Suspend to RAM State (S3)]).

In addition to S3, DRAM is placed into self-refresh in S0 in the following two scenarios:

- NB P-state transitions (see 2.5.4.1 [NB P-states]).
- NB C-states (see 2.5.4.2 [NB C-states]).

The following requirements must be met before hardware places DRAM into self-refresh:
- No pending traffic.
- One of the following is true:
  - The GPU is idle and the internal display buffer is full.
  - The internal GPU is disabled.

Once the above requirements are met, hardware places DRAM into self-refresh.

Early self-refresh occurs when DRAMs are placed in self-refresh before expiration of the cache flush timer. See D18F4x118/D18F4x11C[SelfRefrEarly] and D18F5x128[SelfRefrEarlyDis]. If early self-refresh is enabled, the DRAMs are taken out of self-refresh to perform the flush operation when the cache flush timer expires and then placed back into self-refresh.

The following are events that cause DRAM to transition out of self-refresh:
- Core transitioning to C0.
- Incoming request from any link or the GMC.
- P-state limit update, only in the case when all cores are not in the power gated (CC6) state.

To save additional power, hardware always tristates MEMCLK when entering self-refresh.

2.5.7.3 Stutter Mode

DRAM is most commonly placed in self-refresh due to stutter mode when the internal GPU is in use. The display buffer in the GPU is a combination of a large buffer known as the DMIF (Display Memory Interface FIFO) and a smaller line buffer. The DMIF takes data originating from DRAM and sends it to the line buffer to draw to the screen. When the data level in the DMIF is full, DRAM is placed in self-refresh, and incoming DRAM requests are queued. As the DMIF drains, it eventually falls below a predefined watermark level, at which point hardware pulls DRAM out of self-refresh and services all the requests in the queue. Once all the requests are complete and the DMIF is full again, a transition back into self-refresh occurs if the stutter mode conditions are still met.

2.5.7.3.1 System BIOS Requirements for Stutter Mode Operation During POST

BIOS creates a data structure in memory containing information about the processor for use by the driver. Please see your AMD representative for more information.

2.5.7.4 EVENT_L

EVENT_L is a level sensitive input to the processor. When asserted, the actions specified by D18F2xA4 are taken. EVENT_L is generally asserted to indicate that a DRAM high temperature condition exists. The minimum assertion time for EVENT_L is 15 ns. The minimum deassertion time for EVENT_L is 15 ns.

- EVENT_L is pulled to VDDIO on the motherboard.
- EVENT_L is ignored while:
  - PWROK is de-asserted.
  - RESET_L is asserted.
- BIOS must ensure that throttling is disabled (see D18F2xA4[CmdThrottleMode]) until DRAM training is complete.

See 2.9.14 [DRAM On DIMM Thermal Management and Power Capping].

2.5.8 System Power Management

2.5.8.1 S-states

S-states are ACPI defined sleep states. S0 is the operational state. All other S-states are low-power states in which various voltage rails in the system may or may not be powered. See the ACPI specification for descriptions of each S-state. The only other S-state supported is S5.

2.5.8.1.1 ACPI Suspend to RAM State (S3)

The processor supports the ACPI-defined S3 state. Software is responsible for restoring the state of the processor's registers when resuming from S3. All registers in the processor that BIOS initialized during the initial boot must be restored. The method used to restore the registers is system specific.

During S3 entry, software is responsible for transitioning the processor to Memory Pstate0. See 2.5.7.1 [Memory P-states].

During S3 entry, system memory enters self-refresh mode (see 2.5.7.2 [DRAM Self-Refresh]). Software is responsible for bringing memory out of self-refresh mode when resuming from S3. To bring memory out of self-refresh mode. See 2.9.9 [DCT/DRAM Initialization and Resume].

Many of the systemboard power planes for the processor are powered down during S3. Refer to the Electrical Data Sheet for the following:
- Power plane electrical requirements during S3.
- Power plane sequencing requirements on S3 entry and exit.
- System signal states for both inputs (e.g. PWROK and RESET_L) and outputs (e.g. VID[*], PSI_L bit, THERMTRIP_L, etc.) during S3.
- System signal sequencing requirements on S3 entry and exit.
- System management message sequencing on S3 entry and exit.

2.5.9 Application Power Management (APM)

Application Power Management (APM) allows the processor to deterministically provide maximum performance while remaining within the specified power delivery and removal envelope. APM dynamically monitors processor activity and generates an approximation of power consumption. If power consumption exceeds a defined power limit, a P-state limit is applied by APM hardware to reduce power consumption. APM ensures that average power consumption over a thermally significant time period remains at or below the defined power limit. This allows P-states to be defined with higher frequencies and voltages than could be used without APM.

2.5.9.1 Core Performance Boost (CPB)

These P-states are referred to as boosted P-states.

- Support for APM is specified by CPUID Fn8000_0007_EDX[CPB].
- APM is enabled if all of the following conditions are true:
  - MSRC001_0015[CpbDis] = 0 for all cores.
  - D18F4x15C[ApmMasterEn] = 1.
  - D18F4x15C[BoostSrc] = 01b.

  - D18F4x15C[NumBoostStates] != 0.
- APM can be dynamically enabled and disabled through MSRC001_0015[CpbDis]. If core performance boost (CPB) is disabled , a P-state limit is applied . The P-state limit restricts cores to the highest performance non-boosted P-state.
- All P-states, both boosted and non-boosted, are specified in MSRC001_00[6B:64].
- The number of boosted P-states is specified by D18F4x15C[NumBoostStates].
  - The number of boosted P-states may vary from product to product.
- Two levels of boosted P-states are supported. Compute units can be placed in the first level of boosted P-states if the processor power consumption remains within the TDP limit. The second level of boosted P-states is C-state Boost. See 2.5.9.1.1 [C-state Boost].
- All boosted P-states are always higher performance than non-boosted P-states.
- To ensure proper operation, boosted P-states should be hidden from the operating system. BIOS should not provide ACPI _PSS entries for boosted P-states. See 2.5.3.1.8.3.2 [_PSS (Performance Supported States)].
- The lowest-performance P-state CPB limits the processor to is the highest-performance non-boosted P-state.

2.5.9.1.1 C-state Boost

C-state Boost can only be achieved if a subset of cores/compute units are in CC6 and the processor power consumption remains within the TDP limit. See D18F4x16C[CstateCnt, CstateBoost, CstateCores].

2.5.9.2 TDP Limiting

TDP limiting is a mechanism for capping the power consumption of the processor through a TDP limit.

2.5.9.3 Bidirectional Application Power Management (BAPM)

Bidirectional Application Power Management (BAPM) is an algoirthm to enable fine grained power transfers between the core and GPU.

2.5.9.4 Configurable TDP (cTDP)

Configurable TDP (cTDP) provides flexibility to AMD APUs, traditionally defined to be at fixed nominal TDPs, to fit well in platforms that have thermal solutions designed for lower than nominal TDP. For example, a 35W OPN with the cTDP feature will be able to function and perform well in platforms designed for 30W.

2.6 Performance Monitoring

The processor includes support for two methods of monitoring processor performance:

- 2.6.1 [Performance Monitor Counters].
- 2.6.2 [Instruction Based Sampling (IBS)].

2.6.1 Performance Monitor Counters

The following types of performance counters are supported:

- 2.6.1.1 [Core Performance Monitor Counters], consisting of one set located in each core of each compute unit.
- 2.6.1.2 [NB Performance Monitor Counters], consisting of one set located in each node.

The accuracy of the performance counters is not ensured. The performance counters are not assured of producing identical measurements each time they are used to measure a particular instruction sequence, and they should not be used to take measurements of very small instruction sequences. The RDPMC instruction is not serializing, and it can be executed out-of-order with respect to other instructions around it. Even when bound by serializing instructions, the system environment at the time the instruction is executed can cause events to be counted before the counter value is loaded into EDX:EAX.

To accurately start counting with the write that enables the counter, disable the counter when changing the event and then enable the counter with a second MSR write.

Writing the performance counters can be useful if there is an intention for software to count a specific number of events, and then trigger an interrupt when that count is reached. An interrupt can be triggered when a performance counter overflows. Software should use the WRMSR instruction to load the count as a two's-complement negative number into the performance counter. This causes the counter to overflow after counting the appropriate number of times.

In addition to the RDMSR instruction, the performance counter registers can be read using a special read performance-monitoring counter instruction, RDPMC.

2.6.1.1 Core Performance Monitor Counters

The core performance monitor counters are used by software to count specific events that occur in a core of the compute unit. Each core of each compute unit provides six 48-bit performance counters. Unless otherwise specified, the events count only the activity of the core, not activity caused by the other core of the compute unit.

MSRC001_020[A,8,6,4,2,0] [Performance Event Select (PERF_CTL[5:0])] specify the events to be monitored and how they are monitored. MSRC001_020[B,9,7,5,3,1] [Performance Event Counter (PERF_CTR[5:0])] are the counters. MSRC001_00[03:00] is the legacy alias for MSRC001_020[6,4,2,0]. MSRC001_00[07:04] is the legacy alias for MSRC001_020[7,5,3,1]. Support for MSRC001_020[B:0] is indicated by CPUID Fn8000_0001_ECX[PerfCtrExtCore].

All of the events are specified in 3.23 [Core Performance Counter Events].

Some performance monitor events have a maximum count per clock that exceeds one event per clock. These performance events are called multi-events. Some counters support a greater multi-event count per clock than others. Events that are multi-events will specify the maximum multi-event count per clock. E.g. The number of events logged per cycle can vary from 0 to X. An event that doesn't specify multi-event is implied to be a max-

imum of 1 event per clock. Undefined results will be produced if an multi-event is selected that exceeds that counters capabilities. The following list specifies the maximum number of multi-events supported by each counter:

- PERF_CTL[0]: 31 multi-event per clock maximum.
- PERF_CTL[1]: 7 multi-event per clock maximum.
- PERF_CTL[2]: 7 multi-event per clock maximum.
- PERF_CTL[3]: 63 multi-event per clock maximum.
- PERF_CTL[4]: 7 multi-event per clock maximum.
- PERF_CTL[5]: 7 multi-event per clock maximum.

Not all performance monitor events can be counted on all counters. The performance counter registers are generally assigned to specific blocks of the core according to Table 12; however, there are exceptions when an events is implemented by another block of the core and therefore has the counter restrictions of that block. Each core event description starts with one of the following terms to indicate which counters support that event. Selecting an event for a counter that does not support that counter will produce undefined results.

Table 12: Core PMC mapping to PERF_CTL[5:0]

Term	Definition
PERF_CTL[5:0]	PERF_CTL[5:0] are used to count events in the LS/DC and EX where the number of events logged per cycle can vary up to 7.
PERF_CTL[3,0]	PERF_CTL[3,0] are used to count events in the LS/DC and EX where the number of events logged per cycle can vary up to 31.
PERF_CTL[0]	PERF_CTL[0] are used to count events in the LS/DC, EX, IF/DE and CU where the number of events logged per cycle can vary up to 31.
PERF_CTL[3]	PERF_CTL[3] are used to count events in the LS/DC, EX and FP where the number of events logged per cycle can vary up to 63.
PERF_CTL[2:0]	PERF_CTL[2:0] are used to count events in the IF/DE and CU; The number of events logged per cycle can vary up to 7.
PERF_CTL[5:3]	PERF_CTL[5:3] are used to count events in the FP; The number of events logged per cycle can vary up to 7.

2.6.1.2 NB Performance Monitor Counters

The NB performance monitor counters are used by software to count specific events that occur in the NB. Each node provides four 48-bit performance counters. Since the northbridge performance counter register are shared by all cores on a node, monitoring of northbridge events should only be performed by one core on a node.

These counters are 48 bits. This requires two 32-bit reads to get the entire value. The high bits are not latched when the low bits are read. This means that it is possible for the low bits to overflow into the high bits between the two reads. Software can read the registers multiple times in the sequence below to ensure the proper value is read.

1. Read the low bits [31:0], call the result Lo0.
2. Read the high bits [47:32], call the result Hi0.
3. Read the low bits again, call the result Lo1.
4. Read the high bits again, call the result Hi1.
5. If Hi1 = Hi0, a roll over did not occur and {Hi0,Lo0} is valid.
6. If Hi1 != Hi0, a roll over may have occurred. If so, read again to get Hi2 and Lo2.
7. If Hi2 = Hi1, then {Hi1,Lo1} is a valid counter value.

MSRC001_024[6,4,2,0] [Northbridge Performance Event Select (NB_PERF_CTL[3:0])] and

MSRC001_024[7,5,3,1] [Northbridge Performance Event Counter (NB_PERF_CTR[3:0])] specify the events to be monitored and how they are monitored. Support for MSRC001_024[7:0] is indicated by CPUID Fn8000_0001_ECX[PerfCtrExtNB].

- All of the events are specified in 3.24 [NB Performance Counter Events].
- All NB performance monitor events can be counted on all counters.
- All NB performance events are one event per clock.
- NB performance counters do not support APIC interrupt capability.

2.6.2 Instruction Based Sampling (IBS)

IBS is a code profiling mechanism that enables the processor to select a random instruction fetch or micro-op after a programmed time interval has expired and record specific performance information about the operation. An interrupt is generated when the operation is complete as specified by MSRC001_103A [IBS Control]. An interrupt handler can then read the performance information that was logged for the operation.

The IBS mechanism is split into two parts: instruction fetch performance controlled by MSRC001_1030 [IBS Fetch Control (IbsFetchCtl)]; and instruction execution performance controlled by MSRC001_1033 [IBS Execution Control (IbsOpCtl)]. Instruction fetch sampling provides information about instruction TLB and instruction cache behavior for fetched instructions. Instruction execution sampling provides information about micro-op execution behavior. The data collected for instruction fetch performance is independent from the data collected for instruction execution performance. Support for the IBS feature is indicated by the CPUID Fn8000_0001_ECX[IBS].

Instruction fetch performance is profiled by recording the following performance information for the tagged instruction fetch:

- If the instruction fetch completed or was aborted. See MSRC001_1030.
- The number of clock cycles spent on the instruction fetch. See MSRC001_1030.
- If the instruction fetch hit or missed the IC, hit/missed in the L1 and L2 TLBs, and page size. See MSRC001_1030.
- The linear address, physical address associated with the fetch. See MSRC001_1031, MSRC001_1032.

Instruction execution performance is profiled by tagging one micro-op associated with an instruction. Instructions that decode to more than one micro-op return different performance data depending upon which micro-op associated with the instruction is tagged. These micro-ops are associated with the RIP of the next instruction to retire. The following performance information is returned for the tagged micro-op:

- Branch and execution status for micro-ops. See MSRC001_1035.
- Branch target address for branch micro-ops. See MSRC001_103B.
- The logical address associated with the micro-op. See MSRC001_1034.
- The linear and physical address associated with a load or store micro-op. See MSRC001_1038, MSRC001_1039.
- The data cache access status associated with the micro-op: DC hit/miss, DC miss latency, TLB hit/miss, TLB page size. See MSRC001_1037.
- The number clocks from when the micro-op was tagged until the micro-op retires. See MSRC001_1035.
- The number clocks from when the micro-op completes execution until the micro-op retires. See MSRC001_1035.
- Source information for DRAM and MMIO. See MSRC001_1036.

2.7 Configuration Space

PCI-defined configuration space was originally defined to allow up to 256 bytes of register space for each

function of each device; these first 256 bytes are called base configuration space (BCS). It was expanded to support up to 4096 bytes per function; bytes 256 through 4095 are called extended configuration space (ECS). The processor includes configuration space registers located in both BCS and ECS. Processor configuration space is accessed through bus 0, devices 18h to 1Fh, where device 18h corresponds to node 0 and device 1Fh corresponds to node 7. See 2.7.3 [Processor Configuration Space].

Configuration space is accessed by the processor through two methods:
- IO-space configuration: IO instructions to addresses CF8h and CFCh.
  - Enabled through IOCF8[ConfigEn], which allows access to BCS.
  - Access to ECS enabled through MSRC001_001F[EnableCf8ExtCfg].
  - Use of IO-space configuration can be programmed to generate GP faults through MSRC001_0015[IoCfgGpFault].
  - SMI trapping for these accesses is specified by MSRC001_0054 [IO Trap Control (SMI_ON_IO_TRAP_CTL_STS)] and MSRC001_00[53:50] [IO Trap (SMI_ON_IO_TRAP_[3:0])].
- MMIO configuration: configuration space is a region of memory space.
  - The base address and size of this range is specified by MSRC001_0058 [MMIO Configuration Base Address]. The size is controlled by the number of configuration-space bus numbers supported by the system. Accesses to this range are converted configuration space as follows:
    - Address[31:0] = {0h, bus[7:0], device[4:0], function[2:0], offset[11:0]}.

The BIOS may use either configuration space access mechanism during boot. Before booting the OS, BIOS must disable IO access to ECS, enable MMIO configuration and build an ACPI defined MCFG table. BIOS ACPI code must use MMIO to access configuration space.

Per the link specification, BCS accesses utilize link addresses starting at FD_FE00_0000h and ECS accesses utilize link addresses starting at FE_0000_0000h.

2.7.1 MMIO Configuration Coding Requirements

MMIO configuration space accesses must use the uncacheable (UC) memory type.
Instructions used to read MMIO configuration space are required to take the following form:

```
mov eax/ax/al, any_address_mode;
```

Instructions used to write MMIO configuration space are required to take the following form:

```
mov any_address_mode, eax/ax/al;
```

No other source/target registers may be used other than eax/ax/al.

In addition, all such accesses are required not to cross any naturally aligned DW boundary. Access to MMIO configuration space registers that do not meet these requirements result in undefined behavior.

2.7.2 MMIO Configuration Ordering

Since MMIO configuration cycles are not serializing in the way that IO configuration cycles are, their ordering rules relative to posted may result in unexpected behavior.

Therefore, processor MMIO configuration space is designed to match the following ordering relationship that exists naturally with IO-space configuration: if a core generates a configuration cycle followed by a posted-write cycle, then the posted write is held in the processor until the configuration cycle completes. As a result,

any unexpected behavior that might have resulted if the posted-write cycle were to pass MMIO configuration cycle is avoided.

2.7.3 Processor Configuration Space

The processor includes configuration space as described in 3 [Registers]. Accesses to unimplemented registers of implemented functions are ignored: writes dropped; reads return 0. Accesses to unimplemented functions also ignored: writes are dropped; however, reads return all F's. The processor does not log any master abort events for accesses to unimplemented registers or functions.

Accesses to device numbers of devices not implemented in the processor are routed based on the configuration map registers. If such requests are master aborted, then the processor can log the event.

2.8 Northbridge (NB)

Each node includes a single northbridge that provides the interface to the local core(s), the interface to system memory, and the interface to system IO devices. The NB includes all power planes except VDD; see 2.5.1 [Processor Power Planes And Voltage Control].

The NB is responsible for routing transactions sourced from cores and link to the appropriate core, cache, DRAM, or link. See 2.4.6 [System Address Map].

2.8.1 NB Architecture

Major NB blocks are: System Request Interface (SRI), Memory Controller (MCT), DRAM Controllers (DCTs), and crossbar (XBAR). SRI interfaces with the core(s). MCT maintains cache coherency and interfaces with the DCTs; MCT maintains a queue of incoming requests called MCQ. XBAR is a switch that routes packets between SRI, MCT, and the link.

The MCT operates on physical addresses. Before passing transactions to the DCTs, the MCT converts physical addresses into *normalized* addresses that correspond to the values programmed into D18F2x[5C:40]_dct[3:0] [DRAM CS Base Address]. Normalized addresses include only address bits within the DCTs' range.

2.8.2 NB Routing

2.8.2.1 Address Space Routing

There are four main types of address space routed by the NB:
1. Memory space targeting system DRAM.
2. Memory space targeting IO (MMIO).
3. IO space.
4. Configuration space.

2.8.2.1.1 DRAM and MMIO Memory Space

Memory space transactions provide the NB with the physical address, cacheability type, access type, and DRAM/MMIO destination type as specified in section 2.4.6.1.2 [Determining The Access Destination for Core Accesses].
Memory-space transactions are handled by the NB as follows:
- IO-device accesses are compared against:
  - If the access matches D18F1x[2CC:2A0,1CC:180,BC:80] [MMIO Base/Limit], then the transaction is routed to the root complex;

  - Else, if the access matches D18F1x[17C:140,7C:40] [DRAM Base/Limit], then the access is routed to the DCT;
  - Else, the access is routed to the UMI.
- For core accesses the routing is determined based on the DRAM/MMIO destination:
  - If the destination is DRAM:
    - If the access matches D18F1x[17C:140,7C:40] [DRAM Base/Limit], then the transaction is routed to the DCT;
    - Else, the access is routed to the UMI.
  - If the destination is MMIO:
    - If the access matches the VGA-compatible MMIO address space and D18F1xF4[VE]=1 then D18F1xF4 describes how the access is routed and controlled;
    - Else, If the access matches D18F1x[2CC:2A0,1CC:180,BC:80] [MMIO Base/Limit], then the transaction is routed to the root complex;
    - Else, the access is routed to the UMI.

2.8.2.1.2 IO Space

IO-space transactions from IO links or cores are routed as follows:
- If the access matches D18F1x[DC:C0] [IO-Space Base/Limit], then the transaction is routed to the root complex;
- Else, If the access matches the VGA-compatible IO address space and D18F1xF4[VE]=1 then D18F1xF4 describes how the access is routed and controlled.
- Else, the access is routed to the UMI.

2.8.2.1.3 Configuration Space

Configuration-space transactions from IO links are master aborted. Configuration-space transactions from cores are routed as follows:
- If the access matches D18F1x[1DC:1D0,EC:E0] [Configuration Map], then the transaction is routed to the specified link;
- Else, the access is routed to link that contains compatibility (subtractive) address space.

2.8.2.1.3.1 Recommended Buffer Count Settings Overview

When changing from the recommended settings, see the register programming requirements in the definition of each register. Some chipsets may further optimize these settings for their platform. If values other than the recommended settings are used, see the register requirements in the definition of each register. Table 13 defines commonly used terms for the following tables.

Table 13: ONION Link Definitions

Term	Definition
LinkGanged	Ganged = 0.
IOMMU	Indicates the presence of an IOMMU device on the IOH. IOMMU uses the isochronous flow control channel. If an IOMMU is present, D18F0x[A4,84][IsocEn] must be set for all links.
IFCM	Isochronous Flow Control Mode. IFCM = D18F0x[A4,84][IsocEn].

2.8.3 Memory Scrubbers

The processor includes memory scrubbers specified in D18F3x58, D18F3x5C, and D18F3x60. The scrubbers ensure that all cachelines in memory within or connected to the processor are periodically read and, if correctable errors are discovered, they are corrected.

To enable the scrubber, ensure D18F3x88[DisDramScrub] is cleared. For recommendations on scrub rates, see 2.15.1.8 [Scrub Rate Considerations].

The scrub rate is specified as the time between successive scrub events. A scrub event occurs when a line of memory is checked for errors; the amount of memory that is checked varies based on the memory block (see field descriptions).

The time required to fully scrub the memory of a node is determined as:

- Time = ((memory size in bytes)/64) * (Scrub Rate).
- E.g. If a node contains 1GB of system memory and DramScrub=5.24 ms, then all of the system memory of the node is scrubbed about once every 23 hours.

2.9 DRAM Controllers (DCTs)

The processor includes two DRAM controllers (DCTs), named DCT0 and DCT3. Each DCT controls one 64-bit DDR3 DRAM channel as shown in the following table. Software must not attempt to configure “DCT1” or “DCT2”.

Table 14: DCT Channel Ctrl Map

Channel			
DCT0	DCT2	DCT1	DCT3
Channel A	-	-	Channel B

The following restrictions limit the DIMM types and configurations supported by the DCTs:
- All DIMMs connected to the processor are required to operate at the same MEMCLK frequency.
- Registered DIMMs are not supported.
- LR-DIMMs are not supported.
- Quad rank DIMMs are not supported.
- x4(by 4) DRAM devices are not supported.
- ECC DIMMs are supported on FP3 package:
  - Mixing of ECC and non-ECC DIMMs within a system is not supported.
- ECC DIMMs are not supported on FM2r2 package.
- GDDR5 memory is not supported.

2.9.1 Common DCT Definitions

Table 15: DCT Definitions

Term	Definition
any	Any: SR or DR.
AutoSelfRefresh	DDR3 SPDByte[31][2] of the DIMM being configured.
DataMaskMbType	Motherboard type for processor Data Mask pins. Bits — Description 00b — No connect 01b — Pins are routed per DM rules 10b — Pins are routed per DQS rules
Ddr3Mode	The DRAM controller and the phy are configured for DDR3 mode. Note: this mode may not be supported by this processor. See section 2.9, or consult processor data sheet to determine which modes are supported. See D18F2x78_dct[3:0][DramType], D18F2x9C_x00[F,3:0]0_[F,B:0]04A_dct[3:0][MajorMode], and D18F2x9C_x00[F,8:0]1_[F,B:0]04A_dct[3:0][MajorMode].
DdrRate	The DDR data rate (MT/s) as specified by (if Ddr3Mode then D18F2x94_dct[3:0][MemClkFreq] and D18F2x2E0_dct[3:0][M1MemClkFreq], else D18F2xB1C_dct[3:0][MemClkFreq]).
DeviceWidth	DDR3 SPDByte[7][2:0] of the DIMM being configured.
DIMM	The DIMM being configured.

Table 15: DCT Definitions

Term	Definition
DIMM0	DIMM slots 0-n. The DIMMs on each channel are numbered from 0 to n where DIMM0 is the DIMM closest to the processor on that channel and DIMMn is the DIMM farthest from the processor on that channel.
DIMM1	
DimmsPopulated	The number of DIMMs populated per channel plus rows of Solder-down DRAM devices.
DR	Dual Rank.
DramCapacity	DDR3 SPDByte[4][3:0] of the DIMM being configured.
ExtendedTemperature-Range	DDR3 SPDByte[31][0] of the DIMM being configured.
Gddr5Mode	The DRAM controller and the phy are configured for GDDR5 mode. Note: this mode may not be supported by this processor. See section 2.9, or consult processor data sheet to determine which modes are supported.
MaxDct	The range of values supported by D18F1x10C[DctCfgSel] for registers with the mnemonic D18F2xXXX_dct[MaxDct:0]. MaxDct = 3. See 2.9.3 [DCT Configuration Registers].
MaxDctMstr	The range of values supported by D18F1x10C[DctCfgSel] for registers with the mnemonic D18F2x[B,0]9[C,8]_xXXXX_XXXX_dct[MaxDctMstr:0]. See 2.9.3 [DCT Configuration Registers].
MRS	JEDEC defined DRAM Mode Register Set.
NP	No DIMM populated.
NumDimmSlots	The number of motherboard DIMM slots per channel plus rows of Solder-down DRAM devices.
NumRanks	DDR3 SPDByte[7][5:3] of the DIMM being configured, or the number of ranks soldered down.
Rank	The rank being configured.
RankMap	DDR3 SPDByte[63][0] of the DIMM being configured.
RowAddrBits	DDR3 SPDByte[5][5:3] of the DIMM being configured.
Solder-down DRAM	DRAM devices soldered directly to the motherboard.
SODIMM	DCT is configured for SODIMM if (D18F2x90_dct[3:0][UnbuffDimm]==1) and SODIMMs are populated.
SPD	Serial Presence Detect. In the case of DRAMs soldered on the platform, this refers to a virtual representation of the DRAM vendors' data sheets.
SR	Single Rank.
UDIMM	DCT is configured for UDIMM if (D18F2x90_dct[3:0][UnbuffDimm]==1) and UDIMMs are populated.
VDDIO	DDR VDDIO in V.

2.9.2 DCT Frequency Support

The tables below list the maximum DIMM speeds supported by the processor for different configurations. The motherboard should comply with the relevant AMD socket motherboard design guideline (MBDG) to achieve the rated speeds. In cases where MBDG design options exist, lower-quality options may compromise the maximum achievable speed; motherboard designers should assess the trade-offs.

The FP3 package supports two different voltage levels on the VDDR rail. At the 1.05V nominal setting, the maximum speed of 2133 can be supported while at the 0.95V setting, the maximum speed supported is 1600. See 2.11.3.1 for its effect on PCIe data rate.

Table 16: DDR3 UDIMM Maximum Frequency Support for FM2r2 package

Num-DimmS-lots	Dimms Popu-lated	DRAM		Frequency[1] (MT/s)		
		SR	DR	1.5V	1.35V	1.25V
1	1	1	-	2133	1866	1600
		-	1	1866	1600	1600
2	1	1	-	1866	1600	1333
		-	1	1866	1600	1333
	2	2	-	1866	1600	1333
		1	1	1600	1333	1333
		-	2	1600	1333	1333

1. Population restrictions (including the order for partially populated channels) may apply. NumDimmSlots and DimmsPopulated are per channel.

Table 17: DDR3 UDIMM Maximum Frequency Support for FP3 package

Num-DimmS-lots	Dimms Popu-lated	DRAM		Frequency[1] (MT/s)		
		SR	DR	1.5V	1.35V	1.25V
1	1	1	-	2133	1866	1600
		-	1	1866	1600	1600
2	1	1	-	2133	1866	1600
		-	1	1866	1600	1600
	2	2	-	1866	1600	1333
		1	1	1600	1333	1333
		-	2	1600	1333	1333

1. Population restrictions (including the order for partially populated channels) may apply. NumDimmSlots and DimmsPopulated are per channel.

Table 18: DDR3 SODIMM Maximum Frequency Support for FM2r2 package

Num-DimmS-lots	Dimms Popu-lated	DRAM		Frequency[1] (MT/s)		
		SR	DR	1.5V	1.35V	1.25V
1	1	1	-	2133	1866	1600
		-	1	1866	1600	1600

Table 18: DDR3 SODIMM Maximum Frequency Support for FM2r2 package

Num-DimmS-lots	Dimms Popu-lated	DRAM		Frequency[1] (MT/s)		
		SR	DR	1.5V	1.35V	1.25V
2	1	1	-	1600	1600	1333
		-	1	1600	1600	1333
	2	2	-	1600	1333	1333
		1	1	1333	1333	1333
		-	2	1333	1333	1333

1. Population restrictions (including the order for partially populated channels) may apply. NumDimmSlots and DimmsPopulated are per channel.

Table 19: DDR3 SODIMM Maximum Frequency Support for FP3 package

Num-DimmS-lots	Dimms Popu-lated	DRAM		Frequency[1] (MT/s)		
		SR	DR	1.5V	1.35V	1.25V
1	1	1	-	2133	1866	1600
		-	1	1866	1600	1600
2	1	1	-	1600	1600	1333
		-	1	1600	1600	1333
	2	2	-	1600	1333	1333
		1	1	1333	1333	1333
		-	2	1333	1333	1333

1. Population restrictions (including the order for partially populated channels) may apply. NumDimmSlots and DimmsPopulated are per channel.

2.9.3 DCT Configuration Registers

There are multiple types of DCT configuration registers:

- Registers for which there is one instance for all DCTs. E.g. D18F2xA4.
- Registers for which there is one instance per DCT. E.g. D18F2x78_dct[3:0].
  - For D18F2x78_dct[x], x=D18F1x10C[DctCfgSel]; see D18F1x10C[DctCfgSel].
  - The syntax for this register type is described by example as follows:
    - D18F2x78_dct[3:0] refers to all instances of the D18F2x78 register.
    - D18F2x78_dct[1] refers to the D18F2x78 register instance for DCT1.
- Registers for which there is one instance per NbPstate use D18F1x10C[NbPsSel] for software accesses.
  - D18F2x210_dct[3:0]_nbp[3:0] refers to all instances of the D18F2x210 register.
  - D18F2x210_dct[3:0]_nbp[1] refers to the register for Nb P-state 1 of any or all DCTs.
- Registers for which there is one instance per memory P-state use D18F1x10C[MemPsSel] for software accesses. The syntax for this register type is described by example as follows:
  - D18F2x2E8_dct[3:0]_mp[1:0] refers to all instances of the D18F2x2E8 register.
  - D18F2x2E8_dct[3:0]_mp[1] refers to the register for memory P-state 1 of either or both DCTs.

In Ddr3Mode, the DCT controls 64-bits of data. The phy registers of a 64-bit phy channel are programmed through a single DCT master by setting D18F1x10C[DctCfgSel] to the DCT master as shown in Table 14.

2.9.4 DDR Pad to Processor Pin Mapping

The relationship of pad drivers to processor pins varies by package as shown in the following table.

Table 20: Package pin mapping

Pad	Pin[1]		
	FS2 (not supported)	FM2r2	FP3
MEMCLK0_H[0]	MA_CLK_H[0]		
MEMCLK0_H[1]	MA_CLK_H[1]		
MEMCLK0_H[2]	NC	MA_CLK_H[2]	
MEMCLK0_H[3]	NC	MA_CLK_H[3]	
MEMCLK0_H[4]	NC		
MEMCLK1_H[0]	MB_CLK_H[0]		
MEMCLK1_H[1]	MB_CLK_H[1]		
MEMCLK1_H[2]	NC	MB_CLK_H[2]	
MEMCLK1_H[3]	NC	MB_CLK_H[3]	
MEMCLK1_H[4]	NC		
MEMCS0_L[0]	MA0_CS_L[0]		
MEMCS0_L[1]	MA0_CS_L[1]		
MEMCS0_L[2]	NC	MA1_CS_L[0]	
MEMCS0_L[3]	NC	MA1_CS_L[1]	
MEMCS0_L[4]	NC		
MEMCS0_L[5]	NC		
MEMCS0_L[6]	NC		
MEMCS0_L[7]	NC		
MEMCS1_L[0]	MB0_CS_L[0]		
MEMCS1_L[1]	MB0_CS_L[1]		
MEMCS1_L[2]	NC	MB1_CS_L[0]	
MEMCS1_L[3]	NC	MB1_CS_L[1]	
MEMCS1_L[4]	NC		
MEMCS1_L[5]	NC		
MEMCS1_L[6]	NC		
MEMCS1_L[7]	NC		
MEMODT0[0]	MA0_ODT[0]		
MEMODT0[1]	MA0_ODT[1]		
MEMODT0[2]	NC	MA1_ODT[0]	
MEMODT0[3]	NC	MA1_ODT[1]	
MEMODT1[0]	MB0_ODT[0]		
MEMODT1[1]	MB0_ODT[1]		

Table 20: Package pin mapping

MEMODT1[2]	NC	MB1_ODT[0]	
MEMODT1[3]	NC	MB1_ODT[1]	
MEMCKE0[0]	MA_CKE[0]		
MEMCKE0[1]	MA_CKE[1]		
MEMCKE0[2]	NC		MA_CKE[2]
MEMCKE0[3]	NC		MA_CKE[3]
MEMCKE1[0]	MB_CKE[0]		
MEMCKE1[1]	MB_CKE[1]		
MEMCKE1[2]	NC		MB_CKE[2]
MEMCKE1[3]	NC		MB_CKE[3]

1. For differential pins, only positive polarity pins are shown; negative polarity pins have corresponding mapping and are controlled by the same CSR field.
NC = Not connected. BIOS should tri-state or disable the pad for maximum power savings.

2.9.4.1 DDR Chip to Pad Mapping

The relationship of chip to pad drivers is shown in the following table. BIOS should disable or power down unused chips for maximum power savings.

Table 21: DDR Chip to pad mapping (DDR3 Mode)

Chiplet	Group	Pad Number[1]	Pad[2]
CAD 0	0	3,2,1,0	MEMCKE0[2], MEMCKE0[3], MEMCKE0[0], MEMCKE0[1]
	1		Unused
	2	11,10,9,8, 7,6,5,4	MEMADD0[14,15,12], MEMBANK0[2], MEMADD0[8,7,11,9]
	3		Unused
CAD 1	0	11,10,3,2, 1,0	MEMCLK0_L[4], MEMCLK0_H[4], MEMCLK0_L[2], MEMCLK0_H[2], MEMCLK0_L[0], MEMCLK0_H[0]
	1		Unused
	2	9,8,7,6,5, 4	MEMADD0[5,6], MEMADD0[2,1,3,4]
	3		Unused
CAD 2	0	3,2,1,0	MEMCLK0_L[3], MEMCLK0_H[3], MEMCLK0_L[1], MEMCLK0_H[1]
	1	7,6,5,4	MEMADD0[10], MEMBANK0[0], MEMADD0[0], MEMBANK0[1]
	2	11,10,9,8	MEMCS0_L[6], MEMCS0_L[4], MEMCS0_L[2], MEMCS0_L[0]
	3		Unused

Table 21: DDR Chip to pad mapping (DDR3 Mode)

CAD 3	0	3,2,1,0	MEMADD0[13], MEMCAS0_L, MEMWE0_L, MEMRAS0_L
	1	7,6,5,4	MEMODT0[3], MEMODT0[1], MEMODT0[0], MEMODT0[2]
	2	11,10,9,8	MEMCS0_L[7], MEMCS0_L[5], MEMCS0_L[3], MEMCS0_L[1]
	3		Unused
DATA[3] [7:0]	0	3,2,1,0	DQ[3,2,1,0]
	1 (transmit control)	11,10,9,8	unused, MEMDQS_L[0][4], MEMDQSDM[0][4], MEMDQS_H[0][4]
	1 (receive control)	11,10,9,8	unused, (MEMDQS_L[0][4] and MEMDQSDM[0][4]), unused, unused
	2	7,6,5,4	DQ[7,6,5,4]
DATA 8	0	3,2,1,0	MEMCHECK[3,2,1,0]
	1 (transmit control)	11,10,9,8	unused, MEMDQS_L[0][4], MEMDQSDM[0][4], MEMDQS_H[0][4]
	1 (receive control)	11,10,9,8	unused, (MEMCHECKDQS_L[0][4] and MEMCHECKDQSDM[0][4]), unused, unused
	2	7,6,5,4	MEMCHECK[7,6,5,4]

1. Pad number is the logical address of a CSR addressable timing or impedance control. D18F2x9C_x00[F,3:0]0_0009_dct[3:0][HiAddrMode] = 0.
2. Only channel A is shown. Channel B is similar.
3. Pad column shows pads only for Data chip 0. Data chips [7:1] are repeated with sequential DQ/DQS/DM pin numbers.
4. MEMDQSDM functions as DM when using unbuffered DIMMs. MEMDQS_H is the positive polarity of the “lower nibble” DQS pad used for all devices.

2.9.5 DRAM Controller Direct Response Mode

The DCT supports direct response mode for responding to a cache line fill request before the DCT is initialized. In direct response mode, the target DCT responds to a cache line fill request by returning 64 bytes of all ones without issuing a read transaction on the DRAM bus. The BIOS uses this feature to allocate cache lines for temporary data storage. The controller exits direct response mode when either D18F2x78_dct[3:0][ChanVal] is set to 1. See 2.3.3 [Using L2 Cache as General Storage During Boot].

2.9.6 DRAM Data Burst Mapping

DRAM requests are mapped to data bursts on the DDR bus in the following order:
- When D18F2x110[DctDatIntLv] = 0, a 64 B request is mapped to each of the eight sequential data beats as

QW0, QW1,...QW7.

- When D18F2x110[DctDatIntLv] = 1, the order of cache data to QW on the bus is the same except that even and odd bits are interleaved on the DRAM bus as follows:
  - For every 8 bytes in the cache line, even bits map to QW0, QW2, QW4, and QW6 on the DRAM bus.
  - For every 8 bytes in the cache line, odd bits map to QW1, QW3, QW5, and QW7 on the DRAM bus.

2.9.7 SOC Specific Definitions

Table 22: DCT Definitions

Term	Definition
GraphicsDC	Graphics downcore.
Solder-down DRAM	DRAM devices soldered directly to the motherboard.
SRAMMsgBlk	SRAM message block. See 2.9.8.3 [SRAM Message Block].

2.9.8 PMU

The processor includes a phy micro-controller unit (PMU) used for training the DDR data bus during boot. BIOS communicates with the PMU using one of two methods.

- Mailbox: BIOS waits for upstream messages from the PMU for action synchronization or for status messages.
  - A 16-bit mailbox exists for upstream messages. See 2.9.8.1. Only the lower 8-bits are used. BIOS may safely ignore the upper 8-bits of the message.
  - A 16-bit mailbox exists for upstream data transfer. See 2.9.8.2.
- SRAM: BIOS may read or write the memory used bythe PMU to send or receive complex message data. The PMU must be halted or in the reset state for BIOS to access PMU SRAM.

2.9.8.1 mboxUSPend

To wait for an upstream message BIOS does the following:

1. Wait until D18F2x9C_x0002_0004_dct[3:0][UsRdy]==0.
2. Read D18F2x9C_x0002_0032_dct[3:0][Message]. See Table 23 for a list of message names and values.
3. Program D18F2x9C_x0002_0033_dct[3:0][Rdy] = 1.

See 2.9.9.5 for related information.

Table 23: US Mailbox 1 Messages for DDR3

Name	D18F2x9C_x0002_0032_dct[3:0][Message]	Description
DevInit	00h	PMU has completed DevInit.
TrainWrLvl	01h	PMU has completed TSTAGE_WrLvl
TrainRxEn	02h	PMU has completed TSTAGE_RxEn
TrainRdDqs1D	03h	PMU has completed TSTAGE_RdDqs1D
TrainWrDq1D	04h	PMU has completed TSTAGE_WrDq1D
TrainRd2D	05h	PMU has completed TSTAGE_Rd2D
TrainWr2D	06h	PMU has completed TSTAGE_Wr2D.

Table 23: US Mailbox 1 Messages for DDR3

Name	D18F2x9C_x0002_0032_dct[3:0][Message]	Description
PMUQEmpty	07h	PMU has completed all of its SequenceCtl tasks and is in a power-gated idle state.
US2MsgRdy	08h	PMU is ready to stream a message through US mailbox 2.
FAIL	0FFh	PMU has encountered an error which requires requester to abort waiting for remaining pending upstream messages.

2.9.8.2 mboxUS2Pend

To receive a block of data through US mailbox 2, BIOS does the following:

1. Wait until D18F2x9C_x0002_0004_dct[3:0][Us2Rdy]==0.
2. Read D18F2x9C_x0002_0034_dct[3:0][Message]. The first item received is the COUNT.
3. Program D18F2x9C_x0002_0035_dct[3:0][Rdy] = 1.
4. Decrement COUNT and loop to step 1 until COUNT==-1.

2.9.8.3 SRAM Message Block

The SRAM message block is used to pass information from BIOS to PMU and vice-versa. BIOS accesses the SRAM message block through D18F2x9C_x0005_[0BFF:0000]_dct[3:0].

Table 24: SRAM Message Block for DDR3

Name	Memory P-state[1]	Location[2]	Input for	Output of	Description
Revision	-	00h	DevInit	-	Table revision.
Reserved	-	03:01h		-	
CpuId	-	07:04h	DevInit	-	32-bit CPUID
DramType	-	08h	DevInit	-	Dram type from SPD byte 2 (e.g. 0Bh=DDR3)
ModuleType	-	09h	DevInit	-	ModuleType[6:0]=Module type from SPD byte 3 (e.g. 02h=UDIMM, 03h=SO-DIMM) ModuleType[7]=PMU-train-ECC. BIOS sets to 1 if all DIMMs on the channel are ECC capable; 0 otherwise.
RawCard0	-	0Ah	DevInit	-	DIMM0 reference raw card from module type specific SPD location (e.g. byte 62 is used for UDIMMs).
RawCard1	-	0Bh	DevInit	-	DIMM1 reference raw card from module type specific SPD location (e.g. byte 62 is used for UDIMMs).
Reserved		0D:0Ch			

Table 24: SRAM Message Block for DDR3

Name	Memory P-state[1]	Location[2]	Input for	Output of	Description
ChipSelect	-	0Eh	DevInit	-	Specifies which chipselects are present and should be trained. Bit[0] is chip select 0, Bit[1] is chip select 1, etc.
AddrMirror	-	0Fh	DevInit	-	For each chipselect, specifies which chipselects have address mirroring (BA0 swapped with BA1, A3 swapped with A4, A5 swapped with A6, A7 swapped with A8).
Dimm0Cols	-	10h	DevInit	-	Number of device column address bits for Dimm0.
Dimm0Banks	-	11h	DevInit	-	Number of device bank address bits for Dimm0.
Dimm0Rows	-	12h	DevInit	-	Number of device row address bits for Dimm0.
Dimm1Cols	-	13h	DevInit	-	Number of device column address bits for Dimm1.
Dimm1Banks	-	14h	DevInit	-	Number of device bank address bits for Dimm1.
Dimm1Rows	-	15h	DevInit	-	Number of device row address bits for Dimm1.
Reserved		1B:16h			
TestFail	-	1Ch	-	any	Specifies which chipselects (if any) have failed training. Bit[0] is chip select 0, Bit[1] is chip select 1, etc.
PerRankTiming	-	1Dh	TSTAGE_RxEn	-	1=The channel is configured to use four timing sources for four independent chipselects. 0=The channel is configured to use four timing sources for four pairs of chipselects (logical DIMMs).
CurrentTemp	-	1F:1Eh	DevInit	-	
SequenceCtl	-	21:20h	any	-	PMU Sequence Control Word [0] 1=DevInit [1] 1=WrLvl Training [2] 1=RxEnDly Training [3] 1=1D Rd-Dqs Training [4] 1=1D Wr-Dq Training [5] 1=2D Read Training [6] 1=2D Write Training [15:7] Reserved
Reserved	-	22h			
CkeSetup	0	23h	DevInit	-	Setup time on CAD bus signals. See AddrCmdSetup for data format.
CsOdtSetup	0	24h	DevInit	-	Setup time on CAD bus signals. See AddrCmdSetup for data format.

Table 24: SRAM Message Block for DDR3

Name	Memory P-state[1]	Location[2]	Input for	Output of	Description
AddrCmdSetup	0	25h	DevInit	-	Setup time on CAD bus signals. [4:0] Fine delay, in 1/32 UI increments, relative to prelaunch. [5] Prelaunch, in 1UI increments, relative to positive latching memclock edge. 1=1 memclock, 0=1/2 memclock. If the signal is in 2T timing mode then signal asserts exactly 1 memclock earlier than specified and is 2 memclocks in duration.
SlowAccessMode	0	26h	DevInit	-	1=2T Timing is enabled in the controller (See D18F2x94_dct[3:0][SlowAccessMode].
tRP	0	27h	DevInit	-	In units of memclocks. See D18F2x200_dct[3:0]_mp[1:0][Trp] for definition.
tMRD	0	28h	DevInit	-	In units of memclocks. See D18F2x220_dct[3:0][Tmrd] for definition.
tRFC	0	29h	DevInit	-	In units of memclocks. The maximum value for all DIMMs. See D18F2x208_dct[3:0][Trfc].
MR0	0	2B:2Ah	DevInit	-	
MR1	0	2D:2Ch	DevInit	-	
MR2	0	2F:2Eh	DevInit	-	
CD_R_W	0	30h	-	TSTAGE_Wr2D	Command delay, read to write, any chip select to any other chipselect. Units are memclocks, unsigned integer.
CD_R_R	0	31h	-	TSTAGE_Wr2D	Command delay, read to read, any chip select to any other chipselect. Units are memclocks, unsigned integer.
CD_W_W	0	32h	-	TSTAGE_Wr2D	Command delay, write to write, any chip select to any other chipselect. Units are memclocks, unsigned integer.
CD_W_R	0	33h	-	TSTAGE_Wr2D	Command delay, write to read, any chip select to any other chipselect. Units are memclocks, unsigned integer.
CD_R_R_SD	0	34h	-	TSTAGE_Wr2D	Command delay, read to read, any chip select to another chipselect of same DIMM. Units are memclocks, unsigned integer.
CD_W_W_SD	0	35h	-	TSTAGE_Wr2D	Command delay, write to write, any chip select to another chipselect of same DIMM. Units are memclocks, unsigned integer.
Trdrdban_Phy	0	36h	-	TSTAGE_Rd2D	In memclocks. See D18F2x218_dct[3:0]_mp[1:0][TrdrdBan].
CkeSetup	1	37h	DevInit	-	Setup time on CAD bus signals. See AddrCmdSetup for data format.

Table 24: SRAM Message Block for DDR3

Name	Memory P-state[1]	Location[2]	Input for	Output of	Description
CsOdtSetup	1	38h	DevInit	-	Setup time on CAD bus signals. See AddrCmdSetup for data format.
AddrCmdSetup	1	39h	DevInit	-	Setup time on CAD bus signals. [4:0] Fine delay, in 1/32 UI increments, relative to prelaunch. [5] Prelaunch, in 1UI increments, relative to positive latching memclock edge. 1=1 memclock, 0=1/2 memclock. If the signal is in 2T timing mode then signal asserts exactly 1 memclock earlier than specified and is 2 memclocks in duration.
SlowAccessMode	1	3Ah	DevInit	-	1=2T Timing is enabled in the controller (See D18F2x94_dct[3:0][SlowAccessMode]. Note: Current DCT implementation does not support per memory P-state instances.
tRP	1	3Bh	DevInit	-	In units of memclocks. See D18F2x200_dct[3:0]_mp[1:0][Trp] for definition.
tMRD	1	3Ch	DevInit	-	In units of memclocks. See D18F2x220_dct[3:0][Tmrd] for definition.
tRFC	1	3Dh	DevInit	-	In units of memclocks. The maximum value for all DIMMs. See D18F2x208_dct[3:0][Trfc].
MR0	1	3F:3Eh	DevInit	-	
MR1	1	41:40h	DevInit	-	
MR2	1	43:42h	DevInit	-	
CD_R_W	1	44h	-	TSTAGE_Wr2D	Command delay, read to write, any chip select to any other chipselect. Units are memclocks, unsigned integer.
CD_R_R	1	45h	-	TSTAGE_Wr2D	Command delay, read to read, any chip select to any other chipselect. Units are memclocks, unsigned integer.
CD_W_W	1	46h	-	TSTAGE_Wr2D	Command delay, write to write, any chip select to any other chipselect. Units are memclocks, unsigned integer.
CD_W_R	1	47h	-	TSTAGE_Wr2D	Command delay, write to read, any chip select to any other chipselect. Units are memclocks, unsigned integer.
CD_R_R_SD	1	48h	-	TSTAGE_Wr2D	Command delay, read to read, any chip select to another chipselect of same DIMM. Units are memclocks, unsigned integer.

Table 24: SRAM Message Block for DDR3

Name	Memory P-state[1]	Location[2]	Input for	Output of	Description
CD_W_W_SD	1	49h	-	TSTAGE_Wr2D	Command delay, write to write, any chip select to another chipselect of same DIMM. Units are memclocks, unsigned integer.
Trdrdban_Phy	1	4Ah	-	TSTAGE_Rd2D	In memclocks. See D18F2x218_dct[3:0]_mp[1:0][TrdrdBan]

1. If no memory P-state is specified then the field applies to both states.
2. Locations are byte address offsets and are relative to the start of D18F2x9C_x0005_[0BFF:0000]_dct[3:0]. Thus to access an odd byte, software accesses the upper 8-bits of the even word-address.

2.9.9 DCT/DRAM Initialization and Resume

DRAM initialization involves several steps in order to configure the DRAM controllers and the DRAM, and to tune the DRAM channel for optimal performance. DRAM resume requires several steps to configure the DCTs to properly resume from the S3 state. The following sequence describes the steps needed after a reset for initialization or resume:

- To disable an unused DRAM channel see 2.9.9.8.

1. Configure the DDR supply voltage regulator. See 2.9.9.1.
2. NB P-state specific initialization.
   A. Program the DCT configuration registers which contain multiple internal copies for each NB P-state. See D18F1x10C[NbPsSel].
   B. Force NB P-state to NBP0. See 2.5.4.1.3.2
3. DDR phy initialization. See 2.9.9.2.
4. If BIOS is booting from an unpowered state (ACPI S4, S5 or G3), then it performs the following:
   A. Program DRAM controller general configuration, for both memory P-states. See 2.9.9.3.
   B. Program DCT specific configuration for training, for both memory P-states. See 2.9.9.4.
   C. Program the remaining DCT registers not covered by an explicit sequence dependency.
   D. Program D18F2x9C_x0002_0060_dct[3:0][MemReset_L]=0.
   E. Program D18F2x9C_x0002_000B_dct[3:0]=0004h.
   F. Program D18F2x9C_x0002_000B_dct[3:0]=0000h.
   G. Perform DRAM device initialization and data training. See 2.9.9.5.
   H. Enable phy auto-calibration. See 2.9.9.2.8.3.
   I. Synchronous channel initialization. See 2.9.9.7.
   J. Program D18F2x90_dct[3:0][ExitSelfRef]=1. Wait for D18F2x90_dct[3:0][ExitSelfRef]==0. Wait Tref*2.
   K. Program D18F2x78_dct[3:0][ChanVal]=1.
   L. NB P-state specific training. For each NB P-state from NBP0 to D18F5x170[NbPstateMaxVal]:
      a. Force the NB P-state. See 2.5.4.1.3.2.
      b. MaxRdLatency training. See 2.9.9.6.1.
   M. Program DCT specific configuration for normal operation, for both memory P-states. See 2.9.9.4.
   N. Program DRAM phy for power savings. See 2.9.9.9.
5. If BIOS is resuming the platform from S3 state, then it performs the following:
   A. Restore all DCT and phy registers that were programmed during the first boot from non-volatile storage. See 2.9.9.3, 2.9.9.4, and 2.9.9.9 for a review of registers.
   B. Restore the trained delayed values from nonvolatile storage. See 2.9.9.2.10.
   C. Program D18F2x9C_x0002_0060_dct[3:0][MemReset_L]=1.
   D. Program D18F2x9C_x0002_000B_dct[3:0]=0004h.
   E. Program D18F2x9C_x0002_000B_dct[3:0]=0000h.
   F. Fence the CalOnce. See 2.9.9.2.8.2.
   G. Enable phy auto-calibration. See 2.9.9.2.8.3.
   H. Synchronous channel initialization. See 2.9.9.7.
   I. Program D18F2x90_dct[3:0][ExitSelfRef]=1. Wait for D18F2x90_dct[3:0][ExitSelfRef]==0
   J. Program D18F2x78_dct[3:0][ChanVal]=1.
6. Release NB P-state force. See 2.5.4.1.3.2.

The DRAM subsystem is ready for use.

2.9.9.1 Low Voltage

For DDR3 devices, the processor supports JEDEC defined 1.5V, 1.35V and 1.25V devices

Platforms supporting low voltage devices should power up VDDIO at 135V. BIOS should not operate DIMMs at voltages higher than supported. For DDR3 this is indicated by SPD Byte 6: Module Nominal Voltage, VDD.

BIOS should consult vendor data sheets for the supply voltage regulator programming requirements. On supported platforms, BIOS must take steps to configure the supply voltage regulators as follows:

1. Read the SPD of all devices within the programmable VDDIO domain and check all of the defined bits within the SPD byte to determine the common operating voltages.
2. Configure VDDIO to match the lowest common supported voltage based on the SPD values.
   - If the DIMMs do not specify a common operating voltage then BIOS must take platform vendor defined action to notify the end user of the mismatch and to protect DIMMs from damage.
3. Additional derating of the DDR speed may be necessary for reliable operation at lower voltage.

2.9.9.2 DDR Phy Initialization

The BIOS initializes the phy and the internal interface from the DCT to the phy, after each reset and for each time a MEMCLK frequency change is made.

BIOS obtains size, loading, and frequency information about the DIMMs andchannels using SPDs prior to phy initialization. BIOS then performs the following actions:

1. Program D18F2x9C_x0002_0099_dct[3:0][PmuReset,PmuStall] = 1,1.
2. Program D18F2x9C_x0002_000E_dct[3:0][PhyDisable]=0.
3. According to the type of DRAM attached, program the following:
   - Program D18F2x9C_x00FF_F04A_dct[3:0] = {000000h,0b,MajorMode,0h}. This is a “super-broadcast” to all instances. See:
     - D18F2x9C_x00[F,3:0]0_[F,B:0]04A_dct[3:0][MajorMode]
     - D18F2x9C_x00[F,8:0]1_[F,B:0]04A_dct[3:0][MajorMode]
     - D18F2x9C_x0009_004A_dct[3:0][MajorMode]
   - D18F2x9C_x00[F,8:0]1_[F,B:0]05F_dct[3:0][G5Mode] This register is optimally programmed during data bus driver configuration in 2.9.9.2.5 instead of at this time.
   - D18F2x9C_x0002_000E_dct[3:0][G5_Mode]
   - D18F2x9C_x0002_0098_dct[3:0][CalG5D3].
4. Program general phy static configuration. See 2.9.9.2.1.
5. Phy Voltage Level Programming. See 2.9.9.2.2.
6. Program auto-calibration. See 2.9.9.2.8.
7. Program DRAM channel frequency. See 2.9.9.2.3.
8. Program default CAD bus values. See 2.9.9.2.4.
9. Program default data bus values. See 2.9.9.2.5.
10. Program FIFO pointer init values. See 2.9.9.2.6.
11. Program predriver values. See 2.9.9.2.7.
12. Program D18F2x9C_x0002_0033_dct[3:0][Rdy] = 1.
13. Program D18F2x9C_x0002_0035_dct[3:0][Rdy] = 1.

2.9.9.2.1 Phy General Configuration

BIOS programs the following according to the static configuration:

- Program D18F2x9C_x01F1_F045_dct[3:0]=0040h.
  - See D18F2x9C_x0[3,1:0][F,8:0]1_[F,7:0]045_dct[3:0].
- If Ddr3Mode program D18F2x9C_x00F4_00E[7:0]_dct[3:0].
- Program D18F2x9C_x00F0_0015_dct[3:0][VrefFilt], D18F2x9C_x00F1_0015_dct[3:0][VrefFilt], D18F2x9C_x00F2_0015_dct[3:0][VrefFilt].
- Program D18F2x9C_x00[F,8:0]1_0016_dct[3:0].

BIOS programs the following for maximum power savings prior to training:

- Program D18F2x9C_x03F6_F04E_dct[] = 0B00h.
  - See D18F2x9C_x00[F,3:0]0_[F,B:0]04E_dct[3:0] and D18F2x9C_x00[F,8:0]1_[F,B:0]04E_dct[3:0].
- Program D18F2x9C_x00F0_001A_dct[] (undocumented) = 0022h.
- Program D18F2x9C_x00F1_001A_dct[] (undocumented) = 0033h.
- Program D18F2x9C_x0002_001A_dct[] (undocumented) = 0001h.
- Program D18F2x9C_x0002_005B_dct[3:0] = 0001h.
- Program D18F2x9C_x00F1_F051_dct[] = 0152h.
  - See D18F2x9C_x00[F,8:0]1_[F,B:0]051_dct[3:0].

2.9.9.2.2 Phy Voltage Level Programming

BIOS programs the following according to the desired phy VDDIO voltage level:

1. Program D18F2x9C_x0002_0098_dct[3:0][CalCmptrResTrim].

See 2.9.9.1 [Low Voltage].

2.9.9.2.3 DRAM Channel Frequency

BIOS programs the DCT and the phy according to the data rate. BIOS must ensure that the DCT and the phy operate at a matched rate prior to normal operations. See D18F2x94_dct[3:0][MemClkFreq], D18F2x2E0_dct[3:0][M1MemClkFreq].

To program a new rate in the phy:
1. Program D18F2x9C_x0002_0093_dct[3:0][PllRegWaitTime] = 04Bh.
2. Program D18F2x9C_x0002_0089_dct[3:0][PllLockTime] = 190h.
3. Program D18F2x9C_x0002_0000_dct[3:0][PllMultDiv].
4. Program D18F2x9C_x0002_0080_dct[3:0][PMUClkDiv].
   - See D18F2x9C_x0[1:0]02_0080_dct[3:0].
5. Program D18F2x9C_x0002_0001_dct[3:0][PllMultDiv] = ‘667 MT/s’.
6. Program D18F2x9C_x0102_0080_dct[3:0][PMUClkDiv].
   - See D18F2x9C_x0[1:0]02_0080_dct[3:0].

The new settings will take effect after BIOS or the DCT requests a memory P-state change request via D18F2x9C_x0002_000B_dct[3:0]. See 2.9.9 [DCT/DRAM Initialization and Resume].

2.9.9.2.4 DRAM CAD Bus Configuration

This section describes the settings required for programming the timing and drive settings on the command and

address pins. The following tables document the CAD bus values on a per channel basis. DIMM0 is the DIMM closest to the processor on that channel and DIMM1 is the DIMM farthest from the processor on that channel. DIMMs must be populated from farthest slot to closest slot to the processor on a per channel basis (when a daisy chain topology is used). Populations that are not shown in these tables are not supported. These tables document the optimal settings for motherboards which meet the relevant motherboard design guidelines.

- Only the value for a single control unit register is described. The values in the table should be broadcast to all instances of registers of the same control unit type, unless otherwise noted.

Table 25: BIOS Recommendations for DDR3 SO-DIMM CAD bus configuration

Condition										
Condition:NumDimmSlots	Condition:DdrRate	Condition:VDDIO	Condition:DIMM0	Condition:DIMM1	D18F2x94_dct[3:0][SlowAccessMode]	{0000000000b,AddrCmdSetup[5:0],00b,CsOdtSetup[5:0],00b,CkeSetup[5:0]}[1]	D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0][DrvStrenN][2] for CKE	D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0][DrvStrenN][2] for CS and ODT	D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0][DrvStrenN][2] for AddrCmd	D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0][DrvStrenN][2] for CLK
1	667	1.25, 1.35, 1.5	SR	-	0	00000000h	1Fh	1Fh	1Fh	1Fh
1	667	1.25, 1.35, 1.5	DR	-	0	003B0000h	1Fh	1Fh	1Fh	1Fh
1	800	1.25, 1.35, 1.5	SR	-	0	00000000h	1Fh	1Fh	1Fh	1Fh
1	800	1.25, 1.35, 1.5	DR	-	0	003B0000h	1Fh	1Fh	1Fh	1Fh
1	1066	1.25, 1.35, 1.5	SR	-	0	00000000h	1Fh	1Fh	1Fh	1Fh
1	1066	1.25, 1.35, 1.5	DR	-	0	00380000h	1Fh	1Fh	1Fh	1Fh
1	1333	1.25, 1.35, 1.5	SR	-	0	00000000h	1Fh	1Fh	1Fh	1Fh
1	1333	1.25, 1.35, 1.5	DR	-	0	00360000h	1Fh	1Fh	1Fh	1Fh
1	1600	1.25, 1.35, 1.5	SR	-	0	00000000h	1Fh	1Fh	1Fh	1Fh
1	1600	1.25, 1.35, 1.5	DR	-	1	00000000h	1Fh	1Fh	1Fh	1Fh
1	1866	1.35, 1.5	SR	-	0	00000000h	1Fh	1Fh	1Fh	1Fh
1	1866	1.35, 1.5	DR	-	1	00000000h	1Fh	1Fh	1Fh	1Fh
1	2133	1.5	SR	-	0	00000000h	1Fh	1Fh	1Fh	1Fh
1	2133	1.5	DR	-	1	00000000h	1Fh	1Fh	1Fh	1Fh
2	667	1.25, 1.35, 1.5	NP	SR	0	00000000h	1Fh	1Fh	1Fh	1Fh
2	667	1.25, 1.35, 1.5	NP	DR	0	003B0000h	1Fh	1Fh	1Fh	1Fh
2	667	1.25, 1.35, 1.5	SR	SR	0	00390039h	1Fh	1Fh	3Fh	1Fh
2	667	1.25, 1.35, 1.5	DR	DR	0	00390039h	1Fh	1Fh	3Fh	1Fh

Table 25: BIOS Recommendations for DDR3 SO-DIMM CAD bus configuration

Condition					D18F2x94_dct[3:0] [SlowAccessMode]	{0000000000b,AddrCmdSetup[5:0],00b,CsOdtSetup[5:0], 00b, CkeSetup[5:0]}[1]	D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0] [DrvStrenN][2] for CKE	D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0] [DrvStrenN][2] for CS and ODT	D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0] [DrvStrenN][2] for AddrCmd	D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0] [DrvStrenN][2] for CLK
Condition:NumDimmSlots	Condition:DdrRate	Condition:VDDIO	Condition:DIMM0	Condition:DIMM1						
2	667	1.25, 1.35, 1.5	DR	SR	0	00390039h	1Fh	1Fh	3Fh	1Fh
2	667	1.25, 1.35, 1.5	SR	DR	0	00390039h	1Fh	1Fh	3Fh	1Fh
2	800	1.25, 1.35, 1.5	NP	SR	0	00000000h	1Fh	1Fh	1Fh	1Fh
2	800	1.25, 1.35, 1.5	NP	DR	0	003B0000h	1Fh	1Fh	1Fh	1Fh
2	800	1.25, 1.35, 1.5	SR	SR	0	00390039h	1Fh	1Fh	3Fh	1Fh
2	800	1.25, 1.35, 1.5	DR	DR	0	00390039h	1Fh	1Fh	3Fh	1Fh
2	800	1.25, 1.35, 1.5	DR	SR	0	00390039h	1Fh	1Fh	3Fh	1Fh
2	800	1.25, 1.35, 1.5	SR	DR	0	00390039h	1Fh	1Fh	3Fh	1Fh
2	1066	1.25, 1.35, 1.5	NP	SR	0	00000000h	1Fh	1Fh	1Fh	1Fh
2	1066	1.25, 1.35, 1.5	NP	DR	0	00380000h	1Fh	1Fh	1Fh	1Fh
2	1066	1.25, 1.35, 1.5	SR	SR	0	00350037h	1Fh	1Fh	3Fh	1Fh
2	1066	1.25, 1.35, 1.5	DR	DR	0	00350037h	1Fh	1Fh	3Fh	1Fh
2	1066	1.25, 1.35, 1.5	DR	SR	0	00350037h	1Fh	1Fh	3Fh	1Fh
2	1066	1.25, 1.35, 1.5	SR	DR	0	00350037h	1Fh	1Fh	3Fh	1Fh
2	1333	1.25, 1.35, 1.5	NP	SR	0	00000000h	1Fh	1Fh	1Fh	1Fh
2	1333	1.25, 1.35, 1.5	NP	DR	0	00360000h	1Fh	1Fh	1Fh	1Fh
2	1333	1.25, 1.35, 1.5	SR	SR	1	00000035h	1Fh	1Fh	3Fh	1Fh
2	1333	1.25, 1.35, 1.5	DR	DR	1	00000035h	1Fh	1Fh	3Fh	1Fh
2	1333	1.25, 1.35, 1.5	DR	SR	1	00000035h	1Fh	1Fh	3Fh	1Fh
2	1333	1.25, 1.35, 1.5	SR	DR	1	00000035h	1Fh	1Fh	3Fh	1Fh
2	1600	1.25, 1.35, 1.5	NP	SR	0	00000000h	1Fh	1Fh	1Fh	1Fh
2	1600	1.25, 1.35, 1.5	NP	DR	1	00000000h	1Fh	1Fh	1Fh	1Fh
2	1600	1.35, 1.5	SR	SR	1	0000002Bh	1Fh	1Fh	3Fh	1Fh
2	1600	1.35, 1.5	DR	DR	1	0000002Bh	1Fh	1Fh	3Fh	1Fh
2	1600	1.35, 1.5	DR	SR	1	0000002Bh	1Fh	1Fh	3Fh	1Fh
2	1600	1.35, 1.5	SR	DR	1	0000002Bh	1Fh	1Fh	3Fh	1Fh

Table 25: BIOS Recommendations for DDR3 SO-DIMM CAD bus configuration

Condition					D18F2x94_dct[3:0] [SlowAccessMode]	{0000000000b,AddrCmdSetup[5:0],00b,CsOdtSetup[5:0], 00b, CkeSetup[5:0]}[1]	D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0] [DrvStrenN][2] for CKE	D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0] [DrvStrenN][2] for CS and ODT	D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0] [DrvStrenN][2] for AddrCmd	D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0] [DrvStrenN][2] for CLK
Condition:NumDimmSlots	Condition:DdrRate	Condition:VDDIO	Condition:DIMM0	Condition:DIMM1						
2	1866	1.35, 1.5	NP	SR	0	003C3C3Ch	1Fh	1Fh	1Fh	1Fh
2	1866	1.35, 1.5	NP	DR	1	00003C3Ch	1Fh	1Fh	1Fh	1Fh
2	1866	1.5	SR	SR	1	00000031h	1Fh	1Fh	3Fh	1Fh
2	1866	1.5	DR	DR	1	00000031h	1Fh	1Fh	3Fh	1Fh
2	1866	1.5	DR	SR	1	00000031h	1Fh	1Fh	3Fh	1Fh
2	1866	1.5	SR	DR	1	00000031h	1Fh	1Fh	3Fh	1Fh
2	2133	1.5	NP	SR	0	003B3B3Bh	1Fh	1Fh	1Fh	1Fh
2	2133	1.5	NP	DR	1	00003B3Bh	1Fh	1Fh	1Fh	1Fh

1. BIOS writes the values for AddrCmdSetup, CsOdtSetup, and CkeSetup into the SRAMMsgBlk for each memory P-state.
2. BIOS programs DrvStrenP = DrvStrenN for each instance.

Table 26: BIOS Recommendations for DDR3 UDIMM CAD bus configuration

Condition					D18F2x94_dct[3:0] [SlowAccessMode]	{0000000000b,AddrCmd-Setup[5:0],00b,CsOdt-Setup[5:0], 00b, Cke-Setup[5:0]}[1]	D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0] [DrvStrenN][2] for CKE	D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0] [DrvStrenN][2] for CS and ODT	D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0] [DrvStrenN][2] for AddrCmd	D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0] [DrvStrenN][2] for CLK
Condi-tion:NumDimmS-lots	Condi-tion:DdrRate	Condi-tion:VDDIO	Condi-tion:DIMM0	Condi-tion:DIMM1						
1	667	1.25, 1.35, 1.5	SR	-	0	00000000h	1Fh	1Fh	1Fh	1Fh
1	667	1.25, 1.35, 1.5	DR	-	0	003B0000h	1Fh	1Fh	1Fh	1Fh
1	800	1.25, 1.35, 1.5	SR	-	0	00000000h	1Fh	1Fh	1Fh	1Fh
1	800	1.25, 1.35, 1.5	DR	-	0	003B0000h	1Fh	1Fh	1Fh	1Fh
1	1066	1.25, 1.35, 1.5	SR	-	0	00000000h	1Fh	1Fh	1Fh	1Fh
1	1066	1.25, 1.35, 1.5	DR	-	0	00380000h	1Fh	1Fh	1Fh	1Fh
1	1333	1.25, 1.35, 1.5	SR	-	0	00000000h	1Fh	1Fh	1Fh	1Fh
1	1333	1.25, 1.35, 1.5	DR	-	0	00360000h	1Fh	1Fh	1Fh	1Fh
1	1600	1.25, 1.35, 1.5	SR	-	0	00000000h	1Fh	1Fh	1Fh	1Fh
1	1600	1.25, 1.35, 1.5	DR	-	1	00000000h	1Fh	1Fh	1Fh	1Fh
1	1866	1.35, 1.5	SR	-	0	00000000h	1Fh	1Fh	1Fh	1Fh
1	1866	1.35, 1.5	DR	-	1	00000000h	1Fh	1Fh	1Fh	1Fh
1	2133	1.5	SR	-	0	00000000h	1Fh	1Fh	1Fh	1Fh
1	2133	1.5	DR	-	1	00000000h	1Fh	1Fh	1Fh	1Fh
2	667	1.25, 1.35, 1.5	NP	SR	0	00000000h	1Fh	1Fh	1Fh	1Fh
2	667	1.25, 1.35, 1.5	NP	DR	0	003B0000h	1Fh	1Fh	1Fh	1Fh
2	667	1.25, 1.35, 1.5	SR	SR	0	00390039h	1Fh	1Fh	3Fh	1Fh
2	667	1.25, 1.35, 1.5	DR	DR	0	00390039h	1Fh	1Fh	3Fh	1Fh
2	667	1.25, 1.35, 1.5	DR	SR	0	00390039h	1Fh	1Fh	3Fh	1Fh
2	667	1.25, 1.35, 1.5	SR	DR	0	00390039h	1Fh	1Fh	3Fh	1Fh
2	800	1.25, 1.35, 1.5	NP	SR	0	00000000h	1Fh	1Fh	1Fh	1Fh
2	800	1.25, 1.35, 1.5	NP	DR	0	003B0000h	1Fh	1Fh	1Fh	1Fh
2	800	1.25, 1.35, 1.5	SR	SR	0	00390039h	1Fh	1Fh	3Fh	1Fh
2	800	1.25, 1.35, 1.5	DR	DR	0	00390039h	1Fh	1Fh	3Fh	1Fh
2	800	1.25, 1.35, 1.5	DR	SR	0	00390039h	1Fh	1Fh	3Fh	1Fh

Table 26: BIOS Recommendations for DDR3 UDIMM CAD bus configuration

Condition					D18F2x94_dct[3:0] [SlowAccessMode]	{0000000000b,AddrCmd-Setup[5:0],00b,CsOdt-Setup[5:0], 00b, Cke-Setup[5:0]}[1]	D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0] [DrvStrenN][2] for CKE	D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0] [DrvStrenN][2] for CS and ODT	D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0] [DrvStrenN][2] for AddrCmd	D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0] [DrvStrenN][2] for CLK
Condition:NumDimmSlots	Condition:DdrRate	Condition:VDDIO	Condition:DIMM0	Condition:DIMM1						
2	800	1.25, 1.35, 1.5	SR	DR	0	00390039h	1Fh	1Fh	3Fh	1Fh
2	1066	1.25, 1.35, 1.5	NP	SR	0	00000000h	1Fh	1Fh	1Fh	1Fh
2	1066	1.25, 1.35, 1.5	NP	DR	0	00380000h	1Fh	1Fh	1Fh	1Fh
2	1066	1.25, 1.35, 1.5	SR	SR	0	00350037h	1Fh	1Fh	3Fh	1Fh
2	1066	1.25, 1.35, 1.5	DR	DR	0	00350037h	1Fh	1Fh	3Fh	1Fh
2	1066	1.25, 1.35, 1.5	DR	SR	0	00350037h	1Fh	1Fh	3Fh	1Fh
2	1066	1.25, 1.35, 1.5	SR	DR	0	00350037h	1Fh	1Fh	3Fh	1Fh
2	1333	1.25, 1.35, 1.5	NP	SR	0	00000000h	1Fh	1Fh	1Fh	1Fh
2	1333	1.25, 1.35, 1.5	NP	DR	0	00360000h	1Fh	1Fh	1Fh	1Fh
2	1333	1.25, 1.35, 1.5	SR	SR	1	00000035h	1Fh	1Fh	3Fh	1Fh
2	1333	1.25, 1.35, 1.5	DR	DR	1	00000035h	1Fh	1Fh	3Fh	1Fh
2	1333	1.25, 1.35, 1.5	DR	SR	1	00000035h	1Fh	1Fh	3Fh	1Fh
2	1333	1.25, 1.35, 1.5	SR	DR	1	00000035h	1Fh	1Fh	3Fh	1Fh
2	1600	1.25, 1.35, 1.5	NP	SR	0	00000000h	1Fh	1Fh	1Fh	1Fh
2	1600	1.25, 1.35, 1.5	NP	DR	1	00000000h	1Fh	1Fh	1Fh	1Fh
2	1600	1.35, 1.5	SR	SR	1	0000002Bh	1Fh	1Fh	3Fh	1Fh
2	1600	1.35, 1.5	DR	DR	1	0000002Bh	1Fh	1Fh	3Fh	1Fh
2	1600	1.35, 1.5	DR	SR	1	0000002Bh	1Fh	1Fh	3Fh	1Fh
2	1600	1.35, 1.5	SR	DR	1	0000002Bh	1Fh	1Fh	3Fh	1Fh
2	1866	1.35, 1.5	NP	SR	0	003C3C3Ch	1Fh	1Fh	1Fh	1Fh
2	1866	1.35, 1.5	NP	DR	1	00003C3Ch	1Fh	1Fh	1Fh	1Fh
2	1866	1.5	SR	SR	1	00000031h	1Fh	1Fh	3Fh	1Fh
2	1866	1.5	DR	DR	1	00000031h	1Fh	1Fh	3Fh	1Fh

Table 26: BIOS Recommendations for DDR3 UDIMM CAD bus configuration

Condition					D18F2x94_dct[3:0][SlowAccessMode]	{0000000000b,AddrCmdSetup[5:0],00b,CsOdtSetup[5:0], 00b, CkeSetup[5:0]}[1]	D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0][DrvStrenN][2] for CKE	D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0][DrvStrenN][2] for CS and ODT	D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0][DrvStrenN][2] for AddrCmd	D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0][DrvStrenN][2] for CLK
Condition:NumDimmSlots	Condition:DdrRate	Condition:VDDIO	Condition:DIMM0	Condition:DIMM1						
2	1866	1.5	DR	SR	1	00000031h	1Fh	1Fh	3Fh	1Fh
2	1866	1.5	SR	DR	1	00000031h	1Fh	1Fh	3Fh	1Fh

1. BIOS writes the values for AddrCmdSetup, CsOdtSetup, and CkeSetup into the SRAMMsgBlk for each memory P-state.
2. BIOS programs DrvStrenP = DrvStrenN for each instance.

2.9.9.2.5 DRAM Data Bus Configuration

This section describes the settings required for programming the drive settings and slew rates on the data bus pins. The following tables document the data bus values on a per channel basis. DIMM0 is the DIMM closest to the processor on that channel and DIMM1 is the DIMM farthest from the processor on that channel. DIMMs must be populated from farthest slot to closest slot to the processor on a per channel basis (when a daisy chain topology is used). Populations that are not shown in these tables are not supported. These tables document the optimal settings for motherboards which meet the relevant motherboard design guidelines.

- Program D18F2x9C_x0002_0087_dct[3:0][DisAutoComp, DisPredriverCal] = {1,1}.
- Only the value for a single control unit register is described. The values in the table should be broadcast to all instances of registers of the same control unit type, unless otherwise noted.
- Program D18F2x9C_x0002_0087_dct[3:0][DisAutoComp] = 0.

Table 27: BIOS Recommendations for DDR3 SO-DIMM data bus configuration

Condition					RTT_Nom	RTT_Wr	D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]041_dct[3:0] [DrvStrenP][1] for DQ pins	D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]041_dct[3:0] [DrvStrenP][1] for DQS pins	D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]04D_dct[3:0] [ODTStrenP][2]
Condition:NumDimmSlots	Condition:DdrRate	Condition:VDDIO	Condition:DIMM0	Condition:DIMM1					
1	667	1.25, 1.35, 1.5	SR	-	120	Off	70h	70h	01h
1	667	1.25, 1.35, 1.5	DR	-	120	Off	70h	70h	01h
1	800	1.25, 1.35, 1.5	SR	-	120	Off	70h	70h	01h
1	800	1.25, 1.35, 1.5	DR	-	120	Off	70h	70h	01h
1	1066	1.25, 1.35, 1.5	SR	-	120	Off	70h	70h	04h
1	1066	1.25, 1.35, 1.5	DR	-	120	Off	70h	70h	04h
1	1333	1.25, 1.35, 1.5	SR	-	60	Off	70h	70h	05h
1	1333	1.25, 1.35, 1.5	DR	-	60	Off	70h	70h	05h
1	1600	1.25, 1.35, 1.5	SR	-	60	Off	70h	70h	0Ch
1	1600	1.25, 1.35, 1.5	DR	-	40	Off	70h	70h	0Ch
1	1866	1.35, 1.5	SR	-	40	Off	70h	70h	0Ch
1	1866	1.35, 1.5	DR	-	40	Off	70h	70h	0Ch
1	2133	1.5	SR	-	40	Off	70h	70h	0Ch
1	2133	1.5	DR	-	40	Off	70h	70h	0Ch
2	667	1.25, 1.35, 1.5	NP	SR	120	Off	70h	70h	01h
2	667	1.25, 1.35, 1.5	NP	DR	120	Off	70h	70h	01h
2	667	1.25, 1.35, 1.5	SR	SR	40	120	75h	75h	04h
2	667	1.25, 1.35, 1.5	DR	DR	40	120	75h	75h	04h
2	667	1.25, 1.35, 1.5	DR	SR	40	120	75h	75h	04h
2	667	1.25, 1.35, 1.5	SR	DR	40	120	75h	75h	04h
2	800	1.25, 1.35, 1.5	NP	SR	120	Off	70h	70h	01h
2	800	1.25, 1.35, 1.5	NP	DR	120	Off	70h	70h	01h
2	800	1.25, 1.35, 1.5	SR	SR	40	120	75h	75h	05h
2	800	1.25, 1.35, 1.5	DR	DR	40	120	75h	75h	05h
2	800	1.25, 1.35, 1.5	DR	SR	40	120	75h	75h	05h

Table 27: BIOS Recommendations for DDR3 SO-DIMM data bus configuration

Condition					RTT_Nom	RTT_Wr	D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]041_dct[3:0] [DrvStrenP][1] for DQ pins	D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]041_dct[3:0] [DrvStrenP][1] for DQS pins	D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]04D_dct[3:0] [ODTStrenP][2]
Condition:NumDimmSlots	Condition:DdrRate	Condition:VDDIO	Condition:DIMM0	Condition:DIMM1					
2	800	1.25, 1.35, 1.5	SR	DR	40	120	75h	75h	05h
2	1066	1.25, 1.35, 1.5	NP	SR	120	Off	70h	70h	04h
2	1066	1.25, 1.35, 1.5	NP	DR	120	Off	70h	70h	04h
2	1066	1.25, 1.35, 1.5	SR	SR	40	120	75h	75h	0Ch
2	1066	1.25, 1.35, 1.5	DR	DR	40	120	75h	75h	0Ch
2	1066	1.25, 1.35, 1.5	DR	SR	40	120	75h	75h	0Ch
2	1066	1.25, 1.35, 1.5	SR	DR	40	120	75h	75h	0Ch
2	1333	1.25, 1.35, 1.5	NP	SR	60	Off	70h	70h	05h
2	1333	1.25, 1.35, 1.5	NP	DR	60	Off	70h	70h	05h
2	1333	1.25, 1.35, 1.5	SR	SR	30	120	75h	75h	0Ch
2	1333	1.25, 1.35, 1.5	DR	DR	30	120	75h	75h	0Ch
2	1333	1.25, 1.35, 1.5	DR	SR	30	120	75h	75h	0Ch
2	1333	1.25, 1.35, 1.5	SR	DR	30	120	75h	75h	0Ch
2	1600	1.25, 1.35, 1.5	NP	SR	40	Off	70h	70h	0Ch
2	1600	1.25, 1.35, 1.5	NP	DR	40	Off	70h	70h	0Ch
2	1600	1.35, 1.5	SR	SR	20	60	75h	75h	0Ch
2	1600	1.35, 1.5	DR	DR	20	60	75h	75h	0Ch
2	1600	1.35, 1.5	DR	SR	20	60	75h	75h	0Ch
2	1600	1.35, 1.5	SR	DR	20	60	75h	75h	0Ch
2	1866	1.35, 1.5	NP	SR	40	Off	70h	70h	0Ch
2	1866	1.35, 1.5	NP	DR	40	Off	70h	70h	0Ch
2	1866	1.5	SR	SR	20	60	75h	75h	0Ch
2	1866	1.5	DR	DR	20	60	75h	75h	0Ch
2	1866	1.5	DR	SR	20	60	75h	75h	0Ch
2	1866	1.5	SR	DR	20	60	75h	75h	0Ch

Table 27: BIOS Recommendations for DDR3 SO-DIMM data bus configuration

Condition					RTT_Nom	RTT_Wr	D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]041_dct[3:0] [DrvStrenP][1] for DQ pins	D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]041_dct[3:0] [DrvStrenP][1] for DQS pins	D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]04D_dct[3:0] [ODTStrenP][2]
Condition:NumDimmSlots	Condition:DdrRate	Condition:VDDIO	Condition:DIMM0	Condition:DIMM1					
2	2133	1.5	NP	SR	40	Off	70h	70h	0Ch
2	2133	1.5	NP	DR	40	Off	70h	70h	0Ch

1. BIOS programs DrvStrenN = DrvStrenP for each instance.
   BIOS programs instances for "MEMDQSDM" (when used as a data mask) with the same value as DQ.
2. BIOS programs ODTStrenN = ODTStrenP for each instance.
   BIOS programs all used instances with these values.

Table 28: BIOS Recommendations for DDR3 UDIMM data bus configuration

Condition					RTT_Nom	RTT_Wr	D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]041_dct[3:0] [DrvStrenP][1] for DQ pins	D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]041_dct[3:0] [DrvStrenP][1] for DQS pins	D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]04D_dct[3:0] [ODTStrenP][2]
Condition:NumDimmSlots	Condition:DdrRate	Condition:VDDIO	Condition:DIMM0	Condition:DIMM1					
1	667	1.25, 1.35, 1.5	SR	-	120	Off	70h	70h	01h
1	667	1.25, 1.35, 1.5	DR	-	120	Off	70h	70h	01h
1	800	1.25, 1.35, 1.5	SR	-	120	Off	70h	70h	01h

Table 28: BIOS Recommendations for DDR3 UDIMM data bus configuration

Condition					RTT_Nom	RTT_Wr	D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]041_dct[3:0] [DrvStrenP][1] for DQ pins	D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]041_dct[3:0] [DrvStrenP][1] for DQS pins	D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]04D_dct[3:0] [ODTStrenP][2]
Condition:NumDimmSlots	Condition:DdrRate	Condition:VDDIO	Condition:DIMM0	Condition:DIMM1					
1	800	1.25, 1.35, 1.5	DR	-	120	Off	70h	70h	01h
1	1066	1.25, 1.35, 1.5	SR	-	120	Off	70h	70h	04h
1	1066	1.25, 1.35, 1.5	DR	-	120	Off	70h	70h	04h
1	1333	1.25, 1.35, 1.5	SR	-	60	Off	70h	70h	05h
1	1333	1.25, 1.35, 1.5	DR	-	60	Off	70h	70h	05h
1	1600	1.25, 1.35, 1.5	SR	-	60	Off	70h	70h	0Ch
1	1600	1.25, 1.35, 1.5	DR	-	40	Off	70h	70h	0Ch
1	1866	1.35, 1.5	SR	-	40	Off	70h	70h	0Ch
1	1866	1.35, 1.5	DR	-	40	Off	70h	70h	0Ch
1	2133	1.5	SR	-	40	Off	70h	70h	0Ch
1	2133	1.5	DR	-	40	Off	70h	70h	0Ch
2	667	1.25, 1.35, 1.5	NP	SR	120	Off	70h	70h	01h
2	667	1.25, 1.35, 1.5	NP	DR	120	Off	70h	70h	01h
2	667	1.25, 1.35, 1.5	SR	SR	40	120	75h	75h	04h
2	667	1.25, 1.35, 1.5	DR	DR	40	120	75h	75h	04h
2	667	1.25, 1.35, 1.5	DR	SR	40	120	75h	75h	04h
2	667	1.25, 1.35, 1.5	SR	DR	40	120	75h	75h	04h
2	800	1.25, 1.35, 1.5	NP	SR	120	Off	70h	70h	01h
2	800	1.25, 1.35, 1.5	NP	DR	120	Off	70h	70h	01h
2	800	1.25, 1.35, 1.5	SR	SR	40	120	75h	75h	05h
2	800	1.25, 1.35, 1.5	DR	DR	40	120	75h	75h	05h
2	800	1.25, 1.35, 1.5	DR	SR	40	120	75h	75h	05h
2	800	1.25, 1.35, 1.5	SR	DR	40	120	75h	75h	05h
2	1066	1.25, 1.35, 1.5	NP	SR	120	Off	70h	70h	04h
2	1066	1.25, 1.35, 1.5	NP	DR	120	Off	70h	70h	04h
2	1066	1.25, 1.35, 1.5	SR	SR	40	120	75h	75h	0Ch

Table 28: BIOS Recommendations for DDR3 UDIMM data bus configuration

Condition					RTT_Nom	RTT_Wr	D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]041_dct[3:0] [DrvStrenP][1] for DQ pins	D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]041_dct[3:0] [DrvStrenP][1] for DQS pins	D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]04D_dct[3:0] [ODTStrenP][2]
Condition:NumDimmSlots	Condition:DdrRate	Condition:VDDIO	Condition:DIMM0	Condition:DIMM1					
2	1066	1.25, 1.35, 1.5	DR	DR	40	120	75h	75h	0Ch
2	1066	1.25, 1.35, 1.5	DR	SR	40	120	75h	75h	0Ch
2	1066	1.25, 1.35, 1.5	SR	DR	40	120	75h	75h	0Ch
2	1333	1.25, 1.35, 1.5	NP	SR	60	Off	70h	70h	05h
2	1333	1.25, 1.35, 1.5	NP	DR	60	Off	70h	70h	05h
2	1333	1.25, 1.35, 1.5	SR	SR	30	120	75h	75h	0Ch
2	1333	1.25, 1.35, 1.5	DR	DR	30	120	75h	75h	0Ch
2	1333	1.25, 1.35, 1.5	DR	SR	30	120	75h	75h	0Ch
2	1333	1.25, 1.35, 1.5	SR	DR	30	120	75h	75h	0Ch
2	1600	1.25, 1.35, 1.5	NP	SR	40	Off	70h	70h	0Ch
2	1600	1.25, 1.35, 1.5	NP	DR	40	Off	70h	70h	0Ch
2	1600	1.35, 1.5	SR	SR	20	60	75h	75h	0Ch
2	1600	1.35, 1.5	DR	DR	20	60	75h	75h	0Ch
2	1600	1.35, 1.5	DR	SR	20	60	75h	75h	0Ch
2	1600	1.35, 1.5	SR	DR	20	60	75h	75h	0Ch
2	1866	1.35, 1.5	NP	SR	40	Off	70h	70h	0Ch
2	1866	1.35, 1.5	NP	DR	40	Off	70h	70h	0Ch
2	1866	1.5	SR	SR	20	60	75h	75h	0Ch
2	1866	1.5	DR	DR	20	60	75h	75h	0Ch
2	1866	1.5	DR	SR	20	60	75h	75h	0Ch
2	1866	1.5	SR	DR	20	60	75h	75h	0Ch

Table 28: BIOS Recommendations for DDR3 UDIMM data bus configuration

Condition					RTT_Nom	RTT_Wr	D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]041_dct[3:0] [DrvStrenP][1] for DQ pins	D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]041_dct[3:0] [DrvStrenP][1] for DQS pins	D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]04D_dct[3:0] [ODTStrenP][2]
Condition:NumDimmSlots	Condition:DdrRate	Condition:VDDIO	Condition:DIMM0	Condition:DIMM1					
2	2133	1.5	NP	SR	40	Off	70h	70h	0Ch
2	2133	1.5	NP	DR	40	Off	70h	70h	0Ch

1. BIOS programs DrvStrenN = DrvStrenP for each instance.
   BIOS programs instances for "MEMDQSDM" (when used as a data mask) with the same value as DQ.
2. BIOS programs ODTStrenN = ODTStrenP for each instance.
   BIOS programs all used instances with these values.

2.9.9.2.6 Phy FIFO Configuration

BIOS programs FIFO configuration values based on NCLK, memory clock, CASL, and CWL. A read pointer initial value is specified for each NbPstate as well as one reserved for the PMU during training.

The steps for Ddr3Mode are as follows:

1. For NbP0 broadcast the value to all timing groups and chips as follows:
   - D18F2x9C_x00[F,3:0]0_[F,3:0][8,3:0]2E_dct[3:0][RdPtrInitVal]= Table 29.
   - D18F2x9C_x00[F,8:0]1_0[8,3:0]2E_dct[3:0][RdPtrInitVal] = Table 29.
2. For each NbPstate, excluding the "NbPstate PMU" instance and the NbP0 instance, program:
   - Broadcast the value to all timing groups and chips.
   - D18F2x9C_x00[F,3:0]0_[F,3:0][8,3:0]2E_dct[3:0][RdPtrInitVal]= Table 30.
   - D18F2x9C_x00[F,8:0]1_0[8,3:0]2E_dct[3:0][RdPtrInitVal] = Table 30.
3. D18F2x9C_x0[3,1:0][F,8:0]1_0028_dct[3:0][RxRdPtrOffset] as follows:
   - Broadcast the value to all chips.
   - RxRdPtrOffset = CASL.
4. D18F2x9C_x0[3,1:0][F,8:0]1_0028_dct[3:0][TxRdPtrOffset] as follows:
   - Broadcast the value to all chips.
   - TxRdPtrOffset = CWL.

Table 29: BIOS Recommendations for DDR3 FIFO RdPtrInitVal for NbP0

Condition	NCLK (MHz)						
Condition:DdrRate	800	1000	1200	1400	1600	1800	1900
667	10h	14h	14h	14h	14h	14h	14h
1066	0Ch	10h	10h	10h	10h	10h	10h
1333	08h	0Ch	0Ch	0Ch	10h	10h	10h
1600	08h	08h	08h	0Ch	0Ch	0Ch	0Ch
1866	-	04h	08h	08h	08h	0Ch	0Ch
2133	-	-	04h	04h	08h	08h	08h
2400	-	-	04h	04h	04h	04h	04h
2500	-	-	-	04h	04h	04h	04h

Notes:
1. If exact DdrRate is not shown, use the information from the row of the next highest shown DdrRate.
2. If exact NCLK rate is not shown, use the information from the column of the next highest shown NCLK.
3. Not all conditions are supported. See product definition for details on supported frequencies.

Table 30: BIOS Recommendations for DDR3 FIFO RdPtrInitVal for NbPx

Condition	NCLK (MHz)						
Condition:DdrRate	800	1000	1200	1400	1600	1800	1900
667	10h	10h	10h	14h	14h	14h	14h
1066	0Ch	0Ch	0Ch	0Ch	10h	10h	10h
1333	08h	08h	08h	0Ch	0Ch	0Ch	0Ch
1600	08h	04h	08h	08h	08h	08h	08h
1866	-	00h	04h	04h	04h	08h	08h
2133	-	-	00h	00h	04h	04h	04h
2400	-	-	00h	00h	00h	00h	00h
2500	-	-	-	7Ch	00h	00h	00h

Notes:
1. If exact DdrRate is not shown, use the information from the row of the next highest shown DdrRate.
2. If exact NCLK rate is not shown, use the information from the column of the next highest shown NCLK.
3. Not all conditions are supported. See product definition for details on supported frequencies.

2.9.9.2.7 Phy Predriver Initialization.

Each DDR IO driver has a programmable slew rate controlled by the pre-driver calibration code. The recommended slew rate is a function of the DC drive strength. BIOS initializes the recommended nominal slew rate

values as follows:

1. Program D18F2x9C_x0002_0087_dct[3:0][DisAutoComp, DisPredriverCal] = {1,1}.
2. Program D18F2x9C_x00[F,8:0]1_[F,B:0]05F_dct[3:0][TxPreN, TxPreP] according to Table 31.
   - For each pad, read D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]041_dct[3:0][DrvStrenP] and program the corresponding pad in D18F2x9C_x00[F,8:0]1_[F,B:0]05F_dct[3:0].
   - Use DrvStrenP for memory P-state 0 to determine slew rate.
   - If the chosen DrvStrenP value is not listed in the table for the given DDR rates, then use the next lower DrvStrenP value listed to determine TxPreN and TxPreP.
3. Program D18F2x9C_x00[F,3:0]0_[F,B:0]05F_dct[3:0][TxPreN, TxPreP] for Cmd/Addr according to Table 32.
   - For each Cmd/Addr pad (MEMCKE[3:0], MEMADD[15:0], MEMBANK[2:0], MEMCS_L[7:0], MEMODT[3:0], MEMCAS_L, MEMWE_L, MEMRAS_L):
     - Read D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0][DrvStrenP] and program the corresponding pad in D18F2x9C_x00[F,3:0]0_[F,B:0]05F_dct[3:0][TxPreN, TxPreP].
   - Use DrvStrenP for memory P-state 0 to determine slew rate.
   - If the chosen DrvStrenP value is not listed in the table for the given DDR rates, then use the next lower DrvStrenP value listed to determine TxPreN and TxPreP.
4. Program D18F2x9C_x00[F,3:0]0_[F,B:0]05F_dct[3:0][TxPreN, TxPreP] for clocks according to Table 33.
   - For each clock pad (MEMCLK_H[4:0], MEMCLK_L[4:0]):
     - Read D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0][DrvStrenP] and program the corresponding pad in D18F2x9C_x00[F,3:0]0_[F,B:0]05F_dct[3:0][TxPreN, TxPreP].
   - Use DrvStrenP for memory P-state 0 to determine slew rate.
   - If the chosen DrvStrenP value is not listed in the table for the given DDR rates, then use the next lower DrvStrenP value listed to determine TxPreN and TxPreP.
5. Program D18F2x9C_x0002_0087_dct[3:0][DisAutoComp, DisPredriverCal] = {0,0}.

Table 31: Phy predriver codes for Data/DQS

DDR Rate	DrvStrenP[1]	{TxPreN, TxPreP}[2] VDDIO=1.5V	{TxPreN, TxPreP}[2] VDDIO=1.35V	{TxPreN, TxPreP}[2] VDDIO=1.25V
667 - 1067	31h	101b,111b	101b,111b	101b,111b
	70h	010b,010b	101b,111b	101b,111b
	75h	001b,001b	010b,010b	010b,010b
	7Fh	001b,001b	001b,001b	001b,001b
1333 - 1600	31h	101b,111b	101b,111b	101b,111b
	70h	010b,010b	101b,111b	101b,111b
	75h	010b,010b	010b,010b	011b,011b
	7Fh	010b,010b	010b,010b	011b,011b
1866 - 2400	31h	101b,111b	101b,111b	101b,111b
	70h	011b,011b	101b,111b	101b,111b
	75h	011b,011b	100b,100b	100b,100b
	7Fh	011b,011b	100b,100b	100b,101b

1. See D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]041_dct[3:0].
2. See D18F2x9C_x00[F,8:0]1_[F,B:0]05F_dct[3:0].

Table 32: Phy predriver codes for Cmd/Addr

DDR Rate	DrvStrenP[1]	{TxPreN, TxPreP}[2] VDDIO=1.5V	{TxPreN, TxPreP}[2] VDDIO=1.35V	{TxPreN, TxPreP}[2] VDDIO=1.25V
667 - 1067	07h	000b,000b	001b,001b	001b,001b
	0Fh	000b,000b	001b,001b	001b,001b
	1Fh	000b,000b	001b,001b	001b,001b
	3Fh	000b,000b	001b,001b	001b,001b
1333 - 1600	07h	001b,001b	010b,010b	011b,011b
	0Fh	001b,001b	010b,010b	011b,011b
	1Fh	001b,001b	010b,010b	011b,011b
	3Fh	001b,001b	010b,010b	011b,011b
1866 - 2400	07h	011b,011b	011b,011b	100b,100b
	0Fh	011b,011b	011b,011b	100b,100b
	1Fh	011b,011b	011b,011b	100b,100b
	3Fh	011b,011b	011b,011b	100b,100b

1. See D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0].
2. See D18F2x9C_x00[F,3:0]0_[F,B:0]05F_dct[3:0].

Table 33: Phy predriver codes for CLK

DDR Rate	DrvStrenP[1]	{TxPreN, TxPreP}[2] VDDIO=1.5V	{TxPreN, TxPreP}[2] VDDIO=1.35V	{TxPreN, TxPreP}[2] VDDIO=1.25V
667 - 1067	07h	010b,010b	011b,011b	100b,100b
	0Fh	010b,010b	011b,011b	100b,100b
	1Fh	010b,010b	011b,011b	100b,100b
	3Fh	010b,010b	011b,011b	100b,100b
1333 - 1600	07h	100b,100b	101b,101b	110b,110b
	0Fh	100b,100b	101b,101b	110b,110b
	1Fh	100b,100b	101b,101b	110b,110b
	3Fh	100b,100b	101b,101b	110b,110b
1866 - 2400	07h	111b,111b	111b,111b	111b,111b
	0Fh	111b,111b	111b,111b	111b,111b
	1Fh	111b,111b	111b,111b	111b,111b
	3Fh	111b,111b	111b,111b	111b,111b

1. See D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0].
2. See D18F2x9C_x00[F,3:0]0_[F,B:0]05F_dct[3:0].

2.9.9.2.8 Phy Auto-Calibration

BIOS enables a one-time calibration after configuration dependent values are programmed as follows:

1. Initiate one-time calibration. See 2.9.9.2.8.1.
2. After the PMU firmware is loaded, BIOS ensures that the initial calibration is complete prior to executing PMU firmware. See appropriate section for details.
3. After PMU training is complete, or after complete restore of trained values from NVRAM, BIOS initiates auto calibration. See 2.9.9.2.8.3.

2.9.9.2.8.1 One-Time Pre-PMU Calibration

BIOS initiates one calibration. On S5 boot BIOS does this before loading PMU firmware.

1. Program D18F2x9C_x0002_0088_dct[3:0][CalInitMode, CalOnce] = {1,1}.
2. Program D18F2x9C_x0002_0088_dct[3:0][CalRun] = 1.
3. Program D18F2x9C_x0002_0088_dct[3:0][CalOnce,CalRun] = {0,0}.

2.9.9.2.8.2 Fence CalOnce

BIOS ensures the initial one-time calibration is complete as follows:

1. Read D18F2x9C_x0002_0097_dct[3:0][CalBusy]. This read value is thrown away.
2. Read D18F2x9C_x0002_0097_dct[3:0][CalBusy] until CalBusy == 0.

2.9.9.2.8.3 Auto Calibration

BIOS initiates auto calibration after PMU training or after complete restore of trained values from NVRAM.

1. Program D18F2x9C_x0002_0088_dct[3:0][CalInitMode] = 0.
2. Program D18F2x9C_x0002_0088_dct[3:0][CalRun] = 1.

2.9.9.2.9 PMU Firmware Load

BIOS loads the PMU firmware (see 2.9.8 [PMU]) after each system reset before requesting the PMU to take action with down-stream messages.

Firmware block LENGTH = 16*1024.
1. Program D18F2x9C_x0002_0099_dct[3:0][PmuReset] = 0 for each phy.
2. Program D18F1x10C[DctCfgBcEn] = 1.
3. For each 16-bit word of the firmware block: Write the word to D18F2x[B,0]9C_x0005_[5BFF:4000]_dct[3:0] (while using the autoincrement feature).
4. Program D18F1x10C[DctCfgBcEn] = 0.

Additionally, there is a sequence of register writes provided by AMD to write compiler/tool specific data into the data SRAM for use in the PMU executive.

2.9.9.2.10 Phy Registers Required for S3 Resume

To support suspend-to-RAM, BIOS must save registers to NVRAM prior to S3 entry, and restore them when resuming. The following is not a complete list. See 2.9.9 [DCT/DRAM Initialization and Resume] for information on other registers. BIOS restores the following registers, which have been trained by the PMU during boot:

- D18F2x9C_x0[3,1:0][F,3:0]0_[F,3:0]028_dct[3:0]
- D18F2x9C_x0[3,1:0][F,8:0]1_0028_dct[3:0]
- D18F2x9C_x0[3,1:0][F,3:0]0_[F,3:0]081_dct[3:0]
- D18F2x9C_x0[F,1:0][F,8:0]1_[F,9:0][F,3:0]80_dct[3:0]
- D18F2x9C_x0[F,1:0][F,8:0]1_[F,9:0][F,3:0]81_dct[3:0]
- D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]046_dct[3:0]
- D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]047_dct[3:0]
- D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]048_dct[3:0]

2.9.9.2.11 Calculating Round Trip Command Delays

Software calculates trained round trip delays as follows.

MaxRxCmdDelay, maximum command to data read delay, in units of 2 UI:

- Compute worst case for each chip and when available for each DQ pad within a chip.
- MaxRxCmdDelay = MAX(D18F2x9C_x0[3,1:0][F,8:0]1_0028_dct[3:0][RxRdPtrOffset] + CEIL(D18F2x9C_x0[F,1:0][F,8:0]1_[F,9:0][F,3:0]80_dct[3:0][RxDly]/64))

2.9.9.3 SPD ROM-Based Configuration

The Serial Presence Detect (SPD) ROM is a non-volatile memory device on the DIMM encoded by the DIMM manufacturer. The description of the SPD is usually provided on a data sheet for the DIMM itself along with data describing the memory devices used. The data describes configuration and speed characteristics of the DIMM and the SDRAM components mounted on the DIMM. The associated data sheet also contains the DIMM byte values that are encoded in the SPD on the DIMM.

BIOS reads the values encoded in the SPD ROM through a system-specific interface. BIOS acquires DIMM configuration information, such as the amount of memory on each DIMM, from the SPD ROM on each DIMM and uses this information to program the DRAM controller registers.

For solder-down DRAM, in the absence of an SPD ROM, BIOS provides the information necessary for DRAM configuration.

The SPD ROM provides values for several DRAM timing parameters that are required by the DCT. In general, BIOS should use the optimal value specified by the SPD ROM.

For Ddr3Mode, these parameters are:

- D18F2x84_dct[3:0][Twr]: Write recovery time
- D18F2x8C_dct[3:0][Tref]
- D18F2x200_dct[3:0]_mp[1:0][Tras]: Active to precharge time
- D18F2x200_dct[3:0]_mp[1:0][Trp]: Precharge time
- D18F2x200_dct[3:0]_mp[1:0][Trcd]: RAS to CAS delay
- D18F2x200_dct[3:0]_mp[1:0][Tcl]: CAS latency
- D18F2x204_dct[3:0]_mp[1:0][Trtp]: Internal read to precharge command delay time

- D18F2x204_dct[3:0]_mp[1:0][FourActWindow]: Four activate window delay time
- D18F2x204_dct[3:0]_mp[1:0][Trrd]: Row active to row active delay
- D18F2x204_dct[3:0]_mp[1:0][Trc]: Active to active/refresh time
- D18F2x208_dct[3:0][Trfc3, Trfc2, Trfc1, Trfc0]: Refresh recovery delay time
- D18F2x20C_dct[3:0]_mp[1:0][Twtr]: Internal write to read command delay time

Optimal cycle time is specified for each DIMM and is used to limit or determine bus frequency. See 2.9.9.5 [DRAM Device Initialization and Training].

2.9.9.3.1 DRAM ODT Pin Control

This section applies to Ddr3Mode only.

BIOS configures the DIMM ODT behavior per chip select according to the DIMM population. In all cases, the processor ODT is off for writes and is on for reads. The ODT pin patterns for reads and writes are programmed using D18F2x[234:230]_dct[3:0] and D18F2x[23C:238]_dct[3:0], respectively.

Table 34: DDR3 DIMM ODT Pattern

DIMM0[1]	DIMM1[1]	D18F2x[234:230]_dct[3:0]		D18F2x[23C:238]_dct[3:0]	
		D18F2x230	D18F2x234	D18F2x238	D18F2x23C
-	SR	0000_0000h	0000_0000h	0002_0000h	0000_0000h
-	DR	0000_0000h	0000_0000h	0208_0000h	0000_0000h
SR	-	0000_0000h	0000_0000h	0000_0001h	0000_0000h
DR	-	0000_0000h	0000_0000h	0000_0104h	0000_0000h
SR/DR	SR/DR	0101_0202h	0000_0000h	0903_0603h	0000_0000h

1. DIMM0: MEMCSx[1:0], MEMODTx[2,0].
DIMM1: MEMCSx[3:2], MEMODTx[3,1].
Population restrictions may apply. See 2.9.9.2.4 [DRAM CAD Bus Configuration] for details.

2.9.9.4 DCT Specific Configuration

The DCT requires certain features be disabled during DRAM device initialization and training. BIOS should program the registers in Table 35 before DRAM device initialization and training. For normal operation, BIOS programs the recommended values if provided in Table 35. BIOS must quiesce all other forms of DRAM traffic on the channel being trained. See 2.9.9 [DCT/DRAM Initialization and Resume].

Table 35: DCT Training Specific Register Values

Register	Mode	Training	Normal Operation
D18F2x78_dct[3:0][GsyncDis]	Ddr3Mode	0	0
D18F2x218_dct[3:0]_mp[1:0][TrdrdBan, TrdrdSdSc]	Ddr3Mode	{2h,1h}	See 2.9.9.4.1
D18F2x218_dct[3:0]_mp[1:0][TrdrdSdDc, TrdrdDd]	Ddr3Mode	{Bh, Bh}	See 2.9.9.4.1
D18F2x214_dct[3:0]_mp[1:0][TwrwrSdSc]	Ddr3Mode	1	See 2.9.9.4.1
D18F2x214_dct[3:0]_mp[1:0][TwrwrSdDc, TwrwrDd]	Ddr3Mode	{Bh, Bh}	See 2.9.9.4.1

Table 35: DCT Training Specific Register Values

Register	Mode	Training	Normal Operation
D18F2x218_dct[3:0]_mp[1:0][Twrrd]	Ddr3Mode	Bh	See 2.9.9.4.1
D18F2x21C_dct[3:0]_mp[1:0][TrwtTO]	Ddr3Mode	1Bh	See 2.9.9.4.1
D18F2x78_dct[3:0][AddrCmdTriEn]	Ddr3Mode	0	1
D18F2x8C_dct[3:0][DisAutoRefresh]	Ddr3Mode	1	0
D18F2x90_dct[3:0][ForceAutoPchg]	Ddr3Mode	0	0
D18F2x90_dct[3:0][DynPageCloseEn]	Ddr3Mode	0	0
D18F2x94_dct[3:0][BankSwizzleMode]	Ddr3Mode	0	1
D18F2x94_dct[3:0][DcqBypassMax]	Ddr3Mode	0	1Fh
D18F2x94_dct[3:0][PowerDownEn]	Ddr3Mode	0	1
D18F2x94_dct[3:0][ZqcsInterval]	Ddr3Mode	00b	10b
D18F2xA4[CmdThrottleMode]	Ddr3Mode	000b	xxxb[1]
D18F2xA4[ODTSEn]	Ddr3Mode	0b	x[1]
D18F2xA4[BwCapEn]	Ddr3Mode	0	x[1]
D18F2xA8_dct[3:0][BankSwap]	Ddr3Mode	0	1
D18F1x2[1,0][C,4][DctIntLvEn]	Ddr3Mode	0	x[1]
1. Programmed specifically to the current platform or memory configuration.			

2.9.9.4.1 DDR3 Turnaround Parameters

This section and all of the following sub-sections apply to Ddr3Mode only.

- LD (latency difference) = D18F2x200_dct[3:0]_mp[1:0][Tcl] - D18F2x20C_dct[3:0]_mp[1:0][Tcwl].
- WOD (Write ODT Delay) = MAX(0, D18F2x240_dct[3:0]_mp[1:0][WrOdtOnDuration] - 6).

In all cases, if the computed turn around time is less than the smallest non-reserved value in the register then software programs the smallest non-reserved value.

2.9.9.4.1.1 TrdrdBan, TrdrdSdSc, TrdrdSdDc, and TrdrdDd (Rd->Rd Timing)

This section applies to Ddr3Mode only.

The optimal values for D18F2x218_dct[3:0]_mp[1:0][TrdrdBan, TrdrdSdSc, TrdrdSdDc, TrdrdDd] are platform and configuration specific and should be characterized for best performance. After DRAM training, BIOS should use the guidelines below to configure the recommended platform generic timing values:

- CD_R_R, CD_R_R_SD, and Trdrdban_Phy are obtained from the PMU via the SRAMMsgBlk.
- TrdrdSdSc = 1.
- TrdrdSdDc = CD_R_R_SD.
- TrdrdDd = CD_R_R.
- TrdrdBan = Trdrdban_Phy.

2.9.9.4.1.2 TwrwrSdSc, TwrwrSdDc, TwrwrDd (Wr->Wr Timing)

This section applies to Ddr3Mode only.

The optimal values for D18F2x214_dct[3:0]_mp[1:0][TwrwrSdSc, TwrwrSdDc, TwrwrDd] are platform and configuration specific and should be characterized for best performance. After DRAM training, BIOS should use the guidelines below to configure the recommended platform generic timing values:

- CD_W_W and CD_W_W_SD are obtained from the PMU via the SRAMMsgBlk.
- TwrwrSdSc = 1.
- TwrwrSdDc = CD_W_W_SD.
- TwrwrDd = CD_W_W.

2.9.9.4.1.3 Twrrd (Write to Read DIMM Termination Turn-around)

This section applies to Ddr3Mode only.

The optimal value for D18F2x218_dct[3:0]_mp[1:0][Twrrd] is platform and configuration specific and should be characterized for best performance. Prior to DRAM training, BIOS should program this parameter to the largest defined value. After DRAM training, BIOS should use the guidelines below to configure the recommended platform generic timing values:

- Twrrd = CD_W_R obtained from the PMU via the SRAMMsgBlk.

2.9.9.4.1.4 TrwtTO (Read-to-Write Turnaround for Data, DQS Contention)

This section applies to Ddr3Mode only.

The optimal value for D18F2x21C_dct[3:0]_mp[1:0][TrwtTO] is platform and configuration specific and should be characterized for best performance. Prior to DRAM training, BIOS should program this parameter to the largest defined value. After DRAM training, BIOS should use the guidelines below to configure the recommended platform generic timing values after DDR training is complete:

- TrwtTO = CD_R_W obtained from the PMU via the SRAMMsgBlk.

2.9.9.5 DRAM Device Initialization and Training

BIOS requests the PMU to initialize the bus and devices, as well as train the processor for optimal operation, using the SequenceCtl bitmap in SRAMMsgBlk, and by taking the PMU out of reset to execute the requests.

In the following steps, BIOS performs each step for each DCT={MaxDctMstr:0}, keeping the PMUs in lock-step, before moving to the next step.

1. Perform the PMU firmware load for the module containing Devinit. See 2.9.9.2.9.
2. Program SRAMMsgBlk with all values necessary for Devinit. See 2.9.8.3.
3. Set SRAMMsgBlk, field SequenceCtl = 0x7F for a single module solution, or
   set SRAMMsgBlk, field SequenceCtl = 0x1F for a two module solution (see below).
4. Fence the CalOnce. See 2.9.9.2.8.2.
5. Program D18F2x9C_x0002_0099_dct[3:0][PmuStall] = 0.
6. mboxUSPend(PMUQEmpty). See 2.9.8.1.
   - If message is FAIL then continue to step 7 for that DCT only; In keeping with the requirement above, begin next step only after all DCTs are ready.

7. Read SRAMMsgBlk and store for later use.

If the total firmware size makes it necessary to load and execute two firmware modules consecutively for complete boot then BIOS performs the following additional steps. BIOS performs each step for each DCT={MaxDctMstr:0}, keeping the PMUs in lockstep, before moving to the next step.

1. Program D18F2x9C_x0002_0099_dct[3:0][PmuReset,PmuStall] = 1,1.
2. Program D18F2x9C_x0002_0099_dct[3:0][PmuReset] = 0.
3. Perform the PMU firmware load for the module containing 2D Read Training. See 2.9.9.2.9.
   - SRAMMsgBlk values from first PMU execution should be preserved. Do not overwrite SRAMMsgBlk.
4. Program SRAMMsgBlk with all values necessary for 2D Read Training. See 2.9.8.3.
5. Set SRAMMsgBlk, field SequenceCtl = 60h.
6. Program D18F2x9C_x0002_0099_dct[3:0][PmuStall] = 0.
7. mboxUSPend(PMUQEmpty). See 2.9.8.1.

2.9.9.6 DRAM Training

The PMU trains the I/O timing and electrical parameters on the DDR bus. BIOS initiates the training using a command bitmap in the SRAMMsgBlk of each PMU, keeping each PMU in lockstep. See 2.9.9.5.

Once the I/O timing is trained, the BIOS trains the round trip data latency path from the controller through the channel and back to the northbridge. See 2.9.9.6.1.

2.9.9.6.1 Training MaxRdLatency

After DRAM training, BIOS optimizes D18F2x210_dct[3:0]_nbp[3:0][MaxRdLatency] using the following algorithm. For MaxRdLatency training, BIOS generates a training pattern using continuous read or write data streams. See 2.9.10.1 [DCT Training Pattern Generation].

For each DCT={MaxDct:0}:

1. Calculate a starting MaxRdLatency delay value by converting Tcl to NCLKs. See D18F2x200_dct[3:0]_mp[1:0][Tcl] or D18F2xB18_dct[3:0][Tcl].
2. Select 32 64-byte aligned test addresses associated with the chipselct that has the worst case round trip delay (D18F2x9C_x0[F,1:0][F,8:0]1_[F,9:0][F,3:0]80_dct[3:0][RxDly] (for a DQ pad) + D18F2x9C_x0[F,1:0][F,8:0]1_[F,9:0][F,3:0]80_dct[3:0][RxDly] (for a DQS pad within the same bytelane as the DQ pad).
3. Write the DIMM test addresses with the training pattern.
4. For each MaxRdLatency value incrementing from the value calculated in step 1:
   A. Program D18F2x210_dct[3:0]_nbp[3:0][MaxRdLatency] with the current value.
   B. Read the DIMM test addresses.
   C. Compare the values read against the pattern written.
      - If the pattern is read correctly, go to step 5.
5. Program D18F2x210_dct[3:0]_nbp[3:0][MaxRdLatency] = CEIL(current value + fudge factor).
   - NB P-state 0 fudge factor = 1 NCLK + 3 MEMCLK
   - NB P-state [3:1] fudge factor = 3 NCLK + 3 MEMCLK

2.9.9.7 Synchronous Channel Initialization

- BIOS ensures that the frequency is programmed in the DCT correctly prior to the channel initialization. See D18F2x94_dct[3:0][MemClkFreq], D18F2x2E0_dct[3:0][M1MemClkFreq], and

D18F2xB1C_dct[3:0][MemClkFreq].
- IF (Ddr3Mode) then BIOS programs DCT specific read pointer initial values as specified in step 2 of 2.9.9.2.6 [Phy FIFO Configuration] prior to the channel initialization.

1. IF resuming from an S3 system state and the DRAMs are in self-refresh, then
   - Program D18F2x9C_x00FF_000D_dct[3:0][PhyClkCtl]=1.
2. Program D18F2x78_dct[3:0][PtrInitReq]=1. Wait for D18F2x78_dct[3:0][PtrInitReq]==0.

2.9.9.8 DRAM Channel Disable

The following steps are performed to disable an unused DRAM channel:

1. Program D18F2x9C_x03FF_F041_dct[3:0]=0000_0000h.
   - See D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0], and D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]041_dct[3:0].
2. Program D18F2x9C_x00FA_F04A_dct[] = 0080h.
   - See D18F2x9C_x00[F,3:0]0_[F,B:0]04A_dct[3:0] and D18F2x9C_x0009_004A_dct[3:0].
3. Program D18F2x9C_x0002_000B_dct[3:0] = 0000_0004h.
4. Ensure that D18F2x78_dct[3:0][ChanVal]==0.
5. Ensure that D18F2x90_dct[3:0][DisDllShutdownSR]==1.
6. Program D18F2x94_dct[3:0][DisDramInterface]=1.

If a DCT does not exist then these steps must be skipped.

2.9.9.9 DRAM Phy Power Savings

For power savings, BIOS should perform the following actions for each enabled channel:

1. Program D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0] as follows to disable unused pads.
   - DrvStrenN = DrvStrenP=0.
   - See 2.9.4. Software does this for each unconnected pad in the package or each pad connected to unused pin(s).
2. Program D18F2x9C_x0[3,1:0][F,3:0]0_0014_dct[3:0][MaxDurDllNoLock] = 0.
3. Program D18F2x9C_x0[3,1:0][F,8:0]1_0014_dct[3:0][MaxDurDllNoLock,DllPumpPeriod] as follows:
   - IF (DDR rate < = 1067) MaxDurDllNoLock = 9h ELSE MaxDurDllNoLock = 7h.
   - DllPumpPeriod = 3h.
4. Program D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]04D_dct[3:0] as follows:
   - For M1 context program ODTStrenN = ODTStrenP = 0.
5. Program D18F2x9C_x01F1_F043_dct[3:0] = 0004h.
   - See D18F2x9C_x0[3,1:0][F,8:0]1_[F,7:0]043_dct[3:0].
6. Program D18F2x9C_x00FA_F04A_dct[] = 0080h.
   - See D18F2x9C_x00[F,3:0]0_[F,B:0]04A_dct[3:0] and D18F2x9C_x0009_004A_dct[3:0].
7. Power down unused DBYTE 9 as follows:
   - Program D18F2x9C_x0091_F04A_dct[3:0] = 0280h.
   - Program D18F2x9C_x0091_0F77_dct[3:0] = 07CFh.
   - Program D18F2x9C_x0091_0000_dct[3:0] = 00004.
   - Program D18F2x9C_x0091_0F77_dct[3:0] = 07DFh.
   - Program D18F2x9C_x0391_F04D_dct[3:0] = 0000h.
   - Program D18F2x9C_x0391_F041_dct[3:0] = 0000h.
8. Disable unused DLL components in ABYTE as follows:

- Program D18F2x9C_x0020_0077_dct[3:0] = 07C0h.
- Program D18F2x9C_x0030_0077_dct[3:0] = 07C0h.
- Program D18F2x9C_x0000_0077_dct[3:0] = 07C4h.
- Program D18F2x9C_x0010_0077_dct[3:0] = 07C4h.
- See D18F2x9C_x00[F,3:0]0_0077_dct[3:0]

9. If ECC memory is not connected or is disabled, or the package does not support ECC, then power down data chiplet 8 with the following:
   - Write to all memory P-state instances if available.
   - Program D18F2x9C_x00[F,8:0]1_[F,B:0]04A_dct[3:0] = 0280h.
   - Program D18F2x9C_x00[F,8:0]1_0[F,2:0]77_dct[3:0] = 07CFh.
   - Program D18F2x9C_x00[F,8:0]1_0000_dct[3:0] = 00004.
   - Program D18F2x9C_x00[F,8:0]1_0[F,2:0]77_dct[3:0] = 07DFh.
   - Program D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]04D_dct[3:0] = 0000h.
   - Program D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]041_dct[3:0] = 0000h.
10. Power down unused receivers in data chips as follows:
    - Program D18F2x9C_x00F1_804A_dct[3:0] = 280h.
    - Program D18F2x9C_x00F1_904A_dct[3:0] = 280h.
    - If x4 DIMMs are not present then program D18F2x9C_x00F1_B04A_dct[] = 280h.
    - See D18F2x9C_x00[F,8:0]1_[F,B:0]04A_dct[3:0]
11. Power down the PMU as follows:
    - Program D18F2x9C_x0002_0099_dct[3:0][PmuReset,PmuStall] = {1,1}.
    - Program D18F2x9C_x0002_0099_dct[3:0][SRAM_SD] = 1.
    - For M0 context program D18F2x9C_x0[1:0]02_0080_dct[3:0][PMUClkDiv] = 7.

2.9.10 Continuous Pattern Generation

DRAM training relies on the ability to generate a string of continuous reads or writes between the processor and DRAM, such that worst case electrical interactions can be created. This section describes how these continuous strings of accesses may be generated.

2.9.10.1 DCT Training Pattern Generation

DCT training pattern generation uses pattern generators in the DCT to generate controlled read and write traffic streams. During write pattern generation, data values based off of a deterministic pattern are burst to the DRAM interface. Conversely for reads, data bursts from the DRAM interface are compared against expected data values on a per nibble basis.

Two address modes are available for DRAM training pattern generation, as configured by D18F2x250_dct[3:0][CmdTgt]. For generating a stream of reads or writes to the same rank, address target A mode is used. To generate a stream of accesses to up to two different ranks, address target A and B mode is used.

An overview of the BIOS sequence to generate training patterns is as follows:

- Configure the DCT for pattern generation. See 2.9.9.4 [DCT Specific Configuration].
- Ensure DIMMs are configured to support 8-beat bursts (BL8 or dynamic burst length on the fly).
- Wait for D18F2x250_dct[3:0][CmdSendInProg] = 0.
- Program D18F2x250_dct[3:0][CmdTestEnable] = 1.
- Send activate commands as appropriate. See 2.9.10.1.1 [Activate and Precharge Command Generation].
- Send read or write commands as desired. See 2.9.10.1.2 [Read and Write Command Generation].
- Send precharge commands as appropriate. See 2.9.10.1.1 [Activate and Precharge Command Generation].
- Program D18F2x250_dct[3:0][CmdTestEnable] = 0.

2.9.10.1.1 Activate and Precharge Command Generation

Prior to sending read or write commands, BIOS must send an activate command to a row in a particular bank of the DRAM devices for access. To send an activate command, BIOS performs the following steps:

- Program D18F2x28C_dct[3:0] to the desired address as follows:
  - CmdChipSelect = CS[7:0].
  - CmdBank = BA[2:0].
  - CmdAddress = A[17:0].
- Program D18F2x28C_dct[3:0][SendActCmd] = 1.
- Wait until D18F2x28C_dct[3:0][SendActCmd] = 0.
- Wait 75 MEMCLKs.

After completing its accesses, BIOS must deactivate open rows in the DRAM devices. To send a precharge or precharge all command to deactivate open rows in a bank or in all banks, BIOS performs the following steps:

- Wait 25 MEMCLKs.
- Program D18F2x28C_dct[3:0] to the desired address as follows:
  - CmdChipSelect = CS[7:0].
  - Precharge all command:
    - CmdAddress[10] = 1.
  - Precharge command:
    - CmdAddress[10] = 0.
    - CmdBank = BA[2:0].

- Program D18F2x28C_dct[3:0][SendPchgCmd] = 1.
- Wait until D18F2x28C_dct[3:0][SendPchgCmd] = 0.
- Wait 25 MEMCLKs.

2.9.10.1.2 Read and Write Command Generation

BIOS performs the following steps for read pattern generation:

- Program D18F2x27C_dct[3:0],D18F2x278_dct[3:0], and D18F2x274_dct[3:0] with the data comparison masks for bit lanes of interest.
- Program D18F2x270_dct[3:0][DataPrbsSeed] the seed for the desired PRBS.
- Program D18F2x260_dct[3:0][CmdCount] equal to the number of cache line commands.
- Program D18F2x25C_dct[3:0][BubbleCnt, CmdStreamLen]. See 2.9.10.1.4 [BubbleCnt and CmdStreamLen Programming].
- Program D18F2x25[8,4]_dct[3:0] to the initial address.
- Program D18F2x250_dct[3:0] as follows:
  - ResetAllErr and StopOnErr as desired. See 2.9.10.1.3 [Data Comparison].
  - CmdTgt corresponding to D18F2x25[8,4]_dct[3:0].
  - CmdType = 000b.
  - SendCmd = 1.
- If D18F2x260_dct[3:0][CmdCount] != 0 then
  Wait for D18F2x250_dct[3:0][TestStatus]==1 and D18F2x250_dct[3:0][CmdSendInProg]==0.
  Else
  Wait the desired amount of time.
  Program D18F2x260_dct[3:0][CmdCount] = 1.
  Wait for D18F2x250_dct[3:0][TestStatus] ==1 and D18F2x250_dct[3:0][CmdSendInProg]==0.
- Program D18F2x250_dct[3:0][SendCmd]=0.
- Read D18F2x264_dct[3:0], D18F2x268_dct[3:0], and D18F2x26C_dct[3:0] if applicable.

BIOS performs the following steps for write pattern generation:

- Program D18F2x270_dct[3:0][DataPrbsSeed] the seed for the desired PRBS.
- Program D18F2x260_dct[3:0][CmdCount] equal to the number of cache line commands desired.
- Program D18F2x25C_dct[3:0][BubbleCnt, CmdStreamLen]. See 2.9.10.1.4 [BubbleCnt and CmdStreamLen Programming].
- Program D18F2x25[8,4]_dct[3:0] to the initial address.
- Program D18F2x250_dct[3:0] as follows:
  - CmdTgt corresponding to D18F2x25[8,4]_dct[3:0].
  - CmdType = 001b.
  - SendCmd = 1.
- If D18F2x260_dct[3:0][CmdCount] != 0 then
  Wait for D18F2x250_dct[3:0][TestStatus]==1 and D18F2x250_dct[3:0][CmdSendInProg]==0.
  Else
  Wait the desired amount of time.
  Program D18F2x260_dct[3:0][CmdCount] = 1.
  Wait for D18F2x250_dct[3:0][TestStatus]==1 and D18F2x250_dct[3:0][CmdSendInProg]==0.
- Program D18F2x250_dct[3:0][SendCmd]=0.

BIOS combines the two sets of steps listed above for alternating write and read pattern generation.

2.9.10.1.3 Data Comparison

The DCT compares the incoming read data against the expected pattern sequence during pattern generation. BIOS may choose to continue command generation and accumulate errors or stop command generation on the first error occurrence by programming D18F2x250_dct[3:0][StopOnErr].

Error information is reported via D18F2x264_dct[3:0], D18F2x268_dct[3:0], D18F2x26C_dct[3:0], D18F2x294_dct[3:0], D18F2x298_dct[3:0] and D18F2x29C_dct[3:0]. Error information can be masked on per-bit basis by programming D18F2x274_dct[3:0], D18F2x278_dct[3:0], and D18F2x27C_dct[3:0].

BIOS resets the error information by programming D18F2x250_dct[3:0][ResetAllErr]=1.

Error information is only valid in certain modes of D18F2x250_dct[3:0][CmdType, CmdTgt] and D18F2x260_dct[3:0][CmdCount] and when using 64 byte aligned addresses in D18F2x25[8,4]_dct[3:0][TgtAddress]. Some modes require a series of writes to setup a DRAM data pattern. See Table 36.

Table 36. Command Generation and Data Comparison

Commands	CmdType	Cmd Tgt	Maximum CmdCount[4]
Read	000b	00b[1]	128
		01b[1]	256[2]
Write-Read 010b		00b	Infinite
		01b[3]	256[2]

1. Requires setup writes to store a data pattern in DRAM. The write commands are generated using the same CmdTgt, CmdCount, and DataPrbsSeed settings.
2. D18F2x254[TgtAddress] != D18F2x258[TgtAddress].
3. Requires setup writes to store a data pattern in DRAM. The write commands are generated programming D18F2x254[TgtAddress] to the intended Target B, CmdTgt=00b, CmdCount to 1/2 of the intended command count, and the same DataPrbsSeed setting.
4. D18F2x250_dct[3:0][LsfrRollOver]=0. The maximum CmdCount is infinite for all modes listed if D18F2x250_dct[3:0][LsfrRollOver]=1.

2.9.10.1.4 BubbleCnt and CmdStreamLen Programming

BIOS programs D18F2x25C_dct[3:0][BubbleCnt2, BubbleCnt, CmdStreamLen] to ensure proper channel command spacing in command generation mode.

For continuous pattern generation it is expected that BubbleCnt = 0. In other modes, BIOS programs BubbleCnt, BubbleCnt2, and CmdStreamLen greater than or equal to the relevant DRAM timing parameters shown below to prevent contention on the DRAM bus. In all cases, if the minimum BubbleCnt > 0 or CmdType = 010b then BIOS programs CmdStreamLen = 1.

Table 37. Command Generation and BubbleCnt Programming

Commands	CmdType	CmdTgt	BubbleCnt	BubbleCnt2
Read-Read same CS	000b	0xb	D18F2x218_dct[3:0]_mp[1:0][TrdrdSdSc] - 1; Exclude banned spacing: D18F2x218_dct[3:0]_mp[1:0][TrdrdBan]	xh
Write-Write same CS	001b	0xb	D18F2x214_dct[3:0]_mp[1:0][TwrwrSdSc] - 1	xh
Write-Read same CS	010b	00b	D18F2x20C_dct[3:0]_mp[1:0][Twtr] + D18F2x20C_dct[3:0]_mp[1:0][Tcwl] + 4 - 1	D18F2x21C_dct[3:0]_mp[1:0][TrwtTO] - 1
Read-Read different CS	000b	01b	D18F2x218_dct[3:0]_mp[1:0][TrdrdSdDc] - 1; Exclude banned spacing: D18F2x218_dct[3:0]_mp[1:0][TrdrdBan]	xh
Write-Write different CS	001b	01b	D18F2x214_dct[3:0]_mp[1:0][TwrwrSdDc] - 1	xh
Write-Read different CS	010b	01b	D18F2x218_dct[3:0]_mp[1:0][Twrrd] - 1	D18F2x21C_dct[3:0]_mp[1:0][TrwtTO] - 1
Read-Read different DIMM	000b	01b	D18F2x218_dct[3:0]_mp[1:0][TrdrdDd] - 1; Exclude banned spacing: D18F2x218_dct[3:0]_mp[1:0][TrdrdBan]	xh
Write-Write different DIMM	001b	01b	D18F2x214_dct[3:0]_mp[1:0][TwrwrDd] - 1	xh
Write-Read different DIMM	010b	01b	D18F2x218_dct[3:0]_mp[1:0][Twrrd] - 1	D18F2x21C_dct[3:0]_mp[1:0][TrwtTO] - 1

2.9.11 Memory Interleaving Modes

The processor supports the following memory interleaving modes:

- Chip select: interleaves the physical address space over multiple DIMM ranks on a channel, as opposed to each DIMM owning single consecutive address spaces. See 2.9.11.1 [Chip Select Interleaving].
- Channel: interleaves the physical address space over multiple channels, as opposed to each channel owning single consecutive address spaces. See 2.9.11.2 [Channel Interleaving].

Any combination of these interleaving modes may be enabled concurrently.

Table 38. Recommended Interleave Configurations

Interleaving Mode	Enabled	Disabled
Chip Select Interleaving	Number of chip selects installed on the channel is a power of two.	Requirements not satisfied.
Channel Interleaving	DIMMs are present on a power of two number of channels.	Requirements not satisfied.
Interleave Region Remapping[1]	UMA and DIMMs are present on a power of two number of channels and the channels do not have the same amount of DRAM.	~UMA or all channels have the same amount of DRAMor DIMMs are not present on a power of two number of channels.
1. The channel interleave region should always include the frame buffer.		

2.9.11.1 Chip Select Interleaving

The chip select memory interleaving mode has the following requirements:

- The number of chip selects interleaved is a power of two.
- The chip selects are the same size and type.

A BIOS algorithm for programming D18F2x[5C:40]_dct[3:0] [DRAM CS Base Address] and D18F2x[6C:60]_dct[3:0] [DRAM CS Mask] in memory interleaving mode is as follows:

1. Program all DRAM CS Base Address and DRAM CS Mask registers using contiguous normalized address mapping.
2. For each enabled chip select, swap the corresponding BaseAddr[38:27] bits with the BaseAddr[21:11] bits as defined in Table 39.
3. For each enabled chip select, swap the corresponding AddrMask[38:27] bits with the AddrMask[21:11] bits as defined in Table 39.

Table 39. DDR3 Swapped Normalized Address Lines for CS Interleaving

DIMM Address Map[1]	Chip Select Size	(BankSwap, BankSwapLoAddress)[2]	Swapped Base Address and Address Mask bits	
			4 way CS interleaving	2 way CS interleaving
0001b	256-MB	0b,N/A	[29:28] and [17:16]	[28] and [16]
		1b,8	[29:28] and [12:11]	[28] and [11]
		1b,9	[29:28] and [13:12]	[28] and [12]
0010b	512-MB	0b,N/A	[30:29] and [17:16]	[29] and [16]
		1b,8	[30:29] and [12:11]	[29] and [11]
		1b,9	[30:29] and [13:12]	[29] and [12]
0101b	1-GB	0b,N/A	[31:30] and [17:16]	[30] and [16]
		1b,8	[31:30] and [12:11]	[30] and [11]
		1b,9	[31:30] and [13:12]	[30] and [12]

Table 39. DDR3 Swapped Normalized Address Lines for CS Interleaving

DIMM Address Map[1]	Chip Select Size	(BankSwap, BankSwapLoAddress)[2]	Swapped Base Address and Address Mask bits	
			4 way CS interleaving	2 way CS interleaving
0110b	1-GB		[31:30] and [18:17]	[30] and [17]
0111b	2-GB	0b,N/A	[32:31] and [17:16]	[31] and [16]
		1b,8	[32:31] and [12:11]	[31] and [11]
		1b,9	[32:31] and [13:12]	[31] and [12]
1000b	2-GB, 4-GB, 8-GB		[32:31] and [18:17]	[31] and [17]
1001b	4-GB, 8-GB, 16-GB		[33:32] and [18:17]	[32] and [17]
1010b	4-GB	0b,N/A	[33:32] and [17:16]	[32] and [16]
		1b,8	[33:32] and [12:11]	[32] and [11]
		1b,9	[33:32] and [13:12]	[32] and [12]
1011b	8-GB	0b,N/A	[34:33] and [18:17]	[33] and [17]
		1b,8	[34:33] and [12:11]	[33] and [11]
		1b,9	[34:33] and [13:12]	[33] and [12]
1100b	16-GB		[35:34] and [19:18]	[34] and [18]

1. See D18F2x80_dct[3:0] [DRAM Bank Address Mapping].
2. See D18F2xA8_dct[3:0][BankSwap] and D18F2x110[BankSwapAddr8En, DctSelIntLvAddr]. If BankSwapAddr8En==1 && DctSelIntLvAddr==100b then BankSwapLoAddress=8 ELSE BankSwapLoAddress=9.

The following is an example of interleaving a 64-bit interface to DDR3 DRAM. The DRAM memory consists of two 512 MB dual rank DDR3 DIMMs.

1. The register settings for contiguous memory mapping are:
   - D18F2x80_dct[3:0] = 0000_0011h. // CS0/1 = 256 MB; CS2/3 = 256 MB
   - D18F2x40 = 0000_0001h. // 0 MB base
   - D18F2x44 = 0010_0001h. // 256 MB base = 0 MB + 256 MB
   - D18F2x48 = 0020_0001h. // 512 MB base = 256 MB + 256 MB
   - D18F2x4C = 0030_0001h. // 768 MB base = 512 MB + 256 MB
   - D18F2x60 = 0008_FFE0h. // CS0/CS1 = 256 MB
   - D18F2x64 = 0008_FFE0h. // CS2/CS3 = 256 MB
2. The base address bits to be swapped are defined in Table 39, 256MB chip select size, 4 way CS interleaving column. The BaseAddr[29:28] bits are specified by D18F2x[5C:40]_dct[3:0][21:20]. The BaseAddr[17:16] bits are specified by D18F2x[5C:40]_dct[3:0][11:10].
   - D18F2x40 = 0000_0001h.
   - D18F2x44 = 0000_0401h.
   - D18F2x48 = 0000_0801h.
   - D18F2x4C = 0000_0C01h.
3. The AddrMask bits to be swapped are the same as the BaseAddr bits defined in the previous step. The AddrMask[29:28] bits are specified by D18F2x[6C:60]_dct[3:0][21:20]. The AddrMask[17:16] bits are specified by D18F2x[6C:60]_dct[3:0][11:10].

- D18F2x60 = 0038_F3E0h.
- D18F2x64 = 0038_F3E0h.

4. If BankSwap is enabled and DCT channel interleaving is enabled on system address bit[8], then the Base and AddrMask bits to be swapped are as follows:
   - D18F2x40 = 0000_0001h.
   - D18F2x44 = 0000_0021h.
   - D18F2x48 = 0000_0041h.
   - D18F2x4C = 0000_0061h.
   - D18F2x60 = 0038_FF90h.
   - D18F2x64 = 0038_FF90h.
5. If BankSwap is enabled and DCT channel interleaving is enabled on system address bit[9], then the Base and AddrMask bits to be swapped are as follows:
   - D18F2x40 = 0000_0001h.
   - D18F2x44 = 0000_0041h.
   - D18F2x48 = 0000_0081h.
   - D18F2x4C = 0000_00C1h.
   - D18F2x60 = 0038_FF20h.
   - D18F2x64 = 0038_FF20h.

2.9.11.2 Channel Interleaving

The channel memory interleaving mode requires that DIMMs are present on both channels. Channel interleaving is enabled by programming D18F1x2[1,0][C,4][DctIntLvEn] and D18F2x110[DctSelIntLvAddr] to specify how interleaving is performed among the DCTs. If the channels do not have the same amount of DRAM, D18F1x2[1,0][8,0][DctBaseAddr] and D18F1x2[1,0][C,4][DctLimitAddr] are used to configure the interleaved region. See also 2.9.12 [Memory Hoisting].

2.9.11.2.1 Four Channel Interleaving

Interleaving 4 DCTs requires one D18F1x2[1,0][8,0][DctBaseAddr] and D18F1x2[1,0][C,4][DctLimitAddr] pair to define the interleave region. D18F1x2[1,0][C,4][DctIntLvEn] is programmed to enable 4 DCTs and D18F2x110[DctSelIntLvAddr] determines the interleave addressing. See 2.9 for product specific limitations.

2.9.12 Memory Hoisting

Memory hoisting reclaims the otherwise inaccessible DRAM that would naturally reside in memory regions used by MMIO. When memory hoisting is configured by BIOS, DRAM physical addresses are repositioned above the 4 GB address level in the address map. In operation, the physical addresses are remapped in hardware to the normalized addresses used by a DCT.

The region of DRAM that is hoisted is defined to be from D18F1xF0[DramHoleBase] to the 4 GB level. Hoisting is enabled by programming D18F1xF0 [DRAM Hole Address] and configuring the DCTs per the equations in this section.

DramHoleSize is defined in order to simplify the following equations in this section and is calculated as follows:

- Define the DRAM hole region as DramHoleSize[31:24] = 100h - D18F1xF0[DramHoleBase[31:24]].

2.9.12.1 DramHoleOffset Programming

D18F1xF0[DramHoleOffset] is programmed to account for the addresses from D18F1xF0[DramHoleBase] to 4 GB when it falls inside of a D18F1x2[1,0][8,0][DctBaseAddr] and D18F1x2[1,0][C,4][DctLimitAddr]

region. See Figure 3 as an example memory population.

- Program D18F1xF0[DramHoleOffset[31:23]] = {DramHoleSize[31:24], 0b} + {DctBaseAddr[31:27], 0000b};

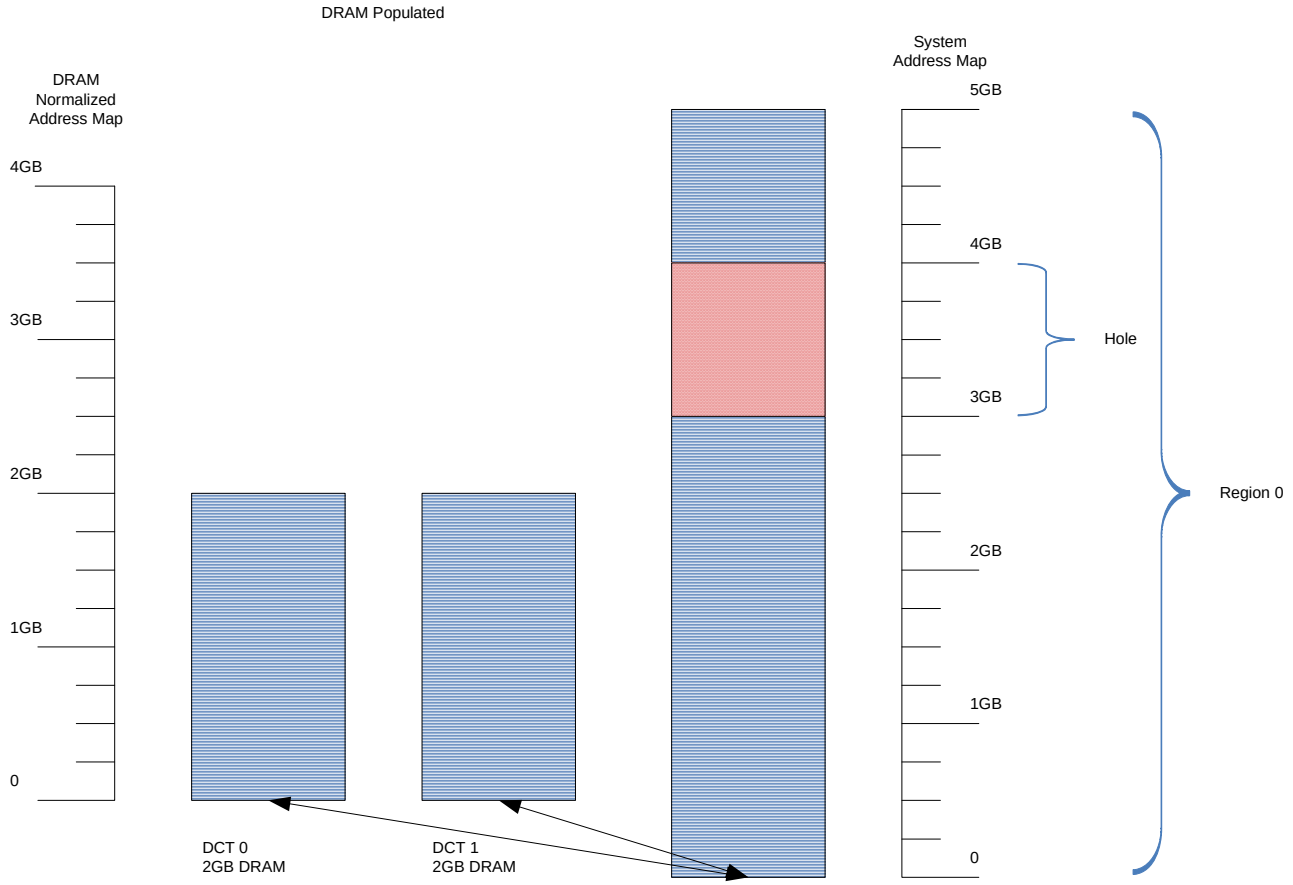

Figure 3: Memory Configuration with Memory Hole inside of Region

D18F1xF0[DramHoleOffset] is unused when the memory hole falls outside of a region. Figure 4 shows an example memory population which uses two memory regions. Region 1 is configured to begin above the memory hole.

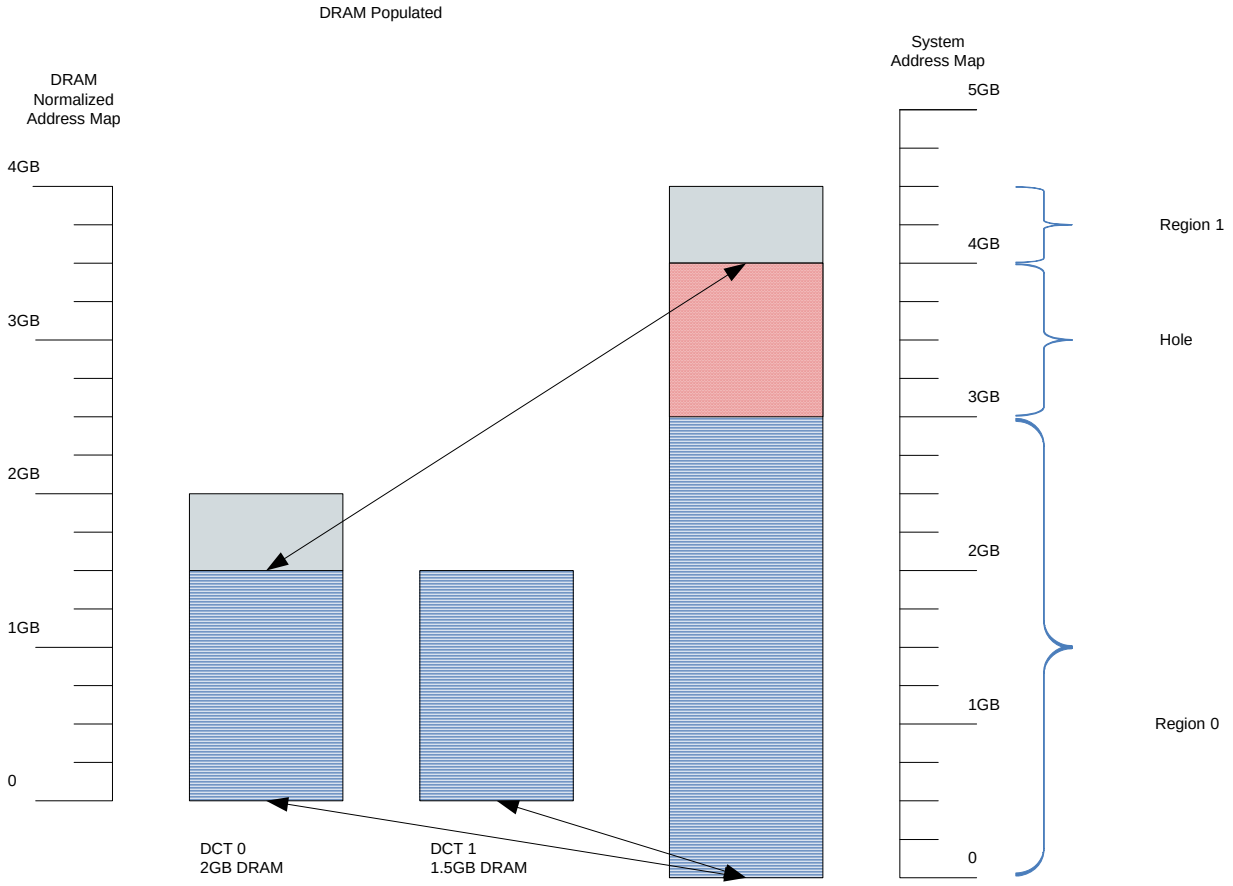

Figure 4: Memory Configuration with Memory Hole outside of Region

2.9.12.2 DctSelBaseOffset Programming

When a DCT is mapped by more than one D18F1x2[1C:00] region, D18F1x2[1,0][8,0][DctOffsetEn] D18F1x2[4C:40][DctHighAddrOffset] are programmed for the second region. In this case, an offset must be applied when forming the normalized address accounting for the DCT addresses mapped by the first region.

Program D18F1x2[4C:40][DctHighAddrOffset[38:27]] = ((DctLimitAddr + 1) - DctBaseAddr - SizeOf(Memory Holes))/(D18F1x2[1,0][C,4][DctIntLvEn] > 0 ? POPCNT(D18F1x2[1,0][C,4][DctIntLvEn]) : 1).

Examples:

- Figure 5: Region 0 maps addresses 0x0 thru 0x7FFF_FFFF, offset Region 1 which is 2x channel interleaved.
  - D18F1x208[DctOffsetEn] = 1.
  - D18F1x240[DctHighAddrOffset] = ((0x7FFF_FFFF + 1) - 0 - 0)/(1) = 2GB. //DCT 0 offset from Region 0.
  - D18F1x244[DctHighAddrOffset] = 0. //DCT 1 is not mapped by Region 0.

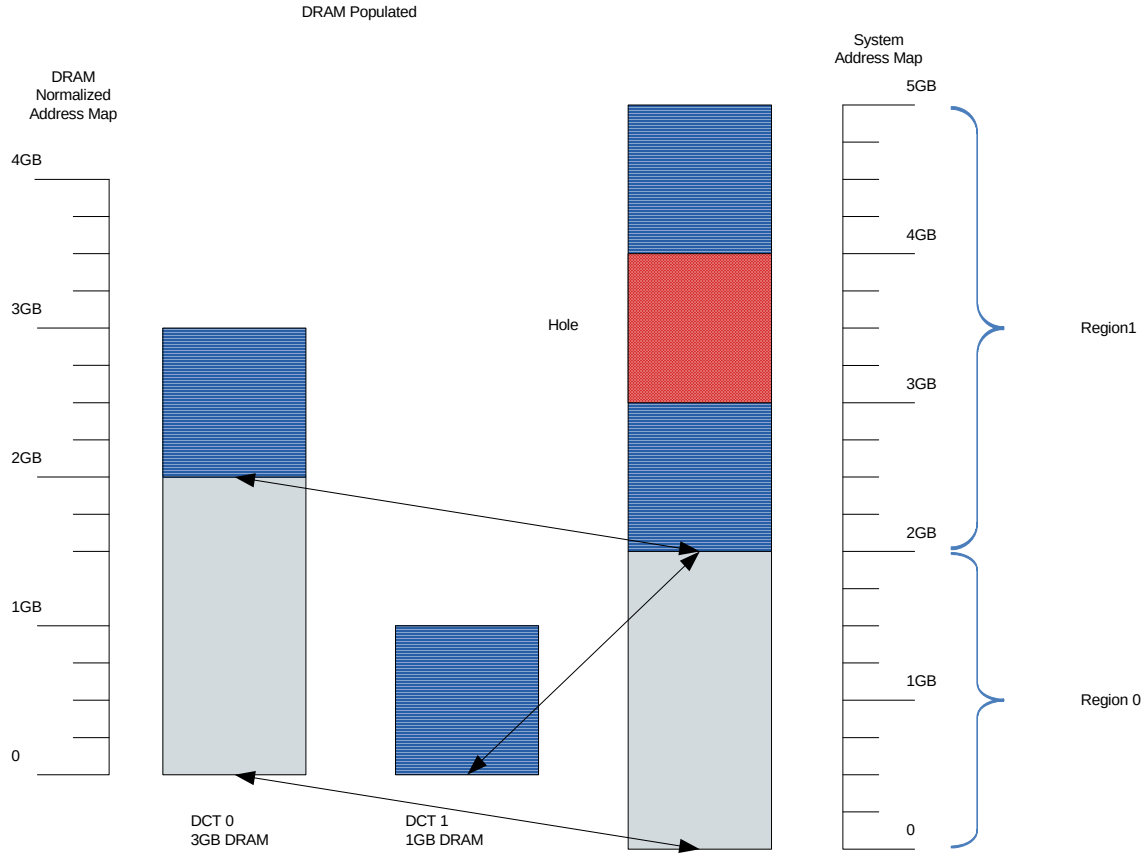

Figure 5: 2 DCT Channel Interleaved

- Figure 6: Region 0 maps addresses 0x0 thru 0x1_3FFF_FFFF which is channel interleaved and contains a 1GB memory hole; offset Region 1 to map the remaining memory.
  - D18F1x208[DctOffsetEn] = 1.
  - D18F1x240[DctHighAddrOffset] = ((0x1_3FFF_FFFF + 1) - 0 - 0x4000_0000)/(2) = 2GB. //DCT 0 offset from Region 0.

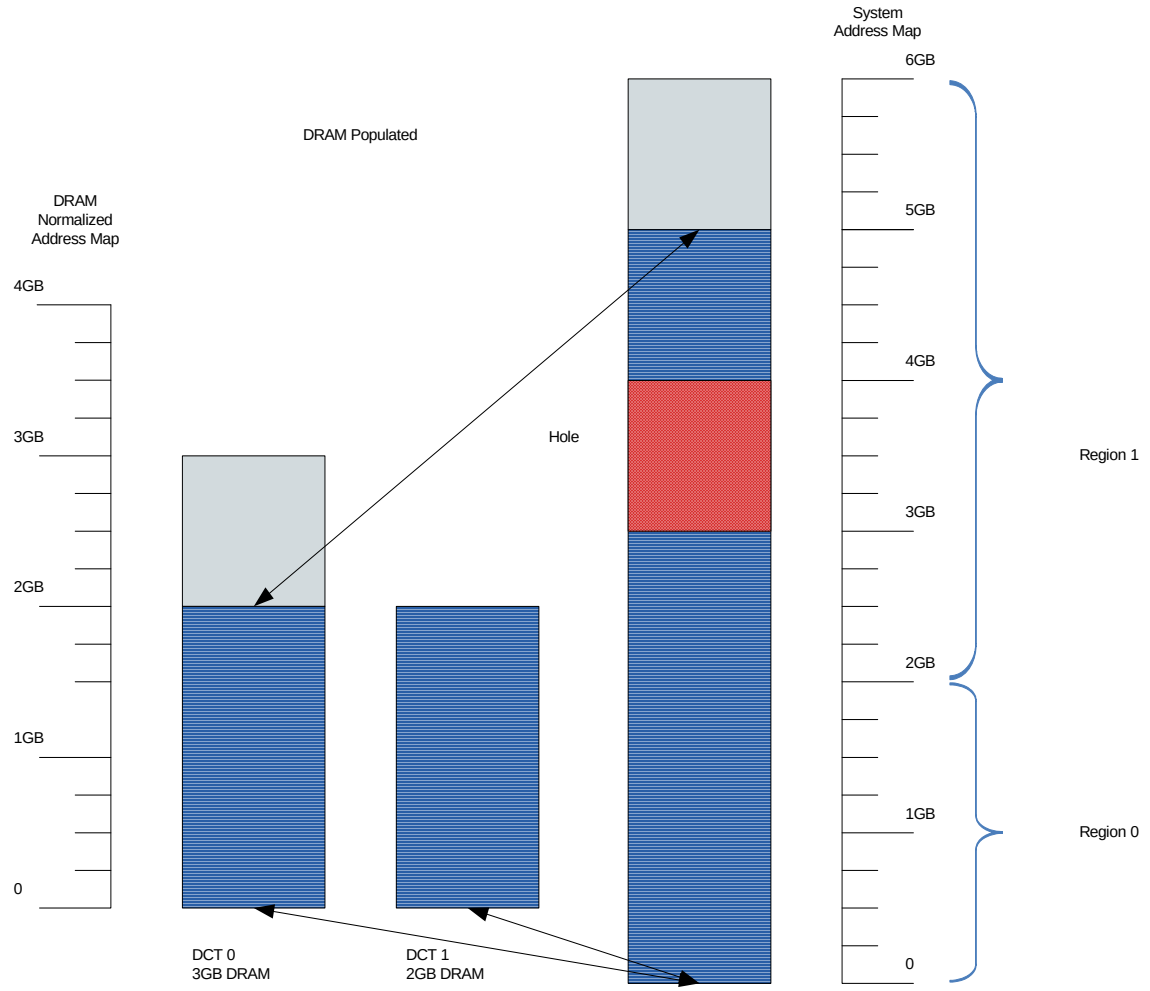

Figure 6: 2 DCT Channel Interleaved with Memory Hole

2.9.13 DRAM CC6/PC6 Storage

DRAM is used to hold the state information of cores entering the CC6 power management state. As part of the system setup if CC6 or PC6 is enabled, BIOS configures a special region of DRAM to hold the state information. In operation, hardware protects this region from general system accesses while allowing the cores access during C-state transitions.

2.9.13.1 Fixed Storage

The size of each special DRAM storage region is defined to be a fixed 16MB. BIOS configures the storage region at the top of the DRAM range, adjusts D18F1x[7:4][C,4][DramLimit] and the processor top of DRAM specified by MSRC001_001A[TOM] or MSRC001_001D[TOM2] downward accordingly. See Table 40.

After finalizing the system DRAM configuration, BIOS must set D18F2x118[LockDramCfg] = 1 to enable the hardware protection.

Table 40. Example storage region configuration

Node	DRAM Populated	D18F1x[17C:140,7C:40] [DramBase, DramLimit]	CC6 DRAM Range	D18F4x128 [CoreStateSaveDestNode]	D18F1x120[DramBaseAddr], D18F1x124[DramLimitAddr]
0	256 MB	0 MB, 240 MB - 1	240 MB, 256 MB - 1	0	0 B, 256 MB - 1

M

2.9.14 DRAM On DIMM Thermal Management and Power Capping

Each DCT can throttle commands based on the state of the channel EVENT_L pin or when D18F2xA4[BwCapEn]==1. The EVENT_L pin is used for thermal management while D18F2xA4[BwCapEn] limits memory power independent of the thermal management solution.

The EVENT_L pin for each channel must be wire OR'ed. If all DCTs enabled throttle commands in lockstep using the amount specified in D18F2xA4[CmdThrottleMode] and D18F2xA4[BwCapCmdThrottleMode].

The recommended BIOS configuration for the EVENT_L pin is as follows:

- BIOS may enable command throttling on a DRAM controller if the platform supports the EVENT_L pin by programming D18F2xA4[ODTSEn] = 1.
  - The recommended usage is for this pin to be connected to one or more JEDEC defined on DIMM temperature sensors. The DIMM SPD ROM indicates on DIMM temperature sensor support.
  - BIOS configures the temperature sensor(s) to assert EVENT_L pin active low when the trip point is exceeded and deassert EVENT_L when the temperature drops below the trip point minus the sensor defined hysteresis.
  - BIOS programs D18F2xA4[CmdThrottleMode] with the throttling mode to employ when the trip point has been exceeded.
  - The hardware enforces a refresh rate of 3.9 us while EVENT_L is asserted.
- BIOS configures D18F2x8C_dct[3:0][Tref] based on JEDEC defined temperature range options, as indicated by the DIMM SPD ROM. The two defined temperature ranges are normal (with a case temperature of 85 °C) and extended (with a case temperature of 95 °C).
  - If all DIMMs support the normal temperature range, or if normal and extended temperature range DIMMs are mixed, BIOS programs Tref to 7.8 us and D18F2xA4[ODTSEn] = 1. BIOS configures the temperature sensor trip point for all DIMMs according to the 85 °C case temperature specification.
  - If all DIMMs support the extended temperature range, BIOS has two options:
    a. Follow the recommendation for normal temperature range DIMMs.
    b. Program Tref = 3.9 us and configure the temperature sensor trip point for all DIMMs according to the 95 °C case temperature specification.
- At startup, the BIOS determines if the DRAMs are hot before enabling a DCT and delays for an amount of time to allow the devices to cool under the influence of the thermal solution. This is accomplished by checking the temperature status in the temperature sensor of each DIMM.
- The DCT latched status of the EVENT_L pin for can be read by system software in D18F2xAC [DRAM Controller Temperature Status].

The relationship between the DRAM case temperature, trip point, and EVENT_L pin sampling interval is outlined as follows:

- The trip point for each DIMM is ordinarily configured to the case temperature specification minus a guardband temperature for the DIMM.
- The temperature guardband is vendor defined and is used to account for sensor inaccuracy, EVENT_L pin

sample interval, and platform thermal design.
- The sampling interval is vendor defined. It is expected to be approximately 1 second.

BIOS may enable bandwidth capping on a DRAM controller by setting D18F2xA4[BwCapEn] = 1 and programming D18F2xA4[BwCapCmdThrottleMode] with the throttling mode to employ. The DCT will employ the larger of the two throttling percentages as specified by D18F2xA4[BwCapCmdThrottleMode] and D18F2xA4[CmdThrottleMode] if the EVENT_L pin is asserted when both D18F2xA4[BwCapEn]==1 and D18F2xA4[ODTSEn]==1.

2.10 Thermal Functions

Thermal functions HTC, PROCHOT_L and THERMTRIP are intended to maintain processor temperature in a valid range by:

- Providing a signal to external circuitry for system thermal management like fan control.
- Lowering power consumption by switching to lower-performance P-state.
- Sending processor to the THERMTRIP state to prevent it from damage.

The processor thermal-related circuitry includes (1) the temperature calculation circuit (TCC) for determining the temperature of the processor and (2) logic that uses the temperature from the TCC.

2.10.1 The Tctl Temperature Scale

Tctl is a processor temperature control value used for processor thermal management. Tctl is accessible through D18F3xA4[CurTmp]. Tctl is a temperature on its own scale aligned to the processors cooling requirements. Therefore Tctl does not represent a temperature which could be measured on the die or the case of the processor. Instead, it specifies the processor temperature relative to the maximum operating temperature, Tctl,max. Tctl,max is specified in the power and thermal data sheet. Tctl is defined as follows for all parts:

A: For Tctl = Tctl_max to 255.875: the temperature of the part is [Tctl - Tctl_max] over the maximum operating temperature. The processor may take corrective actions that affect performance, such as HTC, to support the return to Tctl range B.

B: For Tctl = 0 to Tctl_max - 0.125: the temperature of the part is [Tctl_max - Tctl] under the maximum operating temperature.

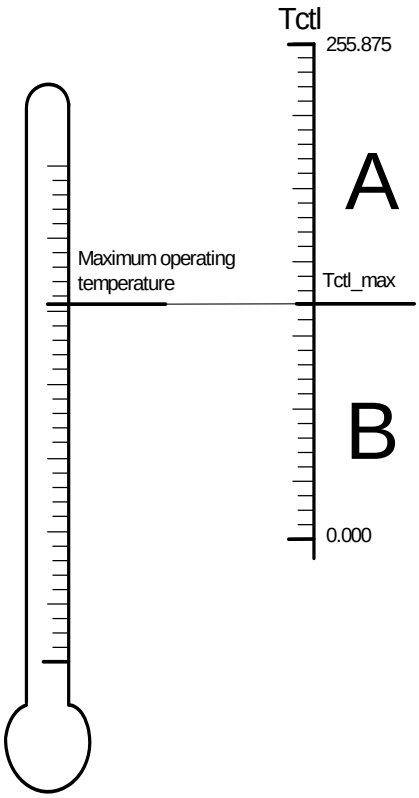

Figure 7: Tctl scale

2.10.2 Temperature Slew Rate Control

The temperature slew rate controls in D18F3xA4 are used to filter the processor temperature provided in D18F3xA4[CurTmp]. Separate controls are provided for increasing and decreasing temperatures. The latest measured temperature is referred to as Tctlm below.

If downward slew control is enabled (D18F3xA4[TmpSlewDnEn]), Tctl is not updated down unless Tctlm remains below Tctl for a time specified byD18F3xA4[PerStepTimeDn]. If at any point before the timer expires Tctlm equals or exceeds Tctl, then the timer resets and Tctl is not updated. If the timer expires, then Tctl is reduced by 0.125. If downard slew control is disabled, then if Tctlm is less than Tctl, Tctl is immediately updated to Tctlm.

The upward slew control works similar to downward slew control except that if Tctlm exceeds Tctl by a value defined by D18F3xA4[TmpMaxDiffUp] then Tctl is immediately updated to Tctlm. Otherwise, Tctlm must remain above Tctl for time specified by D18F3xA4[PerStepTimeUp] before Tctl is incremented by 0.125.

2.10.3 Temperature-Driven Logic

The temperature calculated by the TCC is used by HTC,THERMTRIP, and PROCHOT_L.

2.10.3.1 PROCHOT_L and Hardware Thermal Control (HTC)

The processor *HTC-active state* is characterized by (1) the assertion of PROCHOT_L, (2) reduced power consumption, and (3) reduced performance. While in the HTC-active state, software should not change the following: All D18F3x64 fields (except for HtcActSts and HtcEn), MSRC001_001F[DisProcHotPin]. Any change to the previous list of fields when in the HTC-active state can result in undefined behavior. HTC status and control is provided through D18F3x64.

The PROCHOT_L pin acts as both an input and as an open-drain output. As an output, PROCHOT_L is driven low to indicate that the HTC-active state has been entered due to an internal condition, as described by the following text. The minimum assertion and deassertion time for PROCHOT_L is 200 us with a minimum period of 2 ms.

While in the HTC-active state, the following power reduction actions are taken:

- CPU cores are limited to a P-state (specified by D18F3x64[HtcPstateLimit]); see 2.5.3 [CPU Power Management].
- The GPU may be placed in a low power state based on the state of D18F5x178[ProcHotToGnbEn]

The processor enters the HTC-active state if all of the following conditions are true:

- D18F3xE8[HtcCapable]=1.
- D18F3x64[HtcEn]=1.
- PWROK=1.
- THERMTRIP_L=1.

and any of the following conditions are true:

- Tctl is greater than or equal to the HTC temperature limit (D18F3x64[HtcTmpLmt]).
- PROCHOT_L=0.

The processor exits the HTC-active state when all of the following are true:

- Tctl is less than the HTC temperature limit (D18F3x64[HtcTmpLmt]).
- Tctl has become less than the HTC temperature limit (D18F3x64[HtcTmpLmt]) minus the HTC hysteresis limit (D18F3x64[HtcHystLmt]) since being greater than or equal to the HTC temperature limit

(D18F3x64[HtcTmpLmt]).
- PROCHOT_L=1.

The default value of the HTC temperature threshold (Tctl_max) is specified in the Power and Thermal Datasheet.

2.10.3.2 Software P-state Limit Control

D18F3x68 [Software P-state Limit] provides a software mechanism to limit the P-state MSRC001_0061[CurPstateLimit]. See 2.5.3 [CPU Power Management].

2.10.3.3 THERMTRIP

If the processor supports the THERMTRIP state (as specified by D18F3xE4[ThermtpEn] or CPUID Fn8000_0007_EDX[TTP], which are the same) and the temperature approaches the point at which the processor may be damaged, the processor enters the THERMTRIP state. The THERMTRIP function is enabled after cold reset (after PWROK asserts and RESET_L deasserts). It remains enabled in all other processor states, except during warm reset (while RESET_L is asserted). The THERMTRIP state is characterized as follows:

- The THERMTRIP_L signal is asserted.
- Nearly all clocks are gated off to reduce dynamic power.
- A low-value VID is generated.
- The system is placed into the S5 ACPI state (power off).

A cold reset is required to exit the THERMTRIP state.

2.11 Root Complex

2.11.1 Overview

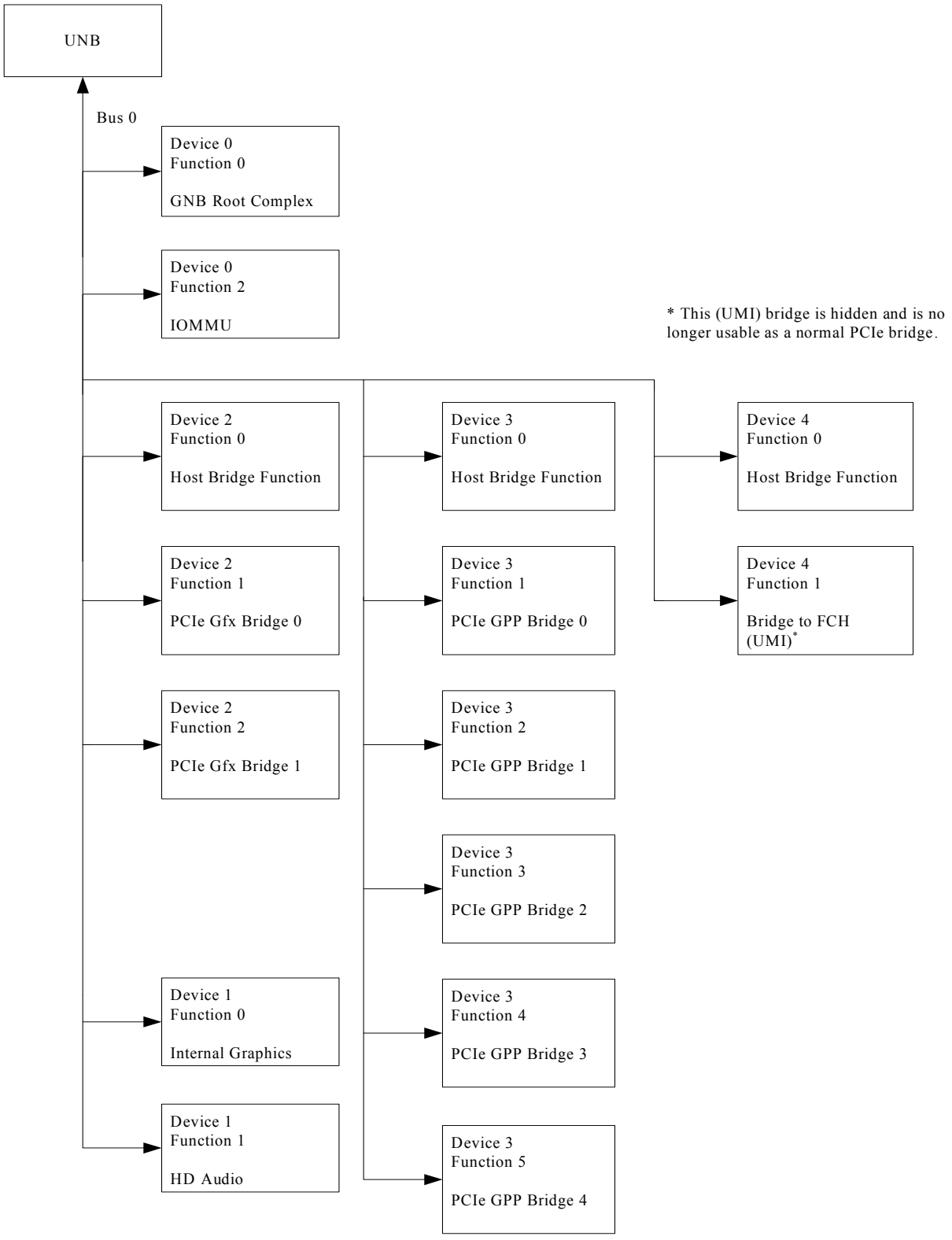

Figure 8: Root complex topology

2.11.2 Interrupt Routing

The GNB includes a fully programmable IOAPIC. The IOAPIC registers are accessed through the D0F0xF8 index and D0F0xFC data pair registers using two back-to-back config cycles. PCI defined INTx interrupts for each bridge are routed to IOAPIC pins via the bridge interrupt routing registers located at D0F0xFC_x1[B:0].

2.11.2.1 IOAPIC Configuration

The IOAPIC configuration is performed by the following sequence:

1. Set the base address for the memory mapped registers by programming D0F0xFC_x01[IoapicAddr] and D0F0xFC_x02[IoapicAddrUpper].
2. Enable IOAPIC by programming D0F0xFC_x00[IoapicEnable] = 1.
3. Only if the system is in PIC mode, program D0F0xFC_x00[IoapicSbFeatureEn] = 1. This bit should be programmed to 0 when the system is in APIC mode.

The IOAPIC has a total of 39 interrupt inputs. These inputs are as follows:

- 7 groups of PCIe interrupts each having a 4-bit external interrupt bus (INT A/B/C/D) and a 1-bit bridge interrupt, and
- a 4-bit external interrupt bus from GBIF.

The recommended interrupt routing and swizzling configuration is as shown in Table 41.

Table 41: Recommended Interrupt Routing and Swizzling Configuration

Device	Register	Setting	Description
Dev2Fn1	D0F0xFC_x10[BrExtIntrGrp]	0h	Map INT A/B/C/D to interrupt 0/1/2/3. Map bridge interrupt to interrupt 16.
	D0F0xFC_x10[BrExtIntrSwz]	0h	
	D0F0xFC_x10[BrIntIntrMap]	10h	
Dev2Fn2	D0F0xFC_x11[BrExtIntrGrp]	1h	Map INT A/B/C/D to interrupt 4/5/6/7. Map bridge interrupt to interrupt 17.
	D0F0xFC_x11[BrExtIntrSwz]	0h	
	D0F0xFC_x11[BrIntIntrMap]	11h	
Dev3Fn1	D0F0xFC_x12[BrExtIntrGrp]	2h	Map INT A/B/C/D to interrupt 8/9/10/11. Map bridge interrupt to interrupt 18.
	D0F0xFC_x12[BrExtIntrSwz]	0h	
	D0F0xFC_x12[BrIntIntrMap]	12h	
Dev3Fn2	D0F0xFC_x13[BrExtIntrGrp]	3h	Map INT A/B/C/D to interrupt 12/13/14/15. Map bridge interrupt to interrupt 19.
	D0F0xFC_x13[BrExtIntrSwz]	0h	
	D0F0xFC_x13[BrIntIntrMap]	13h	

Table 41: Recommended Interrupt Routing and Swizzling Configuration

Device	Register	Setting	Description
Dev3Fn3	D0F0xFC_x14[BrExtIntrGrp]	4h	Map INT A/B/C/D to interrupt 16/17/18/19. Map bridge interrupt to interrupt 20.
	D0F0xFC_x14[BrExtIntrSwz]	0h	
	D0F0xFC_x14[BrIntIntrMap]	14h	
Dev3Fn4	D0F0xFC_x15[BrExtIntrGrp]	5h	Map INT A/B/C/D to interrupt 20/21/22/23. Map bridge interrupt to interrupt 21.
	D0F0xFC_x15[BrExtIntrSwz]	0h	
	D0F0xFC_x15[BrIntIntrMap]	15h	
Dev3Fn5	D0F0xFC_x16[BrExtIntrGrp]	6h	Map INT A/B/C/D to interrupt 24/25/26/27. Map bridge interrupt to interrupt 18.
	D0F0xFC_x16[BrExtIntrSwz]	0h	
	D0F0xFC_x16[BrIntIntrMap]	12h	
GBIF	D0F0xFC_x0F[GBIFExtIntrGrp]	0h	Map INT A/B/C/D to interrupt 2/3/0/1.
	D0F0xFC_x0F[GBIFExtIntrSwz]	2h	

2.11.3 Links

2.11.3.1 Overview

There are 3 PCIe cores: one 2 x16 core and two 5 x8 cores. There are 8 configurable ports, which can be divided into 2 groups:
- Gfx: Contains 2 x8 ports. Each port can be limited to lower link widths for applications that require fewer lanes. Additionally, the two ports can be combined to create a single x16 link.
- GPP: Contains 1 x4 UMI and 5 General Purpose Ports (GPP).

All PCIe links are capable of supporting Gen1/Gen2 data rates. In addition, the Gfx link is capable of supporting Gen3 data rate.

The FP3 package supports two different voltage levels on the VDDP rail. At the 1.05V nominal setting, the Gfx link can support Gen3 data rate, while at the 0.95V setting, the maximum data rate supported by the Gfx link is Gen2. See 2.9.2 for its effect on DDR3 data rate.

Gfx and GPP ports each have a Type 1 Virtual PCI-to-PCI bridge header in the PCI configuration space mapped to devices according to Figure 8.

Each PCIe and DDI lane is assigned a unique lane ID that software uses to communicate configuration information to the SMU.

2.11.3.2 Link Configurations

Lanes of the Gfx ports can be assigned to IO links or DDI links.
The following link configurations are supported for the Gfx links:

Table 42: Supported Gfx Port Configurations

Gfx Port Lanes			
3:0	7:4	11:8	15:12
x16 Link			

Table 42: Supported Gfx Port Configurations

Gfx Port Lanes			
3:0	7:4	11:8	15:12
x8 Link		x8 Link	
x8 Link		x4 Link	DDI
x8 Link		DDI	x4 Link
x8 Link		DDI	DDI
x8 Link		Dual-DVI	
unused	DDI	x4 Link	x4 Link
x4 Link	x4 Link	DDI	DDI
x4 Link	x4 Link	Dual-DVI	
x4 Link	DDI	x4 Link	DDI
x4 Link	DDI	DDI	x4 Link
x4 Link	DDI	DDI	DDI
x4 Link	DDI	Dual-DVI	
x4 Link	DDI	x8 Link	
Dual-DVI		x8 Link	
Dual-DVI		x4 Link	x4 Link
Dual-DVI		DDI	x4 Link
Dual-DVI		x4 Link	DDI
Dual-DVI		DDI	DDI
Dual-DVI		Dual-DVI	

To achieve the above configurations, program the following registers:
- Program Gfx function in D0F0xE4_x013[2:0]_0080[StrapBifLinkConfig].
- Program Gfx PIF 0 and Gfx PIF 1 in the following registers D0F0xE4_x0[210,11[3:0]]_0011.
- Program Gfx TX Lane Mux in the following registers D0F0xE4_x013[3:0]_802[4:1].
- Program Gfx RX Lane Mux in the following registers D0F0xE4_x013[3:0]_802[8:5].
- Program OwnSlice in the Gfx registers in D0F0xE4_x013[3:0]_804[3:0][OwnSlice].

The following DP0/DP1 DDI configurations are supported:

Table 43: Supported DP0/DP1 DDI Link Configurations

Lanes[3:0]	Lanes[7:4]
DDI	DDI
DDI (Dual-link DVI)	

The following link configurations are supported for the GPP links:

Table 44: Supported General Purpose (GPP) Link Configurations

D0F0xE4		GPP Port Lane							
x0130_0080	x0111_0011	0	1	2	3	4	5	6	7
0000_0001h	0000_0300h	x4 Link				x4 Link			
0000_0002h	0000_0203h	x2 Link		x2 Link		x4 Link			
0000_0003h	0000_0201h	x2 Link		x1 Link	x1 Link	x4 Link			
0000_0003h	0000_0202h	x1 Link	x1 Link	x2 Link		x4 Link			
0000_0004h	0000_0200h	x1 Link	x1 Link	x1 Link	x1 Link	x4 Link			
0000_0001h	0000_0300h	x4 Link				DDI			
0000_0002h	0000_0203h	x2 Link		x2 Link		DDI			
0000_0003h	0000_0201h	x2 Link		x1 Link	x1 Link	DDI			
0000_0003h	0000_0202h	x1 Link	x1 Link	x2 Link		DDI			
0000_0004h	0000_0200h	x1 Link	x1 Link	x1 Link	x1 Link	DDI			

2.11.4 Root Complex Configuration

2.11.4.1 LPC MMIO Requirements

To ensure proper operation of LPC generated DMA requests, the UMI must be configured to send processor generated MMIO writes that target the LPC bus to the FCH as non-posted writes. To ensure this requirement the MMIO address space of the LPC bus must not be included in the ranges specified by D18F1x[2CC:2A0,1CC:180,BC:80] [MMIO Base/Limit] and non-posted protocol for memory writes must be enabled using the following sequence before LPC DMA transactions are initiated.

1. Configure the FCH to use the non-posted write protocol. See the FCH register specification for configuration details.
2. Locate the PCIe core that has the UMI link (read D0F0x64_x1F to get location of the FCH).
3. Note that this step should only be performed for the PCIe core with the UMI link (found via step 2 above). Program D0F0xE4_x014[2:0]_0010[UmiNpMemWrite] = 1.
4. Program D0F0x98_x06[UmiNpMemWrEn] = 1.

2.11.4.2 Configuration for non-FCH Bridges

BIOS should program the following in non-FCH bridges:
1. Program D0F0xCC_x01_ib[21,1D:19,12:11][CrsEnable] = 1 for D0F0xC8[NbDevIndSel] = 11h-12h, 19h-1Dh.
2. Program D0F0xCC_x01_ib[21,1D:19,12:11][SetPowEn] = 1 for D0F0xC8[NbDevIndSel] = 11h-12h, 19h-1Dh.

2.11.4.3 Link Configuration and Initialization

Link configuration and initialization is performed by the following sequence:
1. 2.11.4.3.1 [Link Configuration and Core Initialization]
2. 2.11.4.3.2 [Link Training]
3. 2.11.4.5 [Link Power Management]
4. Lock link configuration registers.

- Program D0F0xE4_x014[2:0]_0010[HwInitWrLock] = 1.
- Program D0F0x64_x00[HwInitWrLock] = 1.

5. IF(an external FCH connected through UMI using D0F0xC8[NbDevIndSel]) THEN program D0F0xCC_x01_ib[21,1D:19,12:11][CfgDis] = 1.

2.11.4.3.1 Link Configuration and Core Initialization

Link configuration is done on a per link basis. Lane reversal, IO link/DDI link selection, and lane enablement is configured through this sequence.

1. Place software-reset module into blocking mode:
   A. Program D0F0xE4_x013[3:0]_8062[ConfigXferMode]=0.
   B. Program D0F0xE4_x013[3:0]_8062[BlockOnIdle]=0.
2. If the link is an IO link, Program D0F0xE4_x014[2:0]_0011[DynClkLatency]=Fh.
3. Program D0F0xE4_x013[2:0]_0080 per Table 44.
4. Program D0F0xE4_x013[3:0]_802[4:1] per Table 44.
5. Program D0F0xE4_x0[210,11[3:0]]_0010[RxDetectTxPwrMode]=1.
6. Program D0F0xE4_x0[210,11[3:0]]_0010[Ls2ExitTime]=000b.
7. Program D0F0xE4_x013[3:0]_8013[MasterPciePllA, MasterPciePllB, MasterPciePllC, MasterPciePllD] per Table 44.
8. Initiate core reconfiguration sequence:
   A. Program D0F0xE4_x013[3:0]_8062[ReconfigureEn]=1.
   B. Program D0F0xE4_x013[3:0]_8060[Reconfigure]=1.
   C. Wait for D0F0xE4_x013[3:0]_8060[Reconfigure]==0.
   D. Program D0F0xE4_x013[3:0]_8062[ReconfigureEn]=0.
9. Return software-reset module to non-blocking mode:
   A. Program D0F0xE4_x013[3:0]_8062[ConfigXferMode]=1.
10. Program D[4:2]F[5:1]xE4_xC1[StrapReverseLanes] if necessary.
11. Program D0F0xE4_x0[210,11[3:0]]_0011 per Table 44Table 101.
12. Program D0F0xE4_x0[220,123:120]_[F:E][7:0][8,0]6 per Table 91.
13. For each link mapped to DDI:
   A. Program D0F0xE4_x0[210,11[3:0]]_001[8:7,3:2][PllPowerStateInTxs2]=111b.
   B. Program D0F0xE4_x0[210,11[3:0]]_001[8:7,3:2][PllPowerStateInOff]=111b.
   C. Program D0F0xE4_x0[210,11[3:0]]_001[8:7,3:2][PllRampUpTime]=010b.
14. For each nibble that has no PCIe lanes in use:
   A. Program D0F0xE4_x0[210,11[3:0]]_001[8:7,3:2][PllPowerStateInOff]=111b.
   B. Program D0F0xE4_x0[210,11[3:0]]_001[8:7,3:2][PllPowerStateInTxs2]=111b.
   C. Program D0F0xE4_x0[210,11[3:0]]_001[8:7,3:2][TxPowerStateInTxs2]=111b.
   D. Program D0F0xE4_x0[210,11[3:0]]_001[8:7,3:2][RxPowerStateInRxs2]=111b.
15. For each lane that is not in use, program the corresponding D0F0xE4_x013[3:0]_8029[LaneEnable]=0.
16. If the link is a DDI link:
   A. Program D0F0xE4_x013[3:0]_804[3:0][OwnSlice] per Table 42.
17. Configure PIF parings and disable ganged mode for UMI:
   A. Program D0F0xE4_x0110_0011=0000_0300h.
   B. Program D0F0xE4_x0120_6[3:2][8,0]5[GangedModeEn]=0.

2.11.4.3.2 Link Training

Link training is performed on a per link basis. BIOS may train the links in parallel.

2.11.4.4 Miscellaneous Features

2.11.4.4.1 Lane Reversal

Normally, the lanes of each port are physically numbered from n-1 to 0 where n is the number of lanes assigned to the port. Physical lane numbering can be reversed according to the following methods:

- To reverse the physical lane numbering for a specific port, program D[4:2]F[5:1]xE4_xC1[StrapReverseLanes]=1.
- To reverse the physical lane numbering for all ports in the GPP or GFX interfaces, program D0F0xE4_x014[2:0]_00C0[StrapReverseAll]=1.

Note that logical port numbering is established during link training regardless of the physical lane numbering.

2.11.4.4.2 Link Speed Changes

Link speed changes can only occur on Gen2 and Gen2/Gen3 capable links. To verify that Gen2/Gen3 speeds are supported verify D[4:2]F[5:1]x64[LinkSpeed]==02h or D[4:2]F[5:1]x64[LinkSpeed]==03h. Note that Gen3 support is only for the graphics link.

2.11.4.4.2.1 Autonomous Link Speed Changes

To enable autonomous speed changes on a per port basis:

1. Program D[4:2]F[5:1]x88[TargetLinkSpeed]=2h.
2. Program D0F0xE4_x013[2:0]_0[C:8]03[StrapBifDeemphasisSel]=1.
3. Program D[4:2]F[5:1]xE4_xA4[LcGen2EnStrap]=1.
4. Program D[4:2]F[5:1]xE4_xC0[StrapAutoRcSpeedNegotiationDis]=0.
5. Program D[4:2]F[5:1]xE4_xA4[LcMultUpstreamAutoSpdChngEn]=1.
6. Program D[4:2]F[5:1]xE4_xA2[LcUpconfigureDis]=0.

To enable autonomous speed changes on a per port basis for Gen3:

1. Program D[4:2]F[5:1]x88[TargetLinkSpeed]=3h.
2. Program D[4:2]F[5:1]xE4_xA4[LcGen3EnStrap]=1.
3. Program D[4:2]F[5:1]xE4_xC0[StrapAutoRcSpeedNegotiationDis]=0.

2.11.4.4.3 Deemphasis

Deemphasis strength can be changed on a per-port basis by programming D[4:2]F[5:1]xE4_xB5[LcSelectDeemphasis].

2.11.4.5 Link Power Management

2.11.4.5.1 Link States

To enable support for L1 program D[4:2]F[5:1]xE4_xA0[LcL1Inactivity]=6h.

To enable support for L0s:

- Program D[4:2]F[5:1]xE4_xA1[LcDontGotoL0sifL1Armed]=1.
- Program D[4:2]F[5:1]xE4_xA0[LcL0sInactivity]=9h.

2.11.4.5.2 Dynamic Link-width Control

Dynamic link-width control is a power saving feature that reconfigures the link to run with fewer lanes. The inactive lanes are turned off to conserve power.

Each link can switch among widths of: x1, x2, x4, x8, and x16, up to the maximum port width.

The link width is controlled by the following mechanism:
- Up/Down Reconfiguration: The link is retrained according to the PCI Express® specification.

The core has the capability to turn off the inactive lanes of trained links. To enable this feature program D[4:2]F[5:1]xE4_xA2[LcDynLanesPwrState]=11b.

2.11.4.6 Link Test and Debug Features

2.11.4.6.1 Compliance Mode

To enable Gen1 software compliance mode program D[4:2]F[5:1]xE4_xC0[StrapForceCompliance]=1 for each port to be placed in compliance mode.

To enable Gen2 software compliance mode:
1. BIOS enables Gen2 capability by programming D0F0xE4_x014[2:0]_00C1[StrapGen2Compliance]=1.
2. Program D[4:2]F[5:1]xE4_xA4[LcGen2EnStrap]=1.
3. Program D[4:2]F[5:1]x88[TargetLinkSpeed]=2h for each port to be placed in compliance mode.
4. Program D[4:2]F[5:1]x88[EnterCompliance]=1 for each port to be placed in compliance mode.

To enable Gen3 software compliance mode:
1. BIOS enables Gen3 capability on the Gfx link by programming D0F0xE4_x0140_00C1[StrapGen3Compliance]=1.
2. Program D[4:2]F[5:1]xE4_xA4[LcGen3EnStrap]=1.
3. Program D[4:2]F[5:1]x88[TargetLinkSpeed]=3h for each port to be placed in compliance mode.
4. Program D[4:2]F[5:1]x88[EnterCompliance]=1 for each port to be placed in compliance mode.

2.11.5 FCH Messages

To replace the wires and messages previously used between the processor and the FCH, upstream and downstream messages are defined through a combination of messages and reads or posted writes of special addresses. These message packets look like regular PCIe packets, but are AMD proprietary packets across the UMI link.

2.11.6 BIOS Timer

The root complex implements a 32-bit microsecond timer (see D0F0xE4_x0132_80F0 and D0F0xE4_x0132_80F1) that the BIOS can use to accurately time wait operations between initialization steps.

To ensure that BIOS waits a minimum number of microseconds between steps BIOS should always wait for one microsecond more than the required minimum wait time.

2.11.7 PCIe Client Interface Control

This interface is accessed through the indexed space registers located at D0F2xF8 within the Device 0 Function 2 (IOMMU) Configuration Registers.

BIOS should perform the following steps to initialize the interface:

1. Program D0F0x64_x0D[PciDev0Fn2RegEn] = 1h.
2. Program credits for the BIF client as follows:
   A. Program D0F2xFC_x32_L1i[3][DmaNpHaltDis] = 1h.
   B. Program D0F2xFC_x32_L1i[3][DmaBufCredits] = 20h.
   C. Program D0F2xFC_x32_L1i[3][DmaBufMaxNpCred] = 20h.
3. Program credits for the PGD client as follows:
   A. Program D0F2xFC_x32_L1i[0][DmaBufCredits] = 20h.
   B. Program D0F2xFC_x32_L1i[0][DmaBufMaxNpCred] = 1Fh.
4. Program credits for the INTGEN client as follows:
   A. Program D0F2xFC_x32_L1i[4][DmaNpHaltDis] = 1h.
   B. Program D0F2xFC_x32_L1i[4][DmaBufCredits] = 4h.
   C. Program D0F2xFC_x32_L1i[4][DmaBufMaxNpCred] = 4h.
5. Program clock gating as follows:
   A. Program D0F2xFC_x33_L1i[4:0][L1DmaClkgateEn] = 1h.
   B. Program D0F2xFC_x33_L1i[4:0][L1CacheClkgateEn] = 1h.
   C. Program D0F2xFC_x33_L1i[4:0][L1CpslvClkgateEn] = 1h.
   D. Program D0F2xFC_x33_L1i[4:0][L1DmaInputClkgateEn] = 1h.
   E. Program D0F2xFC_x33_L1i[4:0][L1PerfClkgateEn] = 1h.
   F. Program D0F2xFC_x33_L1i[4:0][L1MemoryClkgateEn] = 1h.
   G. Program D0F2xFC_x33_L1i[4:0][L1RegClkgateEn] = 1h.
   H. Program D0F2xFC_x33_L1i[4:0][L1HostreqClkgateEn] = 1h.
   I. Program D0F2xFC_x33_L1i[4:0][L1L2ClkgateEn] = 1h.
   J. Program D0F2xF4_x33[CKGateL2ARegsDisable] = 0h.
   K. Program D0F2xF4_x33[CKGateL2ADynamicDisable] = 0h.
   L. Program D0F2xF4_x33[CKGateL2ACacheDisable] = 0h.
   M. Program D0F2xF4_x90[CKGateL2BRegsDisable] = 0h.
   N. Program D0F2xF4_x90[CKGateL2BDynamicDisable] = 0h.
   O. Program D0F2xF4_x90[CKGateL2BMiscDisable] = 0h.
6. Program D0F0x64_x0D[PciDev0Fn2RegEn] = 0h.

2.12 IOMMU

The processor includes an IOMMU revision 2. See the *AMD I/O Virtualization Technology™ (IOMMU) Specification*.

2.12.1 IOMMU Configuration Space

The IOMMU configuration space consists of the following four groups:

- PCI Configuration space. See 3.4 [Device 0 Function 2 (IOMMU) Configuration Registers].
- IOMMU Memory Mapped Register space. See 3.16 [IOMMU Memory Mapped Registers].
- IOMMU L1 Indexed space accessed through D0F2xF8 [IOMMU L1 Config Index].
- IOMMU L2 Indexed space accessed through D0F2xF0 [IOMMU L2 Config Index].

2.12.2 IOMMU Initialization

BIOS should perform the following steps to initialize the IOMMU:

1. Program D0F0x64_x0D[PciDev0Fn2RegEn] = 1h.
2. Program D0F2x44 [IOMMU Base Address Low] and D0F2x48 [IOMMU Base Address High] to allocate a 512K region of MMIO space for IOMMU memory mapped registers. This region of MMIO space is reserved for IOMMU and BIOS must not allocate it for use by system software.
3. Program D0F2x50[IommuHtAtsResv] = 0h.
4. Program D0F2x44[IommuEnable]=1h.
5. Program D0F2x70[PrefSupW]=0.
6. Program D[4:2]F[5:1]xE4_xC1[StrapExtendedFmtSupported]=1 and D[4:2]F[5:1]xE4_xC1[StrapE2EPrefixEn]=1.
7. Program IOMMUx18[Isoc]=1h if processors support isochronous channel.
8. Program the registers with BIOS recommendations in L1 (D0F2xFC) and L2 (D0F2xF4) indexed space. See 2.11.7 [PCIe Client Interface Control].
9. Check if any PCIe devices in the system support the Phantom Function. For each PCIe core that has a connected device advertising support for the Phantom Function, program D0F2xFC_x07_L1i[4:0][0]=0 for the L1 corresponding to that PCIe core.
10. If a PCIe port is hot-plug capable, then program D0F2xFC_x07_L1i[4:0][0]=0 for the L1 corresponding to the PCIe core.
11. If at least one PCIe to PCI-x bridge exists on a PCIe port or a HotPlug capable PCIe slot is present on a PCIe port then program D0F2xFC_x0D_L1i[4:0][VOQPortBits]=111b for the L1 corresponding to the particular PCIe core.
12. Program the location of the SBinto D0F2xF4_x49 [L2_SB_LOCATION]. The program value is required to match the value programmed in D0F0x64_x1F [FCH Location].
13. Program the location of the SB into D0F2xFC_x09_L1i[4:0] [L1_SB_LOCATION] for the L1 corresponding to the iFCH or the PCIe core which FCH is located. The program value is required to match the value programmed in D0F0x64_x1F [FCH Location]. Leave register at default value for all L1s corresponding to other PCIe cores.

2.12.2.1 IOMMU L1 Initialization

BIOS should perform the following steps to initialize the IOMMU L1:

1. Program D0F2xFC_x0C_L1i[4:0][L1VirtOrderQueues]=4h.
2. Program D0F2xFC_x32_L1i[4:0][AtsMultipleRespEn]=1h.
3. Program D0F2xFC_x32_L1i[4:0][AtsMultipleL1toL2En]=1h.

4. Program D0F2xFC_x32_L1i[4:0][TimeoutPulseExtEn]=1h.
5. Program D0F2xFC_x07_L1i[4:0][AtsPhysPageOverlapDis]=1h.
6. Program D0F2xFC_x07_L1i[4:0][AtsSeqNumEn]=1h.
7. Program D0F2xFC_x07_L1i[4:0][SpecReqFilterEn]=1h.
8. Program D0F2xFC_x07_L1i[4:0][L1NwEn]=1h.

2.12.2.2 IOMMU L2 Initialization

BIOS should perform the following steps to initialize the IOMMU L2:

1. Program D0F2xF4_x10[DTCInvalidationSel]=2h.
2. Program D0F2xF4_x14[ITCInvalidationSel]=2h.
3. Program D0F2xF4_x18[PTCAInvalidationSel]=2h.
4. Program D0F2xF4_x50[PDCInvalidationSel]=2h.
5. Program D0F2xF4_x80[ERRRuleLock0]=1h.
6. Program D0F2xF4_x30[ERRRuleLock1]=1h.
7. Program D0F2xF4_x34[L2aregHostPgsize]=2h.
8. Program D0F2xF4_x34[L2aregGstPgsize]=2h.
9. Program D0F2xF4_x94[L2bregHostPgsize]=2h.
10. Program D0F2xF4_x94[L2bregGstPgsize]=2h.
11. Program D0F2xF4_x4C[GstPartialPtcCntrl]=3h.
12. If no internal gfx, program D0F2xF4_x57[L1ImuIntGfxDis]=1h.
13. If no external gfx, program D0F2xF4_x57[0]=1h.
14. Program D0F2xF4_x47[TwAtomicFilterEn]=1h.
15. Program D0F2xF4_x47[TwNwEn]=1h.
16. Program D0F2xF4_x56[CPFlushOnWait]=1h.
17. Program D0F2xF4_x56[CPFlushOnInv]=0h.
18. Program D0F2xF4_x53[L2bUpdateFilterBypass]=0h.
19. Program D0F2xF4_x22[L2aUpdateFilterBypass]=0h.

2.12.2.3 IOMMU SMI Filtering

In order to ensure system management interrupts come from valid peripheral sources, the IOMMU supports an SMI filter (IOMMUx30[SmiFSup]==01b). SMI interrupts are filtered according to the values programmed in the SMI filter registers. The registers specify what sources are allowed to send SMI interrupts. IOMMUx30[SmiFRC] indicates the number of SMI filter registers available.

The BIOS should set up the SMI filter registers and lock them. These setting will take effect when system software enables the IOMMU and enables SMI filtering. BIOS should perform the following steps to set up SMI filtering:

1. Program D0F2x70[SmifSupW]=1h.
2. Choose an SMI filter register from the available set described in IOMMUx30[SmiFRC]. Select one register for each SMI source.
3. Program selected SMI filter register to the Device ID of the peripheral issuing the SMI interrupts via IOMMUx[78,70,68,60][SMIDid]. Program one register for each SMI source.
4. Program selected SMI filter register to be valid viaIOMMUx[78,70,68,60][SMIDV]. Program one register for each SMI source.
5. Program selected SMI filter register to be locked via IOMMUx[78,70,68,60][SMIFlock]. Program one register for each SMI source.

2.13 System Management Unit (SMU)

The system management unit (SMU) is a subcomponent of the northbridge that is responsible for a variety of system and power management tasks during boot and runtime. The SMU contains a microcontroller to assist with many of these tasks.

2.13.1 Software Interrupts

The microcontroller can be interrupted to cause it to perform several initialization and runtime tasks. BIOS and ACPI methods can interrupt the SMU to request a specific action using the following sequence:

1. If a service request requires an argument, program D0F0xBC_xC210_003C[Argument] with the desired argument.
1. Wait for D0F0xBC_xC210_0004[IntDone]==1.
2. Program D0F0xBC_xC210_0000[ServiceIndex] to the desired service index and toggle. This may be done in a single write.
3. Wait for D0F0xBC_xC210_0004[IntAck]==1.

After performing the steps above, software may continue execution before the interrupt has been serviced. However, software should not rely on the results of the interrupt until the service is complete (see D0F0xBC_xC210_0004[IntDone]). Interrupting the SMU with a service index that does not exist results in undefined behavior.

Table 45: SMU Software Interrupts

Service Index	Notes
1Eh	Description: **BIOSSMC_MSG_LCLK_DPM_ENABLE**. Enables LCLK DPM. See 2.5.6.1.3 [LCLK DPM].
	Input: D0F0xBC_x3FDC8
	Output: None.
3Ah	Description: **BIOSSMC_MSG_VDDNB_REQUEST**. Request VDDNB voltage.
	Input:Program argument to desired voltage (encoded in mV with two fraction bits). Values outside D18F5x17C[MaxVid, MinVid] range are invalid and result in undefined behavior. • D0F0xBC_xC210_003C[Argument] = (Desired Voltage in mV) * 4.
	Output: None.
43h	Description: **BIOSSMC_MSG_NBDPM_Enable**. Enables NB P-state Adjustments. See 2.5.4.1.1 [Northbridge Dynamic Power Management (NB DPM)].
	Input: D0F0xBC_x3F9E8
	Output: D0F0xBC_x3F9EC

2.14 Graphics Processor (GPU)

The APU contains an integrated DX11 compliant graphics processor.

2.14.1 Graphics Memory Controller (GMC)

The graphics memory controller is responsible for servicing memory requests from the different blocks within

the GPU and forwarding routing them to the appropriate interface. The GMC is also responsible for translating GPU virtual address to GPU physical addresses and for translating GPU physical addresses to system addresses.

2.14.2 Frame Buffer (FB)

The frame buffer is defined as the portion of system memory dedicated for reading and writing of display information.

Table 46: Recommended Frame Buffer Configurations

System Memory Size	Frame Buffer Size
< 2 GB	256 MB
>= 2 GB & < 4 GB	256 MB
>= 4 GB & < 6 GB	512 MB
>= 6 GB	1 GB

2.15 RAS Features

2.15.1 Machine Check Architecture

The processor contains logic and registers to detect, log, and correct errors in the data or control paths in each core and the Northbridge. The Machine Check Architecture (MCA) defines the facilities by which processor and system hardware errors are logged and reported to system software. This allows system software to perform a strategic role in recovery from and diagnosis of hardware errors.

Refer to the AMD64 Architecture Programmer's Manual for an architectural overview and methods for determining the processor's level of MCA support. See 1.2 [Reference Documents].

The ability of hardware to generate a machine check exception upon an error is indicated by CPUID Fn0000_0001_EDX[MCE] or CPUID Fn8000_0001_EDX[MCE].

2.15.1.1 Machine Check Registers

CPUID Fn0000_0001_EDX[MCA] or CPUID Fn8000_0001_EDX[MCA] indicates the presence of the following machine check registers:

- MSR0000_0179 [Global Machine Check Capabilities (MCG_CAP)]
  - Reports how many machine check register banks are supported.
- MSR0000_017A [Global Machine Check Status (MCG_STAT)]
  - Provides basic information about processor state after the occurence of a machine check error.
- MSR0000_017B [Global Machine Check Exception Reporting Control (MCG_CTL)]
  - Used by software to enable or disable the logging and reporting of machine check errors in the error-reporting banks.

The error-reporting machine check register banks supported in this processor are:

- MC0: Load-store unit (LS), including data cache.
- MC1: Instruction fetch unit (IF), including instruction cache.
- MC2: Combined unit (CU), including L2 cache.
- MC3: Reserved.
- MC4: Northbridge (NB), including the IO link. There is only one NB error reporting bank, independent of the number of cores.
- MC5: execution unit (EX), including mapper/scheduler/retire/execute functions and fixed-issue reorder buffer.
- MC6: Floating point unit (FP).

- The register types within each bank are:
  - MCi_CTL, Machine Check Control: Enables error reporting via machine check exception. The MC*i*_CTL register in each bank must be enabled by the corresponding enable bit in MCG_CTL (MSR0000_017B).
  - MCi_STATUS, Machine Check Status: Logs information associated with errors.
  - MCi_ADDR, Machine Check Address: Logs address information associated with errors.
  - MCi_MISC, Machine Check Miscellaneous: Log miscellaneous information associated with errors, as defined by each error type.
  - MCi_CTL_MASK, Machine Check Control Mask: Inhibit detection of an error source unless otherwise specified.

The following table identifies the registers associated with each error-reporting machine check register bank:

Table 47: MCA register cross-reference table

Register Bank (MC*i*)	MCA Register				
	CTL	STATUS	ADDR	MISC	CTL_MASK
MC0	MSR0000_0400	MSR0000_0401	MSR0000_0402	MSR0000_0403	MSRC001_0044
MC1	MSR0000_0404	MSR0000_0405	MSR0000_0406	MSR0000_0407	MSRC001_0045
MC2	MSR0000_0408	MSR0000_0409	MSR0000_040A	MSR0000_040B	MSRC001_0046
MC3	MSR0000_040C	MSR0000_040D	MSR0000_040E	MSR0000_040F	MSRC001_0047
MC4	MSR0000_0410	MSR0000_0411	MSR0000_0412	MSR0000_0413	MSRC001_0048
MC5	MSR0000_0414	MSR0000_0415	MSR0000_0416	MSR0000_0417	MSRC001_0049
MC6	MSR0000_0418	MSR0000_0419	MSR0000_041A	MSR0000_041B	MSRC001_004A

Corrected, deferred, and uncorrected errors are logged in MCi_STATUS and MCi_ADDR as they occur. Uncorrected errors that are enabled in MCi_CTL result in a Machine Check exception.

Each MCi_CTL register must be enabled by the corresponding enable bit in MSR0000_017B [Global Machine Check Exception Reporting Control (MCG_CTL)].

MCi_CTL_MASK allow BIOS to mask the presence of any error source from software for test and debug. When error sources are masked, it is as if theerror was not detected. Such masking consequently prevents error responses and actions.

Each MCA bank implements a number of machine check miscellaneous registers, denoted as MCi_MISCj, where j goes from 0 to a maximum of 8. If there is more than one MCi_MISC register in a given bank, a non-zero value in MCi_MISC0[BlkPtr] points to the contiguous block of additional registers.

The presence of valid information in the first MISC register in the bank (MC*i*_MISC0) is indicated by MC*i*_STATUS[MiscV]. The presence of valid information in additional implemented MISC registers is indicated by MC*i*_MISC*j*[Val] in the target register.

2.15.1.2 Machine Check Errors

The classes of machine check errors are, in priority order from highest to lowest:

- Uncorrected
- Deferred
- Corrected

Uncorrected errors cannot be corrected by hardware and may cause loss of data, corruption of processor state, or both. Uncorrected errors update the status and address registers if not masked from logging in MCi_CTL_MASK. Information in the status and address registers from a previously logged lower priority error is overwritten. Previously logged errors of the same priority are not overwritten. Uncorrected errors that are enabled in MCi_CTL result in reporting to software via machine check exceptions. If an uncorrected error is masked from logging, the erroris ignored by hardware (exceptions are noted in the register definitions). If an uncorrected error is disabled from reporting, containment of the error and logging/reporting of subsequent errors may be affected. Therefore, enable reporting of unmasked uncorrected errors for normal operation. Disable reporting of uncorrected errors only for debug purposes.

Deferred errors are errors that cannot be corrected by hardware, but do not cause an immediate interruption in program flow, loss of data integrity, or corruption of processor state. These errors indicate that data has been corrupted but not consumed; no exception is generated because the data has not been referenced by a core or an IO link. Hardware writes information to the status and address registers in the corresponding bank that identifies the source of the error if deferred errors are enabled for logging. If there is information in the status and address registers from a previously logged lower priority error, it is overwritten. Previously logged errors of the same or higher priority are not overwritten. Deferred errors are not reported via machine check exceptions; they can be seen by polling the MCi_STATUS registers.

Corrected errors are those which have been corrected by hardware and cause no loss of data or corruption of processor state. Hardware writes the status and address registers in the corresponding register bank with information that identifies the source of the error if they are enabled for logging. Corrected errors are not reported via machine check exceptions. Some corrected errors may be reported to software via error thresholding (see 2.15.1.7 [Error Thresholding]).

The implications of these categories of errors are:

1. Uncorrected error; hardware did not deal with the problem.
   - Operationally (error handling), action required, because program flow is affected.
   - Diagnostically (fault management), software may collect information to determine if any components should be de-configured or serviced.
2. Deferred error; hardware partially dealt with the problem via containment.
   - Operationally, action optional, because program flow has not been affected. However, steps may be taken by software to prevent access to the data in error.
   - Diagnostically, software may collect information to determine if any components should be de-configured or serviced.
3. Corrected error; hardware dealt with the problem.
   - Operationally, no action required, because program flow is unaffected.
   - Diagnostically, software may collect information to determine if any components should be de-configured or serviced.

Machine check conditions can be simulated to aid in debugging machine check handlers. See 2.15.3 [Error Injection and Simulation] for more detail.

2.15.1.3 Error Detection, Action, Logging, and Reporting

Error detection is controlled by the MASK registers:
- Error detection for MCA controlled errors is enabled if not masked by MC*i*_CTL_MASK (see Table 47 [MCA register cross-reference table]).
- Error masking is performed regardless of MCA bank enablement in MCG_CTL (MSR0000_017B).

Error action refers to the hardware response to an error, aside from logging and reporting. Enablement of error action for each error is enumerated in the EAC (Error Action Condition) column of the error descriptions tables as follows:
- D: Detected. The error action is taken if the error is detected (i.e., not masked). These actions occur regardless of whether the MCA bank is enabled in MCG_CTL.
- E: Enabled. The error action is taken if the error is detected and the bank is enabled in MCG_CTL.

Error logging refers to the storing of information in the status registers, and is enabled if all of the following are true:
- Error detection is enabled.

- The MCA bank is enabled in MCG_CTL.

Error reporting refers to active notification of errors to software via machine check exceptions, and is enabled if all of the following are true:
- Error logging is enabled.
- The corresponding enable bit for the error in MC*i*_CTL is set to 1.

A machine check exception will be generated if all the following are true:
- The error is uncorrected.
- The error is enabled for reporting.
- CR4.MCE is enabled.

Notes:
1. If CR4.MCE is clear, an error configured to cause a machine check exception will cause a shutdown.
2. If error reporting is disabled, the setting of CR4.MCE has no effect.
3. If an uncorrected error is disabled from reporting, containment of the error and logging/reporting of subsequent errors may be affected. Therefore, unmasked uncorrected errors should be enabled for reporting for normal operation. Uncorrected errors should only be disabled from reporting for debug purposes.
4. Errors not associated with a specific core are reflected to core 0 of the compute unit. The error description tables identify which errors are associated or not associated with a specific core of the compute unit.

Throughout the MCA register descriptions, the terms “enabled” and “disabled” generally refer to reporting, and the terms “masked” and “unmasked” generally refer to logging, unless otherwise noted.

Some logged errors increment a counter in MCi_MISC, which may trigger an interrupt (see 2.15.1.7 [Error Thresholding]). Although no machine check exception will be generated, these notifications can be viewed as “correctable machine check interrupts”.

For debug observability only, D18F3x180[ConvertUnCorToCorErrEn] can be used to log NB uncorrected errors as corrected errors.

2.15.1.3.1 MCA conditions that cause Shutdown

The following architectural conditions cause the processor to enter the Shutdown state; see section “Machine-Check Errors” in APM volume 2 for more detail; see 1.2 [Reference Documents]:
- Attempting to generate an MCE when machine check reporting is disabled at the system level (CR4.MCE=0).
- Attempting to generate an MCE when a machine check is in progess on the same core (MSR0000_017A[MCIP]=1).

The following non-architectural conditions cause the processor to enter the Shutdown state:
- EX “Retire dispatch queue parity” error. See Table 241 [MC5 Error Descriptions].
- EX “Mapper checkpoint array parity” error if UC=1. See Table 241 [MC5 Error Descriptions].
- EX “Retire status queue parity” error. See: Table 241 [MC5 Error Descriptions].

2.15.1.3.2 Error Logging During Overflow

An error to be logged when the status register contains valid data can result in an overflow condition. During error overflow conditions, the new error may not be logged or an error which has already been logged in the status register may be overwritten. For the rules on error overflow, priority, and overwriting, see MSR0000_0401[Overflow].

Overflow alone does not indicate a shutdown condition. Uncorrected errors require software intervention. Therefore, when an uncorrected error cannot be logged, critical error information may have been lost, and MCi_STATUS[PCC] may be set. If PCC is indicated, software should terminate system processing to prevent data corruption (see 2.15.1.6 [Handling Machine Check Exceptions]). If PCC is not indicated, any MCA data lost due to overflow was informational only and not critical to system hardware operation.

The following table indicates which errors are overwritten in the error status registers.

Table 48: Overwrite Priorities for All Banks

			Older Error					
			Uncorrected		Deferred		Corrected	
			Enabled	Disabled	Enabled	Disabled	Enabled	Disabled
Newer Error	Uncorrected	Enabled	-	Overwrite	Overwrite	Overwrite	Overwrite	Overwrite
		Disabled	-	-	Overwrite	Overwrite	Overwrite	Overwrite
	Deferred	Enabled	-	-	-	Overwrite	Overwrite	Overwrite
		Disabled	-	-	-	-	Overwrite	Overwrite
	Corrected	Enabled	-	-	-	-	-	Overwrite
		Disabled	-	-	-	-	-	-

2.15.1.4 MCA Initialization

The following initialization sequence must be followed:

- MCi_CTL_MASK registers (see Table 47 [MCA register cross-reference table] for list):
  - BIOS must initialize the mask registers to inhibit error detection prior to the initialization of MCi_CTL and MSR0000_017B.
  - BIOS must not clear MASK bits that are reset to 1.
- The MCi_CTL registers must be initialized by the operating system prior to enabling the error reporting banks in MCG_CTL.

If initializing after a cold reset (see D18F0x6C[ColdRstDet]), then BIOS must clear the MCi_STATUS MSRs. If initializing after a warm reset, then BIOS should check for valid MCA errors and if present save the status for later diagnostic use (see 2.15.1.6 [Handling Machine Check Exceptions]).

BIOS may initialize the MCA without setting CR4.MCE; this will result in asystem shutdown on any machine check which would have caused a machine check exception (followed by a reboot if configured in the chipset). Alternatively, BIOS that wishes to ensure continued operation in the event that a machine check occurs during boot may write MCG_CTL with all ones and write zeros into each MCi_CTL. With these settings, a machine check error will result in MCi_STATUS being written without generating a machine check exception or a system shutdown. BIOS may then poll MCi_STATUS during critical sections of boot to ensure system integrity. Before passing control to the operating system, BIOS should restore the values of those registers to what the operating system is expecting. (Note that using MCi_CTL to disable error reporting on uncorrected errors may affect error containment; see 2.15.1.3 [Error Detection, Action, Logging, and Reporting].)

Before ECC memory has been initialized with valid ECC check bits, BIOS must ensure that no memory operations are initiated if MCA reporting is enabled. This includes memory operations that may be initiated by hardware prefetching or other speculative execution. It is recommended that, until all of memory has been initialized with valid ECC check bits, the BIOS either does not have any valid MTRRs specifying a DRAM memory type or does not enable DRAM ECC machine check exceptions.

2.15.1.5 Error Code

The MCi_STATUS[ErrorCode] field contains information used to identify the logged error. Table 49 [Error Code Types] identifies how to decode ErrorCode. The MCi_STATUS[ErrorCodeExt] field contains detailed, model-specific information that is used to further narrow identification for error diagnosis, but not error handling by software; see 2.15.1.6 [Handling Machine Check Exceptions].

For a given error-reporting bank, Error Code Type is used in conjunction with the Extended Error Code (MCi_STATUS[ErrorCodeExt]) to uniquely identify the Error Type; the value of ErrorCodeExt is unique within Error Code Type. Details for each Error Type are described in the tables accompanying the MCi_STATUS register for each bank.

- MC0 (LS); Table 223 [MC0 Error Signatures].
- MC1 (IF); Table 226 [MC1 Error Signatures].
- MC2 (CU); Table 230 [MC2 Error Signatures].
- MC4 (NB); Table 233 [MC4 Error Signatures, Part 1] and Table 234 [MC4 Error Signatures, Part 2].
- MC5 (EX); Table 242 [MC5 Error Signatures].
- MC6 (FP); Table 245 [MC6 Error Signatures].

Table 49: Error Code Types

Error Code	Error Code Type	Description
`0000 0000 0001 TTLL`	TLB	TT = Transaction Type LL = Cache Level
`0000 0001 RRRR TTLL`	Memory	Errors in the cache hierarchy (not in NB) RRRR = Memory Transaction Type TT = Transaction Type LL = Cache Level
`0000 1PPT RRRR IILL`	Bus	General bus errors including link and DRAM PP = Participation Processor T = Timeout RRRR = Memory Transaction Type II = Memory or IO LL = Cache Level
`0000 01UU 0000 0000`	Internal Unclassified	Internal unclassified errors UU = Internal Error Type

Table 50: Error codes: transaction type (TT)

TT	Transaction Type
00	Instr: Instruction
01	Data
10	Gen: Generic
11	Reserved

Table 51: Error codes: cache level (LL)

LL	Cache Level
00	Reserved
01	L1: Level 1

Table 51: Error codes: cache level (LL)

LL	Cache Level
10	L2: Level 2
11	LG: Generic

Table 52: Error codes: memory transaction type (RRRR)

RRRR	Memory Transaction Type
0000	Gen: Generic. Includes scrub errors.
0001	RD: Generic Read
0010	WR: Generic Write
0011	DRD: Data Read
0100	DWR: Data Write
0101	IRD: Instruction Fetch
0110	Prefetch
0111	Evict
1000	Snoop (Probe)

Table 53: Error codes: participation processor (PP)

PP	Participation Processor
00	SRC: Local node originated the request
01	RES: Local node responded to the request
10	OBS: Local node observed the error as a third party
11	Generic

Table 54: Error codes: memory or IO (II)

II	Memory or IO
00	Mem: Memory Access
01	Reserved
10	IO: IO Access
11	Gen: Generic

Table 55: Error codes: Internal Error Type (UU)

UU	Internal Error Type
00	Reserved
01	Reserved
10	HWA: Hardware Assertion
11	Reserved

2.15.1.6 Handling Machine Check Exceptions

A machine check handler is invoked to handle an exception for a particular core. Because MCA registers are generally not shared among cores, the handler does not need to coordinate register usage with handler instances

on other cores. Those few MCA registers which are shared are noted in the register description. (See also 2.4.2.1 [Registers Shared by Cores in a Compute Unit].)

For access to the NB MCA registers, D18F3x44[NbMcaToMstCpuEn] allows a single core (the NBC) to access the registers through MSR space without contention from other cores. This organization of registers on a per core basis allows independent execution, simplifies exception handling, and reduces the number of conditions which are globally fatal.

At a minimum, the machine check handler must be capable of logging error information for later examination. The handler should log as much information as is needed to diagnose the error.

More thorough exception handler implementations can analyze errors to determine if each error is recoverable by software. If a recoverable error is identified, the exception handler can attempt to correct the error and restart the interrupted program. An error may not be recoverable for the process or virtual machine it directly affects, but may be containable, so that other processes or virtual machines in the system are unaffected and system operation is recovered; see 2.15.1.6.1 [Differentiation Between System-Fatal and Process-Fatal Errors].

Machine check exception handlers that attempt to recover must be thorough in their analysis and the corrective actions they take. The following guidelines should be used when writing such a handler:

- Data collection:
  - All status registers in all error reporting banks must be examined to identify the cause of the machine check exception.
    - Read MSR0000_0179[Count] to determine the number of status registers visible to the core. The status registers are numbered from 0 to one less than the value found in MSR0000_0179[Count]. For example, if the Count field indicates five status registers are supported, they are numbered MC0_STATUS to MC4_STATUS. These are generically referred to as MC*i*_STATUS.
    - Check the valid bit in each status register (MC*i*_STATUS[Val]). The remainder of the status register should be examined only when its valid bit is set.
    - When identifying the error condition and determining how to handle the error, portable exception handlers should examine the following MC*i*_STATUS fields: ErrorCode, UC, PCC, CECC, UECC, Deferred, Poison. The expected settings of these and other fields in MC*i*_STATUS are identified in the error signatures tables which accompany the descriptions of each MCA status register. See 2.15.1.5 [Error Code] for a discussion of error codes and pointers to the error signatures tables.
      - MC*i*_STATUS[ErrorCodeExt] should generally not be used by portable code to identify the error condition because it is model specific. ErrorCodeExt is useful in determining the error subtype for root cause analysis.
    - Error handlers should collect all available MCA information (status register, address register, miscellaneous register, etc.), but should only interrogate details to the level which affects their actions. Lower level details may be useful for diagnosis and root cause analysis, but not for error handling.
- Recovery:
  - Check the valid MC*i*_STATUS registers to see if error recovery is possible.
    - Error recovery is not possible when theprocessor context corrupt indicator (MC*i*_STATUS[PCC]) is set to 1.
      - The error overflow status indicator (MCi_STATUS[Overflow]) does not indicate whether error recovery is possible. See 2.15.1.3.2 [Error Logging During Overflow].
    - If error recovery is not possible, the handler should log the error information and return to the operating system for system termination.
  - Check MC*i*_STATUS[UC] to see if the processor corrected the error. If UC is set, the processor did not correct the error, and the exception handler must correct the error prior to attempting to restart the interrupted program. If the handler cannot correct the error, it should log the error information and return to

the operating system. If the error affects only process data, it may be possible to terminate only the affected process or virtual machine. If the error affects processor state, continued use of that processor should not occur. See individual error descriptions for further guidance.
  - If MSR0000_017A[RIPV] is set, the interrupted program can be restarted reliably at the instruction pointer address pushed onto the exception handler stack if any uncorrected error has been corrected by software. If RIPV is clear, the interrupted program cannot be restarted reliably, although it may be possible to restart it for debugging purposes. As long as PCC is clear, it may be possible to terminate only the affected process or virtual machine.
  - When logging errors, particularly those that are not recoverable, check MSR0000_017A[EIPV] to see if the instruction pointer address pushed onto the exception handler stack is related to the machine check. If EIPV is clear, the address is not ensured to be related to the error.
  - See 2.15.1.6.1 [Differentiation Between System-Fatal and Process-Fatal Errors] for more explanation on the relationship between PCC, RIPV, and EIPV.
- Exit:
  - When an exception handler is able to successfully log an error condition, clear the MC*i*_STATUS registers prior to exiting the machine check handler. Software is responsible for clearing at least MC*i*_STATUS[Val].
  - Prior to exiting the machine check handler, be sure to clear MSR0000_017A[MCIP]. MCIP indicates that a machine check exception is in progress. If this bit is set when another machine check exception occurs in the same core, the processor enters the shutdown state.

Additional machine check handler portability can be added by having the handler use the CPUID instruction to identify the processor and its capabilities. Implementation specific software can be added to the machine check exception handler based on the processor information reported by CPUID.

In cases where sync flood is the recommended response to a particular error, a machine check exception cannot be used in lieu of the sync flood to stop the propagation of potentially bad data.

2.15.1.6.1 Differentiation Between System-Fatal and Process-Fatal Errors

The bits MC*i*_STATUS[PCC], MSR0000_017A[RIPV], and MSR0000_017A[EIPV] form a hierarchy, used by software to determine the degree of corruption and recoverability in the system.
Table 56 shows how these bits are interpreted.

Table 56: Error Scope Hierarchy

PCC	UC	RIPV	EIPV	Deferred	Poison	Comments
1	1	-	-	-	-	**System fatal error.** Signaled via machine check exception, action required. Error has corrupted system state (PCC=1). The error is fatal to the system and the system processing must be terminated.
0	1	1	1	-	-	

Table 56: Error Scope Hierarchy

PCC	UC	RIPV	EIPV	Deferred	Poison	Comments
0	1	0	-	-	0/1	**Hardware uncorrected, software containable error.** Signaled via machine check exception, action required. The error is confined to the process, however the process cannot be restarted even if the uncorrected error is corrected by software. Poison=1; the error is due to consumption of poison data. If the affected process or virtual machine is terminated, the system may continue operation.
0	0	-	-	1	0	**Deferred error**. Action optional. A latent error has been discovered, but not yet consumed; a machine check exception will be generated if the affected data is consumed. Error handling software may attempt to correct this data error, or prevent access by processes which map the data, or make the physical resource containing the data inaccessible. Note: May be detected on a demand access or a scrub access.
0	0	-	-	0	0	**Corrected error**. Signaled via error thresholding mechanisms (2.15.1.7 [Error Thresholding]); no action required.

2.15.1.7 Error Thresholding

For some types of errors, the hardware maintains counts of the number of errors. When the counter reaches a programmable threshold, an event may optionally be triggered to signal software. This is known as error thresholding. The primary purpose of error thresholding is to help software recognize an excessive rate of errors, which may indicate marginal or failing hardware. This information can be used to make decisions about deconfiguring hardware or scheduling service actions. Counts are incremented for corrected, deferred, and uncorrected errors.

The error thresholding hardware counts only the number of errors; it is up to software to track the errors reported over time in order to determine the rate of errors. Thresholding gives error counts on groups of resources. In order to make decisions on individual resources, a finer granularity of error information, such as MCA information for specific errors, must be utilized in order to obtain more accurate counts and to limit the scope of actions to affected hardware.

Thresholding is performed for “Error Threshold Groups” identified in the list below. For all error threshold groups, some number of corrected errors is expected and normal. There are numerous factors influencing error rates, including temperature, voltage, operating speed, and geographic location. In order to accommodate the various factors, including software latency to respond and track the error thresholding, additional guardband above the normal rates is recommended before error rates are considered abnormal for purposes of hardware action.

The {MC0, MC1, MC2, MC5} error thresholding banks maintains counters, but do not provide interrupts when the threshold is reached; these counters must be polled.

Error thresholding groups:
- MC0
  - MC0 errors are counted and polled via MSR0000_0403.
  - MC0 errors are listed in Table 222 [MC0 Error Descriptions].
- MC1
  - MC1 errors are counted and polled via MSR0000_0407.
  - MC1 errors are listed in Table 225 [MC1 Error Descriptions].
- MC2
  - MC2 errors are counted and polled via MSR0000_040B.
  - MC2 errors are listed in Table 229 [MC2 Error Descriptions].
- DRAM (MC4)
  - Memory errors are counted and polled or reported via MSR0000_0413.

DRAM errors are the errors listed in Table 233 [MC4 Error Signatures, Part 1] as "D" (DRAM) in the ETG (Error Threshold Group) column.
  - Operating systems can avoid or stop using memory pages with excessive errors.
- Links (MC4)
  - Link errors are counted and polled or reported via MSRC000_0408.
  - Link errors are the errors listed in Table 233 [MC4 Error Signatures, Part 1] as "L" (Cache) in the ETG (Error Threshold Group) column.
  - For a link exhibiting excessive errors, it may be possible to reduce errors by lowering the link frequency or reducing the link width (if a bad lane can be avoided). See 2.11 [Root Complex] for details and restrictions on configuring links.
- MC5
  - MC5 errors are counted and polled via MSR0000_0417.
  - MC5 errors are listed in Table 242 [MC5 Error Signatures].

In rare circumstances, such as two simultaneous errors in the same error thresholding group, it is possible for one error not to increment the counter. In these conditions, MCi_STATUS[Overflow] may indicate that an overflow occurred, but the error counter may only indicate one error.

2.15.1.8 Scrub Rate Considerations

This section gives guidelines for the scrub rate settings available in D18F3x58 [Scrub Rate Control]. Scrubbers are used to periodically read cacheline sized data locations and associated tags. There are two primary benefits to scrubbing. First, scrubbing corrects any corrected errors which are discovered before they can migrate into uncorrected errors. This is particularly important for soft errors, which are caused by external sources such as radiation and which are temporary conditions which do not indicate malfunctioning hardware. Second, scrubbers help identify marginal or failed hardware by finding and logging repeated errors at the same locations (see also 2.15.1.7 [Error Thresholding]).

There are many factors which influence scrub rates. Among these are:
- The size of memory or cache to be scrubbed
- Resistance to upsets
- Geographic location and altitude
- Alpha particle contribution of packaging
- Performance sensitivity
- Risk aversion

The baseline recommendations in Table 57 are intended to provide excellent protection at most geographic locations, while having no measurable effect on performance. Adjustments may be necessary due to special circumstances. Refer to JEDEC standards for guidelines on adjusting for geographic location.

Table 57: Recommended Scrub Rates per Node

Register	Memory Size per Node (GB)	Register Setting	Scrub Rate
D18F3x58[DramScrub]	0 GB == Size	00h	Disabled
	0 GB < Size <= 1 GB	12h	5.24 ms
	1 GB < Size <= 2 GB	11h	2.62 ms
	2 GB < Size <= 4 GB	10h	1.31 ms
	4 GB < Size <= 8 GB	0Fh	655.4 us
	8 GB < Size <= 16 GB	0Eh	327.7 us
	16 GB < Size <= 32 GB	0Dh	163.8 us
	32 GB < Size <= 64 GB	0Ch	81.9 us
	64 GB < Size <= 128 GB	0Bh	41.0 us
	128 GB < Size <= 256 GB	0Ah	20.5 us
	256 GB < Size	09h	10.2 us

For steady state operation, finding a range of useful scrub rates may be performed by selecting a scrub rate which is high enough to give good confidence about protection from accumulating errors and low enough that it has no measurable effect on performance. The above baselines are made to maximize error coverage without affecting performance and not based on specific processor soft error rates.

For low power states in which the processor core is halted, the power management configuration may affect scrubbing; see 2.8.3 [Memory Scrubbers].

2.15.1.9 Error Diagnosis

This section describes generalized information and algorithms for diagnosing errors. The primary goal of diagnosis is to identify the failing component for repair purposes. The secondary goal is to identify the smallest possible sub-component for deallocation, deconfiguration, or design/manufacturing root cause analysis.

Indictment means identifying the part in error. The simplest form of indictment is *self-indictment*, where the bank reporting the error is the faulty unit. The next simplest form of indictment is *eyewitness indictment*, where the faulty unit is not the bank reporting the error, but is identified unambiguously. Both of these forms can be considered direct indictment; the information for indictment is contained in the MCA error information. If an error is not directly indicted, then identifying the faulty unit is more difficult and may not be an explicit part of the error log.

In general, an address logged in the MCA is useful for direct indictment only if the address identifies a physical location in error, such as a cache index. Logical addresses, while identifying the data, do not identify the location of the data.

If possible, physical storage locations in caches should be checked to determine whether the error is a soft error (a temporary upset of the stored value) or a hard fault (malfunctioning hardware). A location which has had a soft error can be corrected by writing a new value to the location; a reread of the location should see the new value. Hard faults cannot be corrected by writing a new value; the hardware persistently returns the previous value. If such checking is not possible, a grossly simplifying assumption can be made that uncorrected errors are hard and corrected errors are soft. Repeated corrected errors from the same location are an indication that the fault is actually hard.

Determining whether corrected errors represent a hard fault or a soft error requires understanding the access

patterns and any attempts to correct the faulty data in place. An attempt to correct the data in place creates two *epochs*, one before the correction event, and one after. If an error is seen at the same location in two different epochs (especially back-to-back epochs), it is more likely that the cause is a hard fault, since the error has persisted or repeated through an in place correction. The more epochs in which an error is seen, the higher the likelihood of it being caused by a hard fault.

As an example, consider a corrected error found during a read from DRAM. If the DRAM redirect scrubber is enabled (D18F3x5C[ScrubReDirEn]), the data in error is corrected in place, and this event conceptually creates a new epoch. If the original fault was due to a soft error, a read of the same data in the new epoch should not encounter a data error. If the original fault was due to a hard fault (e.g., a stuck bit), a read of the data in the new epoch will likely result in another corrected or uncorrected error.

There are numerous correction events that can be used to separate time periods into epochs. These include DRAM redirect scrubs, DRAM sequential scrubs, cache scrubs, cache writes, cache flushes, resets, and others.

2.15.1.9.1 Common Diagnosis Information

A common set of diagnosis information is useful for many problems. Table 58 indicates the minimum set of generally useful diagnostic information that should be collected by software, unless the specifics of the problem are known to be narrower, based on the error code or other information.

It is useful to collect configuration information to ensure that the behavior is not caused by misconfiguration.

Table 58: Registers Commonly Used for Diagnosis

MCA Bank	Status	Configuration
MC0	MSR0000_0401 MSR0000_0402 MSR0000_0403	MSR0000_0400 MSRC001_1022 MSRC001_0044
MC1	MSR0000_0405 MSR0000_0406 MSR0000_0407	MSR0000_0404
MC2	MSR0000_0409 MSR0000_040A MSR0000_040B	MSR0000_0408 MSRC001_0046 MSRC001_1023
MC3	Reserved	Reserved

Table 58: Registers Commonly Used for Diagnosis

MCA Bank	Status	Configuration
MC4	MSR0000_0411 MSR0000_0412 MSR0000_0413 MSRC000_0408 D18F3x54 D18F2xAC	MSR0000_0410 MSRC001_0048 D18F3x40 D18F3x44 D18F3xE4 D18F3xE8 MSRC001_001F D18F3x180
MC5	MSR0000_0415 MSR0000_0416 MSR0000_0417	MSR0000_0414
MC6	MSR0000_0419 MSR0000_041A MSR0000_041B	MSR0000_0418 MSRC001_004A

If examining MCA registers after startup, determine the cause of the startup:
- INIT; D18F0x6C[InitDet].
- Cold reset; D18F0x6C[ColdRstDet].
- Warm reset; if not INIT or cold reset.

To see if a link failure occurred, examine D18F0x[E4,C4,A4,84][LinkFail]. If set, look for additional information:
- Receipt of a sync, such as during a sync flood, saves a status of Sync Error in MC4_STATUS.
- CRC error saves a status of CRC Error in MC4_STATUS. See D18F0x[E4,C4,A4,84][CrcErr,CrcFloodEn].
- Link not present does not save status in MC4_STATUS. See D18F0x[E4,C4,A4,84][InitComplete].

Other registers may be needed depending on the specific error symptoms.

2.15.1.10 Deferred Errors and Data Poisoning

Deferred errors indicate error conditions which could not be corrected, but which require no action (i.e., action optional). Data poisoning marks data which has encountered an uncorrectable error, so that it can be tracked until it is consumed or discarded. Together, data poisoning and deferred errors provide an infrastructure for reducing the severity of errors and the number of system outages for some classes of errors.

Processor cores create poison data and deferred errors as identified in the Error Signatures tables. When poison data or data with an uncorrectable ECC error is consumed, a machine check exception for an uncorrected error is signaled (MCi_STATUS[UC]). If the data is poison, MCi_STATUS[Poison] is also set. The NB converts any poison data sent from the core to a machine check exception with error type Compute Unit Data Error. To understand the cause of a machine check exception due to Compute Unit Data Error, examine the core MCA status registers for deferred errors.

The deferred error is logged in the MCA registers for diagnostic purposes at the time the error is discovered

and the data is poisoned. This deferred error can help identify the source of the error. The deferred error is logged independently of any associated poison data machine check. For example, it is possible for a cache eviction to result in a deferred error associated with the cache, and a corresponding machine check exception from the NB which receives the data.

2.15.2 DRAM ECC Considerations

DRAM is protected by an error correcting code (ECC). The DRAM error correcting code features an ECC word formed by a symbol based code. The x4 code uses thirty-six 4-bit symbols to make a 144-bit ECC word made up of 128 data bits and 16 check bits.

The x4 code is a single symbol correcting (SSC) and a double symbol detecting (DSD) code. This means the x4 code is able to correct 100% of single symbol errors (any bit error combination within one symbol), and detect 100% of double symbol errors (any bit error combination within two symbols).

Systems supporting ECC and non-ECC memory regions should use the non-ECC memory for the Frame Buffer only.

2.15.2.1 ECC Syndromes

For memory errors, the sections below describe how to find the DIMM in error. The process varies slightly according to the ECC code in use. To determine which ECC code is being used, see D18F3x180[EccSymbolSize].

For correctable errors, the DIMM in error is uniquely identified by the error address (MSR0000_0412[ErrAddr]) and the ECC syndrome (MSR0000_0411[Syndrome[15:8]] and MSR0000_0411[Syndrome[7:0]]). The error address maps to the two DIMMs composing the 128-bit line, and the ECC syndrome identifies one DIMM by identifying the symbol within the line.

2.15.2.1.1 x4 ECC

The use of x4 ECC is indicated in D18F3x180[EccSymbolSize].

The syndrome field uniquely identifies the failing bit positions of a correctable ECC error. Only syndromes identified by Table 59 are correctable by the error correcting code.

Symbols 00h-0Fh map to data bits [63:0]; symbols 10h-1Fh map to data bits [127:64]; symbols 20-21h map to ECC check bits for data bits [63:0]; symbols 22-23h map to ECC check bits for data bits [127:64].

To use Table 59, first find the 16-bit syndrome value in the table. This is performed by using low order 4 bits of the syndrome to select the appropriate error bitmask column. The entire four digit syndrome should then be in one of the rows of that column. The Symbol In Error row indicates which symbol, and therefore which DIMM has the error, and the column indicates which bits within the symbol.

For example, if the ECC syndrome is 6913h, then symbol 05h has the error, and bits [0] and [1] within that symbol are corrupted, since the syndrome is in column 3h (0011b). Symbol 05h maps to bits [23:20], so the corrupted bits are [20] and [21].

Table 59: x4 ECC Correctable Syndromes

Symbol In Error	Error Bitmask															
	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
Data 0	e821	7c32	9413	bb44	5365	c776	2f57	dd88	35a9	a1ba	499b	66cc	8eed	1afe	f2df
Data 1	5d31	a612	fb23	9584	c8b5	3396	6ea7	eac8	b7f9	4cda	11eb	7f4c	227d	d95e	846f
Data 2	0001	0002	0003	0004	0005	0006	0007	0008	0009	000a	000b	000c	000d	000e	000f
Data 3	2021	3032	1013	4044	6065	7076	5057	8088	a0a9	b0ba	909b	c0cc	e0ed	f0fe	d0df
Data 4	5041	a082	f0c3	9054	c015	30d6	6097	e0a8	b0e9	402a	106b	70fc	20bd	d07e	803f
Data 5	be21	d732	6913	2144	9f65	f676	4857	3288	8ca9	e5ba	5b9b	13cc	aded	c4fe	7adf
Data 6	4951	8ea2	c7f3	5394	1ac5	dd36	9467	a1e8	e8b9	2f4a	661b	f27c	bb2d	7cde	358f
Data 7	74e1	9872	ec93	d6b4	a255	4ec6	3a27	6bd8	1f39	f3aa	874b	bd6c	c98d	251e	51ff
Data 8	15c1	2a42	3f83	cef4	db35	e4b6	f177	4758	5299	6d1a	78db	89ac	9c6d	a3ee	b62f
Data 9	3d01	1602	2b03	8504	b805	9306	ae07	ca08	f709	dc0a	e10b	4f0c	720d	590e	640f
Data 10	9801	ec02	7403	6b04	f305	8706	1f07	bd08	2509	510a	c90b	d60c	4e0d	3a0e	a20f
Data 11	d131	6212	b323	3884	e9b5	5a96	8ba7	1cc8	cdf9	7eda	afeb	244c	f57d	465e	976f
Data 12	e1d1	7262	93b3	b834	59e5	ca56	2b87	dc18	3dc9	ae7a	4fab	642c	85fd	164e	f79f
Data 13	6051	b0a2	d0f3	1094	70c5	a036	c067	20e8	40b9	904a	f01b	307c	502d	80de	e08f
Data 14	a4c1	f842	5c83	e6f4	4235	1eb6	ba77	7b58	df99	831a	27db	9dac	396d	65ee	c12f
Data 15	11c1	2242	3383	c8f4	d935	eab6	fb77	4c58	5d99	6e1a	7fdb	84ac	956d	a6ee	b72f
Data 16	45d1	8a62	cfb3	5e34	1be5	d456	9187	a718	e2c9	2d7a	68ab	f92c	bcfd	734e	369f
Data 17	63e1	b172	d293	14b4	7755	a5c6	c627	28d8	4b39	99aa	fa4b	3c6c	5f8d	8d1e	eeff
Data 18	b741	d982	6ec3	2254	9515	fbd6	4c97	33a8	84e9	ea2a	5d6b	11fc	a6bd	c87e	7f3f
Data 19	dd41	6682	bbc3	3554	e815	53d6	8e97	1aa8	c7e9	7c2a	a16b	2ffc	f2bd	497e	943f
Data 20	2bd1	3d62	16b3	4f34	64e5	7256	5987	8518	aec9	b87a	93ab	ca2c	e1fd	f74e	dc9f
Data 21	83c1	c142	4283	a4f4	2735	65b6	e677	f858	7b99	391a	badb	5cac	df6d	9dee	1e2f
Data 22	8fd1	c562	4ab3	a934	26e5	6c56	e387	fe18	71c9	3b7a	b4ab	572c	d8fd	924e	1d9f
Data 23	4791	89e2	ce73	5264	15f5	db86	9c17	a3b8	e429	2a5a	6dcb	f1dc	b64d	783e	3faf
Data 24	5781	a9c2	fe43	92a4	c525	3b66	6ce7	e3f8	b479	4a3a	1dbb	715c	26dd	d89e	8f1f
Data 25	bf41	d582	6ac3	2954	9615	fcd6	4397	3ea8	81e9	eb2a	546b	17fc	a8bd	c27e	7d3f
Data 26	9391	e1e2	7273	6464	f7f5	8586	1617	b8b8	2b29	595a	cacb	dcdc	4f4d	3d3e	aeaf
Data 27	cce1	4472	8893	fdb4	3155	b9c6	7527	56d8	9a39	12aa	de4b	ab6c	678d	ef1e	23ff
Data 28	a761	f9b2	5ed3	e214	4575	1ba6	bcc7	7328	d449	8a9a	2dfb	913c	365d	688e	cfef
Data 29	ff61	55b2	aad3	7914	8675	2ca6	d3c7	9e28	6149	cb9a	34fb	e73c	185d	b28e	4def
Data 30	5451	a8a2	fcf3	9694	c2c5	3e36	6a67	ebe8	bfb9	434a	171b	7d7c	292d	d5de	818f
Data 31	6fc1	b542	da83	19f4	7635	acb6	c377	2e58	4199	9b1a	f4db	37ac	586d	82ee	ed2f
Check0	be01	d702	6903	2104	9f05	f606	4807	3208	8c09	e50a	5b0b	130c	ad0d	c40e	7a0f
Check1	4101	8202	c303	5804	1905	da06	9b07	ac08	ed09	2e0a	6f0b	f40c	b50d	760e	370f
Check2	c441	4882	8cc3	f654	3215	bed6	7a97	5ba8	9fe9	132a	d76b	adfc	69bd	e57e	213f

Table 59: x4 ECC Correctable Syndromes

Symbol In Error	Error Bitmask														
	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
Check3	7621	9b32	ed13	da44	ac65	4176	3757	6f88	19a9	f4ba	829b	b5cc	c3ed	2efe	58df

2.15.3 Error Injection and Simulation

Error injection allows the introduction of errors into the system for test and debug purposes. See the following sections for error injection details:

- DRAM: See 2.15.3.1 [DRAM Error Injection].
- Link:
  - D18F3x44[GenLinkSel, GenSubLinkSel, GenCrcErrByte1, GenCrcErrByte0].

Error simulation involves creating the appearance to software that an error occurred, and can be used to debug machine check interrupt handlers. This is performed by manually setting the MCA registers with desired values, and then driving the softwarevia INT18. SeeMSRC001_0015[McStatusWrEn] for making MCA registers writable for non-zero values. When McStatusWrEn is set, privileged software can write non-zero values to the specified registers without generating exceptions, and then simulate a machine check using the INT18 instruction (INT*n* instruction with an operand of 18). Setting a reserved bit in these registers does not generate an exception when this mode is enabled. However, setting a reserved bit may result in undefined behavior.

MCA Master Mode influences how error injection and error simulation are used. As described in D18F3x44[NbMcaToMstCpuEn], writes and reads of shared, non-core MCA registers can only be done from the NBC when MCA Master Mode is enabled. Injected errors to these banks, such as DRAM errors, drive exceptions at the NBC. Likewise, simulated errors must ensure that the exception or interrupt is handled on the NBC.

2.15.3.1 DRAM Error Injection

This section gives details and examples on injecting errors into DRAM using D18F3xBC_x8 [DRAM ECC]. The intent of DRAM error injection is to cause a discrepancy between the stored data and the stored ECC value. Therefore, DRAM error injection is only possible on DRAM which supports ECC, and in which D18F2x90_dct[3:0][DimmEccEn] and D18F3x44[DramEccEn] are set.
The memory subsystem operates on 64-byte cachelines. The following fields are used to set how the cacheline is to be corrupted in DRAM:

- D18F3xB8[ArrayAddress] selects a cacheline quadrant (16-byte section) of the cacheline. Each cacheline quadrant is protected by an ECC word. Note that there are special requirements for which bits are used to specify the target quadrant.
- D18F3xBC_x8[ErrInjEn] selects a 16-bit word of the cacheline quadrant selected in ArrayAddress. The 16-bit word identified as ECC[15:0] refers to the bits which store the ECC value; the other 16-bit words address the data on which the ECC is calculated. One or more of these 16-bit words can be selected, and the error bitmask indicated in EccVector is applied to each of the selected words.
- D18F3xBC_x8[EccVector] is a bitmask which selects the individual bits to be corrupted in the 16-bit words selected by ErrInjEn. When selecting the bits to be corrupted for correctable or uncorrectable errors, consider the ECC scheme being used, including symbol size; see 2.15.2 [DRAM ECC Considerations] for more details. Note that corrupting more than two symbols may exceed the limits of the ECC to detect the errors; for testing purposes it is recommended that no more than two symbols be corrupted in a single cacheline quadrant.

The distinction between D18F3xBC_x8[DramErrEn] and D18F3xBC_x8[EccWrReq] is that DramErrEn is used to continuously inject errors on every write. This bit is set and cleared by software. EccWrReq is used to inject an error on only one write. This bit is set by software and is cleared by hardware after the error is injected.

When performing DRAM error injection on multi-node systems, D18F3xB8 and D18F3xBC_x8 of the NB to which the memory is attached must be programmed.

The following can be used to trigger the injection:

- The memory address is not an explicit parameter of the error injection interface. Once the error injection registers D18F3xB8 and D18F3xBC are set, the next non-cached access of the appropriate type will trigger the mechanism and apply it to the accessed address. The access should be non-cached so that it is ensured to be seen by the memory controller. Possible methods to ensure a non-cached access include using the appropriate MTRR to set the memory type to UC or turning off caches. If it is important to know the address, then system activity must be quiesced so that the access can take place under careful software control. Once the error injection pattern is set in D18F3xB8 and D18F3xBC_x8:
  - Set either D18F3xBC_x8[EccWrReq] or D18F3xBC_x8[DramErrEn] to enable the triggering mechanism.
  - The next non-cached access of the appropriate type will trigger the mechanism and apply it to the accessed address.

After the error is injected, the data must be accessed in order for the error detection to be triggered. The error address logged in MSR0000_0412 corresponds to the cacheline quadrant that contains the error.

When using MSR0000_0411 to read MC4_STATUS after an error injection and subsequent error detection, be aware that the setting of D18F3x44[NbMcaToMstCpuEn] can cause different cores to see different values. Alternatively, MC4_STATUS can be read through the PCI-defined configuration space aliases D18F3x4C and D18F3x48, which do not return different values to different cores, regardless of the setting of D18F3x44[NbMcaToMstCpuEn].

Example 1: Injecting a correctable error:

- Program error pattern:
  - D18F3xB8[ArraySelect] = 1000b // select DRAM as target
  - D18F3xB8[ArrayAddress] = 000000000b // select 16-byte (128-bit) section
  - D18F3xBC_x8[ErrInjEn] = 000000001b // select 16-bit word in 16-byte section
  - D18F3xBC_x8[EccRdReq] = 0 // not a read request
  - D18F3xBC_x8[EccVector] = 0001h // set bitmask to inject error into only one symbol
- Program error trigger:
  - D18F3xBC_x8[DramErrEn] = 0 // inject only a single error
  - D18F3xBC_x8[EccWrReq] = 1 // a write request; enable injection on next write
- Clean up // if programmed for continuous errors
  - D18F3xBC_x8[DramErrEn] = 0 // inject only a single error

2.15.4 GIO RAS

The following register should be programmed to enable RAS features in the GIO.

- Program D0F0x98_x07[SyncFloodOnParityErr]=1

3 Registers

This section provides detailed field definitions for the core register sets in the processor.

3.1 Register Descriptions and Mnemonics

Each register in this document is referenced with a mnemonic. Each mnemonic is a concatenation of the register-space indicator and the offset of the register. Here are the mnemonics for the various register spaces:

- **IOXXX**: x86-defined input and output address space registers; XXX specifies the hexidecimal byte address of the IO instruction. This space includes IO-space configuration access registers IOCF8 [IO-Space Configuration Address] and IOCFC [IO-Space Configuration Data Port].
- **APICXX0**: APIC memory-mapped registers; XX0 is the hexidecimal byte address offset from the base address. See 2.4.9.1.2 [APIC Register Space].
- **CPUID FnXXXX_XXXX_EiX[_xYYY]**: processor capabilities information returned by the CPUID instruction. See 3.18 [CPUID Instruction Registers]. Each core may only access this information for itself.
- **MSRXXXX_XXXX**: MSRs; XXXX_XXXX is the hexidecimal MSR number. This space is accessed through x86-defined RDMSR and WRMSR instructions. Unless otherwise specified there is one set of these registers Per-core. See 2.4.1 [Compute Unit].
- **DXFYxZZZ**: PCI-defined configuration space; X specifies the hexadecimal device number (this may be 1or 2 digits), Y specifies the function number, and ZZZ specifies the hexidecimal byte address (this may be 2 or 3 digits); e.g., D18F3x40 specifies the register at device 18h, function 3, and address 40h. See 2.7 [Configuration Space], for details about configuration space.
  - Some register in D18F2xXXX have the _dct[3:0] mnemonic suffix. See 2.9.3 [DCT Configuration Registers].
- **IOMMUxX_XXXX**: IOMMU memory mapped registers; X_XXXX specifies the hexadecimal byte address offset (this may be 2 to 5 digits) from the base address register; The base address for this space is specified by D0F2x44 [IOMMU Base Address Low] and D0F2x48 [IOMMU Base Address High]. See 3.16 [IOMMU Memory Mapped Registers].
- **PMCxXXX**: core performance monitor events; XXX is the hexidecimal event counter number programmed into MSRC001_020[A,8,6,4,2,0][EventSelect]; See 2.6.1.1 [Core Performance Monitor Counters].
  - When PMCxXXX is followed by [z:y] then UnitMask[z:y] is being specified.
- **NBPMCxXXX**: NB performance monitor events; XXX is the hexadecimal event counter number programmed into MSRC001_024[6,4,2,0][EventSelect]; See 2.6.1.2 [NB Performance Monitor Counters].
  - When NBPMCxXXX is followed by [z:y] then UnitMask[z:y] is being specified.

Each mnemonic may specify the location of one or more registers that share the same base definition. A mnemonic that specifies more than one register will contain one or more ranges within braces. The ranges are specified as follows:

- Comma separated lists [A,B]: Define specific instances of a register, e.g., D0F3x[1,0]40 defines two registers D0F3x40 and D0F3x140.
- Colon separated ranges [A:B]: Defines all registers that contain the range between A and B. Examples:
  - D0F3x[50:40] defines five registers D0F3x40, D0F3x44, D0F3x48, D0F3x4C, and D0F3x50.
  - D[8:2]F0x40 defines seven registers D2F0x40, D3F0x40, D4F0x40, D5F0x40, D6F0x40, D7F0x40, and D8F0x40.
  - D0F0xE4_x013[2:0]_0000 defines three registers D0F0xE4_x0130_0000, D0F0xE4_x0131_0000, and D0F0xE4_x0132_0000.
- Colon separated ranges with a explicit step [A:BstepC]: Defines the registers from A to B, C defines the offset between registers., e.g., D0F3x[50:40:step8] defines three registers D0F3x40, D0F3x48, and D0F3x50.

The processor includes a single set of IO-space and configuration-space registers. However, APIC, CPUID, and MSR register spaces are implemented once per processor core. Access to IO-space and configuration space

registers may require software-level techniques to ensure that no more than one core attempts to access a register at a time.

The following is terminology found in the register descriptions.

Table 60: Terminology in Register Descriptions

Term	Definition
BIOS	Software recommendation syntax. See 3.1.2 [Software Recommendation (BIOS, SBIOS)].
SBIOS	
See	Reference to remote definition.
Alias	The alias keyword allows the definition of a soft link between two registers. • X is an alias of Y: X is a soft link to the register Y. • X1, X2 are an alias of Y: Both X1 and X2 are soft links to Y.
IF	Allows conditional definition as a function of register fields. The syntax is: • IF (conditional-expression) THEN definition ENDIF. • IF (conditional-expression) THEN definition ELSE definition ENDIF. • IF (conditional-expression) THEN definition ELSEIF (conditional-expression) THEN definition ELSE definition ENDIF.
THEN	
ELSEIF	
ELSE	
ENDIF	
Access Types	
Read	Capable of being read by software.
Read-only	Capable of being read but not written by software.
Write	Capable of being written by software.
Write-only	Write-only. Capable of being written by software. Reads are undefined.
Read-write	Capable of being written by software and read by software.
Set-by-hardware	Register field is set high by hardware, set low by hardware, or updated by hardware.
Cleared-by-hardware	
Updated-by-hardware	
Updated-by-SMU	
Write-1-to-clear	Software must write a 1 to the bit in order to clear it. Writing a 0 to these bits has no affect.
Write-1-only	Software can set the bit high by writing a 1 to it. Writes of 0 have no effect.
Reset-applied	Takes effect on warm reset.
GP-read	GP exception occurs on read.
GP-write	GP exception occurs on write.
GP-read-write	GP exception occurs on a read or a write.
Per-core	One instance per core. Only valid for MMIO config space. Writes of these bits from one core only affect that core's register. Reads return the values appropriate to that core.
Per-compute-unit	One instance per compute unit. Writes of these bits from one core only affect that compute unit's register. Reads return the values appropriate to that compute unit. See 2.4.2.1 [Registers Shared by Cores in a Compute Unit].
SharedNC	All cores share the one instance per-compute-unit non-coherently; see 2.4.2.1 [Registers Shared by Cores in a Compute Unit]. Valid only with per-compute-unit.

Table 60: Terminology in Register Descriptions

Term	Definition
Per-L2	One instance per L2 cache. See CPUID Fn8000_001D_EAX_x2[NumSharingCache].
Per-node	One instance per node. See 3.1.1 [Northbridge MSRs In Multi-Core Products].
Not-same-for-all	Provide indication as to whether all instances of a given register should be the same across all cores/nodes according to the following equation: SameOnAllCheckEnabled = (Writable && (same-for-all | MSR) && ~(not-same-for-all || UpdatedByHw)). UpdatedByHw = (Updated-by-hardware || set-by-hardware || cleared-by-hardware || set-when-done || cleared-when-done).
Same-for-all	
Field Definitions	
Reserved	Field is reserved for future use. Software is required to preserve the state read from these bits when writing to the register. Software may not depend on the state of reserved fields nor on the ability of such fields to return the state previously written.
Unused	Field is reserved for future use. Software is not required to preserve the state read from these bits when writing to the register. Software may not depend on the state of unused fields nor on the ability of such fields to return the state previously written.
MBZ	Must be zero. If software attempts to set an MBZ bit to 1, a general-protection exception (#GP) occurs.
RAZ	Read as zero. Writes are ignored, unless RAZ is combined with write-only or write-1-only.
Reset Definitions	
Reset	The reset value of each register is provided below the mnemonic or in the field description. Unless otherwise noted, the register state matches the reset value when RESET_L is asserted (either a cold or a warm reset). Reset values may include: • **X**: an X in the reset value indicates that the field resets (warm or cold) to an unspecified state.
Cold reset	The field state is not affected by a warm reset (even if the field is labeled “cold reset: X”); it is placed into the reset state when PWROK is deasserted. See "Reset" above for the definition of characters that may be found in the cold reset value.
Value	The current value of a read-only field or register. A value statement explicitly defines the field or register as read-only and the value returned under all conditions including after reset events. A field labeled “Value:” will not have a separate reset definition.

3.1.1 Northbridge MSRs In Multi-Core Products

MSRs that control Northbridge functions are shared between all cores on the node in a multi-core processor (e.g. MSRC001_001F). If control of Northbridge functions is shared between software on all cores, software must ensure that only one core at a time is allowed to access the shared MSR. Some MSRs are conditionally shared; see D18F3x44[NbMcaToMstCpuEn].

3.1.2 Software Recommendation (BIOS, SBIOS)

The following keywords specify the recommended value to be set by software.

- BIOS: AMD BIOS.
- SBIOS: Platform BIOS.

Syntax: BIOS: integer-expression. Any of the supported tags can be substituted for BIOS.

If “BIOS:” occurs in a register field then the recommended value is applied to the field. If “BIOS:” occurs after a register name but outside of a register field table row then the recommended value is applied to the width of the register.

3.1.3 See Keyword (See:)

There is a special meaning applied to the use of “See:” that differs from the use of See not followed by a “:”.

- See, not followed by a “:”, simply refers the reader to a document location that contains related information.
- See followed by a “:” is a shorthand notation that indicates that the definition for this register or register field inherits all properties and definitions from the register or register field that follows "See:". Any definition local to the register or register field supercedes this inheritance.

“See:” can be used in the following ways:

- Full register width. CPUID Fn0000_0001_EAX inherits it’s full register width definition from D18F3xFC.
- Register field. MSR0000_0277[PA1MemType] inherits it’s definition from PA0MemType, however, the local reset of 4h overrides the inherited PA0MemType reset of 6h.
- Valid values definition. MSR0000_020[E,C,A,8,6,4,2,0][MemType], for example, inherits the valid values definition from Table 218 [Valid Values for Memory Type Definition].

3.1.4 Mapping Tables

The following mapping table types are defined.

3.1.4.1 Register Mapping

The register mapping table specifies the specific function for each register in a range of registers.

Table 190, for example, specifies that the D18F5x160 function is for NB P-state 0.

3.1.4.2 Index Mapping

The index mapping table is similar to the register mapping table, but specifies the register by index instead of by full register mnemonic.

3.1.4.3 Field Mapping

The field mapping table maps the fields of a range of registers. The rows are the registers that are mapped. Each column specifies a field bit range that is mapped by that column for all registers. The cell at the intersection of the register and the field bit range specifies the suffix that is appended to the register field. “Reserved” specifies that the field is reserved for the register of that row.

3.1.4.4 Broadcast Mapping

The broadcast mapping table maps a register address to a range of register addresses that are written as a group when the broadcast register address is written. The register address is formed by the concatenation of the row address with the column address. The cell at the intersection of the row and column address is a range of register addresses that will be written as a group when the row and column address is written.

3.1.4.5 Reset Mapping

The reset mapping table specifies the reset, cold reset, or value for each register in a range of registers.

Table 213 [Reset Mapping for CPUID Fn8000_0000_E[D,C,B]X], for example, specifies that the CPUID Fn0000_0000_EBX register has a value of 6874_7541h, with a comment of "The ASCII characters "h t u A"".

3.1.4.6 Valid Values

The valid values table defines the valid values for one or more register fields. The valid values table is equivalent in function to the Bits/Description tables in register fields (E.g. MSR0000_0277[PA0MemType]) and is most often used when the table becomes too large and unwieldy to be included into the register field. (E.g. Table 218 [Valid Values for Memory Type Definition])

3.1.4.7 BIOS Recommendations

The BIOS recommendations table defines "BIOS:" recommendations that are conditional and complex enough to warrent a table.

Table 180 [BIOS Recommendations for D18F2x1B[4:0]], for example, specifies the BIOS recommendations for D18F2x1B0[DcqBwThrotWm] and D18F2x1B4[DcqBwThrotWm1, DcqBwThrotWm2]. All cells under the "Condition" header for a given row are ANDed to form the condition for the values to the right of the condition. For example, rows 1-3 and column 1 provide the following equivalent BIOS recommendation:

- D18F2x1B0[DcqBwThrotWm]: BIOS: IF (DdrRate==667) THEN 4h ELSEIF (DdrRate==800) THEN 5h ELSEIF (DdrRate==1066) THEN 6h ESEIF etc.

3.2 IO Space Registers

See 3.1 [Register Descriptions and Mnemonics] for a description of the register naming convention.

IOCF8 IO-Space Configuration Address

Reset: 0. IOCF8 [IO-Space Configuration Address], and IOCFC [IO-Space Configuration Data Port], are used to access system configuration space, as defined by the PCI specification. IOCF8 provides the address register and IOCFC provides the data port. Software sets up the configuration address by writing to IOCF8. Then, when an access is made to IOCFC, the processor generates the corresponding configuration access to the address specified in IOCF8. See 2.7 [Configuration Space].

IOCF8 may only be accessed through aligned, DW IO reads and writes; otherwise, the accesses are passed to the appropriate IO link. Accesses to IOCF8 and IOCFC received from an IO link are treated as all other IO transactions received from an IO link and are forwarded based on the settings in D18F1x[DC:C0] [IO-Space Base/Limit]. IOCF8 and IOCFC in the processor are not accessible from an IO link.

Bits	Description
31	**ConfigEn: configuration space enable**. Read-write. 1=IO read and write accesses to IOCFC are translated into configuration cycles at the configuration address specified by this register. 0=IO read and write accesses are passed to the appropriate IO link and no configuration access is generated.
30:28	Reserved.
27:24	**ExtRegNo: extended register number**. Read-write. ExtRegNo provides bits[11:8] and RegNo provides bits[7:2] of the byte address of the configuration register. ExtRegNo is reserved unless it is enabled by MSRC001_001F[EnableCf8ExtCfg].

23:16	**BusNo: bus number**. Read-write. Specifies the bus number of the configuration cycle.
15:11	**Device: bus number**. Read-write. Specifies the device number of the configuration cycle.
10:8	**Function**. Read-write. Specifies the function number of the configuration cycle.
7:2	**RegNo: register address**. Read-write. See IOCF8[ExtRegNo].
1:0	Reserved.

IOCFC IO-Space Configuration Data Port

Bits	Description
31:0	**Data**. Read-write. Reset: 0. See IOCF8.

3.3 Device 0 Function 0 (Root Complex) Configuration Registers

See 3.1 [Register Descriptions and Mnemonics] for a description of the register naming convention. See 2.7 [Configuration Space] for details about how to access this space.

D0F0x00 Device/Vendor ID

Bits	Description
31:16	**DeviceID: device ID**. Read-only. Value: 1422h.
15:0	**VendorID: vendor ID**. Read-only. Value: 1022h.

D0F0x04 Status/Command

Reset: 0000_0004h.

Bits	Description
31:21	Reserved.
20	**CapList: capability list**. Read-only. 1=Capability list supported.
19:3	Reserved.
2	**BusMasterEn: bus master enable**. Read-only.
1	**MemAccessEn: memory access enable**. Read-only.
0	**IoAccessEn: IO access enable**. Read-only.

D0F0x08 Class Code/Revision ID

Reset: 0600_0000h.

Bits	Description
31:8	**ClassCode: class code**. Read-only. Provides the host bridge class code as defined in the PCI specification.
7:0	**RevID: revision ID**. Read-only.

D0F0x0C Header Type

Reset: 0080_0000h.

Bits	Description
31:24	Reserved.
23	**DeviceType**. Read-only. 0=Single function device. 1=Multi-function device.
22:16	**HeaderType**. Read-only.
15:8	**LatencyTimer**. Read-only.
7:0	**CacheLineSize**. Read-only.

D0F0x2C Subsystem and Subvendor ID

Bits	Description
31:16	**SubsystemID**. Read-only. Value: 1410h.
15:0	**SubsystemVendorID**. Read-only. Value: 1022h.

D0F0x34 Capabilities Pointer

Reset: 0000_0000h.

Bits	Description
31:8	Reserved.
7:0	**CapPtr: capabilities pointer**. Read-only. There is no capability list.

D0F0x48 NB Header Write Register

Reset: 0000_0080h.

Bits	Description
31:8	Reserved.
7	**DeviceType: device type**. Read-write. This field sets the value in the corresponding field in D0F0x0C[DeviceType]. 0=Single function device. 1=Multi-function device.
6:0	Reserved.

D0F0x4C PCI Control

Reset: 0000_0000h.

Bits	Description
31:27	Reserved.
26	**HPDis: hot plug message disable**. Read-write. 1=Hot plug message generation is disabled.
25:24	Reserved.
23	**MMIOEnable: memory mapped IO enable**. Read-write. 1=Decoding of MMIO cycles is enabled. The MMIO Base/Limit pair (D0F0x64_x17 and D0F0x64_x18) are decoded. This range is used to create an MMIO hole in the DRAM address range used for DMA decoding. DMA writes that fall into the MMIO range are treated as potential p2p requests. DMA reads that fall into the MMIO range are aborted as unsupported requests.
22:15	Reserved.
14:6	Reserved.
5	**SerrDis**: s**ystem error message disable**. Read-write. 1=The generation of SERR messages is disabled.
4	**PMEDis: PME disable**. Read-write. 1=The generation of PME messages is disabled.
3:0	Reserved.

D0F0x60 Miscellaneous Index

Reset: 0000_0000h. The index/data pair registers, D0F0x60 and D0F0x64, are used to access the registers at D0F0x64_x[FF:00]. To access any of these registers, the address is first written into the index register, D0F0x60, and then the data is read from or written to the data register, D0F0x64.

Bits	Description
31:7	Reserved.
6:0	**MiscIndAddr: miscellaneous index register address**. Read-write.

D0F0x64 Miscellaneous Index Data

See D0F0x60. Address: D0F0x60[MiscIndAddr].

Bits	Description
31:0	**MiscIndData: miscellaneous index data register**.

D0F0x64_x00 Northbridge Control

Reset: 0000_0000h.

Bits	Description
31:8	Reserved.
7	**HwInitWrLock**. Read-write. 1=Lock HWInit registers. 0=Unlock HWInit registers.
6:0	Reserved.

D0F0x64_x0C IOC Bridge Control

Reset: 0000_0000h.

Bits	Description
31:0	Reserved.

D0F0x64_x0D IOC PCI Configuration

Bits	Description
31	**IommuDis**. Read-only. Value: Product specific.
30:1	Reserved.
0	**PciDev0Fn2RegEn**. Read-write. Reset: 1. 1=Enable configuration accesses to device 0 function 2.

D0F0x64_x16 IOC Advanced Error Reporting Control

Reset: 0000_0001h.

Bits	Description
31:1	Reserved.
0	**AerUrMsgEn: AER unsupported request message enable**. Read-write. BIOS: 0. 1=AER unsupported request messages are enabled.

D0F0x64_x17 Memory Mapped IO Base Address

Reset: 0000_0000h.

Bits	Description
31:0	**MmioBase[47:16]: memory mapped IO base address**. Read-write.

D0F0x64_x18 Memory Mapped IO Limit

Reset: 0000_0000h.

Bits	Description
31:0	**MmioLimit[47:16]: memory mapped IO limit**. Read-write.

D0F0x64_x19 Top of Memory 2 Low

Reset: 0000_0000h.

Bits	Description
31:23	**Tom2[31:23]: top of memory 2**. Read-write. BIOS: MSRC001_001D[TOM2[31:23]]. This field specifies the maximum system address for upstream read and write transactions that are forwarded to the host bridge. All addresses less than this system address are forwarded to DRAM and are not checked to determine if the transaction is a peer-to-peer transaction. All upstream reads with addresses greater than or equal to this system address are master aborted.
22:1	Reserved.
0	**TomEn: top of memory enable**. Read-write. BIOS: MSRC001_0010[MtrrTom2En]. 1=Top of memory check enabled.

D0F0x64_x1A Top of Memory 2 High

Reset: 0000_0000h.

Bits	Description
31:8	Reserved.
7:0	**Tom2[39:32]: top of memory 2**. Read-write. BIOS: MSRC001_001D[TOM2[39:32]]. See D0F0x64_x19[Tom2].

D0F0x64_x1D Internal Graphics PCI Control

Reset: 0000_0000h.

Bits	Description
31:4	Reserved.
3	**Vga16En: VGA IO 16 bit decoding enable**. Read-write. BIOS: D0F0x64_x1D[VgaEn]. 1=Address bits [15:10] for VGA IO cycles are decoded. 0=Address bits [15:10] for VGA IO cycles are ignored.
2	Reserved.
1	**VgaEn: VGA enable**. Read-write. 1=Enable VGA range in Intgfx.
0	Reserved.

D0F0x64_x1F FCH Location

Reset: 0004_0001h.

Bits	Description
31:16	**SBLocatedCore: Indicates which GPP Core has the FCH attached to it**. Read-write. Bits — Definition 0000h — No FCH attached. 0001h — FCH located under PGD. 0002h — FCH located under PPD. 0003h — Reserved. 0004h — FCH located under PSD. FFFFh-0005h — Reserved.
15:0	**SBLocatedPort: Indicates which Port on the SBLocatedCore has the FCH**. Read-write. Bits — Definition 0000h — No FCH attached. 0001h — FCH located on Port A of SBLocatedCore. 0002h — FCH located on Port B of SBLocatedCore. 0003h — Reserved. 0004h — FCH located on Port C of SBLocatedCore. 0007h-0005h — Reserved. 0008h — FCH located on Port D of SBLocatedCore. 000Fh-0009h — Reserved. 0010h — FCH located on Port Eof SBLocatedCore. FFFFh-0011h — Reserved.

D0F0x64_x22 LCLK Control 0

Reset: 7F3F_8100h.

Bits	Description
31	Reserved.
30	**SoftOverrideClk0**. Read-write. BIOS: 0. 1=Dynamic clock gating disabled for the host request path to the PCIe cores.

29	**SoftOverrideClk1**. Read-write. BIOS: 0. 1=Dynamic clock gating disabled for the host request path to the internal graphics and the host response path.
28	**SoftOverrideClk2**. Read-write. BIOS: 0. 1=Dynamic clock gating disabled for the host configuration requests.
27	**SoftOverrideClk3**. Read-write. BIOS: 0. 1=Dynamic clock gating disabled for the debug bus path.
26	**SoftOverrideClk4**. Read-write. BIOS: 0. 1=Dynamic clock gating disabled for the host request path to the configuration block.
25:0	Reserved.

D0F0x64_x23 LCLK Control 1

Reset: 7F3F_8100h.

Bits	Description
31	Reserved.
30	**SoftOverrideClk0**. Read-write. BIOS: 0. 1=Dynamic clock gating disabled for upstream DMA requests from all sources.
29	**SoftOverrideClk1**. Read-write. BIOS: 0. 1=Dynamic clock gating disabled for upstream DMA requests from the GPPFCH link core.
28	**SoftOverrideClk2**. Read-write. BIOS: 0. 1=Dynamic clock gating disabled for upstream DMA requests from internal graphics and its DMA response reordering path.
27	**SoftOverrideClk3**. Read-write. BIOS: 0. 1=Dynamic clock gating disabled for upstream DMA requests from internal graphics.
26	**SoftOverrideClk4**. Read-write. BIOS: 0. 1=Dynamic clock gating disabled for upstream DMA requests from the Gfx link core.
25:0	Reserved.

D0F0x64_x3[B:0] Programmable Device Remap Register

Table 61: Reset values for D0F0x64_x3[B:0]

Register	Reset	Function
D0F0x64_x30	0000_0011h	Program [7:3]DevNum, [2:0]FnNum to map to PortA of PGD.
D0F0x64_x31	0000_0012h	Program [7:3]DevNum, [2:0]FnNum to map to PortB of PGD.
D0F0x64_x32	0000_0019h	Program [7:3]DevNum, [2:0]FnNum to map to PortA of PPD.
D0F0x64_x33	0000_001Ah	Program [7:3]DevNum, [2:0]FnNum to map to PortB of PPD.
D0F0x64_x34	0000_001Bh	Program [7:3]DevNum, [2:0]FnNum to map to PortC of PPD.
D0F0x64_x35	0000_001Ch	Program [7:3]DevNum, [2:0]FnNum to map to PortD of PPD.
D0F0x64_x36	0000_001Dh	Program [7:3]DevNum, [2:0]FnNum to map to PortE of PPD.
D0F0x64_x37	0000_0021h	Program [7:3]DevNum, [2:0]FnNum to map to PortA of PSD.
D0F0x64_x38	0000_0022h	Program [7:3]DevNum, [2:0]FnNum to map to PortB of PSD.
D0F0x64_x39	0000_0023h	Program [7:3]DevNum, [2:0]FnNum to map to PortC of PSD.
D0F0x64_x3A	0000_0024h	Program [7:3]DevNum, [2:0]FnNum to map to PortD of PSD.
D0F0x64_x3B	0000_0025h	Program [7:3]DevNum, [2:0]FnNum to map to PortE of PSD.

Software can only utilize device and function number combinations that are used by other (local) PCIe bridges.

This effectively allows swapping of device and function numbers between bridges.

Bits	Description
31:8	Reserved.
7:0	**DevFnMap**. Read-write. Program [7:3]DevNum, [2:0]FnNum to map to PortA/B/C/D of each PCIe core.

D0F0x64_x46 IOC Features Control

Reset: 0000_1063h.

Bits	Description
31:28	Reserved.
27:24	Reserved.
23	Reserved.
22	Reserved.
21:17	Reserved.
16	Reserved.
15:5	Reserved.
4:3	Reserved.
2:1	**P2PMode: peer-to-peer mode**. Read-write. Specifies how upstream write transactions above D0F0x64_x19[Tom2] are completed. Bits — Definition 00b — Mode 0. Master abort writes that do not hit one of the internal PCI bridges. Forward writes that hit one of the internal PCI bridges to the bridge. 01b — Mode 1. Forward writes to the host bridge that do not hit one of the internal PCI bridges. Forward writes that hit one of the internal PCI bridges to the bridge. 10b — Mode 2. Forward all writes to the host bridge0. 11b — Reserved.
0	Reserved.

D0F0x7C IOC Configuration Control

Cold reset: 0000_0000h.

Bits	Description
31:1	Reserved.
0	**ForceIntGfxDisable: internal graphics disable**. Read-write. Setting this bit disables the internal graphics and the HD Audio controller.

D0F0x84 Link Arbitration

Bits	Description
31:10	Reserved.
9	**PmeTurnOff: PME_Turn_Off message trigger**. Read-write. Reset: 0. 1=Trigger a PME_Turn_Off message to all downstream devices if PmeMode=1.
8	**PmeMode: PME message mode**. Read-write. Reset: 0. 1=PME_Turn_Off message is triggered by writing PmeTurnOff. 0=PME_Turn_Off message is triggered by a message from the FCH.
7:4	Reserved.
3	**VgaHole: vga memory hole**. Read-write. Reset: 1. This bit creates a hole in memory for the VGA memory range. 1=Requests hitting the VGA range are checked against PCI bridge memory ranges instead of being forwarded to system memory.
2:0	Reserved.

D0F0x90 Northbridge Top of Memory

Reset: 0000_0000h.

Bits	Description
31:23	**TopOfDram**. Read-write. BIOS: MSRC001_001A[TOM[31:23]]. Specifies the address that divides between MMIO and DRAM. From TopOfDram to 4G is MMIO; below TopOfDram is DRAM.
22:0	Reserved.

D0F0x94 Northbridge ORB Configuration Offset

Reset: 0000_0000h.
The index/data pair registers, D0F0x94 and D0F0x98, are used to access the registers at D0F0x98_x[FF:00]. To access any of these registers, the address is first written into the index register, D0F0x94, and then the data is read from or written to the data register, D0F0x98.

Bits	Description
31:7	Reserved.
6:0	**OrbIndAddr: ORB index register address**. Read-write.

D0F0x98 Northbridge ORB Configuration Data Port

See D0F0x94. Address: D0F0x94[OrbIndAddr].

Bits	Description
31:0	**OrbIndData: ORB index data register**.

D0F0x98_x02 ORB PGMEM Control

Reset: 0000_0000h.

Bits	Description
31:16	**PgmemHysteresis**. Read-write. Hysteresis value for power-gating of ORB TX group of memories. Value represents absolute number of LCLK cycles.
15:8	Reserved.
7:5	**TxPgmemStEn**. Read-write. Power-gating enablement for the ORB TX group of memories. Bits are mutually exclusive. Bit Definition [0] LS (light sleep) mode. [1] DS (deep sleep) mode. [2] SD (shutdown) mode.
4:2	**RxPgmemStEn**. Read-write. Power-gating enablement for the ORB RX group of memories. Bits are mutually exclusive. Bit Definition [0] LS (light sleep) mode. [1] DS (deep sleep) mode. [2] SD (shutdown) mode.
1	**OrbTxPgmemEn**. Read-write. Enables ORB TX memory power-gating.
0	**OrbRxPgmemEn**. Read-write. Enables ORB RX memory power-gating.

D0F0x98_x06 ORB Downstream Control 0

Reset: 0000_0000h.

Bits	Description
31:27	Reserved.
26	**UmiNpMemWrEn**. Read-write. BIOS: See 2.11.4. 1=NP protocol over UMI for memory-mapped writes targeting LPC enabled. This bit may be set to avoid a deadlock condition.
25:0	Reserved.

D0F0x98_x07 ORB Upstream Arbitration Control 0

Reset: 0000_0080h.

Bits	Description
31	**SMUCsrIsocEn**. Read-write. BIOS: 1. 1=CSR accesses go through ISOC channel. If this bit is set, D0F0x98_x1E[HiPriEn] must also be set.
30:17	Reserved.
16	**SyncFloodOnParityErr**. Read-write. Enable short circuit syncflood when arb_np detects a parity error for error containment.
15	**DropZeroMaskWrEn**. Read-write. BIOS: 1. 1=Drop byte write request that have all bytes masked. 0=Forward byte write request that have all bytes masked.

14:8	Reserved.
7	**IommuIsocPassPWMode**. Read-write. BIOS: 1. 1=Always set PassPW for IOMMU upstream isochronous requests.
6	**DmaReqRespPassPWMode**. Read-write. BIOS: 0. Specifies the RespPassPW bit for non-posted upstreamDMA requests. Bits Description 0 Always . 1 1 Value passed from IOC.
5	Reserved.
4	**IommuBwOptEn**. Read-write. BIOS: 1. 1=Optimize IOMMU L2 byte write by detecting consecutive DW mask and translate the request to DW write.
3	Reserved.
2	**IocRdROMapDis**. Read-write. 1=Disable mapping relax ordering bit to RdRespPpw bit for IOC reads.
1	**IocWrROMapDis**. Read-write. 1=Disables mapping relax ordering bit to PassPW bit for IOC writes.
0	**IocBwOptEn**. Read-write. BIOS: 1. 1=Enable optimization of byte writes by detecting consecutive DW masks and translating the request to DW writes.

D0F0x98_x08 ORB Upstream Arbitration Control 1

This register specifies the weights of the weighted round-robin arbiter in stage 1 of the upstream arbitration for non-posted reads.

Bits	Description
31:24	Reserved.
23:16	**NpWrrLenC**. Read-write. Reset: 8h. BIOS: 1h. This field defines the maximum number of non-posted read requests from the SMU that are serviced before the arbiter switches to the next client.
15:8	**NpWrrLenB**. Read-write. Reset: 8h. BIOS: 8h. This field defines the maximum number of non-posted read requests from IOMMU that are serviced before the arbiter switches to the next client.
7:0	**NpWrrLenA**. Read-write. Reset: 8h. BIOS: 8h. This field defines the maximum number of non-posted read requests from IOC that are serviced before the arbiter switches to the next client.

D0F0x98_x09 ORB Upstream Arbitration Control 2

Reset: 0000_0808h.

This register specifies the weights of the weighted round-robin arbiter in stage 1 of the upstream arbitration for posted writes.

Bits	Description
31:16	Reserved.

15:8	**PWrrLenB**. Read-write. This field defines the maximum number of posted write requests from the IOMMUthat are serviced before the arbiter switches to the next client.
7:0	**PWrrLenA**. Read-write. This field defines the maximum number of posted write requests from the IOC that are serviced before the arbiter switches to the next client.

D0F0x98_x0C ORB Upstream Arbitration Control 5

Reset: 0000_0808h. This register specifies the weights of the weighted round-robin arbiter in stage 2 of the upstream arbitration.

Bits	Description
31:24	Reserved.
23:16	Reserved.
15:8	**GcmWrrLenB**. Read-write. BIOS: 08h. This field defines the maximum number of non-posted read requests from stage 1 that are getting serviced in the round-robin before the stage 2 arbiter switches to the next client.
7:0	**GcmWrrLenA**. Read-write. BIOS: 08h. This field defines the maximum number of posted write requests from stage 1 that are getting serviced in the round-robin before the stage 2 arbiter switches to the next client.

D0F0x98_x1E ORB Receive Control 0

Reset: 4800_0000h.

Bits	Description
31:24	**RxErrStatusDelay**. Read-write. BIOS: 48h. Delay error status by number of LCLK cycles to filter false errors caused by reset skew.
23:2	Reserved.
1	**HiPriEn**. Read-write. BIOS: 1. 1=High priority channel enabled. See D0F0x98_x27[IOMMUUrAddr[31:6]]. IF (D0F0x98_x1E[HiPriEn]==0) THEN (D0F0x98_x07[SMUCsrIsocEn]==0). IF (D0F0x98_x1E[HiPriEn]==1) THEN (D18F0x[E4,C4,A4,84][IsocEn]==1) in order to fully enable the Isoc channel on the ONION Link.
0	Reserved.

D0F0x98_x26 ORB IOMMU Control 0

Reset: 0000_0000h.

Bits	Description
31:8	Reserved.
7:0	**IOMMUUrAddr[39:32]**. Read-write. See: D0F0x98_x27[IOMMUUrAddr[31:6]].

D0F0x98_x27 ORB IOMMU Control 1

Reset: 0000_0000h.

Bits	Description
31:6	**IOMMUUrAddr[31:6]**. Read-write. BIOS: IOMMUUrAddr[39:6] must be programmed to a safe system memory address when D0F2x44[IommuEnable]=1. IOMMUUrAddr[39:6] = {D0F0x98_x26[IOMMUUrAddr[39:32]], IOMMUUrAddr[31:6]}. IOMMU requests that are not directed to system memory are redirected to IOMMUUrAddr.
5:0	Reserved.

D0F0x98_x28 ORB Transmit Control 0

Reset: 0000_0002h.

Bits	Description
31:2	Reserved.
1	**ForceCoherentIntr**. Read-write. BIOS: 1. 1=Interrupt request are forced to have coherent bit set.
0	Reserved.

D0F0x98_x2C ORB Clock Control

Reset: 000F_0200h.

Bits	Description
31:16	**WakeHysteresis**.Read-write. BIOS: 19h. Specifies the amount of time hardware waits after ORB becomes idle before deasserting the wake signal to the NB. Wait time = WakeHysteresis * 200ns. Changes to this field should be done prior to setting DynWakeEn.
15:10	Reserved.
9	**SBDmaActiveMask**. Read-write. BIOS: 1. 0=SB_DMA_ACTIVE_L state affects OnInbWake state. 1=SB_DMA_ACTIVE_L state is masked out.
8:3	Reserved.
2	Reserved.
1	**DynWakeEn**.Read-write. BIOS: 1. 1=Enable dynamic toggling of the wake signal between ORB and NB. 0=Disable dynamic toggling of the wake signal. See WakeHysteresis.
0	Reserved.

D0F0x98_x37 ORB Allow LDTSTOP Control 0

Reset: 0020_0000h.

Bits	Description
31:28	Reserved.
27:16	**LDTStopHysteresis**. Read-write. Specifies the number of timer periods (200 ns) the AllowLDTStop signal is held low before ORB asserts the signal again.

15:2	Reserved.
1	**DmaActiveOutEn**. Read-write. 1=Enable ORB to drive the DMAACTIVE_L pin. Meaningful only when D0F0x98_x37[AllowLDTStopPinMode]==0.
0	**AllowLDTStopPinMode**. Read-write. Indicates the definition of the ALLOW_LDTSTOP pin. 0=Pin is used as DMAACTIVE_L. 1=Pin is used as ALLOW_LDTSTOP.

D0F0x98_x3A ORB Source Tag Translation Control 2

Reset: 0000_0000h.

Bits	Description
31:0	**ClumpingEn**. Read-write. BIOS should follow the below requirements. Valid only for PGD, PPD, PSD and GBIF client clumping; internal unit ID ranges 4h-7h, 8h-Ch, Fh-13h, and 14h-17h respectively. Legal PGD clumping settings are: [7:4]=1010b, applicable only in x8/8 system configuration, [7:4]=1110b, applicable only in x0/16 system configuration. Legal PPD clumping settings are: [12:8]=00010b, applicable only in x0/0/0/0/8 system configuration. Legal PSD clumping settings are: [19:15]=00010b, applicable only in x0/0/0/0/8 system configuration. Legal GBIF clumping settings are: [23:20]=0010b, 0110b and 1110b which are applicable in any system configuration. 1110b is the recommended value. All other bits of this register must always remain 0. See D18F0x[11C,118,114,110].

D0F0x98_x3B ORB Source Tag Translation Control 3

Reset: 0000_0000h.

Bits	Description
31:0	**IocOutstandingMask**. Read-write. Limit number of outstanding requests for every DMA client via the IOC.

D0F0x98_x4[A,9] ORB LCLK Clock Control 1-0

Reset: 7F3F_8100h.

Bits	Description
31	Reserved.
30	**SoftOverrideClk0**. Read-write. BIOS: 0. See SoftOverrideClk6.
29	**SoftOverrideClk1**. Read-write. BIOS: 0. See SoftOverrideClk6.
28	**SoftOverrideClk2**. Read-write. BIOS: 0. See SoftOverrideClk6.

27	**SoftOverrideClk3**. Read-write. BIOS: 0. See SoftOverrideClk6.
26	**SoftOverrideClk4**. Read-write. BIOS: 0. See SoftOverrideClk6.
25	**SoftOverrideClk5**. Read-write. BIOS: 0. See SoftOverrideClk6.
24	**SoftOverrideClk6**. Read-write. BIOS: 0. 1=Clock gating disabled. 0=Clock gating enabled.
23:0	Reserved.

D0F0xB8 SMU Index Address

The index/data pair registers, D0F0xB8 and D0F0xBC, are used to access the registers at D0F0xBC_x[FFFFFFFF:00000000]. To access any of these registers, the address is first written into the index register, D0F0xB8, and then the data is read from or written to the data register, D0F0xBC.

Bits	Description
31:0	**NbSmuIndAddr: smu index address**. Read-write. Reset: 0.

D0F0xBC SMU Index Data

See D0F0xB8. Address: D0F0xB8[NbSmuIndAddr].

Bits	Description
31:0	**NbSmuIndData: smu index data**. Reset: 0.

D0F0xBC_x3F800 FIRMWARE_FLAGS

Reset: xxxx_xxxxh.

Bits	Description
31:24	**TestCount**. Read-write. Test count.
23:1	Reserved.
0	**InterruptsEnabled**. Read-write. Bits: Definition 0: Firmware has not yet enabled interrupts. BIOS/Driver cannot yet send message interrupts to SMC. 1: Firmware has enabled interrupts. BIOS/Driver can send message interrupts to SMC.

D0F0xBC_x3F804 FIRMWARE_VID

Reset: xxxx_xxxxh.

Bits	Description
7:0	**FirmwareVid**. Read-write. Current voltage set by firmware voltage controller.

D0F0xBC_x3F820 PM_INTERVAL_CNTL_0

Reset: xxxx_xxxxh.

Bits	Description
31:24	**Loadline**. Read-write.
23:16	**VoltageCntl**. Read-write.
15:8	**ThermalCntl**. Read-write.
7:0	**LclkDpm**. Read-write.

D0F0xBC_x3F828 PM_TIMER_PERIOD

Bits	Description
31:0	**TimerPeriod**. Read-write. Reset: X. Specifies the period at which various power management related algorithms are run. Period = TimerPeriod / REFCLK.

D0F0xBC_x3F9E8 NB_DPM_CONFIG_1

Reset: xxxx_xxxxh.

Bits	Description
31:24	**DpmXNbPsHi**. Read-write. See: Dpm0PgNbPsLo.
23:16	**DpmXNbPsLo**. Read-write. See: Dpm0PgNbPsLo.
15:8	**Dpm0PgNbPsHi**. Read-write. See: Dpm0PgNbPsLo.
7:0	**Dpm0PgNbPsLo**. Read-write. Indexes the NB P-state used during specific levels of GPU activity. See 2.5.4.1 [NB P-states]. Bits — NB P-state Indexed 00b — D18F3x160 (see D18F5x16[C:0]). 01b — D18F3x164 (see D18F5x16[C:0]). 10b — D18F3x168 (see D18F5x16[C:0]). 11b — D18F3x16C (see D18F5x16[C:0]).

D0F0xBC_x3F9EC NB_DPM_CONFIG_2

Reset: xxxx_xxxxh.

Bits	Description
31:25	Reserved.

24	**EnableNbPsi1**. Read-write. Specifies how PSI1_L functions for VDDNB. 0=PSI1_L is deasserted. 1=PSI1_L is asserted whenever the GPU is idle.
23:17	Reserved.
16	**SkipDPM0**. Read-write. Specifies whether SMU waits for SCLK DPM to transition to state 0 before transitioning NB to the NB P-states indexed Dpm0PgNbPsHi and Dpm0PgNbPsLo. 0=Wait for SCLK DPM state 0. 1=Do not wait for SCLK DPM state 0. See 2.5.4.1 [NB P-states].
15:9	Reserved.
8	**SkipPG**. Read-write. Specifies whether SMU waits for the GPU to be power gated before transitioning NB to the NB P-states indexed Dpm0PgNbPsHi and Dpm0PgNbPsLo. 0=Wait for GPU power gating. 1=Do not wait for GPU power gating. See 2.5.4.1 [NB P-states].
7:0	**Hysteresis**. Read-write. Specifies the time the GPU must be idle before transitioning to the NB P-states indexed by Dpm0PgNbPsHi and Dpm0PgNbPsLo.

D0F0xBC_x3FD[8C:00:step14] LCLK DPM Control 0

Reset: xxxx_xxxxh. See 2.5.6.1.3 [LCLK DPM]. Each register in D0F0xBC_x3FD[8C:00:step14] corresponds to one LCLK DPM state as follows.

Table 62: Register Mapping for D0F0xBC_x3FD[8C:00:step14]

Register	Function	Register	Function
D0F0xBC_x3FD00	State 0	D0F0xBC_x3FD50	State 4
D0F0xBC_x3FD14	State 1	D0F0xBC_x3FD64	State 5
D0F0xBC_x3FD28	State 2	D0F0xBC_x3FD78	State 6
D0F0xBC_x3FD3C	State 3	D0F0xBC_x3FD8C	State 7

Bits	Description
31:24	**StateValid**. Read-write. 1=DPM state is valid. 0=DPM state is invalid.
23:16	**LclkDivider**. Read-write. Specifies the LCLK divisor for this DPM state.
15:8	**VID**. Read-write. Specifies the VDDNB VID for this DPM state.
7:0	**LowVoltageReqThreshold**. Read-write.

D0F0xBC_x3FD[94:08:step14] LCLK DPM Control 2

Reset: xxxx_xxxxh. Each register in D0F0xBC_x3FD[94:08:step14] corresponds to one LCLK DPM state as follows.

Table 63: Register Mapping for D0F0xBC_x3FD[94:08:step14]

Register	Function	Register	Function
D0F0xBC_x3FD08	State 0	D0F0xBC_x3FD58	State 4
D0F0xBC_x3FD1C	State 1	D0F0xBC_x3FD6C	State 5
D0F0xBC_x3FD30	State 2	D0F0xBC_x3FD80	State 6
D0F0xBC_x3FD44	State 3	D0F0xBC_x3FD94	State 7

Bits	Description
31:16	**ResidencyCounter**. Read-write.
15:8	**HysteresisUp**. Read-write.
7:0	**HysteresisDown**. Read-write.

D0F0xBC_x3FD[9C:10:step14] LCLK DPM Activity Thresholds

Reset: xxxx_xxxxh. Each register in D0F0xBC_x3FD[9C:10:step14] corresponds to one LCLK DPM state as follows.

Table 64: Register Mapping for D0F0xBC_x3FD[9C:10:step14]

Register	Function	Register	Function
D0F0xBC_x3FD10	State 0	D0F0xBC_x3FD60	State 4
D0F0xBC_x3FD24	State 1	D0F0xBC_x3FD74	State 5
D0F0xBC_x3FD38	State 2	D0F0xBC_x3FD88	State 6
D0F0xBC_x3FD4C	State 3	D0F0xBC_x3FD9C	State 7

Bits	Description
31:24	**ActivityThreshold**. Read-write.
23:16	**EnabledForThrottle**. Read-write.
15:0	Reserved.

D0F0xBC_x3FDC8 SMU_LCLK_DPM_CNTL

Reset: xxxx_xxxxh.

Bits	Description
31:24	**LclkDpmEn**. Read-write. 1=Enable LCLK DPM
23:16	**VoltageChgEn**. Read-write. 1=Enable voltage change during LCLK DPM state transition.
15:8	**LclkDpmBootState**. Read-write.
7:0	Reserved.

D0F0xBC_x3FDD0 SMU_LCLK_DPM_THERMAL_THROTTLING_CNTL

Reset: xxxx_xxxxh.

Bits	Description
31:24	**TtHtcActive**. Read-write.
23:16	**LclkTtMode**. Read-write.
15:8	**TemperatureSel**. Read-write.
7:0	**LclkThermalThrottlingEn**. Read-write.

D0F0xBC_x3FDD4 SMU_LCLK_DPM_THERMAL_THROTTLING_THRESHOLDS

Reset: xxxx_xxxxh.

Bits	Description
31:16	**HighThreshold**. Read-write. Specifies the high thermal threshold for LCLK thermal throttling.
15:0	**LowThreshold**. Read-write. Specifies the low thermal threshold for LCLK thermal throttling.

D0F0xBC_xC010_40A0 SVI Loadline Configuration

Bits	Description
31:27	Reserved.
26:25	**SviLoadLineOffsetVddNb**. Read-only. Value: Product-specific.
24:23	**SviLoadLineOffsetVdd**. Read-only. Value: Product-specific.
22:20	**SviLoadLineTrimVddNb**. Read-only. Value: Product-specific.
19:17	**SviLoadLineTrimVdd**. Read-only. Value: Product-specific.
16:10	**SviLoadLineVddNb**. Read-only. Value: Product-specific.
9:3	**SviLoadLineVdd**. Read-only. Value: Product-specific.
2:0	Reserved.

D0F0xBC_xC020_0110 Activity Monitor Control

Bits	Description
31:11	Reserved.
10	**EnOrbDsCnt**. Read-write. Reset: X. 1=Enable downstream counter.
9	**EnOrbUsCnt**. Read-write. Reset: X. 1=Enable upstream counter.
8	**EnBifCnt**. Read-write. Reset: X. 1=Enable BIF counter.
7:5	Reserved.
4:3	**BusyCntSel**. Read-write. Reset: 0. Specifies subcomponents or activity monitored by the LCLK activity monitor. Bits / Definition / Bits / Definition 00b / GFX DMA (BIF) / 10b / Downstream activity 01b / Upstream activity / 11b / Up/downstream activity max
2	Reserved.
1	**PeriodCntRst**. Read-write. Reset: X.
0	**ActivityCntRst**. Read-write. Reset: X.

D0F0xBC_xC210_0000 CPU Interrupt Request

See 2.13.1 [Software Interrupts].

Bits	Description
31:17	Reserved.

16:1	**ServiceIndex**. Read-write. Reset: 0.
0	**IntToggle**. Read-write. Reset: 0.

D0F0xBC_xC210_0004 CPU Interrupt Status

See 2.13.1 [Software Interrupts].

Bits	Description
31:2	Reserved.
1	**IntDone**. Read-only; updated-by-hardware. Reset: 0.
0	**IntAck**. Read-only; updated-by-hardware. Reset: 0.

D0F0xBC_xC210_003C CPU Interrupt Argument

See 2.13.1 [Software Interrupts].

Bits	Description
31:0	**Argument**. Read-write. Reset: 0. Optional argument for a software interrupt.

D0F0xBC_xC210_0040 CPU Interrupt Response

See 2.13.1 [Software Interrupts].

Bits	Description
31:0	**Argument**. Read-write. Reset: 0. Optional response data upon completing a software interrupt.

D0F0xBC_xE000_3040 CONNECTED_STANDBY_CONTROL

Bits	Description
31:2	Reserved.
1	**S0i3_HINT[1]**. Read-write. Reset: 0.
0	**S0i3_HINT[0]**. Read-write. Reset: 0.

D0F0xC8 DEV Index Address

The index/data pair registers, D0F0xC8 and D0F0xCC are used to access the registers at D0F0xCC_x[FF:00]. To access any of these registers, the address is first written into the index register, D0F0xC8, and then the data is read from or written to the data register, D0F0xCC. Specific IOC bridges (Device/Function) are selected using the D0F0xC8[NbDevIndSel] field and enumerated as *_ib[21,1D:19,12:11]* in the indexed register's mnemonic.

Bits	Description
31:24	Reserved.

23:16	**NbDevIndSel: Device selector**. Read-write. Reset: 0. Bits Definition Bits Definition 10h-00h Reserved 1Bh D3F3 11h D2F1 1Ch D3F4 12h D2F2 1Dh D3F5 18h-13h Reserved 20h-1Eh Reserved 19h D3F1 21h D4F1 1Ah D3F2 FFh-22h Reserved
15:7	Reserved.
6:0	**NbDevIndAddr: Bridge (Device) index address**. Read-write. Reset: 0.

D0F0xCC DEV Index Data

See D0F0xC8. Address: D0F0xC8[NbDevIndAddr].

Bits	Description
31:0	**NbDevIndData: dev index data**.

D0F0xCC_x01_ib[21,1D:19,12:11] IOC Bridge Control

Reset: 0000_0000h.

Bits	Description
31:24	**ApicRange**. Read-write. Sets the bridge APIC range.
23	**ApicEnable**. Read-write. 1=Enables the bridge APIC range decoding. Requests fall in bridge APIC range if addr[39:12]={20'h00_FEC, APIC_Range[7:0]}.
22:21	Reserved.
20	**SetPowEn**. Read-write. BIOS: 1. 1=Enable generation of set_slot_power message to the bridge.
19	Reserved.
18	**CrsEnable**. Read-write. BIOS: 1. 1=Enables the hardware retry on receiving configuration request retry status.
17	**ExtDevCrsEn**. Read-write. 1=Reset the bridge CRS counter when an external device is plugged in or the link is down.
16	**ExtDevPlug**. Read-write. 1=Indicates to IOC that an external device is being plugged on the bridge.
15:4	Reserved.
3	**P2pDis**. Read-write. 1=Disables local peer-to-peer transactions forwarded to this bridge.
2	**CfgDis**. Read-write. 1=Configuration accesses to this bridge are disabled. Non-FCH bridges are not expected to set this bit.
1	**BusMasterDis**. Read-write. 1=The bridge's ability to operate as a bus master is disabled. This overrides the Bus Master Enable bit in the bridge.
0	**BridgeDis**. Read-write. 1=The bridge is hidden and no accesses are allowed to this bridge.

D0F0xD0 GBIF Index Address

The index/data pair registers, D0F0xD0 and D0F0xD4 are used to access the registers at D0F0xD4_x[FFFF_FFFF:0000_0000]. To access any of these registers, the address is first written into the

index register, D0F0xD0, and then the data is read from or written to the data register, D0F0xD4.

Bits	Description
31:0	**NbGbifIndAddr: Gbif index address**. Read-write. Reset: 0.

D0F0xD4 GBIF Index Data

See D0F0xD0. Address: D0F0xD0[NbGbifIndAddr].

Bits	Description
31:0	**NbGbifIndData: Gbif index data**. Reset: 0.

D0F0xD4_x0109_14E1 CC Bif Bx Strap0 Ind

Reset: 0000_C004h.

Bits	Description
31:13	Reserved.
12	**StrapBifDoorbellBarDis**. Read-write.
11:6	Reserved.
5:3	**StrapBifMemApSize**. Read-write. Size of the primary memory apertures claimed in the PCI configuration space. The aperture size should be rounded to the next power of 2 size (up to 128MB) as the frame buffer for frame buffers smaller than 128MB. For frame buffers larger than 128 MB the aperture size should be set to 256 MB. See D0F0xD4_x0109_1507[StrapBifMemApSizePin]. Bits Definition 000b 128 MB 001b 256 MB 010b 64 MB 111b-011b Reserved
2:1	**StrapBifRegApSize**. Read-write. Specifies the register aperture size. Bits Definition 00b 64 MB 01b 128 MB 10b 256 MB 11b 512 MB
0	Reserved.

D0F0xD4_x0109_14E2 CC Bif Bx Strap1 Ind

Reset: 0000_0000h.

Bits	Description
31:14	Reserved.
13	Reserved.
12:11	Reserved.
10	Reserved.
9	Reserved.

8	Reserved.
7:4	Reserved.
3	**StrapBifF064BarDisA**. Read-write.
2	Reserved.
1	**StrapBifIoBarDis**. Read-write.
0	Reserved.

D0F0xD4_x0109_1507 CC Bif Bx Pinstrap0 Ind

Reset: 0000_0802h.

Bits	Description
31:17	Reserved.
16	Reserved.
15:8	Reserved.
7:5	**StrapBifMemApSizePin**. Read-write. See: D0F0xD4_x0109_14E1[StrapBifMemApSize]
4:0	Reserved.

D0F0xE0 Link Index Address

Reset: 0130_8001h.

D0F0xE0 and D0F0xE4 are used to access D0F0xE4_x[FFFF_FFFF:0000_0000]. To read or write to one of these register, the address is written first into the address register D0F0xE0 and then the data is read from or written to the data register D0F0xE4.

The phy index registers (D0F0xE4_x0[2:1]XX_XXXX]) mapping to a specific phy, pin or pin group is shown in a table in the register definition. For example, to perform a read or write operation to configure Gfx phy 0 (P_GFX_[T,R]X[P,N][7:0] pin group) compensation, software should program D0F0xE0[31:0]=0120_0000h. Accessing any register number that is not listed in the mapping table may result in undefined behavior.

Some phy registers support broadcast write operations to groups of 4 or 8 lanes. For example, to perform broadcast write operation to configure Gfx Link[3:0] (P_GFX_RX[P,N][3:0] lanes) receiver phase loop filter, software should program D0F0xE0[31:0]=0120_5602h.

Bits	Description
31:24	**BlockSelect: block select**. Read-write. This field is used to select the specific register block to access. The encodings supported depends on the FrameType selected. FrameType — Encoding 1xh — 1=Phy interface 0, 2=Phy interface 1 (FrameType 12h only) 2xh — 1=Phy 0, 2=Phy 1 (FrameType 22h only) 3xh — 1=Wrapper 4xh — 1=IO link core

23:16	**FrameType: frame type**. Read-write. This field is used to select the type of register block to access. Bits Destination 1Nh Phy interface block registers. 2Nh Phy registers. 3Nh Wrapper registers. 4Nh IO Link registers. N Register Block 0h Gfx PCIe links 1h GPP PCIe Links 2h FCH link 3h DDI
15:0	**PcieIndxAddr: index address**. Read-write.

D0F0xE4 Link Index Data

See D0F0xE0. Address: {D0F0xE0[BlockSelect],D0F0xE0[FrameType],D0F0xE0[PcieIndxAddr]}.

Bits	Description
31:0	**PcieIndxData: index data**.

3.3.1 PIF Registers

Table 65: Mapping for PIF registers

D0F0xE0[31:16]	Wrapper	Port Description
0110h	PGD PIF0	Gfx+Display
0210h	PGD PIF1	Gfx+Display
0111h	PPD	GPP+Display
0112h	PSD	FCH+Display
0113h	DDI	Display

D0F0xE4_x0[210,11[3:0]]_0010 PIF Control

Reset: 3180_54D8h.

Bits	Description
31:20	Reserved.
19:17	**Ls2ExitTime: LS2 exit time**. Read-write. Bits Definition Bits Definition 000b 14us 100b 30us 001b 10us 101b 100ns 010b 15us 110b 100us 011b 20us 111b 50us
16:8	Reserved.
7	**RxDetectTxPwrMode: receiver detection transmitter power mode**. Read-write. 1=Transmitter is powered on.

6	**RxDetectFifoResetMode: receiver detect FIFO reset mode**. Read-write. BIOS: 1. 1=The transmit FIFO is reset after receiver detection. 0=The transmit FIFO is not reset after receiver detection.
5	Reserved.
4	**EiDetCycleMode: electrical idle detect mode**. Read-write. 1=Electrical idle cycle detection mode is enabled in L1. 0=Electrical idle detection is always enabled in L1.
3:0	Reserved.

D0F0xE4_x0[210,11[3:0]]_0011 PIF Pairing

Reset: 0200_0000h.

Bits	Description
31:26	Reserved.
25	**MultiPif: x16 link**. Read-write. 1=Lanes 7:0 are paired with a second PIF to create a x16 link.
24:21	Reserved.
20	**X16Lane150: x16 link lanes 15:0**. Read-write. 1=Lanes 15:0 are paired to create a x16 link.
19:18	Reserved.
17	**X8Lane158: x8 link lanes 15:8**. Read-write. 1=Lanes 15:8 are paired to create a x8 link.
16	**X8Lane70: x8 link lanes 7:0**. Read-write. 1=Lanes 7:0 are paired to create a x8 link.
15:12	Reserved.
11	**X4Lane1512: x4 link lanes 15:12**. Read-write. 1=Lanes 15:12 are paired to create a x4 link.
10	**X4Lane118: x4 link lanes 11:8**. Read-write. 1=Lanes 11:8 are paired to create a x4 link.
9	**X4Lane74: x4 link lanes 7:4**. Read-write. 1=Lanes 7:4 are paired to create a x4 link.
8	**X4Lane30: x4 link lanes 3:0**. Read-write. 1=Lanes 3:0 are paired to create a x4 link.
7	**X2Lane1514: x2 link lanes 15:14**. Read-write. 1=Lanes 15:14 are paired to create a x2 link
6	**X2Lane1312: x2 link lanes 13:12**. Read-write. 1=Lanes 13:12 are paired to create a x2 link
5	**X2Lane1110: x2 link lanes 11:10**. Read-write. 1=Lanes 11:10 are paired to create a x2 link
4	**X2Lane98: x2 link lanes 9:8**. Read-write. 1=Lanes 9:8 are paired to create a x2 link
3	**X2Lane76: x2 link lanes 7:6**. Read-write. 1=Lanes 7:6 are paired to create a x2 link.
2	**X2Lane54: x2 link lanes 5:4**. Read-write. 1=Lanes 5:4 are paired to create a x2 link.
1	**X2Lane32: x2 link lanes 3:2**. Read-write. 1=Lanes 3:2 are paired to create a x2 link.
0	**X2Lane10: x2 link lanes 1:0**. Read-write. 1=Lanes 1:0 are paired to create a x2 link.

D0F0xE4_x0[210,11[3:0]]_001[8:7,3:2] PIF Power Down Control [3:0]

Reset: 0001_1FA2h.

Table 66: Index addresses for D0F0xE4_x0[210,11[3:0]]_001[8:7,3:2]

D0F0xE0[31:16]	D0F0xE0[15:0]			
	0018h	0017h	0013h	0012h
0110h	PIF Lanes 15-12	PIF Lanes 11-8	PIF Lanes 7-4	PIF Lanes 3-0

Table 66: Index addresses for D0F0xE4_x0[210,11[3:0]]_001[8:7,3:2]

0210h	PIF Lanes 15-12	PIF Lanes 11-8	PIF Lanes 7-4	PIF Lanes 3-0
0111h	PIF Lanes 15-12	PIF Lanes 11-8	PIF Lanes 7-4	PIF Lanes 3-0
0112h	PIF Lanes 15-12	PIF Lanes 11-8	PIF Lanes 7-4	PIF Lanes 3-0
0113h	PIF Lanes 15-12	PIF Lanes 11-8	PIF Lanes 7-4	PIF Lanes 3-0

Bits	Description
31:29	**PllPwrOverrideVal: PLL power state override value**. Read-write. See TxPowerStateInTxs2.
28	**PllPwrOverrideEn: PLL power state override enable**. Read-write. 1=PLL forced to the power state specified by PllPwrOverrideVal.
27	Reserved.
26:24	**PllRampUpTime: PLL ramp time**. Read-write. Bits / Definition / Bits / Definition 000b / 10 us / 100b / 50 us 001b / 5 us / 101b / 300 us 010b / 15 us / 110b / 500 us 011b / 22 us / 111b / 800 us
23:17	Reserved.
16	**Tx2p5clkClockGatingEn**. Read-write. 1=The 2.5x TxClk is gated if the lane is idle. 0=The 2.5x TxClk is never gated.
15:13	Reserved.
12:10	**PllPowerStateInOff: PLL off power state**. Read-write. See: TxPowerStateInTxs2. All links associated with the PLL must be in the off state to transition the PLL to this state.
9:7	**PllPowerStateInTxs2: PLL L1 power state**. Read-write. See: TxPowerStateInTxs2. All links associated with the PLL must be in L1 to transition the PLL to this state.
6:4	**RxPowerStateInRxs2: receiver L1 power state**. Read-write. See: TxPowerStateInTxs2.
3	**ForceRxEnInL0s: force receiver enable in L0s**. Read-write. 1=The phy CDR is always enabled in L0s.
2:0	**TxPowerStateInTxs2: transmitter L1 power state**. Read-write. Bits / Definition / Bits / Definition 000b / L0 / 100b / Reserved 001b / LS1 / 101b / Reserved 010b / LS2 / 110b / Reserved 011b / Reserved / 111b / Off

3.3.2 Phy Registers

There are three categories of phy registers: 3.3.2.1 [Global Phy Control Registers], receiver lane control registers and transmitter lane control registers.

3.3.2.1 Global Phy Control Registers

Each global phy control register may have one instance per phy or two instances per phy (one per nibble). When a global register is implemented per phy the mapping to signal pins is shown in Table 67. When a global register is implemented per nibble the mapping to pins is shown in Table 67.

Table 67: Per phy register addresses to pin mappings

D0F0xE0[31:0]	Pin Names
0120_[2:0]xxxh	Gfx Links[7:0]: P_GFX_[T,R]X[P,N][7:0]
0220_[2:0]xxxh	Gfx Links[15:8]: P_GFX_[T,R]X[P,N][15:8]
0121_[2:0]xxxh	GPP Links: P_GPP_[T,R]X[P,N][7:0]
0122_[2:0]xxxh	FCH ports: DDI 0: DP0_TX[P,N][3:0] & P_UMI_[T,R]X[P,N][3:0]
0123_[2:0]xxxh	DDI 1: DP1_TX[P,N][3:0] & DDI 2: DP2_TX[P,N][3:0] &

Table 68: Per nibble register addresses to pin mappings

D0F0xE0[31:12]	Pin Names	
	Address N+1	Address N
0120_[2:0]xxxh	Graphics port lower: P_GFX_[T,R]X[P,N][7:4]	Graphics port lower: P_GFX_[T,R]X[P,N][3:0]
0220_[2:0]xxxh	Graphics port upper: P_GFX_[T,R]X[P,N][15:12]	Graphics port upper: P_GFX_[T,R]X[P,N][11:8]
0121_[2:0]xxxh	GPP ports: P_GPP_[T,R]X[P,N][7:4]	GPP ports: P_GPP_[T,R]X[P,N][3:0]
0122_[2:0]xxxh	DDI 0: DP0_TX[P,N][3:0]	FCH ports: P_UMI_[T,R]X[P,N][3:0]
0123_[2:0]xxxh	DDI 2: DP2_TX[P,N][3:0]	DDI 1: DP1_TX[P,N][3:0]

D0F0xE4_x0[220,123:120]_0000 Phy Compensation Control and Calibration Control I

This register provides general control of various circuits that perform auto-calibration.

Table 69: Index Mapping for D0F0xE4_x0[220,123:120]_0000

D0F0xE0[31:16]	D0F0xE0[15:0]
	0000h
0120h	Gfx Links[7:0]: P_GFX_[T,R]X[P,N][7:0]
0220h	Gfx Links[15:8]: P_GFX_[T,R]X[P,N][15:8]
0121h	GPP Links: P_GPP_[T,R]X[P,N][7:0]
0122h	FCH ports: DDI 0: DP0_TX[P,N][3:0] & P_UMI_[T,R]X[P,N][3:0]
0123h	DDI 1: DP1_TX[P,N][3:0] & DDI 2: DP2_TX[P,N][3:0] &

Bits	Description
31:28	Reserved.
27:23	**RttRawCal: receiver termination resistance (Rtt) raw calibration value**. Read-only. Reset: 0. This field provides the raw Rtt calibration value as determined by the compensation circuit.

22:18	**RonRawCal: transmitter resistance (Ron) raw calibration value**. Read-only. Reset: 0. This field provides the raw Ron calibration value as determined by the compensation circuit.
17:0	Reserved.

D0F0xE4_x0[220,123:120]_000[2:1] Phy Impedance Control

Updates to these registers that result in a change to impedance may not take effect in the phy for up to 2 micro-seconds after the update to this register completes.

Table 70: Recommended Ron settings

		D0F0xE4_x0[220,123:120]_000[2:1]	
Link Type		RonCtl	RonIndex
Display Port		0	0
HDMI		3	3
DVI		0	0
PCIe		0	0

Table 71: Index Mapping for D0F0xE4_x0[220,123:120]_000[2:1]

D0F0xE0[31:16]	D0F0xE0[15:0]	
	0002h	0001h
0120h	Graphics port lower: P_GFX_[T,R]X[P,N][7:4]	Graphics port lower: P_GFX_[T,R]X[P,N][3:0]
0220h	Graphics port upper: P_GFX_[T,R]X[P,N][15:12]	Graphics port upper: P_GFX_[T,R]X[P,N][11:8]
0121h	GPP ports: P_GPP_[T,R]X[P,N][7:4]	GPP ports: P_GPP_[T,R]X[P,N][3:0]
0122h	DDI 0: DP0_TX[P,N][3:0]	FCH ports: P_UMI_[T,R]X[P,N][3:0]
0123h	DDI 2: DP2_TX[P,N][3:0]	DDI 1: DP1_TX[P,N][3:0]

Bits	Description
31:29	**RttCtl: receiver termination resistance (Rtt) control**. Read-write. Reset: 0. Specifies how the receiver termination resistance value is calculated. All values between 00h and 1Fh are valid. Bits — Definition 000b — Rtt is as determined by the compensation circuit, D0F0xE4_x0[220,123:120]_0000[RttRawCal]. 001b — Rtt is (RttIndex - 3). 010b — Rtt is as specified by the difference: RttRawCal - RttIndex. If this results in a value that is less than 00h, then 00h is used. 011b — Rtt is as specified by the sum: RttRawCal + RttIndex. If this results in a value that is greater than 1Fh, then 1Fh is used. 100b — Enable only one tap of the Rtt resistor, as specified by RttIndex, and disable the base resistor that is normally always enabled. This is intended for testing purposes only. 111b-101b — Reserved. For all modes (except 100b), higher values reduce the resistance of Rtt and lower values increase the resistance of Rtt. See for more information about compensation. If RttCtl is programmed to either 011b or 100b, the value of RttRawCal + RttIndex must be less than or equal to 24.
28:21	Reserved.
20:16	**RttIndex: receiver termination resistance (Rtt) index**. Read-write. Reset: 0. See RttCtl.
15:13	**RonCtl: transmitter resistance (Ron) control**. Read-write. Reset: 0. BIOS: This field specifies how the transmitter resistance value is calculated. Bits — Definition 000b — Ron is as determined by the compensation circuit, D0F0xE4_x0[220,123:120]_0000[RonRawCal]. 001b — Ron is (RonIndex - 3). 010b — Ron is as specified by the difference: RonRawCal - RonIndex. If this results in a value that is less than 00h, then 00h is used. 011b — Ron is as specified by the sum: RonRawCal + RonIndex. If this results in a value that is greater than 1Fh, then 1Fh is used. 100b — Enable only one tap of the Ron resistor, as specified by RonIndex, and disable the base resistor that is normally always enabled. This is intended for testing purposes only. 111b-101b — Reserved. For all modes (except 100b), higher values reduce the resistance of Ron and lower values increase the resistance of Ron. If RonCtl is programmed to either 011b or 100b, the value of RonRawCal + RonIndex must be less than or equal to 23.
12:5	Reserved.
4:0	**RonIndex: transmitter resistance (Ron) index**. Read-write.Reset: 0. BIOS: See RonCtl.

D0F0xE4_x0[220,123:120]_000[C:B] Phy Serial Bus Packet Control

This register provides control to enable or disable various fields contained in the phy serial bus primary control

packet, the margining packet and the miscellaneous control packet.

Table 72: Index Mapping for D0F0xE4_x0[220,123:120]_000[C:B]

D0F0xE0[31:16]	D0F0xE0[15:0]	
	000Ch	000Bh
0120h	Graphics port lower: P_GFX_[T,R]X[P,N][7:4]	Graphics port lower: P_GFX_[T,R]X[P,N][3:0]
0220h	Graphics port upper: P_GFX_[T,R]X[P,N][15:12]	Graphics port upper: P_GFX_[T,R]X[P,N][11:8]
0121h	GPP ports: P_GPP_[T,R]X[P,N][7:4]	GPP ports: P_GPP_[T,R]X[P,N][3:0]
0122h	DDI 0: DP0_TX[P,N][3:0]	FCH ports: P_UMI_[T,R]X[P,N][3:0]
0123h	DDI 2: DP2_TX[P,N][3:0]	DDI 1: DP1_TX[P,N][3:0]

Bits	Description
31:18	Reserved.
17	**TxCoeffPktSbiEn**. Read-write. Reset: 1. 1=Enables the transmitter coefficient packet used for controlling transmitter the transmitter coefficient.
16	**RxEqPktSbiEn**. Read-write. Reset: 1. 1=Enables the receiver equalization packet used for controlling receiver equalization.
15	**PllCmpPktSbiEn**. Read-write. Reset: 1. 1=Enables the serial bus PLL component packet used for controlling PLL features such as mode of operation and power states.
14	**MargPktSbiEn**. Read-write. Reset: 1. 1=Enables the serial bus margining update packet used for controlling PCIe transmit margining test.
13:9	Reserved.
8	**EiDetSbiEn**. Read-write. Reset: 1. 1=Enables the electrical idle detector control field in the primary control packet.
7	**IncoherentClkSbiEn**. Read-write. Reset: 1. 1=Enables the incoherent clock control field in the primary control packet.
6	**SkipBitSbiEn**. Read-write. Reset: 1. 1=Enables the skip bit control field in the primary control packet.
5	**OffsetCancelSbiEn**. Read-write. Reset: 1. 1=Enables the offset cancellation control field in the primary control packet.
4	**DllLockSbiEn**. Read-write. Reset: 1. 1=Enables the DLL lock control field in the primary control packet.
3	**FreqDivSbiEn**. Read-write. Reset: 1. 1=Enables the frequency divider control field in the primary control packet.
2	**PcieModeSbiEn**. Read-write. Reset: 1. 1=Enables the phy mode control field in the primary control packet.
1	**RxPwrSbiEn**. Read-write. Reset: 1. 1=Enables the Rx power state control field in the primarycontrol packet.
0	**TxPwrSbiEn**. Read-write. Reset: 1. 1=Enables the Tx power state control field in the primary control packet.

3.3.2.2 Phy Receiver Lane Control Registers

Each receiver lane has a group of registers for controlling the operation of the lane. The mapping from address

register to receiver lane is shown in Table 73. Multiple receiver lanes may be written at the sametime using per nibble and per byte broadcast write addresses. The mapping from broadcast address to receiver lanes is shown in Table 74.

Table 73: Phy per receiver lane register addresses

Pin Group	D0F0xE0[31:16]	D0F0xE0[15:0]							
		438xh	430xh	428xh	420xh	418xh	410xh	408xh	400xh
P_GFX_	0120h	RX[P,N]7	RX[P,N]6	RX[P,N]5	RX[P,N]4	RX[P,N]3	RX[P,N]2	RX[P,N]1	RX[P,N]0
P_GFX_	0220h	RX[P,N]15	RX[P,N]14	RX[P,N]13	RX[P,N]12	RX[P,N]11	RX[P,N]10	RX[P,N]9	RX[P,N]8
P_GPP_	0121h	RX[P,N]7	RX[P,N]6	RX[P,N]5	RX[P,N]4	RX[P,N]3	RX[P,N]2	RX[P,N]1	RX[P,N]0
P_UMI_	0122h	-	-	-	-	RX[P,N]3	RX[P,N]2	RX[P,N]1	RX[P,N]0
P_DP1_	0123h	-	-	-	-	-	-	-	-
P_DP2_	0123h	-	-	-	-	-	-	-	-

Table 74: Phy receiver broadcast register addresses

D0F0xE0[31:16]	D0F0xE0[15:0]		
	57[1,0]xh	56[1,0]xh	50[1,0]xh
0120h	P_GFX_RX[P,N][7:4]	P_GFX_RX[P,N][3:0]	P_GFX_RX[P,N][7:0]
0220h	P_GFX_RX[P,N][15:12]	P_GFX_RX[P,N][11:8]	P_GFX_RX[P,N][15:8]
0121h	P_GPP_RX[P,N][7:4]	P_GPP_RX[P,N][3:0]	P_GPP_RX[P,N][7:0]
0122h	-	P_UMI_RX[P,N][3:0]	P_UMI_RX[P,N][3:0]
0123h	-	-	-

D0F0xE4_x0[220,123:120]_[5:4][7:6,3:0][8,0]2 Phy Receiver Phase Loop Filter Control

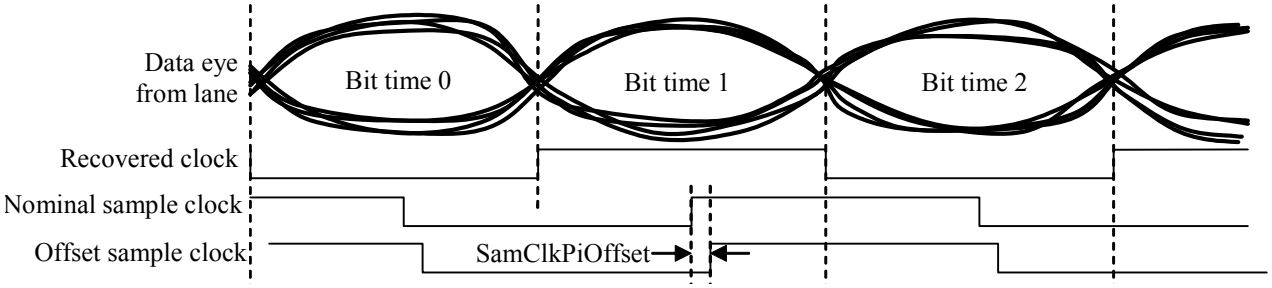

Figure 9: Phy recovered clock and sample clock

When the link is in a mode that relies on dynamic phase alignment (automatic sample-clock correction), then the processor generates a recovered clock for each lane based on transitions in the lane. The ideal recovered clock transitions at exactly the same time as the transitions in the lane. Phase detection logic detects if the recovered clock transitions before or after the lane transition. The digital loop filter (DLF) is logic that adjusts the phase of the recovered clock such that its transitions match the transition time of the lane as much as possible. The DLF counts the number of times the lane transitions before the recovered clock versus after to determine whether the recovered clock phase requires adjustment. The DLF uses an 8-bit counter, called the loop filter counter (LFC) for this purpose. The LFC controls are included in this register. They specify DLF behavior as follows:

- LfcMax is programmed to be greater than LfcMin.

- The LFC is initialized to LfcMin.
- The LFC is updated periodically. The logic keeps a tally of the number of lane transitions occurring before and after the recovered clock transition within each update period.
- To start, if there is a net lane transition occurs after the recovered clock transition within the update period, the LFC is incremented by the net value; on the other hand, if there is a net lane transition occurs before the recovered clock transition, the LFC is decremented. However, if the LFC is ever decremented while it is zero, these rules are reversed (and the LFC is incremented instead). Thus, if there is a phase correction needed, the LFC trends either upward or downward; if it trends downward, it hits zero and then trends upward again.
- If the LFC reaches LfcMax value, then (1) the phase of the recovered clock is adjusted in the appropriate direction, (2) the LFC is set to the LfcMin value.

The LfcMin and LfcMax fields are designed to improve the stability of the recovered clock phase while improving the response time for multiple phase updates in the same direction. For example, if the recovered clock phase needs several adjustments in the same direction, then the LFC increments until it hits LfcMax value and then be set to LfcMin (and trigger a phase adjustment); then it would increment to LfcMax value again to trigger the next phase adjustment. If, however, the next phase adjustment needs to be in the opposite direction, the LFC would decrement to zero, change direction, and then increment up to LfcMax again. In this way, phase adjustments in the same direction occur more quickly than phase adjustments in the opposite direction of the prior phase adjustment.

The nominal sample clock is offset by 90 degrees from the *recovered clock*.

Table 75: Index Mapping for D0F0xE4_x0[220,123:120]_[5:4][7:6,3:0][8,0]2

Pin Group	D0F0xE0[31:16]	D0F0xE0[15:0]							
		4382h	4302h	4282h	4202h	4182h	4102h	4082h	4002h
P_GFX_	0120h	RX[P,N]7	RX[P,N]6	RX[P,N]5	RX[P,N]4	RX[P,N]3	RX[P,N]2	RX[P,N]1	RX[P,N]0
P_GFX_	0220h	RX[P,N]15	RX[P,N]14	RX[P,N]13	RX[P,N]12	RX[P,N]11	RX[P,N]10	RX[P,N]9	RX[P,N]8
P_GPP_	0121h	RX[P,N]7	RX[P,N]6	RX[P,N]5	RX[P,N]4	RX[P,N]3	RX[P,N]2	RX[P,N]1	RX[P,N]0
P_UMI_	0122h	-	-	-	-	RX[P,N]3	RX[P,N]2	RX[P,N]1	RX[P,N]0
P_DP1_	0123h	-	-	-	-	-	-	-	-
P_DP2_	0123h	-	-	-	-	-	-	-	-

Table 76: Broadcast Mapping for D0F0xE4_x0[220,123:120]_[5:4][7:6,3:0][8,0]2

D0F0xE0[31:16]	D0F0xE0[15:0]		
	5702h	5602h	5002h
0120h	D0F0xE4_x0120_4[3:2][8,0]2	D0F0xE4_x0120_4[1:0][8,0]2	D0F0xE4_x0120_4[3:0][8,0]2
0220h	D0F0xE4_x0220_4[3:2][8,0]2	D0F0xE4_x0220_4[1:0][8,0]2	D0F0xE4_x0220_4[3:0][8,0]2
0121h	D0F0xE4_x0121_4[3:2][8,0]2	D0F0xE4_x0121_4[1:0][8,0]2	D0F0xE4_x0121_4[3:0][8,0]2
0122h	D0F0xE4_x0122_4[3:2][8,0]2	D0F0xE4_x0122_4[1:0][8,0]2	D0F0xE4_x0122_4[3:0][8,0]2
0123h	-	-	-

Bits	Description
31:30	Reserved.
29:22	**LfcMax: loop filter counter maximum value**. Read-write. Reset: 08h. BIOS: 08h.

21:14	**LfcMin: loop filter counter minimum value**. Read-write. Reset: 00h. BIOS: 00h.
13:0	Reserved.

D0F0xE4_x0[220,123:120]_[5:4][7:6,3:0][8,0]5 Phy Receiver Timing Margin Test

The built in jitter injection test mode is useful for checking the clock data recovery tracking bandwidth of the receiver. By forcing the sample clock to move from the lock position by a controlled amount and then observing the time it takes to recover, the tracking rate and bandwidth can be estimated. This register provides the control of the test mode.

The jitter injection test mode works as follows.

- The circuit is clocked by a jitter injection clock derived from dividing the link forwarded clock by 2.5; for example, if the link speed is 5.2GT/s and the link forwarded clock frequency is 2.6GHz, the jitter injection clock frequency becomes 1.04GHz.
- There are 2 phases, the on phase and the off phase. It starts with the on phase once the test mode is enabled.
- During the on phase, at every tick of jitter injection clock, the sample clock is moved away from the nominal lock position by 1/96*UI.
- The direction of adjustment is specified by JitterInjDir.
- The on phase adjustment continues for a number of times as specified by JitterInjOnCnt.
- Then the adjustment turns off for a duration specified by {JitterInjOffCnt, JitterInjOnCnt} * jitter injection clock period, this is known as the off phase. During this time, clock data recovery resumes to try to adjust the position of the sample clock back to the center of the data eye.
- The off phase is followed by the on phase again. The process continues to alternate between the on phase and the off phase until the jitter injection test mode is disabled.

In addition, the JitterInjHold bit may be set to inject a hold state at the end of the on phase. This stops clock data recovery from resuming after the on phase, hence holding the sample clock at its last adjusted position until the JitterInjHold bit is cleared. This test mode may be useful for margining the width of the input data eye.

This margining mechanism is not characterized for precision jitter adjustments or measurements.

Table 77: Index Mapping for D0F0xE4_x0[220,123:120]_[5:4][7:6,3:0][8,0]5

Pin Group	D0F0xE0[31:16]	D0F0xE0[15:0]							
		4385h	4305h	4285h	4205h	4185h	4105h	4085h	4005h
P_GFX_	0120h	RX[P,N]7	RX[P,N]6	RX[P,N]5	RX[P,N]4	RX[P,N]3	RX[P,N]2	RX[P,N]1	RX[P,N]0
P_GFX_	0220h	RX[P,N]15	RX[P,N]14	RX[P,N]13	RX[P,N]12	RX[P,N]11	RX[P,N]10	RX[P,N]9	RX[P,N]8
P_GPP_	0121h	RX[P,N]7	RX[P,N]6	RX[P,N]5	RX[P,N]4	RX[P,N]3	RX[P,N]2	RX[P,N]1	RX[P,N]0
P_UMI_	0122h	-	-	-	-	RX[P,N]3	RX[P,N]2	RX[P,N]1	RX[P,N]0
P_DP1_	0123h	-	-	-	-	-	-	-	-
P_DP2_	0123h	-	-	-	-	-	-	-	-

Table 78: Broadcast Mapping for D0F0xE4_x0[220,123:120]_[5:4][7:6,3:0][8,0]5

D0F0xE0[31:16]	D0F0xE0[15:0]		
	5705h	5605h	5005h
0120h	D0F0xE4_x0120_4[3:2][8,0]5	D0F0xE4_x0120_4[1:0][8,0]5	D0F0xE4_x0120_4[3:0][8,0]5
0220h	D0F0xE4_x0220_4[3:2][8,0]5	D0F0xE4_x0220_4[1:0][8,0]5	D0F0xE4_x0220_4[3:0][8,0]5
0121h	D0F0xE4_x0121_4[3:2][8,0]5	D0F0xE4_x0121_4[1:0][8,0]5	D0F0xE4_x0121_4[3:0][8,0]5

Table 78: Broadcast Mapping for D0F0xE4_x0[220,123:120]_[5:4][7:6,3:0][8,0]5

0122h	D0F0xE4_x0122_4[3:2][8,0]5	D0F0xE4_x0122_4[1:0][8,0]5	D0F0xE4_x0122_4[3:0][8,0]5
0123h	-	-	-

Bits	Description
31	Reserved.
30	**JitterInjEn: jitter injection enable**. Read-write. Reset: 0. 1=Jitter injection test mode is enabled.
29	**JitterInjDir: jitter injection direction**. Read-write. Reset: 0. Bits Definition 0 Move clock before the nominal lock position. 1 Move clock after the nominal lock position.
28:23	**JitterInjOnCnt: jitter injection on count**. Read-write. Reset: 0.
22:16	Reserved.
15:10	**JitterInjOffCnt: jitter injection off count**. Read-write. Reset: 0. The jitter injection off time count is a 12-bit code, this field specifies the most significant 6 bits. The least significant 6 bits are the same as JitterInjOnCnt.
9	**JitterInjHold: jitter injection hold**. Read-write. Reset: 0. 1=Jitter injection hold is enabled.
8:0	Reserved.

D0F0xE4_x0[220,123:120]_[5:4][7:6,3:0][8,0]6 Phy Receiver DFE and DFR Control

The processor supports decision feedback restore (DFR), a function that enables on-chip AC coupling on the receiver path, to improve the receiver's ability to operate over a longer channel. In this mode, the receiver on the processor must be programmed with the expected peak single-ended DC voltage level over the single-ended DC common mode voltage level, as seen by the receiver, when a static 1 or 0 is driven. For example, without deemphasis at nominal supply voltage of 1.2V, the peak single ended voltage is expected to be 300mV ideally above the single ended DC common mode voltage level. The value is dependent on the deemphasis setting of the transmitter on the other end of the channel.

Table 79: BIOS Recommendations for D0F0xE4_x0[220,123:120]_[5:4][7:6,3:0][8,0]6[VdcDac]

Far-device deemphasis setting	VdcDac
No deemphasis	4Dh
-2dB postcursor	3Dh
-3dB postcursor	36h
-5dB postcursor	2Bh
-6dB postcursor	27h
-7dB postcursor	22h
-8dB postcursor	1Fh
-9dB postcursor	1Bh
-11dB postcursor	16h

Decision feedback equalization (DFE) can be enabled to enhance link operation. Once enabled, the receiver uses the logic level of the previous data bit to adjust the voltage threshold of the sampler in the direction that causes the sampler to switch sooner when the data bit transitions to the opposite logic level for the next bit. The control and DFE voltage level are included in this register.

Table 80: Index Mapping for D0F0xE4_x0[220,123:120]_[5:4][7:6,3:0][8,0]6

Pin Group	D0F0xE0[31:16]	D0F0xE0[15:0]							
		4386h	4306h	4286h	4206h	4186h	4106h	4086h	4006h
P_GFX_	0120h	RX[P,N]7	RX[P,N]6	RX[P,N]5	RX[P,N]4	RX[P,N]3	RX[P,N]2	RX[P,N]1	RX[P,N]0
P_GFX_	0220h	RX[P,N]15	RX[P,N]14	RX[P,N]13	RX[P,N]12	RX[P,N]11	RX[P,N]10	RX[P,N]9	RX[P,N]8
P_GPP_	0121h	RX[P,N]7	RX[P,N]6	RX[P,N]5	RX[P,N]4	RX[P,N]3	RX[P,N]2	RX[P,N]1	RX[P,N]0
P_UMI_	0122h	-	-	-	-	RX[P,N]3	RX[P,N]2	RX[P,N]1	RX[P,N]0
P_DP1_	0123h	-	-	-	-	-	-	-	-
P_DP2_	0123h	-	-	-	-	-	-	-	-

Table 81: Broadcast Mapping for D0F0xE4_x0[220,123:120]_[5:4][7:6,3:0][8,0]6

D0F0xE0[31:16]	D0F0xE0[15:0]		
	5706h	5606h	5006h
0120h	D0F0xE4_x0120_4[3:2][8,0]6	D0F0xE4_x0120_4[1:0][8,0]6	D0F0xE4_x0120_4[3:0][8,0]6
0220h	D0F0xE4_x0220_4[3:2][8,0]6	D0F0xE4_x0220_4[1:0][8,0]6	D0F0xE4_x0220_4[3:0][8,0]6
0121h	D0F0xE4_x0121_4[3:2][8,0]6	D0F0xE4_x0121_4[1:0][8,0]6	D0F0xE4_x0121_4[3:0][8,0]6
0122h	D0F0xE4_x0122_4[3:2][8,0]6	D0F0xE4_x0122_4[1:0][8,0]6	D0F0xE4_x0122_4[3:0][8,0]6
0123h	-	-	-

Bits	Description
31:9	Reserved.
8	**DfeEn: DFE enable**. Read-write. Reset: 0. 1=Decision feedback equalization is enabled.
7	Reserved.
6:5	**DfeVoltage: DFE offset voltage level**. Read-write. Reset: 0. This field specifies the magnitude of the DFE offset voltage. Bits Definition — Bits Definition 00b DFE offset voltage=25mV. — 10b DFE offset voltage=12.5mV. 01b DFE offset voltage=0mV. — 11b DFE offset voltage=31.25mV.
4:0	Reserved.

D0F0xE4_x0[220,123:120]_[5:4][7:6,3:0][8,0]A Phy DLL Test and Control 3

Table 82: Index Mapping for D0F0xE4_x0[220,123:120]_[5:4][7:6,3:0][8,0]A

Pin Group	D0F0xE0[31:16]	D0F0xE0[15:0]							
		438Ah	430Ah	428Ah	420Ah	418Ah	410Ah	408Ah	400Ah
P_GFX_	0120h	RX[P,N]7	RX[P,N]6	RX[P,N]5	RX[P,N]4	RX[P,N]3	RX[P,N]2	RX[P,N]1	RX[P,N]0
P_GFX_	0220h	RX[P,N]15	RX[P,N]14	RX[P,N]13	RX[P,N]12	RX[P,N]11	RX[P,N]10	RX[P,N]9	RX[P,N]8
P_GPP_	0121h	RX[P,N]7	RX[P,N]6	RX[P,N]5	RX[P,N]4	RX[P,N]3	RX[P,N]2	RX[P,N]1	RX[P,N]0
P_UMI_	0122h	-	-	-	-	RX[P,N]3	RX[P,N]2	RX[P,N]1	RX[P,N]0
P_DP1_	0123h	-	-	-	-	-	-	-	-
P_DP2_	0123h	-	-	-	-	-	-	-	-

Table 83: Broadcast Mapping for D0F0xE4_x0[220,123:120]_[5:4][7:6,3:0][8,0]A

D0F0xE0[31:16]	D0F0xE0[15:0]		
	570Ah	560Ah	500Ah
0120h	D0F0xE4_x0120_4[3:2][8,0]A	D0F0xE4_x0120_4[1:0][8,0]A	D0F0xE4_x0120_4[3:0][8,0]A
0220h	D0F0xE4_x0220_4[3:2][8,0]A	D0F0xE4_x0220_4[1:0][8,0]A	D0F0xE4_x0220_4[3:0][8,0]A
0121h	D0F0xE4_x0121_4[3:2][8,0]A	D0F0xE4_x0121_4[1:0][8,0]A	D0F0xE4_x0121_4[3:0][8,0]A
0122h	D0F0xE4_x0122_4[3:2][8,0]A	D0F0xE4_x0122_4[1:0][8,0]A	D0F0xE4_x0122_4[3:0][8,0]A
0123h	-	-	-

Bits	Description
31:18	Reserved.
17	**DllLockFastModeEn: DLL lock fast mode enable**. Read-write. Reset: 0. 1=Enables DLL lock fast mode. 0=DLL lock operates at standard speed.
16:15	Reserved.
14:13	**AnalogWaitTime: analog wait time to turn on DLL**. Read-write. Reset: 0. The turning on of the DLL circuit after cold reset is delayed by a timer specified by this field. The encodings are as follows: Bits Definition Bits Definition 00b Delay=1.25us. 10 b Delay=2.5us. 01b Delay=0.625us. 1 1b Delay=0.3125us.
12:0	Reserved.

3.3.2.3 Phy Transmitter Lane Control Registers

Each transmitter lane has a group of registers for controlling the operation of the lane. The mapping from address register to transmitter lane is shown in Table 84. Multiple transmitter lanes may be written at the same time using per nibble and per byte broadcast write addresses. The mapping from broadcast address to transmitter lanes is shown in Table 85.

Table 84: Phy per transmitter lane register addresses

Pin Group	D0F0xE0[31:16]	D0F0xE0[15:0]							
		638xh	630xh	628xh	620xh	618xh	610xh	608xh	600xh
P_GFX_	0120h	TX[P,N]7	TX[P,N]6	TX[P,N]5	TX[P,N]4	TX[P,N]3	TX[P,N]2	TX[P,N]1	TX[P,N]0
P_GFX_	0220h	TX[P,N]15	TX[P,N]14	TX[P,N]13	TX[P,N]12	TX[P,N]11	TX[P,N]10	TX[P,N]9	TX[P,N]8
P_GPP_	0121h	TX[P,N]7	TX[P,N]6	TX[P,N]5	TX[P,N]4	TX[P,N]3	TX[P,N]2	TX[P,N]1	TX[P,N]0
P_UMI_	0122h	-	-	-	-	TX[P,N]3	TX[P,N]2	TX[P,N]1	TX[P,N]0
P_DP0_	0122h	TX[P,N]3	TX[P,N]2	TX[P,N]1	TX[P,N]0	-	-	-	-
P_DP1_	0123h	-	-	-	-	TX[P,N]3	TX[P,N]2	TX[P,N]1	TX[P,N]0
P_DP2_	0123h	TX[P,N]3	TX[P,N]2	TX[P,N]1	TX[P,N]0	-	-	-	-

Table 85: Phy transmitter broadcast register addresses

D0F0xE0[31:16]	D0F0xE0[15:0]		
	77[1,0]xh	76[1,0]xh	70[1,0]xh

Table 85: Phy transmitter broadcast register addresses

0120h	P_GFX_TX[P,N][7:4]	P_GFX_TX[P,N][3:0]	P_GFX_TX[P,N][7:0]
0220h	P_GFX_TX[P,N][15:12]	P_GFX_TX[P,N][11:8]	P_GFX_TX[P,N][15:8]
0121h	P_GPP_TX[P,N][7:4]	P_GPP_TX[P,N][3:0]	P_GPP_TX[P,N][7:0]
0122h	P_DP0_TX[P,N][3:0]	P_UMI_TX[P,N][3:0]	P_UMI_TX[P,N][3:0]
0123h	P_DP2_TX[P,N][3:0]	P_DP1_TX[P,N][3:0]	P_DP[2:1]_TX[P,N][3:0]

D0F0xE4_x0[220,123:120]_[7:6][7:6,3:0][8,0]0 Phy Tx Deemphasis and Margining Control

Table 86: Index Mapping for D0F0xE4_x0[220,123:120]_[7:6][7:6,3:0][8,0]0

Pin Group	D0F0xE0[31:16]	D0F0xE0[15:0]							
		6380h	6300h	6280h	6200h	6180h	6100h	6080h	6000h
P_GFX_	0120h	TX[P,N]7	TX[P,N]6	TX[P,N]5	TX[P,N]4	TX[P,N]3	TX[P,N]2	TX[P,N]1	TX[P,N]0
P_GFX_	0220h	TX[P,N]15	TX[P,N]14	TX[P,N]13	TX[P,N]12	TX[P,N]11	TX[P,N]10	TX[P,N]9	TX[P,N]8
P_GPP_	0121h	TX[P,N]7	TX[P,N]6	TX[P,N]5	TX[P,N]4	TX[P,N]3	TX[P,N]2	TX[P,N]1	TX[P,N]0
P_UMI_	0122h	-	-	-	-	TX[P,N]3	TX[P,N]2	TX[P,N]1	TX[P,N]0
P_DP0_	0122h	TX[P,N]3	TX[P,N]2	TX[P,N]1	TX[P,N]0	-	-	-	-
P_DP1_	0123h	-	-	-	-	TX[P,N]3	TX[P,N]2	TX[P,N]1	TX[P,N]0
P_DP2_	0123h	TX[P,N]3	TX[P,N]2	TX[P,N]1	TX[P,N]0	-	-	-	-

Table 87: Broadcast Mapping for D0F0xE4_x0[220,123:120]_[7:6][7:6,3:0][8,0]0

D0F0xE0[31:16]	D0F0xE0[15:0]		
	7700h	7600h	7000h
0120h	D0F0xE4_x0120_6[3:2][8,0]0	D0F0xE4_x0120_6[1:0][8,0]0	D0F0xE4_x0120_6[3:0][8,0]0
0220h	D0F0xE4_x0220_6[3:2][8,0]0	D0F0xE4_x0220_6[1:0][8,0]0	D0F0xE4_x0220_6[3:0][8,0]0
0122h	D0F0xE4_x0122_6[3:2][8,0]0	D0F0xE4_x0122_6[1:0][8,0]0	D0F0xE4_x0122_6[3:0][8,0]0
0122h	D0F0xE4_x0122_6[3:2][8,0]0	D0F0xE4_x0122_6[1:0][8,0]0	D0F0xE4_x0122_6[3:0][8,0]0
0123h	D0F0xE4_x0123_6[3:2][8,0]0	D0F0xE4_x0123_6[1:0][8,0]0	D0F0xE4_x0123_6[3:0][8,0]0

Bits	Description
31:16	Reserved.
15	**DisLoImpIdle: disable low impedance idle**. Read-write. Reset: 0. 1=Disables the low impedance electrical idle feature that requires both the true and complement pins of the transmitter to be pulled to VDDP/2 via low impedance termination in the range of 25 to 50 ohm upon entering electrical idle state. Instead, 5k ohm termination is used. 0=Enables low impedance electrical idle mode.
14:8	Reserved.
7	**TxLs23ClkGateEn: LS2/LS3 clock gating enable**. Read-write. Reset: 1. 1=Internal phy clock grids are gated during LS2 or PHY OFF states to save power.
6:4	Reserved.

3	**Post2Sign: Post-cursor 2 Sign**. Read-write. Cold-reset: 0. 1=Increases output voltage strength. 0=Lowers output voltage strength.
2:0	Reserved.

D0F0xE4_x0[220,123:120]_[7:6][7:6,3:0][8,0]6 Phy Transmit Nominal Deemphasis Control

This register specifies the deemphasis, or preemphasis settings in the case of display port mode, and voltage margining settings for the transmit drivers.

Table 88: Recommended preemphasis settings

Conditions			D0F0xE4_x0[220,123:120]_[7:6][7:6,3:0][8,0]6	
Link Type	Preemphasis	Peak-to-peak Voltage	DeemphGen1Nom	TxMarginNom
Display Port	0dB	1.2V	0	0
		0.8V	0	25
		0.6V	0	58
		0.4V	0	75
	3.5dB	0.8V	40	0
		0.6V	34	24
		0.4V	25	50
	6dB	0.6V	62	0
		0.4V	46	34
	9.5dB	0.4V	75	0
HDMI	-		30	0
DVI	-		11	0
PCIe	-		42	0

Table 89: Index Mapping for D0F0xE4_x0[220,123:120]_[7:6][7:6,3:0][8,0]6

Pin Group	D0F0xE0[31:16]	D0F0xE0[15:0]							
		6386h	6306h	6286h	6206h	6186h	6106h	6086h	6006h
P_GFX_	0120h	TX[P,N]7	TX[P,N]6	TX[P,N]5	TX[P,N]4	TX[P,N]3	TX[P,N]2	TX[P,N]1	TX[P,N]0
P_GFX_	0220h	TX[P,N]15	TX[P,N]14	TX[P,N]13	TX[P,N]12	TX[P,N]11	TX[P,N]10	TX[P,N]9	TX[P,N]8
P_GPP_	0121h	TX[P,N]7	TX[P,N]6	TX[P,N]5	TX[P,N]4	TX[P,N]3	TX[P,N]2	TX[P,N]1	TX[P,N]0
P_UMI_	0122h	-	-	-	-	TX[P,N]3	TX[P,N]2	TX[P,N]1	TX[P,N]0
P_DP0_	0122h	TX[P,N]3	TX[P,N]2	TX[P,N]1	TX[P,N]0	-	-	-	-
P_DP1_	0123h	-	-	-	-	TX[P,N]3	TX[P,N]2	TX[P,N]1	TX[P,N]0
P_DP2_	0123h	TX[P,N]3	TX[P,N]2	TX[P,N]1	TX[P,N]0	-	-	-	-

Table 90: Broadcast Mapping for D0F0xE4_x0[220,123:120]_[7:6][7:6,3:0][8,0]6

D0F0xE0[31:16]	D0F0xE0[15:0]		
	7706h	7606h	7006h
0120h	D0F0xE4_x0120_6[3:2][8,0]6	D0F0xE4_x0120_6[1:0][8,0]6	D0F0xE4_x0120_6[3:0][8,0]6

Table 90: Broadcast Mapping for D0F0xE4_x0[220,123:120]_[7:6][7:6,3:0][8,0]6

0220h	D0F0xE4_x0220_6[3:2][8,0]6	D0F0xE4_x0220_6[1:0][8,0]6	D0F0xE4_x0220_6[3:0][8,0]6
0122h	D0F0xE4_x0122_6[3:2][8,0]6	D0F0xE4_x0122_6[1:0][8,0]6	D0F0xE4_x0122_6[3:0][8,0]6
0122h	D0F0xE4_x0122_6[3:2][8,0]6	D0F0xE4_x0122_6[1:0][8,0]6	D0F0xE4_x0122_6[3:0][8,0]6
0123h	D0F0xE4_x0123_6[3:2][8,0]6	D0F0xE4_x0123_6[1:0][8,0]6	D0F0xE4_x0123_6[3:0][8,0]6

Bits	Description
31:16	Reserved.
15:8	**DeemphGen1Nom**. Read-write. Reset: 42. BIOS: Table 88. This field specifies the post cursor deemphasis setting. Value must be less than or equal to 104.
7:0	**TxMarginNom**. Read-write. Reset: 0. BIOS: Table 88. This field specifies the voltage margining setting of the transmit driver. Value must be less than or equal to 104.

D0F0xE4_x0[220,123:120]_[F:E][7:0][8,0]6 Phy Transmit Link Configuration

Table 91: BIOS Recommendations for GangedModeEn, IsOwnMstr

Link configuration	GangedModeEn	IsOwnMstr
x1 (1 lane per sublink)	0	1
x2 (2 lanes per sublink)	0	1
x4 (4 lanes per sublink)	0	0
x8	1	0

Table 92: Index Mapping for D0F0xE4_x0[220,123:120]_[F:E][7:0][8,0]6

Pin Group	D0F0xE0[31:16]	D0F0xE0[15:0]							
		E386h	E306h	E286h	E206h	E186h	E106h	E086h	E006h
P_GFX_	0120h	TX[P,N]7	TX[P,N]6	TX[P,N]5	TX[P,N]4	TX[P,N]3	TX[P,N]2	TX[P,N]1	TX[P,N]0
P_GFX_	0220h	TX[P,N]15	TX[P,N]14	TX[P,N]13	TX[P,N]12	TX[P,N]11	TX[P,N]10	TX[P,N]9	TX[P,N]8
P_GPP_	0121h	TX[P,N]7	TX[P,N]6	TX[P,N]5	TX[P,N]4	TX[P,N]3	TX[P,N]2	TX[P,N]1	TX[P,N]0
P_UMI_	0122h	-	-	-	-	TX[P,N]3	TX[P,N]2	TX[P,N]1	TX[P,N]0
P_DP0_	0122h	TX[P,N]3	TX[P,N]2	TX[P,N]1	TX[P,N]0	-	-	-	-
P_DP1_	0123h	-	-	-	-	TX[P,N]3	TX[P,N]2	TX[P,N]1	TX[P,N]0
P_DP2_	0123h	TX[P,N]3	TX[P,N]2	TX[P,N]1	TX[P,N]0	-	-	-	-

Table 93: Broadcast Mapping for D0F0xE4_x0[220,123:120]_[F:E][7:0][8,0]6

D0F0xE0[31:16]	D0F0xE0[15:0]		
	F706h	F606h	F006h
0120h	D0F0xE4_x0120_E[3:2][8,0]6	D0F0xE4_x0120_E[1:0][8,0]6	D0F0xE4_x0120_E[3:0][8,0]6
0220h	D0F0xE4_x0220_E[3:2][8,0]6	D0F0xE4_x0220_E[1:0][8,0]6	D0F0xE4_x0220_E[3:0][8,0]6
0122h	D0F0xE4_x0122_E[3:2][8,0]6	D0F0xE4_x0122_E[1:0][8,0]6	D0F0xE4_x0122_E[3:0][8,0]6
0122h	D0F0xE4_x0122_E[3:2][8,0]6	D0F0xE4_x0122_E[1:0][8,0]6	D0F0xE4_x0122_E[3:0][8,0]6
0123h	D0F0xE4_x0123_E[3:2][8,0]6	D0F0xE4_x0123_E[1:0][8,0]6	D0F0xE4_x0123_E[3:0][8,0]6

Bits	Description
31:8	Reserved.
7:5	**RdptInitMode**. Read-write. Cold-reset: 0. Sets the read-pointer init mode. Bits — Description 000b — x1 enabled 001b — x2 enabled 010b — x4 enabled 011b — x8 enabled 100b — x16 enabled 111b-101b — Disable all enables
4	Reserved.
3	**IncoherentCkDet**. Read-write. Reset: 0. 1=Indicates lane is in incoherent clock mode.
2	**IsOwnMstr**. Read-write. Reset: 0. BIOS: Table 91. 1=Enables the lane to self initialize its own read pointer.
1	Reserved
0	**GangedModeEn**. Read-write. Reset: 1. BIOS: Table 91. 1=Enables link ganged mode. 0=Disables link ganged mode.

3.3.3 Wrapper Registers

Table 94: Mapping for wrapper registers

D0F0xE0[31:16]	Wrapper	Port Description
0130h	PGD	Gfx+Display
0131h	PPD	GPP+Display
0132h	PSD	FCH+Display
0133h	DDI	Display

D0F0xE4_x013[2:0]_0046 Subsystem and Vendor ID

Bits	Description
31:16	**SubsystemID: subystem id**. Read-write. Reset: 1234h. Specifies the value returned by D[4:2]F[5:1]xB4[SubsystemID].
15:0	**SubsystemVendorID: subsystem vendor id**. Read-write. Reset: 1022h. Specifies the value returned by D[4:2]F[5:1]xB4[SubsystemVendorID].

D0F0xE4_x013[2:0]_0080 Link Configuration

Reset: 0000_0000h.

Bits	Description
31:4	Reserved.
3:0	**StrapBifLinkConfig**. Read-write; strap. Reset: Product-specific. BIOS: See Table 42 and Table 44. Bits Definition — Bits Definition 0000b x16 IO Link (Gfx Only) — 0100b 4 x1 IO Links (GPPFCH Only) 0001b x4 IO Link (GPPFCH Only) — 0101b 2 x8 IO Links (Gfx Only) 0010b 2 x2 IO Links (GPPFCH Only) — 011xb Reserved 0011b 1 x2 IO Link, 2 x1 IO Links (GPPFCH Only) — 1xxxb Reserved

D0F0xE4_x013[2:0]_0[C:8]00 Link Hold Training Control

Table 95: Index address mapping for D0F0xE4_x013[2:0]_0[C:8]00

Index	Function	Index	Function	Index	Function
0130_0800h	PGD PortA	0131_0800h	PPD PortA	0132_0800h	PSD PortA
0130_0900h	PGD PortB	0131_0900h	PPD PortB	0132_0900h	PSD PortB
-	-	0131_0A00h	PPD PortC	0132_0A00h	PSD PortC
-	-	0131_0B00h	PPD PortD	0132_0B00h	PSD PortD
-	-	0131_0C00h	PPD PortE	0132_0C00h	PSD PortE

Bits	Description
31:1	Reserved.
0	**HoldTraining: hold link training**. Read-write. Reset: 1. 1=Hold training on link.

D0F0xE4_x013[2:0]_0[C:8]03 Link Deemphasis Control

Table 96: Index address mapping for D0F0xE4_x013[2:0]_0[C:8]03

Index	Function	Index	Function	Index	Function
0130_0803h	PGD PortA	0131_0803h	PPD PortA	0132_0803h	PSD PortA
0130_0903h	PGD PortB	0131_0903h	PPD PortB	0132_0903h	PSD PortB
-	-	0131_0A03h	PPD PortC	0132_0A03h	PSD PortC
-	-	0131_0B03h	PPD PortD	0132_0B03h	PSD PortD
-	-	0131_0C03h	PPD PortE	0132_0C03h	PSD PortE

Bits	Description
31:6	Reserved.
5	**StrapBifDeemphasisSel**. Read-write; strap. Reset: 1. Controls the default value of D[4:2]F[5:1]x88[SelectableDeemphasis]. 1=RC advertises -3.5dB. 0=RC advertises -6dB.
4:0	Reserved.

D0F0xE4_x013[3:0]_8002 IO Link Wrapper Scratch

Cold reset: 0000_0000h.

Bits	Description
31:0	**PcieWrapScratch: Scratch**. Read-write.

D0F0xE4_x013[3:0]_8011 Link Transmit Clock Gating Control

Bits	Description
31:26	Reserved.
25	Reserved.
24	**TxclkLcntGateEnable**. Read-write. Reset: 0. BIOS: 1. 1=Enable clock gating the lane counter.
23	**DebugBusClkEnable**. Read-write. Reset: 1. BIOS: 0. 1=Enable the debug bus clock.
22:17	**TxclkPermGateLatency**. Read-write. Reset: 3Fh. Specifies the number of clocks to wait after detecting an entry into L1 before gating off the permanent clock branches.
16	**RcvrDetClkEnable**. Read-write. Reset: 0. 1=Enable the receiver detect clock.
15:10	**TxclkRegsGateLatency**. Read-write. Reset: 3Fh. Specifies the number of clocks to wait after idle is signalled before gating off the register clock branch.
9	**TxclkRegsGateEnable**. Read-write. Reset: 0. BIOS: 1. 1=Enable clock gating the register clock.
8	**TxclkPermStop**. Read-write. Reset: 0. 1=All transmitter clocks disabled. This bit should only be set if all links associated with the PCIe core are unconnected.

7	**TxclkDynGateEnable**. Read-write. Reset: 0. BIOS: 1. 1=Dynamic clock gating enabled. 0=Dynamic clock gating disabled.
6	**TxclkPermGateEven**. Read-write. Reset: 1. 1=Gate the permanent clock branches for an even number of clocks.
5:0	**TxclkDynGateLatency**. Read-write. Reset: 3Fh. Specifies the number of clocks to wait after idle is signalled before gating off the dynamic clock branch.

D0F0xE4_x013[3:0]_8012 Link Idle-Resume Clock Gating Control

Bits	Description
31:14	Reserved.
13:8	**Pif1xIdleResumeLatency**. Read-write. Reset: 00_0111b. Specifies the number of clocks to wait after enabling TXCLK1X_PIF before sending the acknowledge.
7	**Pif1xIdleGateEnable**. Read-write. Reset: 0. BIOS: 1. 1=Enable idle resume gating of TXCLK1X_PIF.
6	Reserved.
5:0	**Pif1xIdleGateLatency**. Read-write. Reset: 00_0001b. Specifies the number of clocks to wait before turning off TXCLK1X_PIF.

D0F0xE4_x013[3:0]_8013 Transmit Clock Pll Control

Reset: 0000_0001h.

Table 97: Reserved field mappings for D0F0xE4_x013[3:0]_8013

Register	Bits			
	31:24	12:11	7:6	3:2
D0F0xE4_x0130_8013	-	-	-	-
D0F0xE4_x0131_8013	Reserved	Reserved	Reserved	Reserved
D0F0xE4_x0132_8013	Reserved	Reserved	Reserved	Reserved
D0F0xE4_x0133_8013	Reserved	Reserved	Reserved	Reserved

Bits	Description
31	**TxclkSelDigDOverride**. Read-write. 1=Override TXCLK_DIGD selection.
30:28	**TxclkSelDigD**. Read-write. Select clock from PLL A, B, C, D.
27	**TxclkSelDigCOverride**. Read-write. 1=Override TXCLK_DIGC selection.
26:24	**TxclkSelDigC**. Read-write. Select clock from PLL A, B, C, D.
23	**TxclkSelDigBOverride**. Read-write. 1=Override TXCLK_DIGB selection.
22:20	**TxclkSelDigB**. Read-write. Select clock from PLL A, B, C, D.
19	**TxclkSelDigAOverride**. Read-write. 1=Override TXCLK_DIGA selection.
18:16	**TxclkSelDigA**. Read-write. Select clock from PLL A, B, C, D.
15:13	Reserved.
12	**TxclkSelPifDOverride**. Read-write.1=Override TxclkPifD selection.

11	**TxclkSelPifCOverride**. Read-write. 1=Override TxclkPifC selection.
10	**TxclkSelPifBOverride**. Read-write. 1=Override TxclkPifB selection.
9	**TxclkSelPifAOverride**. Read-write. 1=Override TxclkPifA selection.
8	**TxclkSelCoreOverride**. Read-write. 1=Override TxclkCore selection.
7	**ClkDividerResetOverrideD**. Read-write. 1=Force clock divider D enabled.
6	**ClkDividerResetOverrideC**. Read-write. 1=Force clock divider C enabled.
5	**ClkDividerResetOverrideB**. Read-write. 1=Force clock divider B enabled.
4	**ClkDividerResetOverrideA**. Read-write. 1=Force clock divider A enabled.
3	**MasterPciePllD**. Read-write. 1=Pll D is the master source for all PCIe transmitter clock branches.
2	**MasterPciePllC**. Read-write. 1=Pll C is the master source for all PCIe transmitter clock branches.
1	**MasterPciePllB**. Read-write. 1=Pll B is the master source for all PCIe transmitter clock branches.
0	**MasterPciePllA**. Read-write. 1=Pll A is the master source for all PCIe transmitter clock branches.

D0F0xE4_x013[3:0]_8014 Link Transmit Clock Gating Control 2

Reset: 0000_0000h.

Table 98: Reserved field mappings for D0F0xE4_x013[3:0]_8014

Register	Bits					
	27	26	15	14	5	4
D0F0xE4_x0130_8014	-	-	-	-	-	-
D0F0xE4_x0131_8014	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved
D0F0xE4_x0132_8014	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved
D0F0xE4_x0133_8014	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved

Bits	Description
31:28	**SpareRegRw**. Read-write. Spare register.
27	**DdiDigdGateEnable**. Read-write. 1=Enable gating of the DIG D clock branch in DDI mode.
26	**DdiDigcGateEnable**. Read-write. 1=Enable gating of the DIG C clock branch in DDI mode.
25	**DdiDigbGateEnable**. Read-write. 1=Enable gating of the DIG B clock branch in DDI mode.
24	**DdiDigaGateEnable**. Read-write. 1=Enable gating of the DIG A clock branch in DDI mode.
23:21	Reserved.
20	**TxclkPermGateOnlyWhenPllPwrDn**. Read-write. BIOS: 1. 1=Gating of the permanent clock branch only occurs when the PLL is powered down.
19:16	Reserved.
15	**PcieGatePifD1xEnable**. Read-write. BIOS: 1. 1=Enable gating of the PIF D 1x clock branches in PCIe mode.

14	**PcieGatePifC1xEnable**. Read-write. BIOS: 1. 1=Enable gating of the PIF C 1x clock branches in PCIe mode.
13	**PcieGatePifB1xEnable**. Read-write. BIOS: 1. 1=Enable gating of the PIF B 1x clock branches in PCIe mode.
12	**PcieGatePifA1xEnable**. Read-write. BIOS: 1. 1=Enable gating of the PIF A 1x clock branches in PCIe mode.
11:6	Reserved.
5	**DdiPifd1xGateEnable**. Read-write. 1=Enable gating of the PIF D 1x clock branch in DDI mode.
4	**DdiPifc1xGateEnable**. Read-write. 1=Enable gating of the PIF C 1x clock branch in DDI mode.
3	**DdiPifb1xGateEnable**. Read-write. 1=Enable gating of the PIF B 1x clock branch in DDI mode.
2	**DdiPifa1xGateEnable**. Read-write. 1=Enable gating of the PIF A 1x clock branches in DDI mode.
1	**TxclkPrbsGateEnable**. Read-write. BIOS: 1. 1=Enable gating of the PRBS clock branch.
0	**TxclkPermGateEnable**. Read-write. BIOS: 1. 1=Enable gating of the permanent clock branch.

D0F0xE4_x013[3:0]_8015 IO Link IOC Control

Bits	Description
31:24	Reserved.
23	**RefclkRegsGateEnable**. Read-write. Reset: 0. BIOS: 1. 1=Enable gating of REFCLK_REGS.
22	Reserved.
21:16	**RefclkRegsGateLatency**. Read-write. Reset: 3Fh. Specifies the number of clocks to wait before turning off REFCLK_REGS.
15:0	Reserved.

D0F0xE4_x013[3:0]_8016 Link Clock Switching Control

Reset: 003F_001Fh.

Bits	Description
31:24	Reserved.
23	**LclkDynGateEnable**. Read-write. 1=Enable LCLK_DYN clock gating.
22	**LclkGateFree**. Read-write. IF (REG==D0F0xE4_x013[1:0]_8016) THEN BIOS: 1. ENDIF. 1=LCLK gating is controlled independent of TXCLK gating.
21:16	**LclkDynGateLatency**. Read-write. Specifies the number of clocks to wait before turning off LCLK_DYN.

15:6	Reserved.
5:0	**CalibAckLatency**. Read-write. BIOS: IF (REG==D0F0xE4_x0132_8016) THEN 0. ELSE 1Fh. ENDIF. Specifies the number of clocks after calibration is complete before the acknowledge signal is asserted.

D0F0xE4_x013[3:0]_802[4:1] Transmitter Lane Mux

Table 99: Lane index addresses for D0F0xE4_x013[3:0]_802[4:1]

D0F0xE0[31:4]	D0F0xE0[3:0]			
	4h	3h	2h	1h
0130_802h	Lanes[15:12]	Lanes[11:8]	Lanes[7:4]	Lanes[3:0]
0131_802h	Lanes[15:12]	Lanes[11:8]	Lanes[7:4]	Lanes[3:0]
0132_802h	Lanes[15:12]	Lanes[11:8]	Lanes[7:4]	Lanes[3:0]
0133_802h	Lanes[15:12]	Lanes[11:8]	Lanes[7:4]	Lanes[3:0]

Table 100: Reset Mapping for D0F0xE4_x013[3:0]_802[4:1]

Register	Reset
D0F0xE4_x013[3:0]_8024	0F0E_0D0Ch
D0F0xE4_x013[3:0]_8023	0B0A_0908h
D0F0xE4_x013[3:0]_8022	0706_0504h
D0F0xE4_x013[3:0]_8021	0302_0100h

Table 101: Field mapping for D0F0xE4_x013[3:0]_802[4:1]

Register	Bits			
	31:24	23:16	15:8	7:0
D0F0xE4_x013[3:0]_8024	TXLane15	TXLane14	TXLane13	TXLane12
D0F0xE4_x013[3:0]_8023	TXLane11	TXLane10	TXLane9	TXLane8
D0F0xE4_x013[3:0]_8022	TXLane7	TXLane6	TXLane5	TXLane4
D0F0xE4_x013[3:0]_8021	TXLane3	TXLane2	TXLane1	TXLane0

Bits	Description
31:24	**TXLane**. Read-write. Specifies the controller lanes that are mapped to TX lane n of the PIF. See: D0F0xE4_x013[3:0]_802[4:1][7:0].
23:16	**TXLane**. Read-write. Specifies the controller lanes that are mapped to TX lane n of the PIF. See: D0F0xE4_x013[3:0]_802[4:1][7:0].

15:8	**TXLane**. Read-write. Specifies the controller lanes that are mapped to TX lane n of the PIF. See: D0F0xE4_x013[3:0]_802[4:1][7:0].
7:0	**TXLane**. Read-write. Specifies the controller lanes that are mapped to TX lane n of the PIF. Bits Definition Bits Definition 0h Controller lane 0. 8h Controller lane 8. 1h Controller lane 1. 9h Controller lane 9. 2h Controller lane 2. 10h Controller lane 10. 3h Controller lane 3. 11h Controller lane 11. 4h Controller lane 4. 12h Controller lane 12. 5h Controller lane 5. 13h Controller lane 13. 6h Controller lane 6. 14h Controller lane 14. 7h Controller lane 7. 15h Controller lane 15.

D0F0xE4_x013[3:0]_802[8:5] Receiver Lane Mux

Reset: 0302_0100h.

Table 102: Lane index addresses for D0F0xE4_x013[3:0]_802[8:5]

D0F0xE0[31:4]	D0F0xE0[3:0]			
	8h	7h	6h	5h
0130_802h	Lanes[15:12]	Lanes[11:8]	Lanes[7:4]	Lanes[3:0]
0131_802h	Lanes[15:12]	Lanes[11:8]	Lanes[7:4]	Lanes[3:0]
0132_802h	Lanes[15:12]	Lanes[11:8]	Lanes[7:4]	Lanes[3:0]
0133_802h	Lanes[15:12]	Lanes[11:8]	Lanes[7:4]	Lanes[3:0]

Table 103: Reset Mapping for D0F0xE4_x013[3:0]_802[8:5]

Register	Reset
D0F0xE4_x013[3:0]_8028	0F0E_0D0Ch
D0F0xE4_x013[3:0]_8027	0B0A_0908h
D0F0xE4_x013[3:0]_8026	0706_0504h
D0F0xE4_x013[3:0]_8025	0302_0100h

Table 104: Field mapping for D0F0xE4_x013[3:0]_802[8:5]

Register	Bits			
	31:24	23:16	15:8	7:0
D0F0xE4_x013[3:0]_8028	RXLane15	RXLane14	RXLane13	RXLane12
D0F0xE4_x013[3:0]_8027	RXLane11	RXLane10	RXLane9	RXLane8
D0F0xE4_x013[3:0]_8026	RXLane7	RXLane6	RXLane5	RXLane4
D0F0xE4_x013[3:0]_8025	RXLane3	RXLane2	RXLane1	RXLane0

Bits	Description
31:24	**RXLane**. Read-write. Specifies the PIF RX lanes that are mapped to controller lane n. See: D0F0xE4_x013[3:0]_802[8:5][7:0].

23:16	**RXLane**. Read-write. Specifies the PIF RX lanes that are mapped to controller lane n. See: D0F0xE4_x013[3:0]_802[8:5][7:0].
15:8	**RXLane**. Read-write. Specifies the PIF RX lanes that are mapped to controller lane n. See: D0F0xE4_x013[3:0]_802[8:5][7:0].
7:0	**RXLane**. Read-write. Specifies the PIF RX lanes that are mapped to controller lane n. Bits Definition Bits Definition 0h PIF RX lane 0. 8h PIF RX lane 8. 1h PIF RX lane 1. 9h PIF RX lane 9. 2h PIF RX lane 2. 10h PIF RX lane 10. 3h PIF RX lane 3. 11h PIF RX lane 11. 4h PIF RX lane 4. 12h PIF RX lane 12. 5h PIF RX lane 5. 13h PIF RX lane 13. 6h PIF RX lane 6. 14h PIF RX lane 14. 7h PIF RX lane 7. 15h PIF RX lane 15.

D0F0xE4_x013[3:0]_8029 Lane Enable

Reset: 0000_FFFFh.

Bits	Description
31:16	Reserved.
15:0	**LaneEnable**. Read-write. 1=Lane enabled for transmit. Bit Definition [15:0] Lane <BIT> enable

D0F0xE4_x013[3:0]_804[3:0] DDI Slice

Reset: 0000_0000h.

Table 105: Index address mapping for D0F0xE4_x013[3:0]_804[3:0]

D0F0xE0[31:16]	D0F0xE0[15:0]			
	8040h	8041h	8042h	8043h
0130h	PGD Lanes 0-3	PGD Lanes 4-7	PGD Lanes 8-11	PGD Lanes 12-15
0131h	PPD Lanes 0-3	PPD Lanes 4-7	PPD Lanes 8-11	PPD Lanes 12-15
0132h	PSD Lanes 0-3	PSD Lanes 4-7	PSD Lanes 8-11	PSD Lanes 12-15
0133h	DDI Lanes 0-3	DDI Lanes 4-7	DDI Lanes 8-11	DDI Lanes 12-15

Bits	Description
31:1	Reserved.
0	**OwnSlice**. Read-write. 1=DDI asserts control over the PCIe lanes specified in Table 105.

D0F0xE4_x013[3:0]_804[E:8] DDI Dig

Reset: 0000_0701h.

Table 106: Register mappings for D0F0xE4_x013[3:0]_804[E:8]

D0F0xE4_x013[3:0]_804[E:8]	Function
D0F0xE4_x013[3:0]_8048	Stream A
D0F0xE4_x013[3:0]_8049	Stream B
D0F0xE4_x013[3:0]_804A	Stream C
D0F0xE4_x013[3:0]_804B	Stream D
D0F0xE4_x013[3:0]_804C	Stream E
D0F0xE4_x013[3:0]_804D	Stream F
D0F0xE4_x013[3:0]_804E	Stream G

Bits	Description
31:26	Reserved.
25	**CntDig**. Read-write. 1=Software asserts control over Dig TxPhyCmd and LinkSpeed.
24	**CntPhy**. Read-write. 1=Software asserts control over the phy state machine.
23	Reserved.
22	**Nxt_Lnspd**. Read-write. 1=Set the value for the dig link speed in case of an override.
21:19	**Nxt_phycmd**. Read-write. 1=Set the value for the dig Tx phy command in case of an override.
18:16	**Nxt_State**. Read-write. This specifies the next state for the DDI FSM.
15:11	Reserved.
10:8	**Dig_pwrdn_value**. Read-write. Specifies the phy power state for links associated with dig streams that are not enabled. Bits Definition Bits Definition 000b On. 100b Receiver detect. 001b Standby 1 (L0s). 101b Reserved. 010b Standby 2 (L1). 110b Reserved. 011b Reserved. 111b Off.
7	Reserved.
6	**Hbr2Support**. Read-write. 1=HBR is supported.
5	Reserved.
4	**Hbr2Active**. Read-write. 1=If (Hbr2Support==1) THEN HBR2 will be enabled.
3	Reserved.
2	**PwrDnCpl**. Read-only. 1=PHY state machine is in the powered up state.
1	Reserved.
0	**PwrDnCpl**. Read-only. 1=PHY state machine is in the power off state.

D0F0xE4_x013[3:0]_8060 Soft Reset Command 0

Cold reset: 0000_0000h.

Table 107: Reserved field mappings for D0F0xE4_x013[3:0]_8060

Register	Bits
	31:16
D0F0xE4_x0130_8060	-
D0F0xE4_x0131_8060	-
D0F0xE4_x0132_8060	-
D0F0xE4_x0133_8060	Reserved

Bits	Description
31:18	Reserved.
17	**Bif0CalibrationReset**. Read-write. 1=The BIF 0 calibration block reset is asserted.
16	**Bif0GlobalReset**. Read-write. 1=The BIF 0 global reset is asserted.
15:4	Reserved.
3	**WaitState**. Read-only. 1=Reset cycle is in the wait state.
2	**ResetComplete**. Read-only. 1=Reset cycle is complete.
1	Reserved.
0	**Reconfigure**. Read-write; Cleared-when-done. 1=Trigger atomic reconfiguration if D0F0xE4_x013[3:0]_8062[ReconfigureEn]=1.

D0F0xE4_x013[3:0]_8062 Soft Reset Control 0

Cold reset: 0001_0880h.

Bits	Description
31:12	Reserved.
11	**ConfigXferMode**. Read-write. 1=PCIe core strap settings take effect immediately. 0=PCIe core strap settings take effect when the PCIe core is reset.
10	**BlockOnIdle**. Read-write. 1=The PCIe core must be idle before hardware initiates a reconfiguration. 0=The PCIe core does not have to be idle before hardware initiates a reconfiguration.
9:5	Reserved.
4:2	**ResetPeriod**. Read-write. BIOS: 0. Specifies the amount of time that resets are asserted during a reconfiguration. 5h-7h: Reserved.
1	Reserved.
0	**ReconfigureEn**. Read-write. 1=Atomic reconfiguration enabled.

D0F0xE4_x0132_80F0 BIOS Timer

Reset: 0000_0000h.

Bits	Description
31:0	**MicroSeconds**. Read-write; Updated-by-hardware. This field increments once every microsecond when the timer is enabled. The counter rolls over and continues counting when it reaches its FFFF_FFFFh. A write to this register causes the counter to reset and begin counting from the value written.

D0F0xE4_x0132_80F1 BIOS Timer Control

Reset: 0000_0064h.

Bits	Description
31:8	Reserved.
7:0	**ClockRate**. Read-write. Specifies the frequency of the reference clock in 1 MHz increments. Bits Definition 00h Timer disabled FFh-01h <ClockRate> MHz

3.3.4 IO Link Registers

Table 108: Mapping for IO link registers

D0F0xE0[31:16]	Wrapper	Port Description
0140h	PGD	Gfx+Display
0141h	PPD	GPP+Display
0142h	PSD	FCH+Display

D0F0xE4_x014[2:0]_0002 IO Link Hardware Debug

Reset: 0000_0000h.

Bits	Description
31:1	Reserved.
0	**HwDebug[0]: ignore DLLPs in L1**. Read-write. BIOS: 1. 1=DLLPs are ignored in L1 so the TXCLK can be turned off.

D0F0xE4_x014[2:0]_0010 IO Link Control 1

Reset: 80E3_110Bh.

Bits	Description
31:13	Reserved.

12:10	**RxUmiAdjPayloadSize**. Read-write. BIOS: 100b. Payload size for the UMI link. Bits Definition Bits Definition 00xb Reserved. 100b 64 bytes 010b 16 bytes 101b Reserved. 011b 32 bytes. 11xb Reserved.
9	**UmiNpMemWrite: memory write mapping enable**. Read-write. 1=Internal non-posted memory writes are transferred to UMI.
8:4	Reserved.
3:1	**LcHotPlugDelSel: enhanced hot plug counter select**. Read-write. Bits Definition Bits Definition 0h 15 ms 4h 150 ms 1h 20 ms 5h 200 ms 2h 50 ms 6h 275 ms 3h 100 ms 7h 335 ms
0	**HwInitWrLock: hardware init write lock**. Read-write. 1=Lock HWInit registers. 0=Unlock HWInit registers.

D0F0xE4_x014[2:0]_0011 IO Link Config Control

Reset: 0000_000Fh.

Bits	Description
31:4	Reserved.
3:0	**DynClkLatency: dynamic clock latency**. Read-write. BIOS: See 2.11.4.3.1 [Link Configuration and Core Initialization]. Specifies the number of clock cycles after logic goes idle before clocks are gated off.

D0F0xE4_x014[2:0]_001C IO Link Control 2

Reset: 0E00_0109h.

Bits	Description
31:11	Reserved.
10:6	**TxArbMstLimit: transmitter arbitration master limit**. Read-write. BIOS: 4h. Defines together with TxArbSlvLimit a round robin arbitration pattern for downstream accesses. TxArbMstLimit defines the weight for downstream CPU requests and TxArbSlvLimit for the downstream read responses.
5:1	**TxArbSlvLimit: transmitter arbitration slave limit**. Read-write. BIOS: 4h. See TxArbMstLimit for details
0	**TxArbRoundRobinEn: transmitter round robin arbitration enabled**. Read-write. BIOS: 1. 1=Enable transmitter round robin arbitration. 0=Disable transmitter round robin arbitration.

D0F0xE4_x014[2:0]_0020 IO Link Chip Interface Control

Reset: 0000_0050h.

Bits	Description
31:10	Reserved.
9	**CiRcOrderingDis: chip interface RC ordering disable**. Read-write. 0=RC ordering logic is enabled. 1=RC ordering logic is disabled.
8:0	Reserved.

D0F0xE4_x014[2:0]_0040 IO Link Phy Control

Reset: 0001_0000h.

Bits	Description
31:16	Reserved.
15:14	**PElecIdleMode: electrical idle mode for physical layer**. Read-write. BIOS: 11b. Defines which electrical idle signal is used, either inferred by link controller of from phy. Bits — Definition 00b — Gen1 - entry:PHY, exit:PHY; Gen2 - entry:INF, exit:PHY. 01b — Gen1 - entry:INF, exit:PHY; Gen2 - entry:INF, exit:PHY. 10b — Gen1 - entry:PHY, exit:PHY; Gen2 - entry:PHY, exit:PHY. 11b — Gen1 - entry: PHY, exit: PHY; Gen2 - entry: PHY, exit: PHY.
13:0	Reserved.

D0F0xE4_x014[2:0]_00B0 IO Link Strap Control

Reset: 0000_8001h.

Bits	Description
31:6	Reserved.
5	**StrapF0AerEn**. Read-write. 1=AER support enabled. 0=AER support disabled.
4:3	Reserved.
2	**StrapF0MsiEn**. Read-write. BIOS: 1. Overrides MSI enable.
1:0	Reserved.

D0F0xE4_x014[2:0]_00C0 IO Link Strap Miscellaneous

Bits	Description
31	Reserved.
30	**StrapFlrEn**. Read-write.
29	**StrapMstAdr64En**. Read-write.
28	**StrapReverseAll**. Read-write. Reset: 0.
27:0	Reserved.

D0F0xE4_x014[2:0]_00C1 IO Link Strap Miscellaneous2

Bits	Description
31:4	Reserved.
3	**StrapGen3Compliance**. Read-write.
2	Reserved.
1	**StrapGen2Compliance**. Read-write. Reset: 1.
0	**StrapLinkBwNotificationCapEn**. Read-write. Reset: 0.

D0F0xF8 Northbridge IOAPIC Index

Reset: 0000_0000h. The index/data pair registers, D0F0xF8 and D0F0xFC, are used to access the registers at D0F0xFC_x[FF:00]. To access any of these registers, the address is first written into the index register, D0F0xF8, and then the data is read from or written to the data register, D0F0xFC.

Bits	Description
31:8	Reserved.
7:0	**IOAPICIndAddr: IOAPIC index register address**. Read-write.

D0F0xFC Northbridge IOAPIC Data

Reset: 0000_0000h. See D0F0xF8. Address: D0F0xF8[IOAPICIndAddr].

Bits	Description
31:0	**IOAPICIndData: IOAPIC index data register**. Read-write.

D0F0xFC_x00 IOAPIC Feature Control Register

Reset: 0000_0004h.

Bits	Description
31:5	Reserved.
4	**IoapicSbFeatureEn.** Read-write. 1=Enable masked interrupts to be routed back to the FCH PIC/IOAPIC.
3	Reserved.
2	**IoapicIdExtEn.** Read-write. Extend the IOAPIC ID from 4-bit to 8-bit. 0=4-bit ID. 1=8-bit ID.
1	Reserved.
0	**IoapicEnable.** Read-write. BIOS: 1. 1=Enables the INTGEN block to decode IOAPIC addresses. BIOS should always set this bit after programming the IOAPIC BAR in the init sequence.

D0F0xFC_x01 IOAPIC Base Address Lower

Reset: FEC0_0000h. See 3.15 [Northbridge IOAPIC Registers].

Bits	Description
31:8	**IoapicAddr.** Read-write. IOAPIC Base Address bits [31:8].
7:0	Reserved.

D0F0xFC_x02 IOAPIC Base Address Upper

Reset: 0000_0000h. See 3.15 [Northbridge IOAPIC Registers].

Bits	Description
31:0	**IoapicAddrUpper.** Read-write. IOAPIC Base Address bits [63:32].

D0F0xFC_x0F IOAPIC GBIF Interrupt Routing Register

Reset: 0000_0000h.

Bits	Description
31:6	Reserved.
5:4	**GBIFExtIntrSwz.** Read-write. Swizzle GBIF INTA/B/C/D based on the value in this field before mapping them onto the IOAPIC pins. Bits — Interrupt Swizzling 00b — ABCD 01b — BCDA 10b — CDAB 11b — DABC
3	Reserved.
2:0	**GBIFExtIntrGrp.** Read-write. Map GBIF INTA/B/C/D to IOAPIC pins [((grp+1)*4)-1:(grp*4)]. For GBIF, only INTA/B are used. INTC/D should be tied off.

D0F0xFC_x1[B:0] IOAPIC BR Interrupt Routing Register

Reset: 0000_0000h.

Bits	Description
31:21	Reserved.
20:16	**BrIntIntrMap**. Read-write. Map bridge n interrupts to IOAPIC redirection table entry.
15:6	Reserved.

5:4	**BrExtIntrSwz**. Read-write. Swizzle bridge n external INTA/B/C/D based on the value in this field before mapping them onto the IOAPIC pins. Bits Definition 00b ABCD 01b BCDA 10b CDAB 11b DABC
3	Reserved.
2:0	**BrExtIntrGrp**. Read-write. Map bridge n external INTA/B/C/D to IOAPIC pins [((grp+1)*4)-1:(grp*4)].

D0F0xFC_x30 IOAPIC Serial IRQ Status

Reset: 0000_0000h.

Bits	Description
31:0	**InternalIrqSts.** Read-only. Shows the status of the 32 IOAPIC interrupt pins.

D0F0xFC_x3[F:E] IOAPIC Scratch [1:0] Register

Reset: 0000_0000h.

Bits	Description
31:0	**Scratch.** Read-write.

3.4 Device 0 Function 2 (IOMMU) Configuration Registers

See 3.1 [Register Descriptions and Mnemonics]. See 2.7 [Configuration Space]. See 2.12.1 [IOMMU Configuration Space].

D0F2x00 Device/Vendor ID

Bits	Description
31:16	**DeviceID: device ID**. Read-only. Value: 1423h.
15:0	**VendorID: vendor ID**. Read-only. Value: 1022h.

D0F2x04 Status/Command

Bits	Description
31	**ParityErrorDetected**. Read; write-1-to-clear. Reset: 0.
30	**SignaledSystemError**. Read-only. Reset: 0.
29	**ReceivedMasterAbort**. Read; write-1-to-clear. Reset: 0.
28	**ReceivedTargetAbort**. Read; write-1-to-clear. Reset: 0.
27	**SignalTargetAbort**. Read-only. Reset: 0.
26:25	Reserved.
24	**MasterDataError**. Read; write-1-to-clear. Reset: 0.
23:21	Reserved.
20	**CapList**. Read-only. Reset: 1. 1=Capability list supported.
19	**IntStatus**. Read-only. Reset: 0. 1=INTx message pending.
18:11	Reserved.
10	**InterruptDis**. Read-write. Reset: 0. 1=INTx interrupt message generation disabled.
9	Reserved.
8	**SerrEn**. Read-only. Reset: 0. 1=Enables reporting of non-fatal and fatal errors detected.
7	Reserved.
6	**ParityErrorEn**. Read-write. Reset: 0. 1=Enables setting of ParityErrorDetected status bit.
5:3	Reserved.
2	**BusMasterEn**. Read-write. Reset: 0. 1=Enables DMA request generation.
1	**MemAccessEn**. Read-only. Reset: 0.
0	**IoAccessEn**. Read-only. Reset: 0.

D0F2x08 Class Code/Revision ID

Reset: 0806_00xxh.

Bits	Description
31:8	**ClassCode: class code**. Read-only. Provides the IOMMU class code as defined in the PCI specification.
7:0	**RevID: revision ID**. Read-only.

D0F2x0C Header Type

Reset: 0080_0000h.

Bits	Description
31:24	**BIST**. Read-only.
23:16	**HeaderTypeReg**. Read-only. 80h=Type 0 multi-function device.
15:8	**LatencyTimer**. Read-only.
7:0	**CacheLineSize**. Read-only.

D0F2x2C Subsystem and Subvendor ID

Bits	Description
31:16	**SubsystemId**. Read-only. Value: 1423h.
15:0	**SubsystemVendorId**. Read-only. Value: 1022h.

D0F2x34 Capabilities Pointer

Bits	Description
31:8	Reserved.
7:0	**CapPtr**. Read-only. Reset: 40h.

D0F2x3C Interrupt Line

Bits	Description
31:16	Reserved.

15:8	**InterruptPin**. Read-only. Reset: 01h. This field indicates the INTx line used to generate legacy interrupts. Bits: Description 00h: Reserved. 01h: INTA. 02h: INTB. 03h: INTC. 04h: INTD. FFh-05h: Reserved.
7:0	**InterruptLine**. Read-write. Reset: 0. This field is read/write for software compatibility. It controls no hardware.

D0F2x40 IOMMU Capability

Bits	Description
31:28	Reserved.
27	**IommuEfrSup**. Read-only. Reset: 1. 1=Indicates IOMMUx30 [Extended Feature Low] is supported. 0=IOMMUx30 is reserved.
26	**IommuNpCache**. Read-only. Reset: 0. 1=Indicates that the IOMMU caches page table entries that are marked as not present. When this bit is set, software must issue an invalidate after any change to a PDE or PTE. 0=Indicates that the IOMMU caches only page table entries that are marked as present. When this bit is clear, software must issue an invalidate after any change to a PDE or PTE marked present before the change.
25	**IommuHtTunnelSup**. Read-only. Reset: 0.
24	**IommuIoTlbsup**. Read-only. Reset: 1. Indicates support for remote IOTLBs.
23:19	**IommuCapRev**. Read-only. Reset: 1. Specifies the IOMMU interface revision.
18:16	**IommuCapType**. Read-only. Reset: 3h. Specifies the layout of the Capability Block as an IOMMU capability block.
15:8	**IommuCapPtr**. Read-only. Reset: 54h. Indicates the location of the next capability block.
7:0	**IommuCapId**. Read-only. Reset: Fh. Indicates a Secure Device capability block.

D0F2x44 IOMMU Base Address Low

Bits	Description
31:14	**IommuBaseAddr[31:14]: IOMMU base address bits[31:14]**. IF (D0F2x44[IommuEnable]) THEN Read-only. ELSE Read-write. ENDIF. Reset: 0. IommuBaseAddr[63:14] = {D0F2x48[IommuBaseAddr[63:32]], IommuBaseAddr[31:14]}. IommuBaseAddr[63:14] specifies the base address of the IOMMU memory mapped control registers. In order to use the IOMMU event counters, IommuBaseAddr[18:14] must be 0_0000b.
13:1	Reserved.
0	**IommuEnable**. Read; write-1-only. Reset: 0. 1=IOMMU accepts memory accesses to the address specified in IommuBaseAddr[63:14]. When this bit is set, all IOMMU RW capability registers in PCI configuration space are locked.

D0F2x48 IOMMU Base Address High

Bits	Description
31:0	**IommuBaseAddr[63:32]: IOMMU base address bits[63:32]**. See: D0F2x44[IommuBase-Addr[31:14]].

D0F2x4C IOMMU Range

Bits	Description
31:24	**IommuLastDevice**. Read-only. Reset: 0. Indicates device and function number of the last integrated device associated with the IOMMU.
23:16	**IommuFirstDevice**. Read-only. Reset: 0. Indicates device and function number of the first integrated device associated with the IOMMU.
15:8	**IommuBusNumber**. Read-only. Reset: 0. Indicates the bus number that IommuLastDevice and Iom-muFirstDevice reside on.
7	**IommuRngValid**. Read-only. Reset: 0. 1=The IommuBusNumber, IommuFirstDevice, and Iommu-LastDevice fields are valid. Although the register contents are valid, software is encouraged to use I/O topology information. 0=Software must use I/O topology information.
6:5	Reserved.
4:0	**IommuUnitId**. Read-only. Reset: 0.

D0F2x50 IOMMU Miscellaneous Information Register

Bits	Description
31:27	**IommuMsiNumPpr**. Read-only. Reset: 0. This field must indicate which MSI vector is used for the interrupt message generated by the IOMMU for the peripheral page service request log when IOMMUx30[PprSup]==1. This field must be 0 when IOMMUx30[PprSup]==0. For MSI there can be only one IOMMU so this field must be 0. This interrupt is not remapped by the IOMMU.
26:23	Reserved.
22	**IommuHtAtsResv**. IF (D0F2x44[IommuEnable]) THEN Read-only. ELSE Read-write. ENDIF. Reset: 0. 1=The link Address Translation address range for ATS responses is reserved and cannot be translated by the IOMMU. 0=The Address Translation address range can be translated by the IOMMU.

21:15	**IommuVaSize**. Read-only. Reset: 40h. This field must indicate the size of the maximum virtual address processed by the IOMMU. The value is the (unsigned) binary log of the maximum address size. Bits — Description 19h-00h — Reserved. 20h — 32 bits. 27h-21h — Reserved. 28h — 40 bits. 2Fh-29h — Reserved. 30h — 48 bits. 3Fh-31h — Reserved. 40h — 64 bits. 7Fh-41h — Reserved.
14:8	**IommuPaSize**. Read-only. Reset: 30h. This field must indicate the size of the maximum physical address generated by the IOMMU. The value is the (unsigned) binary log of the maximum address size. Bits — Description 27h-00h — Reserved. 28h — 40 bits. 29h — Reserved. 30h — 48 bits. 7Fh-31h — Reserved.
7:5	**IommuGvaSize**. Read-only. Reset: 010b. Indicates the size of the maximum guest virtual address processed by the IOMMU. Bits — Description 001b-000b — Reserved. 010b — 48 bits. 111b-011b — Reserved.
4:0	**IommuMsiNum**. Read-only. Reset: 0. Indicates the MSI vector used for interrupt messages generated by the IOMMU.

D0F2x54 IOMMU MSI Capability Register

Bits	Description
31:24	Reserved.
23	**Msi64En**. Read-only. Reset: 1. 1=64-bit MSI addressing is supported
22:20	**MsiMultMessEn**. Read-write. Reset: 0. Specifies the number of MSI messages assigned to this function.
19:17	**MsiMultMessCap**. Read-only. Reset: 0. Specifies the number of MSI messages requested by this function.
16	**MsiEn**. Read-write. Reset: 0. 1=Enables MSI for this function and causes legacy interrupts to be disabled.
15:8	**MsiCapPtr**. Read-only. Reset: 64h. Pointer to the next capability register offset.
7:0	**MsiCapId**. Read-only. Reset: 5h. Indicates that this is the MSI capability.

D0F2x58 IOMMU MSI Address Low

Bits	Description
31:2	**MsiAddr[31:2]**. Read-write. Reset: 0. This register specifies the lower address bits used to issue MSI messages.
1:0	Reserved.

D0F2x5C IOMMU MSI Address High

Bits	Description
31:0	**MsiAddr[63:32]**. Read-write. Reset: 0. This register specifies the upper address bits used to issue MSI messages.

D0F2x60 IOMMU MSI Data

Bits	Description
31:16	Reserved.
15:0	**MsiData**. Read-write. Reset: 0. This register specifies the data issued with MSI messages.

D0F2x64 IOMMU MSI Mapping Capability

Bits	Description
31:27	**MsiMapCapType**. Read-only. Reset: 15h. Indicates the MSI Mapping Capability.
26:18	Reserved.
17	**MsiMapFixd**. Read-only. Reset: 1. 1=MSI interrupt mapping range is not programmable.
16	**MsiMapEn**. Read-only. Reset: 1. Always set to 1 to indicate that the MSI Mapping Capability is always enabled.
15:8	**MsiMapCapPtr**. Read-only. Reset: 0. Points to the next capability list item.
7:0	**MsiMapCapId**. Read-only. Reset: 8h. Indicates a link capability list item.

D0F2x6C IOMMU Control

Bits	Description
31:14	Reserved.
13	**CapExtW**. Read-write. Reset: 1. This field sets the value of D0F2x40[IommuCapExt].
12:10	**MsiMultMessCapW**. Read-write. Reset: 2h.
9	**EfrSupW**. Read-write. Reset: 1. This field sets the value of D0F2x40[IommuEfrSup].
8	**IoTlbsupW**. Read-write. Reset: 1. This field sets the value of D0F2x40[IommuIoTlbsup].
7:4	**MinorRevIdW**. Read-write. Reset: 0. This field sets the value of D0F2x08[RevID[3:0]].

3	Reserved.
2:0	**InterruptPinW**. Read-write. Reset: 1. This field sets the value of D0F2x3C[InterruptPin].

D0F2x70 IOMMU MMIO Control Low

Bits	Description
31:18	Reserved.
17:16	**SmifSupW**. Read-write. Reset: 0.
15:12	Reserved.
11:10	**HatsW**. Read-write. Reset: 2h. This field sets the value of IOMMUx30[HATS].
9	**PcSupW**. Read-write. Reset: 1. This field sets the value of IOMMUx30[PcSup].
8	Reserved.
7	Reserved.
6	**IaSupW**. Read-write. Reset: 1. This field sets the value of IOMMUx30[IaSup].
5	Reserved.
4	**GtSupW**. Read-write. Reset: 1. This field sets the value of IOMMUx30[GtSup].
3	**NxSupW**. Read-write. Reset: 0. This field sets the value of IOMMUx30[NxSup]. BIOS: Program D0F2xFC_x07_L1i[4:0][ForceNoExePerm]=1 when NxSupW==0.
2	Reserved.
1	**PprSupW**. Read-write. Reset: 1. This field sets the value of IOMMUx30[PprSup].
0	**PrefSupW**. Read-write. Reset: 1. BIOS: 0. This field sets the value of IOMMUx30[PrefSup].

D0F2x74 IOMMU MMIO Control High

Bits	Description
31:4	Reserved.
3:0	**PasMaxW**. Read-write. Reset: 8h. This field sets the value of IOMMUx34[PasMax].

D0F2x78 IOMMU Range Control

The fields in this register set the values of the corresponding fields in D0F2x4C.

Bits	Description
31:24	**LastDeviceW**. Read-write. Reset: 0.
23:16	**FirstDeviceW**. Read-write. Reset: 0.
15:8	**BusNumberW**. Read-write. Reset: 0.
7	**RngValidW**. Read-write. Reset: 0.
6:0	Reserved.

D0F2xF0 IOMMU L2 Config Index

The index/data pair registers, D0F2xF0 and D0F2xF4 are used to access the registers at D0F2xF4_x[FF:00].

To access any of these registers, the address is first written into the index register, D0F2xF0, and then the data is read from or written to the data register, D0F2xF4. See 2.12.1 [IOMMU Configuration Space].

Bits	Description
31:9	Reserved.
8	**L2cfgWrEn**. Read-write. Reset: 0.
7:0	**L2cfgIndex**. Read-write. Reset: 0.

D0F2xF4 IOMMU L2 Config Data

IF (D0F2xF0[L2cfgWrEn]) THEN Read-write. ELSE Read-only. Reset: 0000_0000h. See D0F2xF0. Address: D0F2xF0[L2cfgIndex].

Bits	Description
31:0	**L2cfgData**.

D0F2xF4_x00 L2_PERF_CNTL_0

Bits	Description
31:24	**L2PerfCountUpper1**. Read-only. Reset: 0. Upper 8 bits of IOMMU L2 performance counter 1.
23:16	**L2PerfCountUpper0**. Read-only. Reset: 0. Upper 8 bits of IOMMU L2 performance counter 0.
15:8	**L2PerfEvent1**. Read-write. Reset: 0. Selects the IOMMU L2 performance counter event for counter 1.
7:0	**L2PerfEvent0**. Read-write. Reset: 0. Selects the IOMMU L2 performance counter event for counter 0.

D0F2xF4_x01 L2_PERF_COUNT_0

Bits	Description
31:0	**L2PerfCount0**. Read-only. Reset: 0. Lower 32 bits of IOMMU L2 performance counter 0.

D0F2xF4_x02 L2_PERF_COUNT_1

Bits	Description
31:0	**L2PerfCount1**. Read-only. Reset: 0. Lower 32 bits of IOMMU L2 performance counter 1.

D0F2xF4_x03 L2_PERF_CNTL_1

Bits	Description
31:24	**L2PerfCountUpper3**. Read-only. Reset: 0. Upper 8 bits of IOMMU L2 performance counter 3.
23:16	**L2PerfCountUpper2**. Read-only. Reset: 0. Upper 8 bits of IOMMU L2 performance counter 2.

15:8	**L2PerfEvent3**. Read-write. Reset: 0. Selects the IOMMU L2 performance counter event for counter 3.
7:0	**L2PerfEvent2**. Read-write. Reset: 0. Selects the IOMMU L2 performance counter event for counter 2.

D0F2xF4_x04 L2_PERF_COUNT_2

Bits	Description
31:0	**L2PerfCount2**. Read-only. Reset: 0. Lower 32 bits of IOMMU L2 performance counter 2.

D0F2xF4_x05 L2_PERF_COUNT_3

Bits	Description
31:0	**L2PerfCount3**. Read-only. Reset: 0. Lower 32 bits of IOMMU L2 performance counter 3.

D0F2xF4_x08 L2_STATUS_0

Bits	Description
31:0	**L2STATUS0**. Read-only. Reset: 0. Internal IOMMU L2A status.

D0F2xF4_x0C L2_CONTROL_0

Bits	Description
31:24	**IFifoClientPriority**. Read-write. Reset: 0. Each bit of this register controls whether the corresponding L1 client is arbitrated as high priority or not. Not all implementations will use all of the priority bits due to a lower number of clients versus the register width.
23:20	**IFifoBurstLength**. Read-write. Reset: 1. Sets the burst length when arbitrating between clients coming into the L2.
19	Reserved.
18	**FLTCMBPriority**. Read-write. Reset: 0. 0=Round-robin arbitration between cache responses and table-walker responses at the fault combiner. 1=Table-walker responses always win arbitration at the fault combiner.
17:12	**IFifoCMBCredits**. Read-write. Reset: 4h. Controls the initial number of credits for the ififo to fault/CMB interface. Credits are loaded whenever the register value changes. This register may only be programmed when IOMMU is not enabled to preserve correct operation.
11	**SIDEPTEOnAddrTransExcl**. Read-write. Reset: 0. 0=Caches return DTE to L1 on an address translation exclusion range access. 1=Caches return PTE to L1 on an address translation exclusion range access.
10	**SIDEPTEOnUntransExcl**. Read-write. Reset: 0. 0=Caches return DTE to L1 on an untranslated exclusion range access. 1=Caches return PTE to L1 on an untranslated exclusion range access.
9:4	**IFifoTWCredits**. Read-write. Reset: 4h. Controls the initial number of credits for the ififo to TW interface. Credits are loaded whenever the register changes value. This register may only be programmed when IOMMU is not enabled to preserve correct operation.

3	**DTCHitVZeroOrIVZero**. Read-write. Reset: 0. 0=A DTE is refetched if a DTE with V=0 for a memory request or IV=1 for an interrupt request ishit in the DTC. 1=A DTE is not refetched if a DTE with V=0 for a memory request or IV=1 for an interrupt request is hit in the DTC. This DTE is used.
2	**AllowL1CacheATSRsp**. Read-write. Reset: 0. 0=L2 does not allow L1 to cache responses to ATS address translation requests. 1=L2 allows L1 to cache responses to ATS address translation requests.
1	**AllowL1CacheVZero**. Read-write. Reset: 0. 0=L2 does not allow L1 to cache DTEs where V=0. 1=L2 allows L1 to cache DTEs where V=1. L1 stores IR and IW as if they are both set to 1.
0	**PTCAddrTransReqCheck**. Read-write. Reset: 0. 0=Address translation requests do not check the PTC. 1=Address translation requests check the PTC.

D0F2xF4_x0D L2_CONTROL_1

Bits	Description
31:24	**PerfThreshold**. Read-write. Reset: 0. Fifo threshold level used to calculate certain performance counter values.
23:17	Reserved.
16	**SeqInvBurstLimitEn**. Read-write. Reset: 1. Enable stalling L2 requests to allow invalidation cycles to make forward progress based upon SeqInvBurstLimitInv and SeqInvBurstLimitL2Req.
15:8	**SeqInvBurstLimitL2Req**. Read-write. Reset: 8h. Sets the number of consecutive IOMMU L2 requests to perform when doing sequential invalidation. Regular L2 and invalidation requests will alternate access to the main L2 caches based upon SeqInvBurstLimitInv and SeqInvBurstLimitL2Req.
7:0	**SeqInvBurstLimitInv**. Read-write. Reset: 8h. Sets the number of consecutive invalidation requests to perform when doing sequential invalidation. Regular L2 and invalidation requests will alternate access to the main L2 caches based upon SeqInvBurstLimitInv and SeqInvBurstLimitL2Req.

D0F2xF4_x10 L2_DTC_CONTROL

Bits	Description
31:28	**DTCEntries**. Read-only. Reset: 0. The number of entries in the DTC is indicated as 2^DTCEntries.
27:24	Reserved.
23:16	**DTCWays**. Read-only. Reset: 0. Indicates the number of ways in the DTC.
15	**DTCParitySupport**. Read-only. Reset: 0. 0=The DTC does not support parity protection. 1=The DTC supports parity protection.
14	Reserved.
13	**DTCBypass**. Read-write. Reset: 0. When set, all requests bypass the DTC.
12:11	Reserved.
10	**DTCSoftInvalidate**. Read-write. Reset: 0. Software may write this register to 1 to invalidate all entries in the DTC.

9:8	**DTCInvalidationSel**. Read-write. Reset: 0. BIOS: 10b. Selects the DTC invalidation algorithm. Bits — Description 00b — Invalidate the entire DTC. 01b — Fast imprecise invalidation. 10b — Sequential precise invalidation. 11b — Partial sequential precise invalidation.
7:5	Reserved.
4	**DTCParityEn**. Read-write. Reset: 0. Enable parity protection of the DTC.
3	**DTCLRUUpdatePri**. Read-write. Reset: 0. 0=Reads update replacement state bits when there is a simultaneous read and write to the same DTC index. 1=Writes update replacement state bits when there is a simultaneous read and write to the same DTC index.
2	Reserved.
1:0	**DTCReplacementSel**. Read-write. Reset: 1. Selects the DTC replacement algorithm. Implementation may not support all replacement algorithms.

D0F2xF4_x11 L2_DTC_HASH_CONTROL

Bits	Description
31:16	**DtcAddressMask**. Read-write. Reset: 0h. This field is a bit-wise AND mask that selects which bits from the untranslated interrupt {MT[2:0],Vector} are used to index into the DTC.
15:11	Reserved.
10	**DtcAltHashEn**. Read-write. Reset: 0. Enable alternative algorithm for generating hash index into the DTC.
9	Reserved.
8:5	**DTCBusBits**. Read-write. Reset: 3h. Set the number of bus bits to use when using ReqID to form the DTC address. The following equation must be satisified. Func_bits + Dev_Bits + Bus_Bits <= log2(DTC entries / DTC associativity).
4:2	**DTCDevBits**. Read-write. Reset: 0. Set the number of device bits to use when using ReqID to form the DTC address.
1:0	**DTCFuncBits**. Read-write. Reset: 2h. Set the number of function bits to use when using ReqID to form the DTC address.

D0F2xF4_x12 L2_DTC_WAY_CONTROL

Bits	Description
31:16	**DTCWayAccessDisable**. Read-write. Reset: 0.
15:0	**DTCWayDisable**. Read-write. Reset: 0. Each bit in this register disables a way in the DTC when set to 1. An implementation may have less than 32 ways. The entire cache may be disabled by setting the DTCWays lower bits of this register.

D0F2xF4_x14 L2_ITC_CONTROL

Bits	Description
31:28	**ITCEntries**. Read-only. Reset: 0. The number of entries in the ITC is indicated as 2^ITCEntries.
27:24	Reserved.
23:16	**ITCWays**. Read-only. Reset: 0. Indicates the number of ways in the ITC.
15	**ITCParitySupport**. Read-only. Reset: 0. 0=The ITC does not support parity protection. 1=The ITC supports parity protection.
14	Reserved.
13	**ITCBypass**. Read-write. Reset: 0. When set, all requests bypass the ITC.
12:11	Reserved.
10	**ITCSoftInvalidate**. Read-write. Reset: 0. Software may write this register to 1 to invalidate all entries in the ITC.
9:8	**ITCInvalidationSel**. Read-write. Reset: 0. BIOS: See 2.12.2. Selects the ITC invalidation algorithm. Bits — Description 00b — Invalidate the entire ITC. 01b — Fast imprecise invalidation. 10b — Sequential precise invalidation. 11b — Partial sequential precise invalidation.
7:5	Reserved.
4	**ITCParityEn**. Read-write. Reset: 0. Enable parity protection of the ITC.
3	**ITCLRUUpdatePri**. Read-write. Reset: 0. 0=Reads update replacement state bits when there is a simultaneous read and write to the same ITC index. 1=Writes update replacement state bits when there is a simultaneous read and write to the same ITC index.
2	Reserved.
1:0	**ITCReplacementSel**. Read-write. Reset: 1. Selects the ITC replacement algorithm. Implementation may not support all replacement algorithms.

D0F2xF4_x15 L2_ITC_HASH_CONTROL

Bits	Description
31:16	**ITCAddressMask**. Read-write. Reset: 0. This register is a bit-wise AND mask that selects which bits from the untranslated interrupt {MT[2:0],Vector} are used to index into the ITC.
15:11	Reserved.
10	**ItcAltHashEn**. Read-write. Reset: 0. Enable alternative algorithm for generating hash index into the ITC.
9	Reserved.
8:5	**ITCBusBits**. Read-write. Reset: 3h. Set the number of bus bits to use when using ReqID to form the ITC address. The following equation must be satisified. Func_bits + Dev_Bits + Bus_Bits <= log2(ITC entries / ITC associativity).

4:2	**ITCDevBits**. Read-write. Reset: 0. Set the number of device bits to use when using ReqID to form the ITC address.
1:0	**ITCFuncBits**. Read-write. Reset: 2h. Set the number of function bits to use when using ReqID to form the ITC address.

D0F2xF4_x16 L2_ITC_WAY_CONTROL

Bits	Description
31:16	**ITCWayAccessDisable**. Read-write. Reset: 0.
15:0	**ITCWayDisable**. Read-write. Reset: 0. Each bit in this register disables a way in the ITC when set to 1. An implementation may have less than 32 ways. The entire cache may be disabled by setting the ITCWays lower bits of this register.

D0F2xF4_x18 L2_PTC_A_CONTROL

Bits	Description
31:28	**PTCAEntries**. Read-only. Reset: 0. The number of entries in the PTC A sub-cache is indicated as 2^PTCAEntries.
27:24	Reserved.
23:16	**PTCAWays**. Read-only. Reset: 0. Indicates the number of ways in the PTC A sub-cache.
15	**PTCAParitySupport**. Read-only. Reset: 0. 0=The PTC A sub-cache does not support parity protection. 1=The PTC A sub-cache supports parity protection.
14	Reserved.
13	**PTCABypass**. Read-write. Reset: 0. When set, all requests bypass the PTC A sub-cache.
12	Reserved.
11	**PTCA2MMode**. Read-write. Reset: 0. When set, the PTC A sub-cache stores 2M pages instead of 4K pages.
10	**PTCASoftInvalidate**. Read-write. Reset: 0. Software may write this register to 1 to invalidate all entries in the PTC A sub-cache.
9:8	**PTCAInvalidationSel**. Read-write. Reset: 0. BIOS: See 2.12.2. Selects the PTC A sub-cache invalidation algorithm. Bits — Description 00b — Invalidate the entire PTC A sub-cache. 01b — Fast imprecise invalidation. 10b — Sequential precise invalidation. 11b — Partial sequential precise invalidation.
7:5	Reserved.
4	**PTCAParityEn**. Read-write. Reset: 0. Enable parity protection of the PTC A sub-cache.
3	**PTCALRUUpdatePri**. Read-write. Reset: 0. 0=Reads update replacement state bits when there is a simultaneous read and write to the same PTCA index. 1=Writes update replacement state bits when there is a simultaneous read and write to the same PTCA index.

2	Reserved.
1:0	**PTCAReplacementSel**. Read-write. Reset: 1. Selects the PTC A sub-cache replacement algorithm. Implementation may not support all replacement algorithms.

D0F2xF4_x19 L2_PTC_A_HASH_CONTROL

Bits	Description
31:16	**PTCAAddressMask**. Read-write. Reset: 0. This register is a bit-wise AND mask that selects which virtual address bits are used to index into the PTC A sub-cache.
15:11	Reserved.
10	**PtcAltHashEn**. Read-write. Reset: 0. Enable alternative algorithm for generating hash index into the PTC.
9	Reserved.
8:5	**PTCABusBits**. Read-write. Reset: 3h. Set the number of bus bits to use when using ReqID to form the PTC A sub-cache address. The following equation must be satisified: FuncBits + DevBits + Bus-Bits <= log2(PTC A sub-cache entries / PTC A sub-cache associativity).
4:2	**PTCADevBits**. Read-write. Reset: 0. Set the number of device bits to use when using ReqID to form the PTC A sub-cache address.
1:0	**PTCAFuncBits**. Read-write. Reset: 2h. Set the number of function bits to use when using ReqID to form the PTC A sub-cache address.

D0F2xF4_x1A L2_PTC_A_WAY_CONTROL

Bits	Description
31:16	**PTCAWayAccessDisable**. Read-write. Reset: 0.
15:0	**PTCAWayDisable**. Read-write. Reset: 0. Each bit in this register disables a way in the PTC A sub-cache when set to 1. An implementation may have less than 32 ways. The entire cache may be disabled by setting the PTCAWays lower bits of this register.

D0F2xF4_x1C L2_PTC_B_CONTROL

Bits	Description
31:28	**PTCBEntries**. Read-only. Reset: 0. The number of entries in the PTC B sub-cache is indicated as 2^PTCBEntries.
27:24	Reserved.
23:16	**PTCBWays**. Read-only. Reset: 0. Indicates the number of ways in the PTC B sub-cache.
15	**PTCBParitySupport**. Read-only. Reset: 0. 0=The PTC B sub-cache does not support parity protection. 1=The PTC B sub-cache supports parity protection.
14	Reserved.
13	**PTCBBypass**. Read-write. Reset: 0. 1=All requests bypass the PTC B sub-cache.
12	Reserved.
11	**PTCB2MMode**. Read-write. Reset: 0. 1=The PTC B sub-cache stores 2M pages instead of 4K pages.

10	**PTCBSoftInvalidate**. Read-write. Reset: 0. 1=Invalidate all entries in the PTC B sub-cache.
9:8	**PTCBInvalidationSel**. Read-write. Reset: 0. Selects the PTC B sub-cache invalidation algorithm. Bits Description 00b Invalidate the entire PTC B sub-cache. 01b Fast imprecise invalidation. 10b Sequential precise invalidation. 11b Partial sequential precise invalidation.
7:5	Reserved.
4	**PTCBParityEn**. Read-write. Reset: 0. Enable parity protection of the PTC B sub-cache.
3	**PTCBLRUUpdatePri**. Read-write. Reset: 0. 0=Reads update replacement state bits when there is a simultaneous read and write to the same PTCB index. 1=Writes update replacement state bits when there is a simultaneous read and write to the same PTCB index.
2	Reserved.
1:0	**PTCBReplacementSel**. Read-write. Reset: 1. Selects the PTC B sub-cache replacement algorithm. Implementation may not support all replacement algorithms.

D0F2xF4_x1D L2_PTC_B_HASH_CONTROL

Bits	Description
31:16	**PTCBAddressMask**. Read-write. Reset: 0. This register is a bit-wise AND mask that selects which virtual address bits are used to index into the PTC B sub-cache.
15:9	Reserved.
8:5	**PTCBBusBits**. Read-write. Reset: 3h. Set the number of bus bits to use when using ReqID to form the PTC B sub-cache address. The following equation must be satisified. FuncBits + DevBits + Bus-Bits <= log2(PTC B sub-cache entries / PTC B sub-cache associativity).
4:2	**PTCBDevBits**. Read-write. Reset: 0. Set the number of device bits to use when using ReqID to form the PTC B sub-cache address.
1:0	**PTCBFuncBits**. Read-write. Reset: 2h. Set the number of function bits to use when using ReqID to form the PTC B sub-cache address.

D0F2xF4_x1E L2_PTC_B_WAY_CONTROL

Bits	Description
31:16	**PTCBWayAccessDisable**. Read-write. Reset: 0.
15:0	**PTCBWayDisable**. Read-write. Reset: 0. Each bit in this register disables a way in the PTC A sub-cache when set to 1. An implementation may have less than 32 ways. The entire cache may be disabled by setting the PTCBWays lower bits of this register.

D0F2xF4_x20 L2_CREDIT_CONTROL_2

Bits	Description
31:28	Reserved.
27:24	**PprLoggerCredits**. Read-write. Reset: 4h. PPR log buffer credit override value.

23	**FCELOverride**. Read-write. Reset: 0. Changing this register from 0 to 1 overrides the FCEL credit counter with FCELCredits. This should only be performed when the IOMMU is idle.
22	Reserved.
21:16	**FCELCredits**. Read-write. Reset: 0. FCEL credit override value.
15	**FLTCMBOverride**. Read-write. Reset: 0. Changing this register from 0 to 1 overrides the FLTCMB credit counter with FLTCMBCredits. This should only be performed when the IOMMU is idle.
14	Reserved.
13:8	**FLTCMBCredits**. Read-write. Reset: 0. FLTCMB credit override value.
7	**QUEUEOverride**. Read-write. Reset: 0. Changing this register from 0 to 1 overrides the QUEUE credit counter with QUEUECredits. This should only be performed when the IOMMU is idle.
6	Reserved.
5:0	**QUEUECredits**. Read-write. Reset: 0. QUEUE credit override value.

D0F2xF4_x22 L2A_UPDATE_FILTER_CNTL

Bits	Description
31:5	Reserved.
4:1	**L2aUpdateFilterRdlatency**. Read-write. Reset: 3h. When L2aUpdateFilterBypass is 0, assume the invalidation read has completed in the number of clock cycles specified by this field.
0	**L2aUpdateFilterBypass**. Read-write. Reset: 1. 1=Disable duplicate update filtering. 0=Enable the dropping of updates that are already in the L2aUpdateFilter or in the destination L2A cache.

D0F2xF4_x30 L2_ERR_RULE_CONTROL_3

Bits	Description
31:4	**ERRRuleDisable3**. Read-write. Reset: 0. Each bit in this register disables an error detection rule in the IOMMU.
3:1	Reserved.
0	**ERRRuleLock1**. Read; write-once. Reset: 0. BIOS: See 2.12.2. Setting this register bit locks the error detection rule set in ERRRuleDisable3, D0F2xF4_x31[ERRRuleDisable4] and D0F2xF4_x32[ERRRuleDisable5].

D0F2xF4_x31 L2_ERR_RULE_CONTROL_4

Bits	Description
31:0	**ERRRuleDisable4**. Read-write. Reset: 0. Each bit in this register disables an error detection rule in the IOMMU.

D0F2xF4_x32 L2_ERR_RULE_CONTROL_5

Bits	Description
31:0	**ERRRuleDisable5**. Read-write. Reset: 0. Each bit in this register disables an error detection rule in the IOMMU.

D0F2xF4_x33 L2_L2A_CK_GATE_CONTROL

Bits	Description
31:8	Reserved.
7:6	**CKGateL2AStop**. Read-write. Reset: 01b. Bits Description 00b Allow 2 clock cycles delay before stopping the clocks when clkready deasserts. 01b Allow 4 clock cycles delay before stopping the clocks when clkready deasserts. 10b Allow 8 clock cycles delay before stopping the clocks when clkready deasserts. 11b Allow 16 clock cycles delay before stopping the clocks when clkready deasserts.
5:4	**CKGateL2ALength**. Read-write. Reset: 01b. Bits Description 00b Allow 128 clock cycles delay before stopping the clocks when idle asserts. 01b Allow 256 clock cycles delay before stopping the clocks when idle asserts. 10b Allow 512 clock cycles delay before stopping the clocks when idle asserts. 11b Allow 1024 clock cycles delay before stopping the clocks when idle asserts.
3	**CKGateL2ASpare**. Read-write. Reset: 0. Spare bit.
2	**CKGateL2ACacheDisable**. Read-write. Reset: 1. BIOS: 0. 1=Disable the gating of the L2A upper cache ways.
1	**CKGateL2ADynamicDisable**. Read-write. Reset: 1. BIOS: 0. 1=Disable the gating of the L2A dynamic clock branch.
0	**CKGateL2ARegsDisable**. Read-write. Reset: 1. BIOS: 0. 1=Disable the gating of the L2A register clock branch.

D0F2xF4_x34 L2_L2A_PGSIZE_CONTROL

Bits	Description
31:4	Reserved.
3:2	**L2aregHostPgsize**. Read-write. Reset: 0. BIOS: See 2.12.2.
1:0	**L2aregGstPgsize**. Read-write. Reset: 0. BIOS: See 2.12.2.

D0F2xF4_x3B IOMMU_PGFSM_CONFIG

Bits	Description
31:28	**RegAddr**. Read-write. Reset: 0. Indicate the register address for write or read operation.
27	**SrbmOverride**. Read-write. Reset: 0.

26:14	Reserved.
13	**PGRead**. Read-write. Reset: 0. Indicate a read operation is performed.
12	**PGWrite**. Read-write. Reset: 0. Indicate a write operation is performed.
11	Reserved.
10	**P1Select**. Read-write. Reset: 0. Indicate the power up or down is for P1 domain.
9	**PowerUp**. Read-write. Reset: 0. Request power up.
8	**PowerDown**. Read-write. Reset: 0. Request power down.
7:0	**FsmAddr**. Read-write. Reset: 0. Indicate the address of the PGFSM. FFh = broadcast to all PGFSM.

D0F2xF4_x3C IOMMU_PGFSM_WRITE

Bits	Description
31:0	**WriteValue**. Read-write. Reset: 0.

D0F2xF4_x3D IOMMU_PGFSM_READ

Bits	Description
31:24	Reserved.
23:0	**ReadValue**. Read-only. Reset: 0.

D0F2xF4_x40 L2_PERF_CNTL_2

Bits	Description
31:24	**L2PerfCountUpper5**. Read-only. Reset: 0. Upper 8 bits of IOMMU L2 performance counter 5.
23:16	**L2PerfCountUpper4**. Read-only. Reset: 0. Upper 8 bits of IOMMU L2 performance counter 4.
15:8	**L2PerfEvent5**. Read-write. Reset: 0. Selects the IOMMU L2 performance counter event for counter 5.
7:0	**L2PerfEvent4**. Read-write. Reset: 0. Selects the IOMMU L2 performance counter event for counter 4.

D0F2xF4_x41 L2_PERF_COUNT_4

Bits	Description
31:0	**L2PerfCount4**. Read-only. Reset: 0. Lower 32 bits of IOMMU L2 performance counter 4.

D0F2xF4_x42 L2_PERF_COUNT_5

Bits	Description
31:0	**L2PerfCount5**. Read-only. Reset: 0. Lower 32 bits of IOMMU L2 performance counter 5.

D0F2xF4_x43 L2_PERF_CNTL_3

Bits	Description
31:24	**L2PerfCountUpper7**. Read-only. Reset: 0. Upper 8 bits of IOMMU L2 performance counter 7.
23:16	**L2PerfCountUpper6**. Read-only. Reset: 0. Upper 8 bits of IOMMU L2 performance counter 6.
15:8	**L2PerfEvent7**. Read-write. Reset: 0. Selects the IOMMU L2 performance counter event for counter 7.
7:0	**L2PerfEvent6**. Read-write. Reset: 0. Selects the IOMMU L2 performance counter event for counter 6.

D0F2xF4_x44 L2_PERF_COUNT_6

Bits	Description
31:0	**L2PerfCount6**. Read-only. Reset: 0. Lower 32 bits of IOMMU L2 performance counter 6.

D0F2xF4_x45 L2_PERF_COUNT_7

Bits	Description
31:0	**L2PerfCount7**. Read-only. Reset: 0. Lower 32 bits of IOMMU L2 performance counter 7.

D0F2xF4_x48 L2_STATUS_1

Bits	Description
31:0	**L2STATUS1**. Read-only. Reset: 0. Internal IOMMU L2B status.

D0F2xF4_x49 L2_SB_LOCATION

Bits	Description

31:16	**SbLocatedCore**. Read-write. Reset: 0. Specifies the core location of the FCH. Bit PortLocation [0] FCH is located under GPP0 [1] FCH is located under GPP1 [2] FCH is located under GPP2 [3] FCH is located under GPP3 [15:4] Reserved.
15:0	**SbLocatedPort**. Read-write. Reset: 0. BIOS: See 2.12.2 [IOMMU Initialization]. Specifies the port location of the FCH. Bit PortLocation [0] FCH is located on port A of the corresponding PCIe core or internal FCH. [1] FCH is located on port B of the corresponding PCIe core. [2] FCH is located on port C of the corresponding PCIe core. [3] FCH is located on port D of the corresponding PCIe core. [15:4] Reserved.

D0F2xF4_x4C L2_CONTROL_5

Bits	Description
31:10	Reserved.
9:8	**GstPartialPtcCntrl**. Read-write. Reset: 0. BIOS: 11b.
7	**FC2AltMode**. Read-write. Reset: 0. 0=FC2 primary flow-control mode. 1=FC2 alternate flow-control mode.
6	**FC3Dis**. Read-write. Reset: 0. 0=FC3 flow-control loop is enabled. 1=FC3 flow-control look is disabled.
5	**FC2Dis**. Read-write. Reset: 0. 0=FC2 flow-control loop is enabled. 1=FC2 flow-control look is disabled.
4	**DTCUpdateVZeroIVOne**. Read-write. Reset: 0. 0=DTEs with V=0 and IV=1 are not cached in the DTC. 1=DTEs with V=0 and IV=1 are cached in the DTC.
3	**DTCUpdateVOneIVZero**. Read-write. Reset: 0. 0=DTEs with V=1 and IV=0 are not cached in the DTC. 1=DTEs with V=1 and IV=0 are cached in the DTC.
2	**FC1Dis**. Read-write. Reset: 0. 0=FC1 flow control loop enabled. 1=FC1 flow control loop disabled.
1	**PTCAddrTransReqUpdate**. Read-write. Reset: 1. 0=PTEs from address translation requests are not cached. 1=PTEs from address translation requests are cached in the L2 according to the Cache bit in the DTE.
0	**QueueArbFBPri**. Read-write. Reset: 1. 0=Requests in the miss queue and the feedback queue are arbitrated in a round-robin manner. 1=Requests in the feedback queue are given priority over requests in the miss queue.

D0F2xF4_x4D L2_CONTROL_6

Bits	Description
31:24	**Perf2Threshold**. Read-write. Reset: 0. Fifo threshold level used to calculate certain performance counter values.

23:17	Reserved.
16	**SeqInvBurstLimitEn**. Read-write. Reset: 1. Enable stalling PDC requests to allow invalidation cycles to make forward progress based upon SeqInvBurstLimitInv and SeqInvBurstLimitPDCReq.
15:8	**SeqInvBurstLimitPDCReq**. Read-write. Reset: 8h. Sets the number of consecutive IOMMU PDC requests to perform when doing sequential invalidation. PDC and invalidation requests will alternate access to the PDC based upon SeqInvBurstLimitInv and SeqInvBurstLimitPDCReq.
7:0	**SeqInvBurstLimitInv**. Read-write. Reset: 8h. Sets the number of consecutive invalidation requests to perform when doing sequential invalidation. PDC and invalidation requests will alte rnate access to the PDC based upon SeqInvBurstLimitInv and SeqInvBurstLimitPDCReq.

D0F2xF4_x50 L2_PDC_CONTROL

Bits	Description
31:28	**PDCEntries**. Read-only. Reset: 0. Indicates the number of entries in the PDC is indicated as 2^PDCEntries.
27:24	Reserved.
23:16	**PDCWays**. Read-only. Reset: 0. Indicates the number of ways in the PDC.
15	**PDCParitySupport**. Read-only. Reset: 0. 0=The PDC does not support parity protection. 1=The PDC supports parity protection.
14	Reserved.
13	**PDCBypass**. Read-write. Reset: 0. When set, all requests bypass the PDC. This prevents the multiple issue of requests and increases maximum rate of requests to the table-walker.
12	**PDCSearchDirection**. Read-write. Reset: 0. 0=Search PDC from higher levels down. 1=Search PDC from lower levels up.
11	Reserved.
10	**PDCSoftInvalidate**. Read-write. Reset: 0. Software may write this register to 1 to invalidate all entries in the PDC.
9:8	**PDCInvalidationSel**. Read-write. Reset: 0. BIOS: See 2.12.2. Selects the PDC invalidation algorithm. Bits — Description 00b — Invalidate the entire PDC. 01b — Fast imprecise invalidation. 10b — Sequential precise invalidation. 11b — Partial sequential precise invalidation.
7:5	Reserved.
4	**PDCParityEn**. Read-write. Reset: 0. Enable parity protection of the PDC if the device supports parity.
3	**PDCLRUUpdatePri**. Read-write. Reset: 0. 0=Reads update replacement state bits when there is a simultaneous read and write to the same PDC index. 1=Writes update replacement state bits when there is a simultaneous read and write to the same PDC index.
2	Reserved.
1:0	**PDCReplacementSel**. Read-write. Reset: 1. Selects the PDC replacement algorithm. Implementation may not support all replacement algorithms.

D0F2xF4_x51 L2_PDC_HASH_CONTROL

Bits	Description
31:16	**PDCAddressMask**. Read-write. Reset: 0. This register is a bit-wise AND mask that selects which virtual address bits are used to index into the PDC.
15:11	Reserved.
10	**PdcAltHashEn**. Read-write. Reset: 0. 1=Enable alternative algorithm for generating hash index into the PDC.
9	**PDCUpperLvlAddrHash**. Read-write. Reset: 1. When set to 1, the PDC cache index is partially formed using the xor of the LSBs of virtual address bits for all levels greater than or equal to the stored/searched level.
8	**PDCLvlHash**. Read-write. Reset: 1. When set to 1, the PDE level is used as part of the hash for the cache index.
7:6	Reserved.
5:0	**PDCDomainBits**. Read-write. Reset: 7h. Selects the number of domain bits to use as part of the index into the PDC.

D0F2xF4_x52 L2_PDC_WAY_CONTROL

Bits	Description
31:16	**PDCWayAccessDisable**. Read-write. Reset: 0.
15:0	**PDCWayDisable**. Read-write. Reset: 0. Each bit in this register disables a way in the PDC when set to 1. An implementation may have less than 32 ways. The entire cache may be disabled by setting the PDCWays lower bits of this register.

D0F2xF4_x53 L2B_UPDATE_FILTER_CNTL

Bits	Description
31:5	Reserved.
4:1	**L2bUpdateFilterRdlatency**. Read-write. Reset: 3h. When L2bUpdateFilterBypass is 0, assume the invalidation read has completed in the number of clock cycles specified by this field.
0	**L2bUpdateFilterBypass**. Read-write. Reset: 1. 1=Disable duplicate update filtering. 0=Enable the dropping of updates that are already in the l2b_update_filter or in the PDC.

D0F2xF4_x54 L2_TW_CONTROL

Bits	Description
31:19	Reserved.
18	**TwContWalkPErrDis**. Read-write. Reset: 0. 0=Continue walking tables on a write permission error. 1=Stop walking tables on a write permission error.
17	**Twfilter64bDis**. Read-write. Reset: 0.
16	**TwfilterDis**. Read-write. Reset: 0.

15	Reserved.
14:12	**TWPrefetchRange**. Read-write. Reset: 1. Selects the number of pages to prefetch.
11	**TWPTEOnAddrTransExcl**. Read-write. Reset: 0. 0=Table walker returns DTE to L1 on an address translation exclusion range access. 1=Table walker returns PTE to L1 on an address translation exclusion range access.
10	**TWPTEOnUntransExcl**. Read-write. Reset: 0. 0=Table walker returns DTE to L1 on an untranslated exclusion range access. 1=Table walker returns PTE to L1 on an untranslated exclusion range access.
9	**TWPrefetchOnly4KDis**. Read-write. Reset: 0. 1=Allow non-4K pages to be prefetched. 0=Only 4K pages are prefetched.
8	**TWPrefetchEn**. Read-write. Reset: 0. Enable prefetching in the table-walker.
7	Reserved.
6	**TWForceCoherent**. Read-write. Reset: 0. 1=Table-walker always genereates coherent requests. The DTE SD bit is ignored when this bit is set to 1.
5:0	**TWQueueLimit**. Read-write. Reset: 10h. Limit the number of outstanding table-walker requests.

D0F2xF4_x56 L2_CP_CONTROL

Bits	Description
31:16	**CPRdDelay**. Read-write. Reset: 0. Command processor read delay.
15:3	Reserved.
2	**CPFlushOnInv**. Read-write. Reset: 1. BIOS: 0. 1=Command processor flushes out old requests on every invalidation command. 0=No flush is performed during invalidations.
1	**CPFlushOnWait**. Read-write. Reset: 0. BIOS: 1. 1=Command processor flushes out old requests on completion wait. 0=No flush is performed on completion wait.
0	**CPPrefetchDis**. Read-write. Reset: 0. 1=Command processor fetches and executes only one command at a time. 0=Command processor prefetches available commands into its internal storage.

D0F2xF4_x57 L2_CP_CONTROL_1

Bits	Description
31:16	Reserved.
15:3	**CPL1Off[15:3]**. Read-write. Reset: 0. Each bit in this register indicates to the IOMMU command processor that a corresponding L1 TLB is inaccessible due to static clock or power gating. System software is responsible for programming this register.
2	**L1ImuIntGfxDis**. Read-write. Reset: 0. BIOS: IF (GpuEnabled) THEN 0. ELSE 1. ENDIF.
1	**CPL1Off[1]**. Read-write. Reset: 0.
0	**L1ImuPcieGfxDis**. Read-write. Reset: 0. BIOS: This bit should be set if there is no external graphics in the system.

D0F2xF4_x58 IOMMU_L2_GUEST_ADDR_CNTRL

Bits	Description
31:24	Reserved.
23:0	**IommuL2GuestAddrMask**. Read-write. Reset: 0.

D0F2xF4_x6A L2_INT_CONTROL

Bits	Description
31:3	Reserved.
2	**IntPPROrderEn**. Read-write. Reset: 1. 1=Enable ordering between interrupts and PPR log writes.
1	**IntCPOrderEn**. Read-write. Reset: 1. 1=Enable ordering between interrupts and command processor writes.
0	**IntEventOrderEn**. Read-write. Reset: 1. 1=Enable ordering between interrupts and event log writes.

D0F2xF4_x70 L2_CREDIT_CONTROL_0

Bits	Description
31	**DTEOverride**. Read-write. Reset: 0. 1=Override the DTE credit counter with DTECredits. Setting should only be performed when the IOMMU is idle.
30	Reserved.
29:24	**DTECredits**. Read-write. Reset: 2h. DTE credit override value.
23	**FC3Override**. Read-write. Reset: 0. 1=Override the FC3 credit counter with FC3Credits. Setting should only be performed when the IOMMU is idle.
22	Reserved.
21:16	**FC3Credits**. Read-write. Reset: 0. FC3 credit override value.
15	**FC2Override**. Read-write. Reset: 0. 1=Override the FC2 credit counter with FC2Credits. This should only be performed when the IOMMU is idle.
14	Reserved.
13:8	**FC2Credits**. Read-write. Reset: 0. FC2 credit override value.
7	**FC1Override**. Read-write. Reset: 0. 1=Override the FC1 credit counter with FC1Credits. Setting should only be performed when the IOMMU is idle.
6	Reserved.
5:0	**FC1Credits**. Read-write. Reset: 0. FC1 credit override value.

D0F2xF4_x71 L2_CREDIT_CONTROL_1

Bits	Description
31:24	Reserved.
23:20	**PprMcifCredits**. Read-write. Reset: 4h. PPR logger credit override value.

19:16	**CpPrefetchCredits**. Read-write. Reset: 4h. Command processor prefetch credit override value.
15	**TWELOverride**. Read-write. Reset: 0. 1=Override the TWEL credit counter with TWELCredits. Setting should only be performed when the IOMMU is idle.
14	Reserved.
13:8	**TWELCredits**. Read-write. Reset: 4h. TWEL credit override value.
7	**PDTIEOverride**. Read-write. Reset: 0. 1=Override the PDTIE credit counter with PDTIECredits. Setting should only be performed when the IOMMU is idle.
6	Reserved.
5:0	**PDTIECredits**. Read-write. Reset: 4h. PDTIE credit override value.

D0F2xF4_x78 L2_MCIF_CONTROL

Bits	Description
31:29	Reserved.
28:24	**MCIFBaseWriteDataCredits**. Read-write. Reset: 8h. Sets the number of base-channel write data credits between the IOMMU L2 and the HTIU/ORB. Software must ensure no traffic is on this data path while programming this register.
23:21	Reserved.
20:16	**MCIFBaseWriteHdrCredits**. Read-write. Reset: 8h. Sets the number of base-channel write header credits between the IOMMU L2 and the HTIU/ORB. Software must ensure no traffic is on this data path while programming this register.
15:13	Reserved.
12:8	**MCIFIsocReadCredits**. Read-write. Reset: 8h. Sets the number of isoc-channel read credits between the IOMMU L2 and the HTIU/ORB. Software must ensure no traffic is on this data path while programming this register.
7:5	Reserved.
4:0	**MCIFBaseReadCredits**. Read-write. Reset: 8h. Sets the number of base-channel read credits between the IOMMU L2 and the HTIU/ORB. Software must ensure no traffic is on this data path while programming this register.

D0F2xF4_x80 L2_ERR_RULE_CONTROL_0

Bits	Description
31:4	**ERRRuleDisable0**. Read-write. Reset: 0. Each bit in this register disables an error detection rule in the IOMMU.
3:1	Reserved.
0	**ERRRuleLock0**. Read-write. Reset: 0. BIOS: See 2.12.2. This register is write-once. Setting this register bit locks the error detection rule set in ERRRuleDisable0/1/2.

D0F2xF4_x81 L2_ERR_RULE_CONTROL_1

Bits	Description
31:0	**ERRRuleDisable1**. Read-write. Reset: 0. Each bit in this register disables an error detection rule in the IOMMU.

D0F2xF4_x82 L2_ERR_RULE_CONTROL_2

Bits	Description
31:0	**ERRRuleDisable2**. Read-write. Reset: 0. Each bit in this register disables an error detection rule in the IOMMU.

D0F2xF4_x90 L2_L2B_CK_GATE_CONTROL

Bits	Description
31:8	Reserved.
7:6	**CKGateL2BStop**. Read-write. Reset: 01b. Bits Description 00b Allow 2 clock cycles delay before stopping the clocks when clkready deasserts. 01b Allow 4 clock cycles delay before stopping the clocks when clkready deasserts. 10b Allow 8 clock cycles delay before stopping the clocks when clkready deasserts. 11b Allow 16 clock cycles delay before stopping the clocks when clkready deasserts.
5:4	**CKGateL2BLength**. Read-write. Reset: 01b. Bits Description 00b Allow 128 clock cycles delay before stopping the clocks when idle asserts. 01b Allow 256 clock cycles delay before stopping the clocks when idle asserts. 10b Allow 512 clock cycles delay before stopping the clocks when idle asserts. 11b Allow 1024 clock cycles delay before stopping the clocks when idle asserts.
3	**CKGateL2BCacheDisable**. Read-write. Reset: 0. 1=Disable the gating of the L2B upper cache ways.
2	**CKGateL2BMiscDisable**. Read-write. Reset: 1. 1=Disable the gating of the L2B miscellaneous clock branch.
1	**CKGateL2BDynamicDisable**. Read-write. Reset: 1. BIOS: 0. 1=Disable the gating of the L2B dynamic clock branch.
0	**CKGateL2BRegsDisable**. Read-write. Reset: 1. BIOS: 0. 1=Disable the gating of the L2B TLBregister clock branch.

D0F2xF4_x92 PPR_CONTROL

Bits	Description
31:17	Reserved.
16	**PprIntcoallesceEn**. Read-write. Reset: 0. BIOS: See 2.12.2.

15:8	**PprIntreqdelay**. Read-write. Reset: 0. BIOS: See 2.12.2.
7:0	**PprInttimedelay**. Read-write. Reset: 0. BIOS: See 2.12.2.

D0F2xF4_x94 L2_L2B_PGSIZE_CONTROL

Bits	Description
31:4	Reserved.
3:2	**L2bregHostPgsize**. Read-write. Reset: 0. BIOS: See 2.12.2.
1:0	**L2bregGstPgsize**. Read-write. Reset: 0. BIOS: See 2.12.2.

D0F2xF8 IOMMU L1 Config Index

The index/data pair registers, D0F2xF8 and D0F2xFC are used to access the registers at D0F2xFC_x[FFFF:0000]_L1[3:0]. To access any of these registers, the address is first written into the index register, D0F2xF8, and then the data is read from or written to the data register, D0F2xFC.

See 2.12.1 [IOMMU Configuration Space]. There are various L1s in the IOMMU. Registers in the L1 indexed space have one instance per L1 denoted by _L1i[x] where x=D0F2xF8[L1cfgSel]. The syntax for this register type is described by the following example:

- D0F2xFC_x00 refers to all instances of the D0F2xFC_x00 registers.
- D0F2xFC_x00_L1i[0] refers to the D0F2xFC_x00 register instance for the PGD L1.

Bits	Description
31	**L1cfgEn**. Read-write. Reset: 0. 1=Enable writes to D0F2xFC.
30:20	Reserved.
19:16	**L1cfgSel**. Read-write. Reset: 0. This field selects one of the following L1s to access. Bits Definition Bits Definition 0h PGD 3h BIF 1h PSD1 4h INTGEN 2h PSD0 Fh-5h Reserved
15:0	**L1cfgIndex**. Read-write. Reset: 0.

D0F2xFC IOMMU L1 Config Data

IF (D0F2xF8[L1cfgEn]) THEN Read-write. ELSE Read-only. ENDIF. Reset: 0000_0000h. See D0F2xF8. Address: D0F2xF8[L1cfgIndex].

Bits	Description
31:0	**L1cfgData**.

D0F2xFC_x00_L1i[4:0] L1_PERF_CNTL

Bits	Description
31:24	**L1PerfCountHi1**. Read-only. Reset: 0. Read back of perf counter 1 bits [39:32].

23:16	**L1PerfCountHi0**. Read-only. Reset: 0. Read back of perf counter 0 bits [39:32].
15:8	**L1PerfEvent1**. Read-write. Reset: 0. Perf counter event 1.
7:0	**L1PerfEvent0**. Read-write. Reset: 0. Perf counter event 0.

D0F2xFC_x01_L1i[4:0] L1_PERF_COUNT_0

Bits	Description
31:0	**L1PerfCount0**. Read-only. Reset: 0. Read back of perf counter 0 bits [31:0].

D0F2xFC_x02_L1i[4:0] L1_PERF_COUNT_1

Bits	Description
31:0	**L1PerfCount1**. Read-only. Reset: 0. Read back of perf counter 1 bits [31:0].

D0F2xFC_x07_L1i[4:0] L1_DEBUG_1

Bits	Description
31:18	Reserved.
17	**L1NwEn**. Read-write. Reset: 0. BIOS: 1. 1=Enable NW bit on ATS requests.
16:15	Reserved.
14	**AtsPhysPageOverlapDis**. Read-write. Reset: 0. BIOS: 1. 1=Prevent physical page overlap for ATS responses.
13	Reserved.
12	**AtsSeqNumEn**. Read-write. Reset: 0. BIOS: 1. 1=Enable logging of ATS sequence number.
11	**SpecReqFilterEn**. Read-write. Reset: 0. BIOS: 1. 1=Filter special requests in L1 work queue.
10:1	Reserved.
0	**PhantomFuncDis**. Read-write. Reset: 0. BIOS: See 2.12.2. 1=Disable phantom function support.

D0F2xFC_x09_L1i[4:0] L1_SB_LOCATION

Bits	Description
31:16	**SbLocatedCore**. Read-only. Reset: 0.
15:0	**SbLocatedPort**. Read-write. Reset: 0. BIOS: See 2.12.2 [IOMMU Initialization]. Specifies the port location of the FCH. Bit — PortLocation [0] — FCH is located on port A of the corresponding PCIe core or internal FCH. [1] — FCH is located on port B of the corresponding PCIe core. [2] — FCH is located on port C of the corresponding PCIe core. [3] — FCH is located on port D of the corresponding PCIe core. [15:4] — Reserved.

D0F2xFC_x0C_L1i[4:0] L1_CNTRL_0

Bits	Description
31	Reserved.
30:28	**L1VirtOrderQueues**. Read-write. Reset: 0. BIOS: See 2.12.2. This field controls number of virtual queues in the L1 work queue. Bits: Description 0h: 1 1h: 2 2h: 4 3h: 8 4h: 16 7h-5h: Reserved
27:24	**L1Entries**. Read-only; updated-by-hardware. Reset: 0. This field specifies the number of entries in each L1 cache as 2^L1 entries.
23:22	Reserved.
21:20	**L1Banks**. Read-only; updated-by-hardware. Reset: 1. This field specifies number of caches in L1.
19:14	Reserved.
13:8	**L2Credits**. Read-write. Reset: 4h. This field controls credits for L1 to L2 interface.
7:6	Reserved.
5	**ReplacementSel**. Read-write. Reset: 0.
4	Reserved.
3	**CacheiwOnly**. Read-write. Reset: 1. 1=Cache write only pages in L1.
2	**CacheirOnly**. Read-write. Reset: 1. 1=Cache read only pages in L1.
1	**FragmentDis**. Read-write. Reset: 0. 1=Disable variable page size support in L1 cache - only 4K pages.
0	**UnfilterDis**. Read-write. Reset: 0. 1=Disable unfiltering in L1 wq of aborted L2 requests.

D0F2xFC_x0D_L1i[4:0] L1_CNTRL_1

Bits	Description
31:30	Reserved.
29	**Untrans2mFilteren**. Read-write. Reset: 0. Enable filtering of requests on a 2M boundry instead of 4K.
28	**PretransNovaFilteren**. Read-write. Reset: 0. When set, VA is not used for filtering pretrans requests.
27	**L1CacheSelInterleave**. Read-write. Reset: 0. When set causes cache updates to toggle between multiple caches.
26	**L1CacheSelReqid**. Read-write. Reset: 0. When set will allow the reqid to be used in hashing between multiple L1 caches.
25:23	**SelectTimeoutPulse**. Read-write. Reset: 0.
22	**L1CacheInvAllEn**. Read-write. Reset: 0. Enables invalidation of entire cache when invalidation command is sent.

21	**L1orderEn**. Read-write. Reset: 0. Enables strict ordering of all requests through L1.
20	**SndFilterDis**. Read-write. Reset: 0. Disables filtering of requests to L2.
19	**AtsNobufferInsert**. Read-write. Reset: 0. Disables buffering of read completion data when inserting ats responses.
18:14	**WqEntrydis**. Read-write. Reset: 0. Value indicates how many cache entries in L1 to disable.
13	**BlockL1Dis**. Read-only. Reset: 0.
12	**L1DTEDis**. Read-write. Reset: 0. Disables L1 caching of DTE.
11	**L1ParityEn**. Read-write. Reset: 0.
10	**L1CacheParityEn**. Read-write. Reset: 0. Enables forced miss of L1 cache due to failed parity check.
9	**CacheByPass**. Read-write. Reset: 0. Enables L1 cache bypass.
8	**VOQXorMode**. Read-write. Reset: 0.
7	Reserved.
6:4	**VOQFuncBits**. Read-write. Reset: 0.
3	Reserved.
2:0	**VOQPortBits**. Read-write. Reset: 0. !000b=Enable virtual queue hashing using port id, controls number of bits to use from port id for hashing.

D0F2xFC_x0E_L1i[4:0] L1_CNTRL_2

Bits	Description
31:28	Reserved.
27:20	**MsiHtRsvIntVector**. Read-write. Reset: 00h. This field defines the interrupt vector used when an MSI interrupt is received that has a reserved DM field.
19:12	**MsiHtRsvIntDestination**. Read-write. Reset: FFh. This field defines the interrupt destination used when an MSI interrupt is received that has a reserved DM field.
11	Reserved.
10	**MsiHtRsvIntDM**. Read-write. Reset: 0. Defines the interrupt destination mode when an MSI interrupt is received that has a reserved DM field.
9	**MsiHtRsvIntRqEio**. Read-write. Reset: 0. Specifies the RQEOI state when an MSI interrupt is received that has a reserved DM field.
8:6	**MsiHtRsvIntMt**. Read-write. Reset: 011b. Specifies the message type used when an MSI interrupt is received that has a reserved DM field.
5:3	Reserved.
2	**L1AbrtAtsDis**. Read-write. Reset: 0. 1=Disable abort of ats requests when IOMMU is disabled.
1	**MsiToHtRemapDis**. Read-write. Reset: 0. 1=Disable mapping of MSI to link interrupts.
0	Reserved.

D0F2xFC_x0F_L1i[4:0] L1_CNTRL_3

Bits	Description
31:0	**AtsTlbinvPulseWidth**. Read-write. Reset: C350h. Specifies the pulse width of the ats invalidation counters.

D0F2xFC_x10_L1i[4:0] L1_BANK_SEL_0

Bits	Description
31:16	Reserved.
15:0	**L1cachebanksel0**. Read-write. Reset: 1. Specifies value is used to determine the virtual address bit that selects between the 2 banks of the L1 cache (if present). The bank is selected by bitwise ANDing this register against virtual address bits [19:12] and XORing the result.

D0F2xFC_x11_L1i[4:0] L1_BANK_DISABLE_0

Bits	Description
31:14	Reserved.
13:8	**L1cachelinedis1**. Read-write. Reset: 0. Sets the number of cache entries to disable in cache 1.
7:6	Reserved.
5:0	**L1cachelinedis0**. Read-write. Reset: 0. Sets the number of cache entries to disable in cache 0.

D0F2xFC_x20_L1i[4:0] L1_WQ_STATUS_0

Table 109: Valid Values for D0F2xFC_x20_L1i[4:0]

Bits	Description
0h	Idle.
1h	Wait_L1.
2h	Wait_L2.
3h	Sending special request to L2.
4h	Waiting for completion of special request.
5h	Done.

Bits	Description
31:30	Reserved.
29:27	**EntryStatus9**. See: EntryStatus0.
26:24	**EntryStatus8**. See: EntryStatus0.
23:21	**EntryStatus7**. See: EntryStatus0.
20:18	**EntryStatus6**. See: EntryStatus0.
17:15	**EntryStatus5**. See: EntryStatus0.

14:12	**EntryStatus4**. See: EntryStatus0.
11:9	**EntryStatus3**. See: EntryStatus0.
8:6	**EntryStatus2**. See: EntryStatus0.
5:3	**EntryStatus1**. See: EntryStatus0.
2:0	**EntryStatus0**. Read-only. Reset: 0. See: Table 109 [Valid Values for D0F2xFC_x20_L1i[4:0]].

D0F2xFC_x21_L1i[4:0] L1_WQ_STATUS_1

Bits	Description
31:30	Reserved.
29:27	**EntryStatus19**. See: EntryStatus10.
26:24	**EntryStatus18**. See: EntryStatus10.
23:21	**EntryStatus17**. See: EntryStatus10.
20:18	**EntryStatus16**. See: EntryStatus10.
17:15	**EntryStatus15**. See: EntryStatus10.
14:12	**EntryStatus14**. See: EntryStatus10.
11:9	**EntryStatus13**. See: EntryStatus10.
8:6	**EntryStatus12**. See: EntryStatus10.
5:3	**EntryStatus11**. See: EntryStatus10.
2:0	**EntryStatus10**. Read-only. Reset: 0. See: Table 109 [Valid Values for D0F2xFC_x20_L1i[4:0]].

D0F2xFC_x22_L1i[4:0] L1_WQ_STATUS_2

Bits	Description
31:30	Reserved.
29:27	**EntryStatus29**. See: EntryStatus20.
26:24	**EntryStatus28**. See: EntryStatus20.
23:21	**EntryStatus27**. See: EntryStatus20.
20:18	**EntryStatus26**. See: EntryStatus20.
17:15	**EntryStatus25**. See: EntryStatus20.
14:12	**EntryStatus24**. See: EntryStatus20.
11:9	**EntryStatus23**. See: EntryStatus20.
8:6	**EntryStatus22**. See: EntryStatus20.
5:3	**EntryStatus21**. See: EntryStatus20.
2:0	**EntryStatus20**. Read-only. Reset: 0. See: Table 109 [Valid Values for D0F2xFC_x20_L1i[4:0]].

D0F2xFC_x23_L1i[4:0] L1_WQ_STATUS_3

Bits	Description
31:16	Reserved.
15:8	**InvalidationStatus**. Read-only. Reset: 0. Status of invalidation state machine.
7:6	Reserved.
5:3	**EntryStatus31**. See: EntryStatus30.
2:0	**EntryStatus30**. Read-only. Reset: 0. See: Table 109 [Valid Values for D0F2xFC_x20_L1i[4:0]].

D0F2xFC_x32_L1i[4:0] L1_CNTRL_4

Bits	Description
31:20	Reserved.
19:17	**ForceDmaAttrLow**. Read-write. Reset: 0.
16	**DmaNpHaltDis**. Read-write. Reset: 0.
15:10	**DmaBufMaxNpCred**. Read-write. Reset: Fh.
9:4	**DmaBufCredits**. Read-write. Reset: 10h.
3	**TlpprefixerrEn**. Read-write. Reset: 0.
2	**TimeoutPulseExtEn**. Read-write. Reset: 0.
1	**AtsMultipleL1toL2En**. Read-write. Reset: 0. BIOS: See 2.12.2.
0	**AtsMultipleRespEn**. Read-write. Reset: 0. BIOS: See 2.12.2.

D0F2xFC_x33_L1i[4:0] L1_CLKCNTRL_0

Bits	Description
31	**L1L2ClkgateEn**. Read-write. Reset: 0. BIOS: 1.
30:12	Reserved.
11	**L1HostreqClkgateEn**. Read-write. Reset: 0. BIOS: 1.
10	**L1RegClkgateEn**. Read-write. Reset: 0. BIOS: 1.
9	**L1MemoryClkgateEn**. Read-write. Reset: 0. BIOS: 1.
8	**L1PerfClkgateEn**. Read-write. Reset: 0. BIOS: 1.
7	**L1DmaInputClkgateEn**. Read-write. Reset: 0. BIOS: 1.
6	**L1CpslvClkgateEn**. Read-write. Reset: 0. BIOS: 1.
5	**L1CacheClkgateEn**. Read-write. Reset: 0. BIOS: 1.
4	**L1DmaClkgateEn**. Read-write. Reset: 0. BIOS: 1.
3:2	Reserved.
1:0	**L1ClkgateLen**. Read-write. Reset: 0.

D0F2xFC_x34_L1i[4:0] L1_MEMPWRCNTRL_0

Bits	Description
31:24	**L1MempwrTimer2**. Read-write. Reset: Fh.
23:16	**L1MempwrTimer1**. Read-write. Reset: Fh.
15:8	**L1MempwrTimer0**. Read-write. Reset: Fh.
7:1	Reserved.
0	**L1MempwrEn**. Read-write. Reset: 0.

D0F2xFC_x35_L1i[4:0] L1_MEMPWRCNTRL_1

Bits	Description
31:8	Reserved.
7:0	**L1MempwrTimer3**. Read-write. Reset: Fh.

D0F2xFC_x36_L1i[4:0] L1_GUEST_ADDR_CNTRL

Bits	Description
31:8	**L1GuestAddrMsk**. Read-write. Reset: 0.
7:1	Reserved.
0	**L1CanonicalErrEn**. Read-write. Reset: 0.

D0F2xFC_x37_L1i[4:0] L1_FEATURE_SUP_CNTRL

Bits	Description
31:2	Reserved.
1	**L1PprSup**. Read-write. Reset: 1.
0	**L1EfrSup**. Read-write. Reset: 1.

D0F2xFC_x38_L1i[4:0] L1_CNTRL_5

Bits	Description
31:14	Reserved.
13:8	**ClkOffWaitTime**. Read-write. Reset: 00_0011b. Programmable delay between clkready de-assert and lclk_idle assert (ie. turning off clk).
7:6	Reserved.
5:4	**HstCredits**. Read-write. Reset: 10b. Number of credits available for host response credit/debit interface.
3:0	**DmaCredits**. Read-write. Reset: 8h. Number of credits available for dma request credit/debit interface.

3.5 Device 1 Function 0 (Internal Graphics) Configuration Registers

See 3.1 [Register Descriptions and Mnemonics]. See 2.7 [Configuration Space].

D1F0x00 Device/Vendor ID

Bits	Description
31:16	**DeviceID: device ID**. Read-only. Value: Product-specific.
15:0	**VendorID: vendor ID**. Read-only. Value: 1002h.

D1F0x04 Status/Command Register

Reset: 0010_0000h.

Bits	Description
31	**ParityErrorDetected: detected parity error**. Read; Write-1-to-clear. 1=Poisoned TLP received.
30	**SignaledSystemError: signaled system error**. Read; Write-1-to-clear. 1=A non-fatal or fatal error message was sent and SerrEn=1.
29	**ReceivedMasterAbort: received master abort**. Read; Write-1-to-clear. 1=A completion with an unsupported request completion status was received.
28	**ReceivedTargetAbort: received target abort**. Read; Write-1-to-clear. 1=A completion with completer abort completion status was received.
27	**SignalTargetAbort: Signaled target abort**. Read-only.
26:25	**DevselTiming: DEVSEL# Timing**. Read-only.
24	**MasterDataPerr: master data parity error**. Read; Write-1-to-clear. 1=ParityErrorEn=1 and either a poisoned completion was received or the device poisoned a write request.
23	**FastBackCapable: fast back-to-back capable**. Read-only.
22	**UDFEn: UDF enable**. Read-only.
21	**PCI66En: 66 MHz capable**. Read-only.
20	**CapList: capability list**. Read-only. 1=Capability list supported.
19	**IntStatus: interrupt status**. Read-only. 1=INTx interrupt message pending.
18:11	Reserved.
10	**IntDis: interrupt disable**. Read-write. 1=INTx interrupt messages generation disabled.
9	**FastB2BEn: fast back-to-back enable**. Read-only.
8	**SerrEn: System error enable**. Read-write. 1=Enables reporting of non-fatal and fatal errors detected.
7	**Stepping: Stepping control**. Read-only.
6	**ParityErrorEn: parity error response enable**. Read-write.
5	**PalSnoopEn: VGA palette snoop enable**. Read-only.
4	**MemWriteInvalidateEn: memory write and invalidate enable**. Read-only.

3	**SpecialCycleEn: special cycle enable**. Read-only.
2	**BusMasterEn: bus master enable**. Read-write. 1=Memory and IO read and write request generation enabled.
1	**MemAccessEn: IO access enable**. Read-write. This bit controls if memory accesses targeting this device are accepted. 1=Enabled. 0=Disabled.
0	**IoAccessEn: IO access enable**. Read-write. This bit controls if IO accesses targeting this device are accepted. 1=Enabled. 0=Disabled.

D1F0x08 Class Code/Revision ID Register

Bits	Description
31:8	**ClassCode**. Value: 03_0000h.
7:0	**RevID: revision ID**. Value: Product-specific.

D1F0x0C Header Type Register

Reset: 0080_0000h.

Bits	Description
31:24	**BIST**. Read-only.
23:16	**HeaderTypeReg**. Read-only. The header type field indicates a header type 0 and that this is a multi-function device.
15:8	**LatencyTimer**. Read-only. These bits are fixed at their default value.
7:0	**CacheLineSize**. Read-write. This field specifies the system cache line size in units of double words.

D1F0x10 Graphic Memory Base Address

IF (D0F0xD4_x0109_14E2[StrapBifF064BarDisA]==1) THEN Reset: 0000_0008h. ELSE Reset: 0000_000Ch. ENDIF.

Bits	Description
31:26	**BaseAddr[31:26]: base address**. Read-write. The amount of memory requested by the graphics memory BAR is controlled by D0F0xD4_x0109_1507[StrapBifMemApSizePin] and D0F0xD4_x0109_14E1[StrapBifMemApSize].
25:4	**BaseAddr[25:4]: base address**. Read-only.
3	**Pref: prefetchable**. Read-only. 1=Prefetchable memory region.
2:1	**Type: base address register type**. Read-only. Bits — Description 00b — 32-bit BAR 01b — Reserved 10b — 64-bit BAR 11b — Reserved
0	**MemSpace: memory space type**. Read-only. 0=Memory mapped base address.

D1F0x14 Graphics Memory Base Address 64

Reset: 0000_0000h.

Bits	Description
31:0	**BaseAddr[63:32]: base address**. Read-write. This field is reseved if (D0F0xD4_x0109_14E2[StrapBifF064BarDisA]==1).

D1F0x18 Graphics Doorbell Base Address

IF (D0F0xD4_x0109_14E2[StrapBifF064BarDisA]==1) THEN Reset: 0000_0008h. ELSE Reset: 0000_000Ch. ENDIF. This register is reserved and reset is 0000_0000h if (D0F0xD4_x0109_14E1[StrapBif-DoorbellBarDis]==1).

Bits	Description
31:23	**BaseAddr[31:23]: base address**. Read-write.
22:4	**BaseAddr[22:4]: base address**. Read-only.
3	**Pref: prefetchable**. Read-only. 1=Prefetchable memory region.
2:1	**Type: base address register type**. Read-only. Bits Description 00b 32-bit BAR 01b Reserved 10b 64-bit BAR 11b Reserved
0	**MemSpace: memory space type**. Read-only. 0=Memory mapped base address.

D1F0x1C Graphics Doorbell Base Address 64

Reset: 0000_0000h.

Bits	Description
31:0	**BaseAddr[63:32]: base address**. Read-write. This field is reserved if (D0F0xD4_x0109_14E1[StrapBifDoorbellBarDis]==1 || D0F0xD4_x0109_14E2[StrapBifF064BarDisA]==1).

D1F0x20 Graphics IO Base Address

Reset: 0000_0000h. This register is called Base Address 4 if (D0F0xD4_x0109_14E2[StrapBifF064BarDisA]==1).

Bits	Description
31:0	Reserved.

D1F0x24 Graphics Memory Mapped Registers Base Address

Reset: 0000_0000h.

Bits	Description
31:16	**BaseAddr[31:16]: base address**. Read-write. The amount of memory requested by the graphics memory mapped registers BAR is controlled by D0F0xD4_x0109_14E1[StrapBifRegApSize].
15:4	**BaseAddr[15:4]: base address**. Read-only.
3	**Pref: prefetchable**. Read-only. 0=Non-prefetchable memory region.
2:1	**Type: base address register type**. Read-only. 00b=32-bit BAR.
0	**MemSpace: memory space type**. Read-only. 0=Memory mapped base address.

D1F0x2C Subsystem and Subvendor ID Register

Reset: 0000_0000h. This register can be modified through D1F0x4C

Bits	Description
31:16	**SubsystemID**. Read-only.
15:0	**SubsystemVendorID**. Read-only.

D1F0x30 Expansion ROM Base Address

Reset: 0000_0000h.

Bits	Description
31:0	Reserved.

D1F0x34 Capabilities Pointer

Reset: 0000_0050h.

Bits	Description
31:8	Reserved.
7:0	**CapPtr: capabilities pointer**. Read-only. Pointer to PM capability.

D1F0x3C Interrupt Line

Reset: 0000_01FFh.

Bits	Description
31:16	Reserved.
15:8	**InterruptPin: interrupt pin**. Read-only. This field identifies the legacy interrupt message the function uses.
7:0	**InterruptLine: interrupt line**. Read-write. This field contains the interrupt line routing information.

D1F0x4C Subsystem and Subvendor ID Mirror

Reset: 0000_0000h.

Bits	Description
31:16	**SubsystemID**. Read-write. This field sets the value in the corresponding field in D1F0x2C.
15:0	**SubsystemVendorID**. Read-write. This field sets the value in the corresponding field in D1F0x2C.

D1F0x50 Power Management Capability

Bits	Description
31:27	**PmeSupport**. Value: 0_0000b. Indicates that there is no PME support.
26	**D2Support: D2 support**. Value: 1. D2 is supported.
25	**D1Support: D1 support**. Value: 1. D1 is supported.
24:22	**AuxCurrent: auxiliary current**. Value: 0.
21	**DevSpecificInit: device specific initialization**. Value: 0. Indicates that there is no device specific initialization necessary.
20	Reserved.
19	**PmeClock**. Value: 0.
18:16	**Version: version**. Value: 011b.
15:8	**NextPtr: next pointer**. Value: 58h.
7:0	**CapID: capability ID**. Value: 01h. Indicates that the capability structure is a PCI power management data structure.

D1F0x54 Power Management Control and Status

Reset: 0000_0000h.

Bits	Description
31:24	**PmeData**. Read-only.
23	**BusPwrEn**. Read-only.
22	**B2B3Support**. Read-only. B states are not supported.
21:16	Reserved.
15	**PmeStatus: PME status**. Read-only.
14:13	**DataScale: data scale**. Read-only.
12:9	**DataSelect: data select**. Read-only.
8	**PmeEn: PME# enable**. Read-only.
7:4	Reserved.
3	**NoSoftReset: no soft reset**. Read-only. Software is required to re-initialize the function when returning from $D3_{hot}$.

2	Reserved.
1:0	**PowerState: power state**. Read-write. This 2-bit field is used both to determine the current power state of the root port and to set the root port into a new power state. Bits Definition 00b D0 11b $D3_{hot}$

D1F0x58 PCI Express Capability

Bits	Description
31:30	Reserved.
29:25	**IntMessageNum: interrupt message number**. Value: 0. This field indicates which MSI vector is used for the interrupt message.
24	**SlotImplemented: Slot implemented**. Value: 0.
23:20	**DeviceType: device type**. Value: 9h.
19:16	**Version**. Value: 2h.
15:8	**NextPtr: next pointer**. Value: Product-specific.
7:0	**CapID: capability ID**. Value: 10h.

D1F0x5C Device Capability

Bits	Description
31:29	Reserved.
28	**FlrCapable: function level reset capability**. Value: 0.
27:26	**CapturedSlotPowerScale: captured slot power limit scale**. Value: 0.
25:18	**CapturedSlotPowerLimit: captured slot power limit value**. Value: 0.
17:16	Reserved.
15	**RoleBasedErrReporting: role-based error reporting**. Value: 1.
14:12	Reserved.
11:9	**L1AcceptableLatency: endpoint L1 Acceptable Latency**. Value: 111b.
8:6	**L0SAcceptableLatency: endpoint L0s Acceptable Latency**. Value: 110b.
5	**ExtendedTag: extended tag support**. Value: 1. 8-bit tag support.
4:3	**PhantomFunc: phantom function support**. Value: 0. No phantom functions supported.
2:0	**MaxPayloadSupport: maximum supported payload size**. Value: 000b. 128 bytes max payload size.

D1F0x60 Device Control and Status

Reset: 0000_0810h.

Bits	Description
31:22	Reserved.

21	**TransactionsPending: transactions pending**. Read-only.
20	**AuxPwr: auxiliary power**. Read-only.
19	**UsrDetected: unsupported request detected**. Read; Write-1-to-clear. 1=Unsupported request received.
18	**FatalErr: fatal error detected**. Read; Write-1-to-clear. 1=Fatal error detected.
17	**NonFatalErr: non-fatal error detected**. Read; Write-1-to-clear. 1=Non-fatal error detected.
16	**CorrErr: correctable error detected**. Read; Write-1-to-clear. 1=Correctable error detected.
15	**BridgeCfgRetryEn: bridge configuration retry enable**. Read-only.
14:12	**MaxRequestSize: maximum request size**. Read-only.
11	**NoSnoopEnable: enable no snoop**. Read-write. 1=The device is permitted to set the No Snoop bit in requests.
10	**AuxPowerPmEn: auxiliary power PM enable**. Read-only. This capability is not implemented.
9	**PhantomFuncEn: phantom functions enable**. Read-only. Phantom functions are not supported.
8	**ExtendedTagEn: extended tag enable**. Read-write. 1=8-bit tag request tags. 0=5-bit request tag.
7:5	**MaxPayloadSize: maximum supported payload size**. Read-only. 000b=Indicates a 128 byte maximum payload size.
4	**RelaxedOrdEn: relaxed ordering enable**. Read-write. 1=The device is permitted to set the Relaxed Ordering bit.
3	**UsrReportEn: unsupported request reporting enable**. Read-write. 1=Enables signaling unsupported requests by sending error messages.
2	**FatalErrEn: fatal error reporting enable**. Read-write. 1=Enables sending ERR_FATAL message when a fatal error is detected.
1	**NonFatalErrEn: non-fatal error reporting enable**. Read-write. 1=Enables sending ERR_NONFATAL message when a non-fatal error is detected.
0	**CorrErrEn: correctable error reporting enable**. Read-write. 1=Enables sending ERR_CORR message when a correctable error is detected.

D1F0x64 Link Capability

Bits	Description
31:24	**PortNumber: port number**. Read-only. Value: 0. This field indicates the PCI Express port number for the given PCI Express link.
23	Reserved.
22	**AspmOptionalityCompliance: ASP Optionality ECN capability**. Read-only. Value: 0.
21	**LinkBWNotificationCap: link bandwidth notification capability**. Read-only. Value: 0.
20	**DlActiveReportingCapable: data link layer active reporting capability**. Read-only. Value: 0.
19	**SurpriseDownErrReporting: surprise down error reporting capability**. Read-only. Value: 0.
18	**ClockPowerManagement: clock power management**. Read-only. Value: 0.
17:15	**L1ExitLatency: L1 exit latency**. Read-only. Value: 0.
14:12	**L0sExitLatency: L0s exit latency**. Read-only. Value: 0.
11:10	**PMSupport: active state power management support**. Read-only. Value: 0.

9:4	**LinkWidth: maximum link width**. Read-only. Value: 0.
3:0	**LinkSpeed: link speed**. Read-only. Value: 0.

D1F0x68 Link Control and Status

Reset: 0000_0000h.

Bits	Description
31	**LinkAutonomousBWStatus: link autonomous bandwidth status**. Read-only.
30	**LinkBWManagementStatus: link bandwidth management status**. Read-only.
29	**DlActive: data link layer link active**. Read-only. This bit indicates the status of the data link control and management state machine. Reads return a 1 to indicate the DL_Active state, otherwise 0 is returned.
28	**SlotClockCfg: slot clock configuration**. Read-only. 1=Root port uses the same clock that the platform provides.
27	**LinkTraining: link training**. Read-only. 1=Indicates that the physical layer link training state machine is in the configuration or recovery state, or that 1b was written to the RetrainLink bit but link training has not yet begun. Hardware clears this bit when the link training state machine exits the configuration/recovery state.
26	Reserved.
25:20	**NegotiatedLinkWidth: negotiated link width**. Read-only. This field indicates the negotiated width of the given PCI Express link.
19:16	**LinkSpeed: link speed**. Read-only.
15:12	Reserved.
11	**LinkAutonomousBWIntEn: link autonomous bandwidth interrupt enable**. Read-only.
10	**LinkBWManagementEn: link bandwidth management interrupt enable**. Read-only.
9	**HWAutonomousWidthDisable: hardware autonomous width disable**. Read-only. 1=Hardware not allowed to change the link width except to correct unreliable link operation by reducing link width.
8	**ClockPowerManagementEn: clock power management enable**. Read-only.
7	**ExtendedSync: extended sync**. Read-only. 1=Forces the transmission of additional ordered sets when exiting the L0s state and when in the recovery state.
6	**CommonClockCfg: common clock configuration**. Read-only. 1=Indicates that the root port and the component at the opposite end of this Link are operating with a distributed common reference clock. 0=Indicates that the upstream port and the component at the opposite end of this Link are operating with asynchronous reference clock.
5	**RetrainLink: retrain link**. Read-only. This bit does not apply to endpoints.
4	**LinkDis: link disable**. Read-only. This bit does not apply to endpoints.
3	**ReadCplBoundary: read completion boundary**. Read-only. 0=64 byte read completion boundary.
2	Reserved.
1:0	**PmControl: active state power management enable**. Read-only. This field controls the level of ASPM supported on the given PCI Express link. Bits Definition — Bits Definition 00b Disabled. — 10b L1 Entry Enabled. 01b L0s Entry Enabled. — 11b L0s and L1 Entry Enabled.

D1F0x7C Device Capability 2

Reset: 0000_0000h.

Bits	Description
31:24	Reserved.
23:22	**MaxEndEndTlpPrefixes: Max number of End-End TLP prefixes supported**. Read-only. IF (D1F0x7C[EndEndTlpPrefixSupported]==0) THEN Reserved. ENDIF. Bits Definition Bits Definition 00b 4 End-End TLP Prefixes. 10b 2 End-End TLP Prefixes. 01b 1 End-End TLP Prefix. 11b 3 End-End TLP Prefixes.
21	**EndEndTlpPrefixSupported: End-End TLP Prefix supported**. Read-only.
20	**ExtendedFmtFieldSupported**. Read-only. 1=Function supports 3-bit definition of Fmt field. 0=Function supports 2-bit definition of Fmt field.
19:18	**ObffSupported: Optimized buffer flush/fill supported**. Read-only.
17:14	Reserved.
13:12	**TphCplrSupported**. Read-only.
11	**LtrSupported: Latency Tolerance Reporting supported**. Read-only.
10	**NoRoEnabledP2pPassing**. Read-only.
9:6	Reserved.
5	**AriForwardingSupported: ARI forwarding supported**. Read-only.
4	**CplTimeoutDisSupported: completion timeout disable supported**. Read-only.
3:0	**CplTimeoutRangeSupported: completion timeout range supported**. Read-only.

D1F0x80 Device Control and Status 2

Reset: 0000_0000h.

Bits	Description
31:16	Reserved.
15	**EndEndTlpPrefixBlocking**. Read-only.
14:13	**ObffEn**. Read-only.
12:11	Reserved.
10	**LtrEn**. Read-only.
9	**IdoCompletionEn**. Read-only.
8	**IdoRequestEn**. Read-only.
7:6	Reserved.
5	**AriForwardingEn**. Read-only.
4	**CplTimeoutDis: completion timeout disable**. Read-only.
3:0	**CplTimeoutValue: completion timeout range supported**. Read-only.

D1F0x84 Link Capability 2

Bits	Description
31:9	Reserved.
8	**CrosslinkSupported: Crosslink Spported**. Read-only. Reset: 0. 1=Crosslink supported.
7:1	**SupportedLinkSpeed: Supported Link Speed**. Read-only. Reset: 07h. Specifies what link speeds are supported. Bit [1] = 2.5 GT/s, Bit [2] = 5.0 Gt/s, Bit [3] = 8.0 GT/s. The rest are reserved.
0	Reserved.

D1F0x88 Link Control and Status 2

Reset: 0000_0000h.

Bits	Description
31:22	Reserved.
21	**LinkEqualizationRequest**. Read-only. Set when hardware requests link equalization to be performed.
20	**EqualizationPhase3Success: Phase3 of Tx equalization procedure completed**. Read-only.
19	**EqualizationPhase2Success: Phase2 of Tx equalization procedure completed**. Read-only.
18	**EqualizationPhase1Success: Phase1 of Tx equalization procedure completed**. Read-only.
17	**EqualizationComplete: Tx equalization procedure completed**. Read-only.
16	**CurDeemphasisLevel: current deemphasis level**. Read-only. 1=-3.5 dB. 0=-6 dB.
15:13	Reserved.
12	**ComplianceDeemphasis: compliance deemphasis**. Read-only. This bit definesthe deemphasis level used in compliance mode. 1=-3.5 dB. 0=-6 dB.
11	**ComplianceSOS: compliance SOS**. Read-only. 1=The device transmits skip ordered sets in between the modified compliance pattern.
10	**EnterModCompliance: enter modified compliance**. Read-only. 1=The device transmits modified compliance pattern.
9:7	**XmitMargin: transmit margin**. Read-only. This field controls the non-deemphasized voltage level at the transmitter pins.
6	**SelectableDeemphasis: selectable deemphasis**. Read-only.
5	**HwAutonomousSpeedDisable: hardware autonomous speed disable**. Read-only. 1=Disables hardware generated link speed changes.
4	**EnterCompliance: enter compliance**. Read-only. 1=Force link to enter compliance mode.
3:0	**TargetLinkSpeed: target link speed**. Read-only. This field defines the upper limit of the link operational speed.

D1F0xA0 MSI Capability

Bits	Description
31:24	Reserved.

23	**Msi64bit: MSI 64 bit capability**. Read-only. Reset: 1. 1=The device is capable of sending 64-bit MSI messages. 0=The device is not capable of sending a 64-bit message address.
22:20	**MsiMultiEn: MSI multiple message enable**. Read-write. Reset: 000b. Software writes to this field to indicate the number of allocated vectors (equal to or less than the number of requested vectors). When MSI is enabled, a function is allocated at least 1 vector.
19:17	**MsiMultiCap: MSI multiple message capability**. Read-only. Reset: 000b. 000b=The device is requesting one vector.
16	**MsiEn: MSI enable**. Read-write. Reset: 0. 1=MSI generation is enabled and INTx generation is disabled. 0=MSI generation disabled and INTx generation is enabled.
15:8	**NextPtr: next pointer**. Read-only. Reset:00h.
7:0	**CapID: capability ID**. Read-only. Reset: 05h. 05h=MSI capability structure.

D1F0xA4 MSI Message Address Low

Reset: 0000_0000h.

Bits	Description
31:2	**MsiMsgAddrLo: MSI message address**. Read-write. This register specifies the dword aligned address for the MSI memory write transaction.
1:0	Reserved.

D1F0xA8 MSI Message Address High

Reset: 0000_0000h.

Bits	Description
31:8	Reserved.
7:0	**MsiMsgAddrHi: MSI message address**. Read-write. This register specifies the upper 8 bits of the MSI address in 64-bit MSI mode.

D1F0xAC MSI Message Data

Reset: 0000_0000h.

Bits	Description
31:16	Reserved.
15:0	**MsiData: MSI message data**. Read-write. This register specifies lower 16 bits of data for the MSI memory write transaction. The upper 16 bits are always 0.

D1F0x100 Vendor Specific Enhanced Capability

Reset: 0061_000Bh.

Bits	Description
31:20	**NextPtr: next pointer**. Read-only.

19:16	**CapVer: capability version**. Read-only.
15:0	**CapID: capability ID**. Read-only.

D1F0x104 Vendor Specific Header

Reset: 0101_0001h.

Bits	Description
31:20	**VsecLen: vendor specific enhanced next pointer**. Read-only.
19:16	**VsecRev: vendor specific enhanced capability version**. Read-only.
15:0	**VsecID: vendor specific enhanced capability ID**. Read-only.

D1F0x108 Vendor Specific 1

Reset: 0000_0000h.

Bits	Description
31:0	**Scratch: scratch**. Read-write.

D1F0x10C Vendor Specific 2

Reset: 0000_0000h.

Bits	Description
31:0	**Scratch: scratch**. Read-write.

3.6 Device 1 Function 1 (Audio Controller) Configuration Registers

See 3.1 [Register Descriptions and Mnemonics] for a description of the register naming convention. See 2.7 [Configuration Space] for details about how to access this space.

D1F1x00 Device/Vendor ID

Bits	Description
31:16	**DeviceID: device ID**. Read-only. Value: Product-specific.
15:0	**VendorID: vendor ID**. Read-only. Value: 1002h.

D1F1x04 Status/Command

Reset: 0010_0000h.

Bits	Description
31	**ParityErrorDetected: detected parity error**. Read; Write-1-to-clear. 1=Poisoned TLP received.
30	**SignaledSystemError: signaled system error**. Read; Write-1-to-clear. 1=A non-fatal or fatal error message was sent and SerrEn=1.
29	**ReceivedMasterAbort: received master abort**. Read; Write-1-to-clear. 1=A completion with an unsupported request completion status was received.
28	**ReceivedTargetAbort: received target abort**. Read; Write-1-to-clear. 1=A completion with completer abort completion status was received.
27	**SignalTargetAbort: Signaled target abort**. Read-only.
26:25	**DevselTiming: DEVSEL# Timing**. Read-only.
24	**MasterDataPerr: master data parity error**. Read; Write-1-to-clear. 1=(ParityErrorEn==1) and either a poisoned completion was received or the device poisoned a write request.
23	**FastBackCapable: fast back-to-back capable**. Read-only.
22	**UDFEn: UDF enable**. Read-only.
21	**PCI66En: 66 MHz capable**. Read-only.
20	**CapList: capability list**. Read-only. 1=Capability list supported.
19	**IntStatus: interrupt status**. Read-only. 1=INTx interrupt message pending.
18:11	Reserved.
10	**IntDis: interrupt disable**. Read-write. 1=INTx interrupt messages generation disabled.
9	**FastB2BEn: fast back-to-back enable**. Read-only.
8	**SerrEn: System error enable**. Read-write. 1=Enables reporting of non-fatal and fatal errors detected.
7	**Stepping: Stepping control**. Read-only.
6	**ParityErrorEn: parity error response enable**. Read-write.
5	**PalSnoopEn: VGA palette snoop enable**. Read-only.

4	**MemWriteInvalidateEn: memory write and invalidate enable**. Read-only.
3	**SpecialCycleEn: special cycle enable**. Read-only.
2	**BusMasterEn: bus master enable**. Read-write. 1=Memory and IO read and write request generation enabled.
1	**MemAccessEn: IO access enable**. Read-write. This bit controls if memory accesses targeting this device are accepted. 1=Enabled. 0=Disabled.
0	**IoAccessEn: IO access enable**. Read-write. This bit controls if IO accesses targeting this device are accepted. 1=Enabled. 0=Disabled.

D1F1x08 Class Code/Revision ID

Reset: 0403_0000h.

Bits	Description
31:8	**ClassCode**. Read-only.
7:0	**RevID: revision ID**. Read-only.

D1F1x0C Header Type

Reset: 0080_0000h.

Bits	Description
31:24	**BIST**. Read-only. These bits are fixed at their default values.
23:16	**HeaderTypeReg**. Read-only. 80h=Type 0 multi-function device.
15:8	**LatencyTimer**. Read-only. These bits are fixed at their default value.
7:0	**CacheLineSize**. Read-write. This field specifies the system cache line size in units of double words.

D1F1x10 Audio Registers Base Address

Reset: 0000_0000h.

Bits	Description
31:14	**BaseAddr: base address**. Read-write.
13:4	Reserved.
3	**Pref: prefetchable**. Read-only. 0=Non-prefetchable memory region.
2:1	**Type: base address register type**. Read-only. 00b=32-bit base address register.
0	**MemSpace: memory space type**. Read-only. 0=Memory mapped base address.

D1F1x14 Base Address 1

Reset: 0000_0000h.

Bits	Description
31:0	Reserved.

D1F1x18 Base Address 2

Reset: 0000_0000h.

Bits	Description
31:0	Reserved.

D1F1x1C Base Address 3

Reset: 0000_0000h.

Bits	Description
31:0	Reserved.

D1F1x20 Base Address 4

Reset: 0000_0000h.

Bits	Description
31:0	Reserved.

D1F1x24 Base Address 5

Reset: 0000_0000h.

Bits	Description
31:0	Reserved.

D1F1x2C Subsystem and Subvendor ID

Reset: 0000_0000h. This register can be modified through D1F1x4C.

Bits	Description
31:16	**SubsystemID**. Read-only.
15:0	**SubsystemVendorID**. Read-only.

D1F1x30 Expansion ROM Base Address

Reset: 0000_0000h.

Bits	Description
31:0	Reserved.

D1F1x34 Capabilities Pointer

Reset: 0000_0050h.

Bits	Description
31:8	Reserved.
7:0	**CapPtr: capabilities pointer**. Read-only. Pointer to PM capability.

D1F1x3C Interrupt Line

Reset: 0000_02FFh.

Bits	Description
31:16	Reserved.
15:8	**InterruptPin: interrupt pin**. Read-only. This field identifies the legacy interrupt message the function uses.
7:0	**InterruptLine: interrupt line**. Read-write. This field contains the interrupt line routing information.

D1F1x4C Subsystem and Subvendor ID Mirror

Reset: 0000_0000h.

Bits	Description
31:16	**SubsystemID**. Read-write. This field sets the value in the corresponding field in D1F1x2C.
15:0	**SubsystemVendorID**. Read-write. This field sets the value in the corresponding field in D1F1x2C.

D1F1x50 Power Management Capability

Bits	Description
31:27	**PmeSupport**. Value: 0_0000b. Indicates that there is no PME support.
26	**D2Support: D2 support**. Value: 1. D2 is supported.
25	**D1Support: D1 support**. Value: 1. D1 is supported.
24:22	**AuxCurrent: auxiliary current**. Value: 0.
21	**DevSpecificInit: device specific initialization**. Value: 0. Indicates that there is no device specific initialization necessary.
20	Reserved.
19	**PmeClock**. Value: 0.
18:16	**Version: version**. Value: 011b.
15:8	**NextPtr: next pointer**. Value: 00h.
7:0	**CapID: capability ID**. Value: 01h. Indicates that the capability structure is a PCI power management data structure.

D1F1x54 Power Management Control and Status

Reset: 0000_0000h.

Bits	Description
31:24	**PmeData**. Read-only.
23	**BusPwrEn**. Read-only.
22	**B2B3Support**. Read-only. B states are not supported.
21:16	Reserved.
15	**PmeStatus: PME status**. Read-only.
14:13	**DataScale: data scale**. Read-only.
12:9	**DataSelect: data select**. Read-only.
8	**PmeEn: PME# enable**. Read-only.
7:4	Reserved.
3	**NoSoftReset: no soft reset**. Read-only. Software is required to re-initialize the function when returning from $D3_{hot}$.
2	Reserved.
1:0	**PowerState: power state**. Read-write. This 2-bit field is used both to determine the current power state of the root port and to set the root port into a new power state. Bits — Definition 00b — D0 10b-01b — Reserved 11b — $D3_{hot}$

D1F1x58 PCI Express Capability

Bits	Description
31:30	Reserved.
29:25	**IntMessageNum: interrupt message number**. Value: 0. This field indicates which MSI vector is used for the interrupt message.
24	**SlotImplemented: Slot implemented**. Value: 0.
23:20	**DeviceType: device type**. Value: 9h.
19:16	**Version**. Value: 2h.
15:8	**NextPtr: next pointer**. Value: Product-specific.
7:0	**CapID: capability ID**. Value: 10h.

D1F1x5C Device Capability

Bits	Description
31:29	Reserved.
28	**FlrCapable: function level reset capability**. Value: Product-specific.
27:26	**CapturedSlotPowerScale: captured slot power limit scale**. Value: 0.

25:18	**CapturedSlotPowerLimit: captured slot power limit value**. Value: 0.
17:16	Reserved.
15	**RoleBasedErrReporting: role-based error reporting**. Value: 1.
14:12	Reserved.
11:9	**L1AcceptableLatency: endpoint L1 Acceptable Latency**. Value: 111b.
8:6	**L0SAcceptableLatency: endpoint L0s Acceptable Latency**. Value: 110b.
5	**ExtendedTag: extended tag support**. Value: 1. 8-bit tag support.
4:3	**PhantomFunc: phantom function support**. Value: 0. No phantom functions supported.
2:0	**MaxPayloadSupport: maximum supported payload size**. Value: 000b. 128 bytes max payload size.

D1F1x60 Device Control and Status

Reset: 0000_0810h.

Bits	Description
31:22	Reserved.
21	**TransactionsPending: transactions pending**. Read-only.
20	**AuxPwr: auxiliary power**. Read-only.
19	**UsrDetected: unsupported request detected**. Read; Write-1-to-clear. 1=Unsupported request received.
18	**FatalErr: fatal error detected**. Read; Write-1-to-clear. 1=Fatal error detected.
17	**NonFatalErr: non-fatal error detected**. Read; Write-1-to-clear. 1=Non-fatal error detected.
16	**CorrErr: correctable error detected**. Read; Write-1-to-clear. 1=Correctable error detected.
15	**BridgeCfgRetryEn: bridge configuration retry enable**. Read-only.
14:12	**MaxRequestSize: maximum request size**. Read-only. 0=The root port never generates read requests with size exceeding 128 bytes.
11	**NoSnoopEnable: enable no snoop**. Read-write. 1=The device is permitted to set the No Snoop bit in requests.
10	**AuxPowerPmEn: auxiliary power PM enable**. Read-only. This capability is not implemented.
9	**PhantomFuncEn: phantom functions enable**. Read-only. Phantom functions are not supported.
8	**ExtendedTagEn: extended tag enable**. Read-write. 1=8-bit tag request tags. 0=5-bit request tag.
7:5	**MaxPayloadSize: maximum supported payload size**. Read-only. 000b=Indicates a 128 byte maximum payload size.
4	**RelaxedOrdEn: relaxed ordering enable**. Read-write. 1=The device is permitted to set the Relaxed Ordering bit.
3	**UsrReportEn: unsupported request reporting enable**. Read-write. 1=Enables signaling unsupported requests by sending error messages.
2	**FatalErrEn: fatal error reporting enable**. Read-write. 1=Enables sending ERR_FATAL message when a fatal error is detected.

1	**NonFatalErrEn: non-fatal error reporting enable**. Read-write. 1=Enables sending ERR_NONFATAL message when a non-fatal error is detected.
0	**CorrErrEn: correctable error reporting enable**. Read-write. 1=Enables sending ERR_CORR message when a correctable error is detected.

D1F1x64 Link Capability

Bits	Description
31:24	**PortNumber: port number**. Value: 0. This field indicates the PCI Express port number for the given PCI Express link.
23:22	Reserved.
21	**LinkBWNotificationCap: link bandwidth notification capability**. Read-only. Value: 0b.
20	**DlActiveReportingCapable: data link layer active reporting capability**. Read-only. Value: 0b.
19	**SurpriseDownErrReporting: surprise down error reporting capability**. Read-only. Value: 0b.
18	**ClockPowerManagement: clock power management**. Read-only. Value: 0b.
17:15	**L1ExitLatency: L1 exit latency**. Read-only. Value: 0b.
14:12	**L0sExitLatency: L0s exit latency**. Read-only. Value: 0b.
11:10	**PMSupport: active state power management support**. Read-only. Value: 0b.
9:4	**LinkWidth: maximum link width**. Read-only. Value: 0.
3:0	**LinkSpeed: link speed**. Read-only. Value: 0b.

D1F1x68 Link Control and Status

Reset: 0000_0000h.

Bits	Description
31	**LinkAutonomousBWStatus: link autonomous bandwidth status**. Read-only.
30	**LinkBWManagementStatus: link bandwidth management status**. Read-only.
29	**DlActive: data link layer link active**. Read-only. This bit indicates the status of the data link control and management state machine. Reads return a 1 to indicate the DL_Active state, otherwise 0 is returned.
28	**SlotClockCfg: slot clock configuration**. Read-only. 1=The root port uses the same clock that the platform provides.
27	**LinkTraining: link training**. Read-only. 1=Indicates that the physical layer link training state machine is in the configuration or recovery state, or that 1b was written to the RetrainLink bit but link training has not yet begun. Hardware clears this bit when the link training state machine exits the configuration/recovery state.
26	Reserved.
25:20	**NegotiatedLinkWidth: negotiated link width**. Read-only. This field indicates the negotiated width of the given PCI Express link.

19:16	**LinkSpeed: link speed**. Read-only. Bits: Description 0h: Reserved 1h: 2.5 Gb/s. 2h: 5 Gb/s. Fh-3h: Reserved
15:12	Reserved.
11	**LinkAutonomousBWIntEn: link autonomous bandwidth interrupt enable**. Read-only.
10	**LinkBWManagementEn: link bandwidth management interrupt enable**. Read-only.
9	**HWAutonomousWidthDisable: hardware autonomous width disable**. Read-only. 1=Hardware not allowed to change the link width except to correct unreliable link operation by reducing link width.
8	**ClockPowerManagementEn: clock power management enable**. Read-only.
7	**ExtendedSync: extended sync**. Read-only. 1=Forces the transmission of additional ordered sets when exiting the L0s state and when in the recovery state.
6	**CommonClockCfg: common clock configuration**. Read-only. 1=Indicates that the root port and the component at the opposite end of this Link are operating with a distributed common reference clock. 0=Indicates that the upstream port and the component at the opposite end of this Link are operating with asynchronous reference clock.
5	**RetrainLink: retrain link**. Read-only. This bit does not apply to endpoints.
4	**LinkDis: link disable**. Read-only. This bit does not apply to endpoints.
3	**ReadCplBoundary: read completion boundary**. Read-only. 0=64 byte read completion boundary.
2	Reserved.
1:0	**PmControl: active state power management enable**. Read-only. This field controls the level of ASPM supported on the given PCI Express link. Bits: Definition: Bits: Definition 00b: Disabled. 10b: L1 Entry Enabled. 01b: L0s Entry Enabled. 11b: L0s and L1 Entry Enabled.

D1F1x7C Device Capability 2

Reset: 0000_0000h.

Bits	Description
31:5	Reserved.
4	**CplTimeoutDisSup: completion timeout disable supported**. Read-only.
3:0	**CplTimeoutRangeSup: completion timeout range supported**. Read-only.

D1F1x80 Device Control and Status 2

Reset: 0000_0000h.

Bits	Description
31:5	Reserved.
4	**CplTimeoutDis: completion timeout disable**. Read-only.
3:0	**CplTimeoutValue: completion timeout range supported**. Read-only.

D1F1x84 Link Capability 2

Bits	Description
31:0	Reserved.

D1F1x88 Link Control and Status 2

Reset: 0000_0000h.

Bits	Description
31:17	Reserved.
16	**CurDeemphasisLevel: current deemphasis level**. Read-only. 1=-3.5 dB. 0=-6 dB.
15:13	Reserved.
12	**ComplianceDeemphasis: compliance deemphasis**. Read-only. This bit defines the deemphasis level used in compliance mode. 1=-3.5 dB. 0=-6 dB.
11	**ComplianceSOS: compliance SOS**. Read-only. 1=The device transmits skip ordered sets in between the modified compliance pattern.
10	**EnterModCompliance: enter modified compliance**. Read-only. 1=The device transmits modified compliance pattern.
9:7	**XmitMargin: transmit margin**. Read-only. This field controls the non-deemphasized voltage level at the transmitter pins.
6	**SelectableDeemphasis: selectable deemphasis**. Read-only.
5	**HwAutonomousSpeedDisable: hardware autonomous speed disable**. Read-only. 1=Disables hardware generated link speed changes.
4	**EnterCompliance: enter compliance**. Read-only. 1=Force link to enter compliance mode.
3:0	**TargetLinkSpeed: target link speed**. Read-only. This fields defines the upper limit of the link operational speed.

D1F1xA0 MSI Capability

Bits	Description
31:24	Reserved.
23	**Msi64bit: MSI 64 bit capability**. Read-only. Reset: 1. 1=The device is capable of sending 64-bit MSI messages. 0=The device is not capable of sending a 64-bit message address.
22:20	**MsiMultiEn: MSI multiple message enable**. Read-write. Reset: 000b. Software writes to this field to indicate the number of allocated vectors (equal to or less than the number of requested vectors). When MSI is enabled, a function is allocated at least 1 vector.
19:17	**MsiMultiCap: MSI multiple message capability**. Read-only. Reset: 000b. 000b=The device is requesting one vector.
16	**MsiEn: MSI enable**. Read-write. Reset: 0. 1=MSI generation is enabled and INTx generation is disabled. 0=MSI generation disabled and INTx generation is enabled.
15:8	**NextPtr: next pointer**. Read-only. Reset: 00h.
7:0	**CapID: capability ID**. Read-only. Reset: 05h. 05h=MSI capability structure.

D1F1xA4 MSI Message Address Low

Reset: 0000_0000h.

Bits	Description
31:2	**MsiMsgAddrLo: MSI message address**. Read-write. This register specifies the dword aligned address for the MSI memory write transaction.
1:0	Reserved.

D1F1xA8 MSI Message Address High

Reset: 0000_0000h.

Bits	Description
31:8	Reserved.
7:0	**MsiMsgAddrHi: MSI message address**. Read-write. This register specifies the upper 8 bits of the MSI address in 64-bit MSI mode.

D1F1xAC MSI Message Data

Reset: 0000_0000h.

Bits	Description
31:16	Reserved.
15:0	**MsiData: MSI message data**. Read-write. This register specifies lower 16 bits of data for the MSI memory write transaction. The upper 16 bits are always 0.

D1F1x100 Vendor Specific Enhanced Capability

Reset: 0111_000Bh.

Bits	Description
31:20	**NextPtr: next pointer**. Read-only.
19:16	**CapVer: capability version**. Read-only.
15:0	**CapID: capability ID**. Read-only.

D1F1x104 Vendor Specific Header

Reset: 0101_0001h.

Bits	Description
31:20	**VsecLen: vendor specific enhanced next pointer**. Read-only.
19:16	**VsecRev: vendor specific enhanced capability version**. Read-only.
15:0	**VsecID: vendor specific enhanced capability ID**. Read-only.

D1F1x108 Vendor Specific 1

Reset: 0000_0000h.

Bits	Description
31:0	**Scratch: scratch**. Read-write.

D1F1x10C Vendor Specific 2

Reset: 0000_0000h.

Bits	Description
31:0	**Scratch: scratch**. Read-write.

3.7 Device [4:2] Function 0 (Host Bridge) Configuration Registers

See 3.1 [Register Descriptions and Mnemonics] for a description of the register naming convention. See 2.7 [Configuration Space] for details about how to access this space. D[4:2]F0 registers do not control any hardware. They ensure that software can configure functions 1 through 4.

D[4:2]F0x00 Device/Vendor ID (Host Bridge)

Bits	Description
31:16	**DeviceID: device ID**. Read-only. Value: 1424h.
15:0	**VendorID: vendor ID**. Read-only. Value: 1022h.

D[4:2]F0x04 Status/Command

Reset: 0000_0000h.

Bits	Description
31:16	**Status**. Read-only.
15:0	**Command**. Read-only.

D[4:2]F0x08 Class Code/Revision ID

Reset: 0600_0000h.

Bits	Description
31:8	**ClassCode: class code**. Read-only.
7:0	**RevId: revision identifier**. Read-only.

D[4:2]F0x0C Header Type

Reset: 0080_0000h.

Bits	Description
31:24	Reserved.
23	**DeviceType**. Read-only. 1=Indicates that the northbridge block is a multi-function device. 0=Indicates that the northbridge block is a single function device.
22:16	**HeaderType**. Read-only. Indicates multiple functions present in this device.
15:0	Reserved.

D[4:2]F0x40 Header Type Write

Reset: 0080_0000h.

Bits	Description
31:8	Reserved.
7	**DeviceType**. Read-write. This field sets the value in D[4:2]F0x0C[DeviceType]. 0=Single function device. 1=Multi-function device.
6:0	Reserved.

3.8 Device [4:2] Function [5:1] (Root Port) Configuration Registers

See 3.1 [Register Descriptions and Mnemonics] for a description of the register naming convention. See 2.7 [Configuration Space] for details about how to access this space. See 2.11.1 [Overview].

D[4:2]F[5:1]x00 Device/Vendor ID

Table 110: Register Mapping for D[4:2]F[5:1]x00

D[4:2]F[5:1]x00	Function
D2F1x00	Gfx Bridge 0
D2F2x00	Gfx Bridge 1
D3F1x00	GPP Bridge 0
D3F2x00	GPP Bridge 1
D3F3x00	GPP Bridge 2
D3F4x00	GPP Bridge 3
D3F5x00	GPP Bridge 4
D4F1x00	Bridge to FCH

Table 111: Reset Mapping for D[4:2]F[5:1]x00

Register	Value
D2F1x00	1425_1022h
D2F2x00	1425_1022h
D3F1x00	1426_1022h
D3F2x00	1426_1022h
D3F3x00	1426_1022h
D3F4x00	1426_1022h
D3F5x00	1426_1022h
D4F1x00	1426_1022h

Bits	Description
31:16	**DeviceID: device ID**. Read-only.
15:0	**VendorID: vendor ID**. Read-only.

D[4:2]F[5:1]x04 Status/Command Register

Reset: 0010_0000h.

Bits	Description
31	**ParityErrorDetected: detected parity error**. Read; Write-1-to-clear.
30	**SignaledSystemError: signaled system error**. Read; Write-1-to-clear. 1=System error signaled.
29	**ReceivedMasterAbort: received master abort**. Read; Write-1-to-clear.
28	**ReceivedTargetAbort: received target abort**. Read; Write-1-to-clear.
27	**SignalTargetAbort: signaled target abort**. Read; Write-1-to-clear.
26:25	**DevselTiming: DEVSEL# Timing**. Read-only.
24	**DataPerr: data parity error**. Read; Write-1-to-clear.
23	**FastBackCapable: fast back-to-back capable**. Read-only.
22	Reserved.
21	**PCI66En: 66 MHz capable**. Read-only.
20	**CapList: capability list**. Read-only. 1= Capability list present.
19	**IntStatus: interrupt status**. Read-only. 1=An INTx interrupt Message is pending in the device.
18:11	Reserved.
10	**IntDis: interrupt disable**. Read-write.
9	**FastB2BEn: fast back-to-back enable**. Read-only.
8	**SerrEn: system error enable**. Read-write. 1=System error reporting enabled.
7	**Stepping: Stepping control**. Read-only.
6	**ParityErrorEn: parity error response enable**. Read-write.
5	**PalSnoopEn: VGA palette snoop enable**. Read-only.
4	**MemWriteInvalidateEn: memory write and invalidate enable**. Read-only.
3	**SpecialCycleEn: special cycle enable**. Read-only.
2	**BusMasterEn: bus master enable**. Read-write.
1	**MemAccessEn: IO access enable**. Read-write. This bit controls if memory accesses targeting this device are accepted or not. 1=Enabled. 0=Disabled.
0	**IoAccessEn: IO access enable**. Read-write. This bit controls if IO accesses targeting this device are accepted or not. 1=Enabled. 0=Disabled.

D[4:2]F[5:1]x08 Class Code/Revision ID Register

Reset: 0604_00xxh.

Bits	Description
31:8	**ClassCode**. Read-only. Provides the host bridge class code as defined in the PCI specification.
7:0	**RevID: revision ID**. Read-only.

D[4:2]F[5:1]x0C Header Type Register

Reset: 0001_0000h.

Bits	Description
31:24	**BIST**. Read-only. These bits are fixed at their default values.
23	**DeviceType**. Read-only. 0=Single function device. 1=Multi-function device.
22:16	**HeaderType**. Read-only. These bits are fixed at their default values. Indicates a Type 0 or Type 1 configuration space.
15:8	**LatencyTimer**. Read-only. This field does not control any hardware.
7:0	**CacheLineSize**. Read-write.

D[4:2]F[5:1]x18 Bus Number and Secondary Latency Register

Reset: 0000_0000h.

Bits	Description
31:24	**SecondaryLatencyTimer: secondary latency timer**. Read-only. This field is always 0.
23:16	**SubBusNumber: subordinate number**. Read-write. This field contains the highest-numbered bus that exists on the secondary side of the bridge.
15:8	**SecondaryBus: secondary bus number**. Read-write. This field defines the bus number of the secondary bus interface.
7:0	**PrimaryBus: primary bus number**. Read-write. This field defines the bus number of the primary bus interface.

D[4:2]F[5:1]x1C IO Base and Secondary Status Register

Reset: 0000_0101h.

Bits	Description
31	**ParityErrorDetected: detected parity error**. Read; Write-1-to-clear. A Poisoned TLP was received regardless of the state of the D[4:2]F[5:1]x04[ParityErrorEn].
30	**ReceivedSystemError: signaled system error**. Read; Write-1-to-clear. 1=A System Error was detected.
29	**ReceivedMasterAbort: received master abort**. Read; Write-1-to-clear. 1=A CPU transaction is terminated due to a master-abort.
28	**ReceivedTargetAbort: received target abort**. Read; Write-1-to-clear. 1=A CPU transaction (except for a special cycle) is terminated due to a target-abort.

27	**SignalTargetAbort: signaled target abort**. Read; Write-1-to-clear.
26:25	**DevselTiming: DEVSEL# Timing**. Read-only.
24	**MasterDataPerr: master data parity error**. Read; Write-1-to-clear. 1=The link received a poisoned or poisoned a downstream write and D[4:2]F[5:1]x3C[ParityResponseEn]==1.
23	**FastBackCapable: fast back-to-back capable**. Read-only.
22	Reserved.
21	**PCI66En: 66 MHz capable**. Read-only.
20	**CapList: capability list**. Read-only.
19:16	Reserved.
15:12	**IOLimit[15:12]**. Read-write. Lower part of the limit address. Upper part is defined in D[4:2]F[5:1]x30.
11:8	**IOLimitType**. Read-only. 0=16-bit. 1=32-bit.
7:4	**IOBase[15:12]**. Read-write. Lower part of the base address. Upper part is defined in D[4:2]F[5:1]x30.
3:0	**IOBaseType**. Read-only. 0=16-bit. 1=32-bit.

D[4:2]F[5:1]x20 Memory Limit and Base Register

Reset: 0000_0000h.

Bits	Description
31:20	**MemLimit[31:20]**. Read-write.
19:16	**MemLimitType**. Read-only. 0=32-bit. 1=64-bit.
15:4	**MemBase[31:20]**. Read-write.
3:0	**MemBaseType**. Read-only. 0=32-bit. 1=64-bit.

D[4:2]F[5:1]x24 Prefetchable Memory Limit and Base Register

Reset: 0001_0001h.

Bits	Description
31:20	**PrefMemLimit**. Read-write. Lower part of the limit address. Upper part is defined in D[4:2]F[5:1]x2C.
19:16	**PrefMemLimitType**. Read-only. 0=32-bit. 1=64-bit.
15:4	**PrefMemBase[31:20]**. Read-write. Lower part of the base address. Upper part is defined in D[4:2]F[5:1]x28.
3:0	**PrefMemBaseType**. Read-only. 0=32-bit. 1=64-bit.

D[4:2]F[5:1]x28 Prefetchable Memory Base High Register

Reset: 0000_0000h.

Bits	Description
31:0	**PrefMemBase[63:32]**. Read-write. Upper part of the base address. Lower part is defined in D[4:2]F[5:1]x24.

D[4:2]F[5:1]x2C Prefetchable Memory Limit High Register

Reset: 0000_0000h.

Bits	Description
31:0	**PrefMemLimit[63:32]**. Read-write. Upper part of the limit address. Lower part is defined in D[4:2]F[5:1]x24.

D[4:2]F[5:1]x30 IO Base and Limit High Register

Reset: 0000_0000h.

Bits	Description
31:16	**IOLimit[31:16]**. Read-write. Upper part of the limit address. Lower part is defined in D[4:2]F[5:1]x1C.
15:0	**IOBase[31:16]**. Read-write. Upper part of the base address. Lower part is defined in D[4:2]F[5:1]x1C.

D[4:2]F[5:1]x34 Capabilities Pointer Register

Reset: 0000_0050h.

Bits	Description
31:8	Reserved.
7:0	**CapPtr: capabilities pointer**. Read-only. Pointer to PM capability.

D[4:2]F[5:1]x3C Bridge Control Register

Reset: 0000_00FFh.

Bits	Description
31:24	Reserved.
23	**FastB2BCap: Fast back-to-back capability**. Read-only.
22	**SecondaryBusReset: Secondary bus reset**. Read-write. Setting this bit triggers a hot reset on the corresponding PCI Express Port.
21	**MasterAbortMode: Master abort mode**. Read-only.
20	**Vga16En: VGA IO 16 bit decoding enable**. Read-write. 1=Address bits [15:10] for VGA IO cycles are decoded. 0=Address bits [15:10] for VGA IO cycles are ignored.

19	**VgaEn: VGA enable**. Read-write. Affects the response by the bridge to compatible VGA addresses. When it is set, the bridge decodes and forwards the following accesses on the primary interface to the secondary interface: Memory accesses in the range of A_0000h to B_FFFFh and IO address where address bits [9:0] are in the ranges of 3B0h to 3BBh or 3C0h to 3DFh. For IO cycles the decoding of address bits [15:10] depends on Vga16En.
18	**IsaEn: ISA enable**. Read-write.
17	**SerrEn: SERR enable**. Read-write.
16	**ParityResponseEn: Parity response enable**. Read-write. Controls the bridge's response to poisoned TLPs on its secondary interface. 1=The bridge takes its normal action when a poisoned TLP is received. 0=The bridge ignores any poisoned TLPs that it receives and continues normal operation.
15:11	**IntPinR: interrupt pin**. Read-only.
10:8	**IntPin: interrupt pin**. IF (D0F0xE4_x0140_0010[HwInitWrLock]==1) THEN Read-only. ELSE Read-write. ENDIF.
7:0	**IntLine: Interrupt line**. Read-write.

D[4:2]F[5:1]x50 Power Management Capability Register

Reset: 0003_5801h.

Bits	Description
31:27	**PmeSupport**. Read-only.
26	**D2Support: D2 support**. Read-only. D2 is not supported.
25	**D1Support: D1 support**. Read-only. D1 is not supported.
24:22	**AuxCurrent: auxiliary current**. Read-only. Auxiliary current is not supported.
21	**DevSpecificInit: device specific initialization**. Read-only. This field is hardwired to 0 to indicate that there is no device specific initialization necessary.
20	Reserved.
19	**PmeClock**. Read-only. 0=Indicate that PCI clock is not needed to generate PME messages.
18:16	**Version: version**. Read-only. 3=PMI Spec 1.2.
15:8	**NextPtr: next pointer**. Read-only. 58h=Address of the next capability structure.
7:0	**CapID: capability ID**. Read-only. 01h=PCI power management data structure.

D[4:2]F[5:1]x54 Power Management Control and Status Register

Bits	Description
31:24	**PmiData**. Read-only. Reset: 0.
23	**BusPwrEn**. Read-only. Reset: 0.
22	**B2B3Support**. Read-only. Reset: 0. B states are not supported.
21:16	Reserved.
15	**PmeStatus: PME status**. Read; Write-1-to-clear. Reset: 0. This bit is set when the root port would issue a PME message (independent ofthe state of the PmeEn bit). Once set, this bit remains set until it is reset by writing a 1 to this bit location. Writing a 0 has no effect.

14:13	**DataScale: data scale**. Read-only. Reset: 0.
12:9	**DataSelect: data select**. Read-only. Reset: 0.
8	**PmeEn: PME# enable**. Read-write. Reset: 0.
7:4	Reserved.
3	**NoSoftReset: no soft reset**. Read-only. Reset: 0. Software is required to re-initialize the function when returning from $D3_{hot}$.
2	Reserved.
1:0	**PowerState: power state**. Read-write. Reset: 0. This 2-bit field is used both to determine the current power state of the root port and to set the root port into a new power state. Bits Definition Bits Definition 00b D0 10b Reserved 01b Reserved 11b D3

D[4:2]F[5:1]x58 PCI Express Capability Register

Reset: 0042_A010h.

Bits	Description
31:30	Reserved.
29:25	**IntMessageNum: interrupt message number**. Read-only. This register indicates which MSI vector is used for the interrupt message.
24	**SlotImplemented: Slot implemented**. Read-only. 1=The IO Link associated with this port is connected to a slot.
23:20	**DeviceType: device type**. Read-only. 4h=Root complex.
19:16	**Version**. Read-only. 2h=GEN 2 compliant.
15:8	**NextPtr: next pointer**. Read-only. A0h=Pointer to the next capability structure.
7:0	**CapID: capability ID**. Read-only. 10h=PCIe® Capability structure.

D[4:2]F[5:1]x5C Device Capability Register

Reset: 0000_0020h.

Bits	Description
31:29	Reserved.
28	**FlrCapable: function level reset capability**. Read-only.
27:26	**CapturedSlotPowerScale: captured slot power limit scale**. Read-only.
25:18	**CapturedSlotPowerLimit: captured slot power limit value**. Read-only.
17:16	Reserved.
15	**RoleBasedErrReporting: role-based error reporting**. Read-only.
14:12	Reserved.
11:9	**L1AcceptableLatency: endpoint L1 Acceptable Latency**. Read-only.
8:6	**L0SAcceptableLatency: endpoint L0s Acceptable Latency**. Read-only.
5	**ExtendedTag: extended tag support**. Read-only. 1=8-bit tag supported. 0=5-bit tag supported.

4:3	**PhantomFunc: phantom function support**. Read-only. 0=No phantom functions supported.
2:0	**MaxPayloadSupport: maximum supported payload size**. Read-only. 000b=128 bytes max payload size.

D[4:2]F[5:1]x60 Device Control and Status Register

Reset: 0000_2810h.

Bits	Description
31:22	Reserved.
21	**TransactionsPending: transactions pending**. Read-only. 0=No internally generated non-posted transactions pending.
20	**AuxPwr: auxiliary power**. Read-only.
19	**UsrDetected: unsupported request detected**. Read; Write-1-to-clear. 1=The port received an unsupported request. Errors are logged in this register even if error reporting is disabled.
18	**FatalErr: fatal error detected**. Read; Write-1-to-clear. 1=The port detected a fatal error. Errors are logged in this register even if error reporting is disabled.
17	**NonFatalErr: non-fatal error detected**. Read; Write-1-to-clear. T1=The port detected a non-fatal error. Errors are logged in this register even if error reporting is disabled.
16	**CorrErr: correctable error detected**. Read; Write-1-to-clear. 1=The port detected a correctable error. Errors are logged in this register even if error reporting is disabled.
15	**BridgeCfgRetryEn: bridge configuration retry enable**. Read-only.
14:12	**MaxRequestSize: maximum request size**. Read-write.
11	**NoSnoopEnable: enable no snoop**. Read-write. 1=The port is permitted to set the No Snoop bit in the Requester Attributes of transactions it initiates that do not require hardware enforced cache coherency.
10	**AuxPowerPmEn: auxiliary power PM enable**. Read-only.
9	**PhantomFuncEn: phantom functions enable**. Read-only.
8	**ExtendedTagEn: extended tag enable**. Read-write. 1=8-bit tag generation enabled. 0=5-bit tags are used.
7:5	**MaxPayloadSize: maximum supported payload size**. Read-write. Bits Definition Bits Definition 0h 128B 3h 1024B 1h 256B 4h 2048B 2h 512B 5h 4096B
4	**RelaxedOrdEn: relaxed ordering enable**. Read-write. 1=The root port is permitted to set the relaxed ordering bit in the attributes field of transactions it initiates that do not require strong write ordering.
3	**UsrReportEn: unsupported request reporting enable**. Read-write. 1=Reporting of unsupported requests enabled.
2	**FatalErrEn: fatal error reporting enable**. Read-write. 1=Enable sending ERR_FATAL messages.

1	**NonFatalErrEn: non-fatal error reporting enable**. Read-write. 1=Enable sending ERR_NONFATAL messages.
0	**CorrErrEn: correctable error reporting enable**. Read-write. 1=Enable sending ERR_CORR messages.

D[4:2]F[5:1]x64 IO Link Capability Register

Read-only.

Bits	Description
31:24	**PortNumber: port number**. Reset: 0. This field indicates the port number for the given IO link.
23	Reserved.
22	**AspmOptionalityCompliance**. Reset: 1. This field indicates if the compenent supports the ASPM Optionality ECN.
21	**LinkBWNotificationCap: link bandwidth notification capability**. Reset: 0.
20	**DlActiveReportingCapable: data link layer active reporting capability**. Reset: 0.
19	**SurpriseDownErrReporting**. Reset: 0. 1=This field indicates if the component supports the detecting and reporting of a Surprise Down error condition.
18	**ClockPowerManagement: clock power management**. Reset: 0. 0=Indicates that the reference clock must not be removed while in L1 or L2/L3 ready link states.
17:15	**L1ExitLatency: L1 exit latency**. Reset: 010b. 010b=Indicate an exit latency between 2 us and 4 us.
14:12	**L0sExitLatency: L0s exit latency**. Reset: 001b. 001b=Indicates an exit latency between 64 ns and 128 ns.
11:10	**PMSupport: active state power management support**. Reset: 11b. 11b=Indicates support of L0s and L1.

9:4	**LinkWidth: maximum link width**. Value: 10h. Bits — Definition 00h — Reserved. 01h — 1 lanes 02h — 2 lanes 03h — Reserved. 04h — 4 lanes 07h-05h — Reserved. 08h — 8 lanes 0Bh-09h — Reserved. 0Ch — 12 lanes 0Fh-0Dh — Reserved. 10h — 16 lanes 1Fh-11h — Reserved. 20h — 32 lanes 3Fh-21h — Reserved.
3:0	**LinkSpeed: link speed**. Value: IF (D[4:2]F[5:1]xE4_xA4[LcGen2EnStrap]==0 && D[4:2]F[5:1]xE4_xA4[LcGen3EnStrap]==0) THEN 1h. ELSEIF (D[4:2]F[5:1]xE4_xA4[LcGen2EnStrap]==1 && D[4:2]F[5:1]xE4_xA4[LcGen3EnStrap]==0) THEN 2h. ELSEIF (D[4:2]F[5:1]xE4_xA4[LcGen2EnStrap]==0 && D[4:2]F[5:1]xE4_xA4[LcGen3EnStrap]==1) THEN 3h. ELSEIF (D[4:2]F[5:1]xE4_xA4[LcGen2EnStrap]==1 && D[4:2]F[5:1]xE4_xA4[LcGen3EnStrap]==1) THEN 3h. ENDIF. Bits — Definition 0h — Reserved. 1h — 2.5 Gb/s. 2h — 5.0 Gb/s. 3h — 8.0 Gb/s. Fh-4h — Reserved.

D[4:2]F[5:1]x68 IO Link Control and Status Register

Reset: 1001_0000h.

Bits	Description
31	**LinkAutonomousBWStatus: link autonomous bandwidth status**. IF (D[4:2]F[5:1]x64[LinkBWNotificationCap]==0) THEN Read-only. ELSE Read-write; updated-by-hardware. ENDIF.
30	**LinkBWManagementStatus: link bandwidth management status**. IF (D[4:2]F[5:1]x64[LinkBWNotificationCap]==0) THEN Read-only. ELSE Read-write; updated-by-hardware. ENDIF.
29	**DlActive: data link layer link active**. Read-only; updated-by-hardware. This bit indicates the status of the data link control and management state machine. 1=DL_Active state. 0=All other states.
28	**SlotClockCfg: slot clock configuration**. Read-only; updated-by-hardware. 1=The root port uses the same clock that the platform provides.
27	**LinkTraining: link training**. Read-only; updated-by-hardware. This read-only bit indicates that the physical layer link training state machine is in the configuration or recovery state, or that 1b was written to the RetrainLink bit but link training has not yet begun. Hardware clears this bit when the link training state machine exits the configuration/recovery state.

26	Reserved.
25:20	**NegotiatedLinkWidth: negotiated link width**. Read-only; updated-by-hardware. This field indicates the negotiated width of the given PCI Express link. Bits — Definition 00h — Reserved. 01h — 1 lanes 02h — 2 lanes 03h — Reserved. 04h — 4 lanes 07h-05h — Reserved. 08h — 8 lanes 0Bh-09h — Reserved. 0Ch — 12 lanes 0Fh-0Dh — Reserved. 10h — 16 lanes 1Fh-11h — Reserved. 20h — 32 lanes 3Fh-21h — Reserved.
19:16	**LinkSpeed: link speed**. Read-only; updated-by-hardware. Bits — Definition 00h — Reserved. 01h — 2.5 Gb/s. 02h — 5.0 Gb/s. 03h — 8.0 Gb/s. Fh-4h — Reserved.
15:12	Reserved.
11	**LinkAutonomousBWIntEn: link autonomous bandwidth interrupt enable**. Read-write. 1=Enables the generation of an interrupt to indicate that the Link AutonomousBWStatus bit has been set.
10	**LinkBWManagementIntEn: link bandwidth management interrupt enable**. Read-write. 1=Enables the generation of an interrupt to indicate that the LinkBWManagementStatus has been set.
9	**HWAutonomousWidthDisable: hardware autonomous width disable**. Read-write. 1=Disables hardware from changing the link width for reasons other than attempting to correct unreliable link operation by reducing link width.
8	**ClockPowerManagementEn: clock power management enable**. Read-write.
7	**ExtendedSync: extended sync**. Read-write. 1=Forces the transmission of additional ordered sets when exiting the L0s state and when in the recovery state.
6	**CommonClockCfg: common clock configuration**. Read-write. 1=Indicates that the root port and the component at the opposite end of this IO link are operating with a distributed common reference clock. 0=Indicates that the root port and the component at the opposite end of this IO Link are operating with asynchronous reference clock.
5	**RetrainLink: retrain link**. Read-write; cleared-when-done. 1=Initiate link retraining.
4	**LinkDis: link disable**. Read-write. 1=Disable link. Writes to this bit are immediately reflected in the value read from the bit, regardless of actual link state.
3	**ReadCplBoundary: read completion boundary**. Read-only. 0=64 byte read completion boundary.

2	Reserved.
1:0	**PmControl: active state power management enable**. Read-write. This field controls the level of ASPM supported on the given IO link. Bits Definition Bits Definition 00b Disabled. 10b L1 Entry Enabled. 01b L0s Entry Enabled. 11b L0s and L1 Entry Enabled.

D[4:2]F[5:1]x6C Slot Capability Register

Reset: 0004_0000h.

Bits	Description
31:19	**PhysicalSlotNumber: physical slot number**. Read-write. This field indicates the physical slot number attached to this port. This field is set to a value that assigns a slot number that is unique within the chassis, regardless of the form factor associated with the slot. This field must be initialized to 0 for ports connected to devices that are on the system board.
18	**NoCmdCplSupport: no command completed support**. Read-write. 1=Indicates that this slot does not generate software notification when an issued command is completed by the hot-plug controller.
17	**ElecMechIlPresent: electromechanical interlock present**. Read-write. 0=Indicates that a electro-mechanical interlock is not implemented for this slot.
16:15	**SlotPwrLimitScale: slot power limit scale**. Read-write. Specifies the scale used for the SlotPwrLimitValue. Range of Values: Bits Definition Bits Definition 00b 1.0 10b 0.01 01b 0.1 11b 0.001
14:7	**SlotPwrLimitValue: slot power limit value**. Read-write. In combination with the SlotPwrLimitScale value, specifies the upper limit on power supplied by slot. Power limit (in Watts) calculated by multiplying the value in this field by the value in the SlotPwrLimitScale field.
6	**HotplugCapable: hot-plug capability**. Read-write. 1=Indicates that this slot is capable of supporting hot-plug operations.
5	**HotplugSurprise: hot-plug surprise**. Read-write. 1=Indicates that an adapter present in this slot might be removed from the system without any prior notification.
4	**PwrIndicatorPresent: power indicator present**. Read-write. 0=Indicates that a power indicator is not implemented for this slot.
3	**AttnIndicatorPresent: attention indicator present**. Read-write. 0=Indicates that a attention indicator is not implemented for this slot.
2	**MrlSensorPresent: manual retention latch sensor present**. Read-write. 0=Indicates that a manual retention latch sensor is not implemented for this slot.
1	**PwrControllerPresent: power controller present**. Read-write. 0=A power controller is not implemented for this slot.
0	**AttnButtonPresent: attention button present**. Read-write. 0=An attention button is not implemented for this slot.

D[4:2]F[5:1]x70 Slot Control and Status Register

IF (D[4:2]F[5:1]x58[SlotImplemented]==0) THEN Reset: 0040_0000h. ELSE Reset: 0000_0000h. ENDIF.

Bits	Description
31:25	Reserved.
24	**DlStateChanged: data link layer state change**. Read; Write-1-to-clear. This bit is set when the value reported in the D[4:2]F[5:1]x68[DlActive] is changed. In response to a data link layer state changed event, software must read D[4:2]F[5:1]x68[DlActive] to determine if the link is active before initiating configuration cycles to the hot plugged device.
23	**ElecMechIlSts: electromechanical interlock status**. Read-only.
22	**PresenceDetectState: presence detect state**. Read-only. This bit indicates the presence of an adapter in the slot based on the physical layer in-band presence detect mechanism. The in-band presence detect mechanism requires that power be applied to an adapter for its presence to be detected. 0=Slot empty. 1=Card present in slot. For root ports not connected to slots (D[4:2]F[5:1]x58[SlotImplemented]=0b), this bit always returns 1.
21	**MrlSensorState**. Read-only.
20	**CmdCpl: command completed**. Read-only.
19	**PresenceDetectChanged: presence detect changes**. Read; Write-1-to-clear. This bit is set when the value reported in PresenceDetectState is changed.
18	**MrlSensorChanged**. Read; Write-1-to-clear.
17	**PwrFaultDetected**. Read; Write-1-to-clear.
16	**AttnButtonPressed: attention button pressed**. Read-only.
15:13	Reserved.
12	**DlStateChangedEn: data link layer state changed enable**. Read-write. 1=Enables software notification when D[4:2]F[5:1]x68[DlActive] is changed.
11	**ElecMechIlCntl: electromechanical interlock control**. Read-only.
10	**PwrControllerCntl: power controller control**. Read-only.
9:8	**PwrIndicatorCntl: power indicator control**. Read-only.
7:6	**AttnIndicatorControl: attention indicator control**. Read-only.
5	**HotplugIntrEn: hot-plug interrupt enable**. Read-only.
4	**CmdCplIntrEn: command complete interrupt enable**. Read-only.
3	**PresenceDetectChangedEn: presence detect changed enable**. Read-only.
2	**MrlSensorChangedEn: manual retention latch sensor changed enable**. Read-only.
1	**PwrFaultDetectedEn: power fault detected enable**. Read-only.
0	**AttnButtonPressedEn: attention button pressed enable**. Read-only.

D[4:2]F[5:1]x74 Root Complex Capability and Control Register

Reset: 0001_0000h.

Bits	Description
31:17	Reserved.
16	**CrsSoftVisibility: CRS software visibility**. Read-only. 1=Indicates that the root port supports returning configuration request retry status (CRS) completion status to software.
15:5	Reserved.
4	**CrsSoftVisibilityEn: CRS software visibility enable**. Read-write. 1=Enables the root port returning configuration request retry status (CRS) completion status to software.
3	**PmIntEn: PME interrupt enable**. Read-write. 1=Enables interrupt generation upon receipt of a PME message as reflected D[4:2]F[5:1]x78[PmeStatus]. A PME interrupt is also generated if D[4:2]F[5:1]x78[PmeStatus]=1 and this bit is set by software.
2	**SerrOnFatalErrEn: system error on fatal error enable**. Read-write. 1=Indicates that a system error should be generated if a fatal error (ERR_FATAL) is reported by any of the devices in the hierarchy associated with this root port, or by the root port itself.
1	**SerrOnNonFatalErrEn: system error on non-fatal error enable**. Read-write. 1=Indicates that a system error should be generated if a non-fatal error (ERR_NONFATAL) is reported by any of the devices in the hierarchy associated with this root port, or by the root port itself.
0	**SerrOnCorrErrEn: system error on correctable error enable**. Read-write. 1=Indicates that a system error should be generated if a correctable error (ERR_COR) is reported by any of the devices in the hierarchy associated with this root port, or by the root port itself.

D[4:2]F[5:1]x78 Root Complex Status Register

Reset: 0000_0000h.

Bits	Description
31:18	Reserved.
17	**PmePending: PME pending**. Read-only. This bit indicates that another PME is pending when PmeStatus is set. When PmeStatus is cleared by software; the PME is delivered by hardware by setting the PmeStatus bit again and updating the requestor ID appropriately. PmePending is cleared by hardware if no more PMEs are pending.
16	**PmeStatus: pme status**. Read; Write-1-to-clear. 1=PME was asserted by the requestor ID indicated in the PmeRequestorID field. Subsequent PMEs are kept pending until PmeStatus is cleared by writing a 1.
15:0	**PmeRequestorId: pme requestor ID**. Read-only. This field indicates the PCI requestor ID of the last PME requestor.

D[4:2]F[5:1]x7C Device Capability 2

Reset: 0000_0000h.

Bits	Description
31:24	Reserved.

23:22	**MaxEndEndTlpPrefixes: Max number of End-End TLP prefixes supported**. Read-only. IF (D[4:2]F[5:1]x7C[EndEndTlpPrefixSupported]==0) THEN Reserved. ENDIF. Bits Definition Bits Definition 00b 4 End-End TLP Prefixes. 10b 2 End-End TLP Prefixes. 01b 1 End-End TLP Prefix. 11b 3 End-End TLP Prefixes.
21	**EndEndTlpPrefixSupported: End-End TLP Prefix supported**. Read-only.
20	**ExtendedFmtFieldSupported**. Read-only. 1=Supports the 3-bit definition of the Fmt field. 0=Supports the 2-bit definition of the Fmt field. BIOS: Must be set for functions that support End-End TLP prefixes.
19:18	**ObffSupported: optimized buffer flush/fill supported**. Read-only.
17:14	Reserved.
13:12	Reserved.
11	**LtrSupported: latency tolerance supported**. Read-only.
10	Reserved.
9:6	Reserved.
5	**AriForwardingSupported**. Read-only.
4	**CplTimeoutDisSupported: completion timeout disable supported**. Read-only.
3:0	**CplTimeoutRangeSupported: completion timeout range supported**. Read-only. Fh=Completion timeout range is 64s to 50us.

D[4:2]F[5:1]x80 Device Control and Status 2

Reset: 0000_8000h.

Bits	Description
31:16	Reserved.
15	**EndEndeTlpPrefixBlocking**. Read-only. 1=Forwarding of End-End TLP Prefixes is not supported. This bit is hardwired to 1b.
14:13	**ObffEn: optimized buffer flush/fill enable**. Read-write.
12:11	Reserved.
10	**LtrEn: latency tolerance reporting enable**. Read-write.
9	Reserved.
8	Reserved.
7:6	Reserved.
5	**AriForwardingEn**. Read-write.

4	**CplTimeoutDis: completion timeout disable**. Read-write. 1=Completion timeout disabled.
3:0	**CplTimeoutValue: completion timeout value**. Read-write. BIOS: 6h. Bits Timeout Range Bits Timeout Range 0h 50ms-50us 9h 900ms-260ms 1h 100us-50us Ah 3.5s-1s 2h 10ms-1ms Ch-Bh Reserved 4h-3h Reserved Dh 13s-4s 5h 55ms-16ms Eh 64s-4s 6h 210ms-65ms Fh Reserved 8h-7h Reserved

D[4:2]F[5:1]x84 IO Link Capability 2

Bits	Description
31:9	Reserved.
8	**CrossLinkSupported**. Read-only. Reset: 0.
7:3	Reserved.
2:1	**SupportedLinkSpeed**. Read-only. Reset: 3h. Specifies the supported link speeds. Bit [1]=2.5GT/s, Bit [2]=5.0GT/s.
0	Reserved.

D[4:2]F[5:1]x88 IO Link Control and Status 2

Bits	Description
31:22	Reserved.
21	**LinkEqualizationRequest**. Read; write-1-to-clear. Reset: 0. 1=Hardware requests link equalization to be performed.
20	**EqualizationPhase3Success**. Read-only. Reset: 0. 1=Phase 3 of the Transmitter Equalization procedure has completed successfully. Write 1 to clear.
19	**EqualizationPhase2Success**. Read-only. Reset: 0. 1=Phase 2 of the Transmitter Equalization procedure has completed successfully. Write 1 to clear.
18	**EqualizationPhase1Success**. Read-only. Reset: 0. 1=Phase 1 of the Transmitter Equalization procedure has completed successfully. Write 1 to clear.
17	**EqualizationComplete**. Read-only. Reset: 0. 1=Transmitter Equalization procedure has completed. Write 1 to clear.
16	**CurDeemphasisLevel: current deemphasis level**. Read-only. Reset: D[4:2]F[5:1]xE4_xA4[LcGen2EnStrap]. 1=-3.5 dB. 0=-6 dB

15:12	**ComplianceDeemphasis: compliance deemphasis**. Read-write. Reset: 0. In Gen2, this field defines the compliance deemphasis level when EnterCompliance is set. Software should leave this field in its default state. Bits — Definition 0h — DeEmph=-6 dB, Preshoot=0 dB. 1h — DeEmph=-3.5 dB, Preshoot=0 dB. 2h — DeEmph=-4.5 dB, Preshoot=0 dB. 3h — DeEmph=-2.5 dB, Preshoot=0 dB. 4h — DeEmph=-0 dB, Preshoot=0 dB. 5h — DeEmph=-0 dB, Preshoot=2 dB. 6h — DeEmph=-0 dB, Preshoot=2.5 dB. 7h — DeEmph=-6 dB, Preshoot=3.5 dB. 8h — DeEmph=-3.5 dB, Preshoot=3.5 dB. 9h — DeEmph=-0 dB, Preshoot=3.5 dB. Fh-Ah — Reserved.
11	**ComplianceSOS: compliance SOS**. Read-write. Reset: 0. 1=The device transmits skip ordered sets in between the modified compliance pattern.
10	**EnterModCompliance: enter modified compliance**. Read-write. Reset: 0. 1=The device transmits modified compliance pattern. Software should leave this field in its default state.
9:7	**XmitMargin: transmit margin**. Read-write. Reset: 0. This field controls the non-deemphasized voltage level at the transmitter pins. Software should leave this field in its default state.
6	**SelectableDeemphasis: selectable deemphasis**. Read-only. Reset: D[4:2]F[5:1]xE4_xA4[LcGen2EnStrap]. 0=Selectable deemphasis is not supported. 1=Selectable deemphasis supported.
5	**HwAutonomousSpeedDisable: hardware autonomous speed disable**. Read-write. Cold reset: 0. 1=Support for hardware changing the link speed for device specific reasons disabled.
4	**EnterCompliance: enter compliance**. Read-write. Cold reset: 0. 1=Force the link to enter the compliance mode.
3:0	**TargetLinkSpeed: target link speed**. Read-write. Reset: 2h. This field defines the upper limit of the link operational speed. Writes of reserved encodings are not valid. Hardware prevents writes of reserved encodings from changing the state of this field. Bits — Definition 0h — Reserved 1h — 2.5GT/s 2h — 5.0GT/s 3h — 8.0GT/s Fh-4h — Reserved

D[4:2]F[5:1]x8C Slot Capability 2

Reset: 0000_0000h.

Bits	Description
31:0	Reserved.

D[4:2]F[5:1]x90 Slot Control and Status 2

Reset: 0000_0000h.

Bits	Description
31:0	Reserved.

D[4:2]F[5:1]xA0 MSI Capability Register

Reset: 0000_B005h.

Bits	Description
31:24	Reserved.
23	**Msi64bit: MSI 64 bit capability**. Read-only. 1=The device is capable of sending 64-bit MSI messages. 0=The device is not capable of sending a 64-bit message address.
22:20	**MsiMultiEn: MSI multiple message enable**. Read-write. Software writes to this field to indicate the number of allocated vectors (equal to or less than the number of requested vectors). When MSI is enabled, a function is allocated at least 1 vector.
19:17	**MsiMultiCap: MSI multiple message capability**. Read-only. 000b=The device is requesting one vector.
16	**MsiEn: MSI enable**. Read-write. 1=MSI generation is enabled and INTx generation is disabled. 0=MSI generation disabled and INTx generation is enabled.
15:8	**NextPtr: next pointer**. Read-only.
7:0	**CapID: capability ID**. Read-only. 05h=MSI capability structure.

D[4:2]F[5:1]xA4 MSI Message Address Low

Reset: 0000_0000h.

Bits	Description
31:2	**MsiMsgAddrLo: MSI message address**. Read-write. This register specifies the dword aligned address for the MSI memory write transaction.
1:0	Reserved.

D[4:2]F[5:1]xA8 MSI Message Address High

Reset: 0000_0000h.

Bits	Description
31:0	**MsiMsgAddrHi: MSI message address**. Read-write. This register specifies the upper 32 bits of the MSI address.

D[4:2]F[5:1]xAC MSI Message Data

Reset: 0000_0000h.

Bits	Description
31:16	Reserved.
15:0	**MsiData: MSI message data**. Read-write. This register specifies lower 16 bits of data for the MSI memory write transaction. The upper 16 bits are always 0.

D[4:2]F[5:1]xB0 Subsystem and Subvendor Capability ID Register

Reset: 0000_B80Dh.

Bits	Description
31:16	Reserved.
15:8	**NextPtr: next pointer**. Read-only.
7:0	**CapID: capability ID**. Read-only.

D[4:2]F[5:1]xB4 Subsystem and Subvendor ID Register

Reset: 0000_0000h.

Bits	Description
31:16	**SubsystemID**. Read-only.
15:0	**SubsystemVendorID**. Read-only.

D[4:2]F[5:1]xB8 MSI Capability Mapping

Reset: A803_0008h.

Bits	Description
31:27	**CapType: capability type**. Read-only.
26:18	Reserved.
17	**FixD**. Read-only.
16	**En**. Read-only.
15:8	**NextPtr: next pointer**. Read-only.
7:0	**CapID: capability ID**. Read-only.

D[4:2]F[5:1]xBC MSI Mapping Address Low

Bits	Description
31:20	**MsiMapAddrLo**. Read-only. Reset: 0. Lower 32 bits of the MSI address.
19:0	Reserved.

D[4:2]F[5:1]xC0 MSI Mapping Address High

Bits	Description
31:0	**MsiMapAddrHi**. Read-only. Reset: 0. Upper 32 bits of the MSI address.

D[4:2]F[5:1]xE0 Root Port Index

Reset: 0000_0000h.

The index/data pair registers, D[4:2]F[5:1]xE0 and D[4:2]F[5:1]xE4, are used to access the registers at D[4:2]F[5:1]xE4_x[FF:00]. To access any of these registers, the address is first written into the index register, D[4:2]F[5:1]xE0, and then the data is read from or written to the data register, D[4:2]F[5:1]xE4.

Bits	Description
31:8	Reserved.
7:0	**PcieIndex**. Read-write.

D[4:2]F[5:1]xE4 Root Port Data

See D[4:2]F[5:1]xE0. Address: D[4:2]F[5:1]xE0[PcieIndex].

Bits	Description
31:0	**PcieData**. Read-write.

D[4:2]F[5:1]xE4_x20 Root Port TX Control

Reset: 0050_8000h.

Bits	Description
31:16	Reserved.
15	**TxFlushTlpDis: TLP flush disable**. Read-write. 1=Disable flushing TLPs when the link is down.
14:0	Reserved.

D[4:2]F[5:1]xE4_x50 Root Port Lane Status

Reset: 0000_0000h.

Bits	Description
31:7	Reserved.
6:1	**PhyLinkWidth: port link width**. Read-only; updated-by-hardware. Bits / Definition / Bits / Definition 00_0000b disabled 00_1000b x8 00_0001b x1 01_0000b x12 00_0010b x2 10_0000b x16 00_0100b x4
0	**PortLaneReversal: port lane reversal**. Read-only. 1=Port lanes order is reversed.

D[4:2]F[5:1]xE4_x6A Root Port Error Control

Reset: 0000_0500h.

Bits	Description
31:1	Reserved.
0	**ErrReportingDis: advanced error reporting disable**. Read-write. BIOS: 1. 1=Error reporting disabled. 0=Error reporting enabled.

D[4:2]F[5:1]xE4_x70 Root Port Receiver Control

Reset: 0188_4000h.

Bits	Description
31:20	Reserved.
19	**RxRcbCplTimeoutMode: RCB completion timeout mode**. Read-write. BIOS: 1. 1=Timeout on link down.
18:16	**RxRcbCplTimeout: RCB completion timeout**. Read-write. Bits / Definition / Bits / Definition 000b Disabled 100b 50ms 001b 50us 101b 100ms 010b 10ms 110b 500ms 011b 25ms 111b 1ms
15:0	Reserved.

D[4:2]F[5:1]xE4_xA0 Per Port Link Controller (LC) Control

Reset: 4000_0030h.

Bits	Description
31:24	Reserved.
23	**LcL1ImmediateAck: immediate ACK ASPM L1 entry**. Read-write. BIOS: 1. 1=Alwyas ACK ASPM L1 entry DLLPs.
22:16	Reserved.
15:12	**LcL1Inactivity: L1 inactivity timer**. Read-write. Bits / Definition / Bits / Definition 0h L1 disabled 8h 400us 1h 1us 9h 1ms 2h 2us Ah 40us 3h 4us Bh 10ms 4h 10us Ch 40ms 5h 20us Dh 100ms 6h 40us Eh 400ms 7h 100us Fh Reserved

11:8	**LcL0sInactivity: L0s inactivity timer**. Read-write. Bits Definition Bits Definition 0h L0s disabled 8h 4us 1h 40ns 9h 10us 2h 80ns Ah 40us 3h 120ns Bh 100us 4h 200ns Ch 400us 5h 400ns Dh 1ms 6h 1us Eh 4ms 7h 2us Fh Reserved
7:4	**Lc16xClearTxPipe**. Read-write. BIOS: 1h. Specifies the number of clock to drain the TX pipe.
3:0	Reserved.

D[4:2]F[5:1]xE4_xA1 LC Training Control

Reset: 9400_1880h.

Bits	Description
31:12	Reserved.
11	**LcDontGotoL0sifL1Armed: prevent Ls0 entry is L1 request in progress**. Read-write. BIOS: 1. 1=Prevent the LTSSM from transitioning to Rcv_L0s if an acknowledged request to enter L1 is in progress.
10:0	Reserved.

D[4:2]F[5:1]xE4_xA2 LC Link Width Control

Reset: 00A0_0006h.

Bits	Description
31:24	Reserved.
23	Reserved.
22:21	**LcDynLanesPwrState: unused link power state**. Read-write. Controls the state of unused links after a reconfiguration. Bits Definition Bits Definition 00b On 10b SB2 01b SB1 11b Off
20	**LcUpconfigCapable: upconfigure capable**. Read-only; updated-by-hardware. 1=Both ends of the link are upconfigure capable. 0=Both ends of the link are not upconfigure capable.
19:14	Reserved.
13	**LcUpconfigureDis: upconfigure disable**. Read-write. 1=Disable link upconfigure.
12	**LcUpconfigureSupport: upconfigure support**. Read-write.
11	**LcShortReconfigEn: short re-configuration enable**. Read-write. 1=Enable short link re-configuration
10	**LcRenegotiateEn: link reconfiguration enable**. Read-write. 1=Enable link re-negotiation.
9	**LcRenegotiationSupport: re-negotiation support**. Read-only; updated-by-hardware. 1=Link re-negotiation not supported by the downstream device.

8	**LcReconfigNow: re-configure link**. Read-write; cleared-when-done. 1=Initiate link width change.
7	**LcReconfigArcMissingEscape**. Read-write. 1=Expedite transition from Recovery.Idle to Detect during a long reconfiguration.
6:4	**LcLinkWidthRd: current link width**. Read-only; updated-by-hardware. Bits / Definition / Bits / Definition 000b / 0 / 100b / 8 001b / 1 / 101b / 12 010b / 2 / 110b / 16 011b / 4 / 111b / Reserved
3	Reserved.
2:0	**LcLinkWidth: link width required**. Read-write. See: LcLinkWidthRd.

D[4:2]F[5:1]xE4_xA3 LC Number of FTS Control

Reset: 00FF_020Ch.

Bits	Description
31:10	Reserved.
9	**LcXmitFtsBeforeRecovery: transmit FTS before recovery**. Read-write. 1=Transmit FTS before recovery.
8	**LcXmitNFtsOverrideEn: number of FTS override enable**. Read-write. BIOS: 1. 1=Override the number of FTS specified by the strap value.
7:0	**LcXmitNFts: number of FTS**. Read-write. BIOS: 40h. Specifies the number of FTS to sent if LcXmitNFtsOverideEn==1.

D[4:2]F[5:1]xE4_xA4 LC Link Speed Control

Reset: 3440_0100h.

Bits	Description
31:28	Reserved.
27	**LcMultUpstreamAutoSpdChngEn: enable multiple automatic speed changes**. Read-write. 1=Enable multiple automatic speed changes when D[4:2]F[5:1]xE4_xC0[StrapAutoRcSpeedNegotiationDis]==0 and no failures occured in previous speed change attempts.
26:20	Reserved.
19	**LcOtherSideSupportsGen2: downstream link supports gen2**. Read-only; updated-by-hardware. 1=The downstream link currently supports gen2.
18:15	Reserved.
14:13	Reserved.
12	**LcSpeedChangeAttemptFailed: speed change attempt failed**. Read-only; updated-by-hardware. 1=LcSpeedChangeAttemptsAllowed has been reached.
11:10	Reserved.
9	**LcInitiateLinkSpeedChange: initiate link speed change**. Read-write; cleared-when-done. 1=Initiate link speed negotiation.

8:7	Reserved.
6	**LcForceDisSwSpeedChange: force disable software speed changes**. Read-write. 1=Force the PCIe core to disable speed changes initiated by private registers.
5:2	Reserved.
1	**LcGen3EnStrap: Gen3 PCIe support enable**. Read-write. 1=Gen3 PCIe support enabled. 0=Gen3 PCIe support disabled.
0	**LcGen2EnStrap: Gen2 PCIe support enable**. Read-write. 1=Gen2 PCIe support enabled. 0=Gen2 PCIe support disabled.

D[4:2]F[5:1]xE4_xA5 LC State 0

Cold reset: 0000_0000h.

Bits	Description
31:30	Reserved.
29:24	**LcPrevState3: previous link state 3**. Read-only; updated-by-hardware. See: Table 112 [Link controller state encodings].
23:22	Reserved.
21:16	**LcPrevState2: previous link state 2**. Read-only; updated-by-hardware. See: Table 112 [Link controller state encodings]
15:14	Reserved.
13:8	**LcPrevState1: previous link state 1**. Read-only; updated-by-hardware. See: Table 112 [Link controller state encodings].
7:6	Reserved.
5:0	**LcCurrentState: current link state**. Read-only; updated-by-hardware. See: Table 112 [Link controller state encodings].

Table 112: Link controller state encodings

Bits	Description	Bits	Description	Bits	Description
00h	s_Detect_Quiet.	12h	Rcv_L0_and_Tx_L0s.	24h	s_Rcvd_Loopback.
01h	s_Start_common_Mode.	13h	Rcv_L0_and_Tx_L0s_FTS.	25h	s_Rcvd_Loopback_Idle.
02h	s_Check_Common_Mode.	14h	Rcv_L0s_and_Tx_L0.	26h	s_Rcvd_Reset_Idle.
03h	s_Rcvr_Detect. 15	h	Rcv_L0s_and_Tx_L0_Idle.	27h	s_Rcvd_Disable_Entry.
04h	s_No_Rcvr_Loop.	16h	Rcv_L0s_and_Tx_L0s.	28h	s_Rcvd_Disable_Idle.
05h	s_Poll_Quiet.	17h	Rcv_L0s_and_Tx_L0s_FTS.	29h	s_Rcvd_Disable.
06h	s_Poll_Active.	18h	s_L1_Entry.	2Ah	s_Detect_Idle.
07h	s_Poll_Compliance.	19h	s_L1_Idle.	2Bh	s_L23_Wait.
08h	s_Poll_Config.	1Ah	s_L1_Wait.	2Ch	Rcv_L0s_Skp_and_Tx_L0.
09h	s_Config_Step1.	1Bh	s_L1. 2Dh		Rcv_L0s_Skp_and_Tx_L0_Idle.
0Ah	s_Config_Step3.	1Ch	s_L23_Stall. 2Eh		Rcv_L0s_Skp_and_Tx_L0s.
0Bh	s_Config_Step5.	1Dh	s_L23_Entry.	2Fh	Rcv_L0s_Skp_and_Tx_L0_FTS.
0Ch	s_Config_Step2.	1Eh	s_L23_Entry.	30h	s_Config_Step2b.
0Dh	s_Config_Step4.	1Fh	s_L23_Ready.	31h	s_Recovery_Speed.

Table 112: Link controller state encodings

0Eh	s_Config_Step6.	20h	s_Recovery_lock.	32h	s_Poll_Compliance_Idle.
0Fh	s_Config_Idle.	21h	s_Recovery_Config.	33h	s_Rcvd_Loopback_Speed.
10h	Rcv_L0_and_Tx_L0.	22h	s_Recovery_Idle.	3Fh-34h	Reserved.
11h	Rcv_L0_and_Tx_L0_Idle.	23h	s_Training_Bit.		

D[4:2]F[5:1]xE4_xB1 LC Control 2

Reset: 8608_0280h.

Bits	Description
31:21	Reserved.
20	**LcBlockElIdleinL0: block electrical idle in l0**. Read-write. BIOS: 1. 1=Prevent electrical idle from causing the receiver to transition from L0 to L0s.
19	**LcDeassertRxEnInL0s: deassert RX_EN in L0s**. Read-write. 1=Turn off transmitters in L0s.
18:16	Reserved.
15:14	**LcElecIdleMode: electrical idle mode**. Read-write. BIOS: 01b. Specifies the electrical idle entry and exit mode. Bits Definition 00b, 11b GEN1: Entry and exit controlled by phy. GEN2: Entry controlled by logic, exit controlled by phy. 01b Entry controlled by logic, exit controlled by phy. 10b Entry and exit controlled by phy.
13:0	Reserved.

D[4:2]F[5:1]xE4_xB5 LC Control 3

Reset: 2850_5020h.

Bits	Description
31	Reserved.
30	**LcGoToRecovery: go to recovery**. Read-write. 1=Force link in the L0 state to transition to the Recovery state.
29:4	Reserved.
3	**LcRcvdDeemphasis: received deemphasis**. Read-only; updated-by-hardware. Deemphasis advertised by the downstream device. 1=3.5dB. 0=6dB.
2:1	**LcSelectDeemphasisCntl: deemphasis control**. Read-write. Specifies the deemphasis used by the transmitter. Bits Definition 00b Use deemphasis from LcSelectDeemphasis. 01b Use deemphasis advertised by the downstream device. 10b 6dB. 11b 3.5dB.
0	**LcSelectDeemphasis: downstream deemphasis**. Read-write. Specifies the downstream deemphasis. 1=3.5dB. 0=6dB.

D[4:2]F[5:1]xE4_xC0 LC Strap Override

Reset: 0000_0000h.

Bits	Description
31:16	Reserved.
15	**StrapAutoRcSpeedNegotiationDis: autonomous speed negotiation disable strap override**. Read-write. 1=Disable autonomous root complex speed negotiation to Gen2.
14	Reserved.
13	**StrapForceCompliance: force compliance strap override**. Read-write.
12:0	Reserved.

D[4:2]F[5:1]xE4_xC1 Root Port Miscellaneous Strap Override

Reset: 0000_0000h.

Bits	Description
31:6	Reserved.
5	**StrapLtrSupported**. Read-write.
4:3	**StrapObffSupported**. Read-write.
2	**StrapExtendedFmtSupported: Extended Fmt Supported strap override**. Read-write.
1	**StrapE2EPrefixEn: E2E Prefix En strap override**. Read-write.
0	**StrapReverseLanes: reverse lanes strap override**. Read-write.

D[4:2]F[5:1]xE4_xD0 Root Port ECC Skip OS Feature

Reset: 0000_0100h.

Bits	Description
31:16	**BchEccErrorStatus**. Read-write. Indicates that lane errors are above the specified threshold. (One bit per lane.)
15:8	**BchEccErrorThreshold**. Read-write. Error threshold.
7:1	Reserved.
0	**StrapBchEccEn**. Read-write.

D[4:2]F[5:1]x100 Vendor Specific Enhanced Capability Register

Bits	Description
31:20	**NextPtr: next pointer**. Read-only. IF (D0F0xE4_x014[2:0]_00B0[StrapF0AerEn] == 1) THEN Reset: 150h. ELSE Reset: 000h. ENDIF.

19:16	**CapVer: capability version**. Read-only. Reset: 1h.
15:0	**CapID: capability ID**. Read-only. Reset: Bh.

D[4:2]F[5:1]x104 Vendor Specific Header Register

Reset: 0101_0001h.

Bits	Description
31:20	**VsecLen: vendor specific enhanced capability structure length**. Read-only. Defined the number of bytes of the entire vendor specific enhanced capability structure including the header.
19:16	**VsecRev: vendor specific enhanced capability version**. Read-only.
15:0	**VsecID: vendor specific enhanced capability ID**. Read-only.

D[4:2]F[5:1]x108 Vendor Specific 1 Register

Reset: 0000_0000h.

Bits	Description
31:0	**Scratch: scratch**. Read-write. This field does not control any hardware.

D[4:2]F[5:1]x10C Vendor Specific 2 Register

Reset: 0000_0000h.

Bits	Description
31:0	**Scratch: scratch**. Read-write. This field does not control any hardware.

D[4:2]F[5:1]x128 Virtual Channel 0 Resource Status Register

Reset: 0002_0000h.

Bits	Description
31:18	Reserved.
17	**VcNegotiationPending: virtual channel negotiation pending**. Read-only; updated-by-hardware. 1=Virtual channel negotiation in progress. This bit must be 0 before the virtual channel can be used.
16	**PortArbTableStatus: port arbitration table status**. Read-only.
15:0	Reserved.

D[4:2]F[5:1]x150 Advanced Error Reporting Capability

Bits	Description
31:20	**NextPtr: next pointer**. Read-only. IF (D0F0xE4_x014[2:0]_00B0[StrapF0AcsEn] == 1) THEN 2A0h. ELSE Reset: 000h. ENDIF.

19:16	**CapVer: capability version**. Read-only. Reset: 2h.
15:0	**CapID: capability ID**. Read-only. Reset: 1h.

D[4:2]F[5:1]x154 Uncorrectable Error Status

Cold reset: 0000_0000h.

Bits	Description
31:26	Reserved.
25	**TlpPrefixStatus: TLP prefix blocked status**. Read; Write-1-to-clear.
24	**AtomicOpEgressBlockedTLPStatus: atomic op egress blocked TLP status**. Read; Write-1-to-clear.
23	**McBlockedTLPStatus: MC blocked TLP status**. Read; Write-1-to-clear.
22	**UncorrInteralErrStatus: uncorrectable internal error status**. Read; Write-1-to-clear.
21	**AcsViolationStatus: access control service status**. Read; Write-1-to-clear.
20	**UnsuppReqErrStatus: unsupported request error status**. Read; Write-1-to-clear. The header of the unsupported request is logged.
19	**EcrcErrStatus: end-to-end CRC error status**. Read; Write-1-to-clear.
18	**MalTlpStatus: malformed TLP status**. Read; Write-1-to-clear. The header of the malformed TLP is logged.
17	**RcvOvflStatus: receiver overflow status**. Read-only.
16	**UnexpCplStatus: unexpected completion timeout status**. Read; Write-1-to-clear. The header of the unexpected completion is logged.
15	**CplAbortErrStatus: completer abort error status**. Read; Write-1-to-clear.
14	**CplTimeoutStatus: completion timeout status**. Read; Write-1-to-clear.
13	**FcErrStatus: flow control error status**. Read-only.
12	**PsnErrStatus: poisoned TLP status**. Read; Write-1-to-clear. The header of the poisoned transaction layer packet is logged.
11:6	Reserved.
5	**SurprdnErrStatus: surprise down error status**. Read-only. 0=Detection and reporting of surprise down errors is not supported.
4	**DlpErrStatus: data link protocol error status**. Read; Write-1-to-clear.
3:0	Reserved.

D[4:2]F[5:1]x158 Uncorrectable Error Mask

Cold reset: 0000_0000h.

Bits	Description
31:26	Reserved.
25	**TlpPrefixMask: TLP prefix blocked mask**. Read-only.
24	**AtomicOpEgressBlockedTLPMask: atomic op egress blocked TLP mask**. Read-only.
23	**McBlockedTLPMask: MC blocked TLP mask**. Read-only.

22	**UncorrInteralErrMask: uncorrectable internal error mask**. Read-write.
21	**AcsViolationMask: access control service mask**. Read-only. 1=ACS violation errors are not reported.
20	**UnsuppReqErrMask: unsupported request error mask**. Read-write. 1=Unsupported request errors are not reported.
19	**EcrcErrMask: end-to-end CRC error mask**. Read-write.
18	**MalTlpMask: malformed TLP mask**. Read-write. 1=Malformed TLP errors are not reported.
17	**RcvOvflMask: receiver overflow mask**. Read-only.
16	**UnexpCplMask: unexpected completion timeout mask**. Read-write. 1=Unexpected completion errors are not reported.
15	**CplAbortErrMask: completer abort error mask**. Read-write.
14	**CplTimeoutMask: completion timeout mask**. Read-write. 1=Completion timeout errors are not reported.
13	**FcErrMask: flow control error mask**. Read-only.
12	**PsnErrMask: poisoned TLP mask**. Read-write. 1=Poisoned TLP errors are not reported.
11:6	Reserved.
5	**SurprdnErrMask: surprise down error mask**. Read-only.
4	**DlpErrMask: data link protocol error mask**. Read-write. 1=Data link protocol errors are not reported.
3:0	Reserved.

D[4:2]F[5:1]x15C Uncorrectable Error Severity

Cold reset: 0006_2030h.

Bits	Description
31:26	Reserved.
25	**TlpPrefixSeverity: TLP prefix blocked severity**. Read-only.
24	**AtomicOpEgressBlockedTLPSeverity: atomic op egress blocked TLP severity**. Read-only.
23	**McBlockedTLPSeverity: MC blocked TLP severity**. Read-only.
22	**UncorrInteralErrSeverity: uncorrectable internal error severity**. Read-only.
21	**AcsViolationSeverity: access control service severity**. Read-only. 1=Fatal error. 0=Non-fatal error.
20	**UnsuppReqErrSeverity: unsupported request error severity**. Read-write. 1=Fatal error. 0=Non-fatal error.
19	**EcrcErrSeverity: end-to-end CRC error severity**. Read-only.
18	**MalTlpSeverity: malformed TLP severity**. Read-write. 1=Fatal error. 0=Non-fatal error.
17	**RcvOvflSeverity: receiver overflow severity**. Read-only.
16	**UnexpCplSeverity: unexpected completion timeout severity**. Read-write. 1=Fatal error. 0=Non-fatal error.
15	**CplAbortErrSeverity: completer abort error severity**. Read-only.
14	**CplTimeoutSeverity: completion timeout severity**. Read-write. 1=Fatal error. 0=Non-fatal error.
13	**FcErrSeverity: flow control error severity**. Read-only.

12	**PsnErrSeverity: poisoned TLP severity**. Read-write. 1=Fatal error. 0=Non-fatal error.
11:6	Reserved.
5	**SurprdnErrSeverity: surprise down error severity**. Read-only.
4	**DlpErrSeverity: data link protocol error severity**. Read-write. 1=Fatal error. 0=Non-fatal error.
3:0	Reserved.

D[4:2]F[5:1]x160 Correctable Error Status

Cold reset: 0000_0000h.

Bits	Description
31:16	Reserved.
15	**HdrLogOvflStatus: header log overflow status**. Read-only.
14	**CorrIntErrStatus: corrected internal error status**. Read; Write-1-to-clear.
13	**AdvisoryNonfatalErrStatus: advisory non-fatal error status**. Read; Write-1-to-clear. 1=A non-fatal unsupported request errors or a non-fatal unexpected completion errors occurred.
12	**ReplayTimerTimeoutStatus: replay timer timeout status**. Read; Write-1-to-clear.
11:9	Reserved.
8	**ReplayNumRolloverStatus: replay**. Read; Write-1-to-clear. 1=The same transaction layer packet has been replayed three times and has caused the link to re-train.
7	**BadDllpStatus: bad data link layer packet status**. Read; Write-1-to-clear. 1=A link CRC error was detected.
6	**BadTlpStatus: bad transaction layer packet status**. Read; Write-1-to-clear. 1=A bad non-duplicated sequence ID or a link CRC error was detected.
5:1	Reserved.
0	**RcvErrStatus: receiver error status**. Read-only. 1=An 8b10b or disparity error was detected.

D[4:2]F[5:1]x164 Correctable Error Mask

Cold reset: 0000_6000h.

Bits	Description
31:16	Reserved.
15	**HdrLogOvflMask: header log overflow mask**. Read-only.
14	**CorrIntErrMask: corrected internal error mask**. Read-write.
13	**AdvisoryNonfatalErrMask: advisory non-fatal error mask**. Read-write. 1=Error is not reported.
12	**ReplayTimerTimeoutMask: replay timer timeout mask**. Read-write. 1=Error is not reported.
11:9	Reserved.
8	**ReplayNumRolloverMask: replay**. Read-write.1=Error is not reported.
7	**BadDllpMask: bad data link layer packet mask**. Read-write. 1=Error is not reported.
6	**BadTlpMask: bad transaction layer packet mask**. Read-write. 1=Error is not reported.
5:1	Reserved.
0	**RcvErrMask: receiver error mask**. Read-only. 1=Error is not reported.

D[4:2]F[5:1]x168 Advanced Error Control

Cold reset: 0000_0000h.

Bits	Description
31:12	Reserved.
11	**TlpPrefixLogPresent**. Read-only. IF (D[4:2]F[5:1]x7C[EndEndTlpPrefixSupported]==0) THEN Reserved. ENDIF. 1=If FirstErrPtr is valid then the TLP Prefix Log register contains valid information.
10	**MultiHdrRecdEn**. Read-only. 1=Enables recording more than one error header.
9	**MultiHdrRecdCap**. Read-only. 1=Specifies that the function is capable of recording more than one error header.
8	**EcrcCheckEn: data link protocol error severity**. Read-write. 0=Specifies that End-to-end CRC generation is not supported.
7	**EcrcCheckCap: data link protocol error severity**. Read-only. 0=Specifies that end-to-end CRC check is not supported.
6	**EcrcGenEn: end-to-end CRC enable**. Read-only. 0=Specifies that End-to-end CRC generation is not supported.
5	**EcrcGenCap: end-to-end CRC capability**. Read-only. 0=Specifies that end-to-end CRC generation is not supported.
4:0	**FirstErrPtr: first error pointer**. Read-only. The First Error Pointer identifies the bit position of the first error reported in the Uncorrectable Error Status register.

D[4:2]F[5:1]x16C Header Log DW0

Cold reset: 0000_0000h.

Bits	Description
31:0	**TlpHdr: transaction layer packet header log**. Read-only. Contains the header for a transaction layer packet corresponding to a detected error. The upper byte represents byte 0 of the header.

D[4:2]F[5:1]x170 Header Log DW1

Cold reset: 0000_0000h.

Bits	Description
31:0	**TlpHdr: transaction layer packet header log**. Read-only. Contains the header for a transaction layer packet corresponding to a detected error. The upper byte represents byte 4 of the header.

D[4:2]F[5:1]x174 Header Log DW2

Cold reset: 0000_0000h.

Bits	Description
31:0	**TlpHdr: transaction layer packet header log**. Read-only. Contains the header for a transaction layer packet corresponding to a detected error. The upper byte represents byte 8 of the header.

D[4:2]F[5:1]x178 Header Log DW3

Cold reset: 0000_0000h.

Bits	Description
31:0	**TlpHdr: transaction layer packet header log**. Read-only. Contains the header for a transaction layer packet corresponding to a detected error. The upper byte represents byte 12 of the header.

D[4:2]F[5:1]x17C Root Error Command

Reset: 0000_0000h.

Bits	Description
31:3	Reserved.
2	**FatalErrRepEn: fatal error reporting enable**. Read-write. 1=Enables the generation of an interrupt when a fatal error is reported by any of the devices in the hierarchy associated with this Root Port.
1	**NonfatalErrRepEn: non-fatal error reporting enable**. Read-write. 1=Enables generation of an interrupt when a non-fatal error is reported by any of the devices in the hierarchy associated with this Root Port.
0	**CorrErrRepEn: correctable error reporting enable**. Read-write. 1=Enables generation of an interrupt when a correctable error is reported by any of the devices in the hierarchy associated with this Root Port.

D[4:2]F[5:1]x180 Root Error Status

Cold reset: 0000_0000h.

Bits	Description
31:27	**AdvErrIntMsgNum: advanced error interrupt message number**. Read-only.
26:7	Reserved.
6	**NFatalErrMsgRcvd: fatal error message received**. Read; Write-1-to-clear. Set to 1 when one or more fatal uncorrectable error messages have been received.
5	**NonFatalErrMsgRcvd: non-fatal error message received**. Read; Write-1-to-clear. Set to 1 when one or more non-fatal uncorrectable error messages have been received.
4	**FirstUncorrFatalRcvd: first uncorrectable fatal error message received**. Read; Write-1-to-clear. Set to 1 when the first uncorrectable error message received is for a fatal error.
3	**MultErrFatalNonfatalRcvd: ERR_FATAL/NONFATAL message received**. Read; Write-1-to-clear. Set when either a fatal or a non-fatal error is received and ErrFatalNonfatalRcvd is already set.
2	**ErrFatalNonfatalRcvd: ERR_FATAL/NONFATAL message received**. Read; Write-1-to-clear. Set when either a fatal or a non-fatal error is received and this bit is not already set.
1	**MultErrCorrRcvd: multiple ERR_COR messages received**. Read; Write-1-to-clear. Set when a correctable error message is received and ErrCorrRcvd is already set.
0	**ErrCorrRcvd: ERR_COR message received**. Read; Write-1-to-clear. Set when a correctable error message is received and this bit is not already set.

D[4:2]F[5:1]x184 Error Source ID

Cold reset: 0000_0000h.

Bits	Description
31:16	**ErrFatalNonfatalSrcID: ERR_FATAL/ERR_NONFATAL source identification**. Read-only. Loaded with the requestor ID indicated in the received ERR_FATAL or ERR_NONFATAL message when D[4:2]F[5:1]x180[ErrFatalNonfatalRcvd] is not already set.
15:0	**ErrCorlSrcID: ERR_COR source identification**. Read-only. Loaded with the requestor ID indicated in the received ERR_COR message when D[4:2]F[5:1]x180[ErrCorrRcvd] is not already set.

3.9 Device 18h Function 0 Configuration Registers

See 3.1 [Register Descriptions and Mnemonics]. See 2.7 [Configuration Space].

D18F0x00 Device/Vendor ID

Bits	Description
31:16	**DeviceID: device ID**. Read-only. Value: 141Ah.
15:0	**VendorID: vendor ID**. Read-only. Value: 1022h.

D18F0x04 Status/Command

Bits	Description
31:16	**Status**. Read-only. Value: 0010h. Bit[20] is set to indicate the existence of a PCI-defined capability block.
15:0	**Command**. Read-only. Value: 0000h.

D18F0x08 Class Code/Revision ID

Bits	Description
31:8	**ClassCode**. Read-only. Value: 06_0000h. Provides the host bridge class code as defined in the PCI specification.
7:0	**RevID: revision ID**. Read-only. Value: 00h.

D18F0x0C Header Type

Read-only. Value: 0080_0000h.

Bits	Description
31:0	**HeaderTypeReg**. These bits are fixed at their default values. The header type field indicates that there are multiple functions present in this device.

D18F0x34 Capabilities Pointer

Bits	Description
31:8	Reserved.
7:0	**CapPtr: capabilities pointer**. Read-only. Value: 00h.

D18F0x[5C:40] Routing Table

Reset: 0004_0201h.

Table 113: Register Mapping for D18F0x[5C:40]

Register	Function
D18F0x40	Node 0
D18F0x[5C:44]	Reserved

Bits	Description
31:0	Reserved.

D18F0x60 Node ID

Bits	Description
31:21	Reserved.
20:16	**CpuCnt[4:0]: CPU count bits[4:0]**. Read-write. Reset: 0. Specifies the number of cores to be enabled (the boot core plus those cores enabled through D18F0x1DC[CpuEn]). Bits — Description 00h — 1 core 02h-01h — <CpuCnt[4:0] + 1> cores 03h — 4 cores 1Fh-04h — Reserved
15:0	Reserved.

D18F0x64 Unit ID

Reset: 0000_00E0h.

Bits	Description
31:16	Reserved.
15:11	Reserved.
10:8	Reserved.
7:6	**HbUnit: host bridge Unit ID**. Read-only. Specifies the coherent link Unit ID of the host bridge used by the coherent fabric.
5:4	**MctUnit: memory controller Unit ID**. Read-only. Specifies the coherent link Unit ID of the memory controller.
3:0	Reserved.

D18F0x68 Link Transaction Control

Bits	Description
31	Reserved.
30:28	Reserved.
27:26	Reserved.
25	Reserved.
24	Reserved.
23	**InstallStateS**. Read-write. Reset: 0. 1=Forces the default read block (RdBlk) install state to be shared instead of exclusive.
22:21	**DsNpReqLmt: downstream non-posted request limit**. Read-write. Reset: 00b. BIOS: 10b. This specifies the maximum number of downstream non-posted requests issued by core(s) which may be outstanding on the IO links attached to this node at one time. Bits Description 00b No limit 01b limited to 1 10b limited to 4 11b limited to 8
20	**SeqIdSrcNodeEn: sequence ID source node enable**. Read-write. Reset: 0. 1=The source node ID of requests is provided in the SeqID field of the corresponding downstream IO link request packets. This may be useful for debug applications, in order to match downstream packets with their originating node. For normal operation, this bit should be cleared. Correct ordering of requests between different nodes is not ensured when this bit is set. Semaphore sharing between differing nodes may not work properly in systems which are capable of processing IO requests with differing non-zero SeqIds out of request order.
19	**ApicExtSpur: APIC extended spurious vector enable**. Read-write. Reset: 0. This enables the extended APIC spurious vector functionality; it affects APICF0[Vector]. 0=The lower 4 bits of the spurious vector are read-only 1111b. 1=The lower 4 bits of the spurious vector are writable.
18	**ApicExtId: APIC extended ID enable**. Read-write. Reset: 0. Enables the extended APIC ID functionality. 0=APIC ID is 4 bits. 1=APIC ID is 8 bits.
17	**ApicExtBrdCst: APIC extended broadcast enable**. Read-write. Reset: 0. Enables the extended APIC broadcast functionality. 0=APIC broadcast is 0Fh. 1=APIC broadcast is FFh. If ApicExtBrdCst==1 then software must assert ApicExtId.
16	**LintEn: local interrupt conversion enable**. Read-write. Reset: 0. 1=Enables the conversion of broadcast ExtInt and NMI interrupt requests to LINT0 and LINT1 local interrupts, respectively, before delivering to the local APIC. This conversion only takes place if the local APIC is hardware enabled. LINT0 and LINT1 are controlled by APIC3[60:50]. 0=ExtInt/NMI interrupts delivered unchanged.
15	**LimitCldtCfg: limit coherent link configuration space range**. Read-write. Reset: 0. BIOS: 1.
14:13	Reserved.
12	Reserved.

11	**RespPassPW: response PassPW**. Read-write. Reset: 0. BIOS: 1. 1=The PassPW bit in all downstream link responses is set, regardless of the originating request packet. This technically breaks the PCI ordering rules but it is not expected to be an issue in the downstream direction. Setting this bit improves the latency of upstream requests by allowing the downstream responses to pass posted writes. 0=The PassPW bit in downstream responses is based on the RespPassPW bit of the original request.
10	**DisFillP: disable fill probe**. Read-write. Reset: 0. BIOS: 0. Controls probes for core-generated fills. 0=Probes issued for cache fills. 1=Probes not issued for cache fills. BIOS may set this bit if the processor is a single core device.
9	**DisRmtPMemC: disable remote probe memory cancel**. Read-write. Reset: 0. 1=Only probed caches on the same node as the target memory controller may generate MemCancel coherent link packets. MemCancels are used to attempt to save DRAM and/or link bandwidth associated with the transfer of stale DRAM data. 0=Probes hitting dirty blocks may generate MemCancel packets, regardless of the location of the probed cache.
8	**DisPMemC: disable probe memory cancel**. Read-write. Reset: 0. Controls generation of MemCancel coherent link packets. MemCancels are used to attempt to save DRAM and/or coherent link bandwidth associated with the transfer of stale DRAM data. 0=Probes hitting dirty blocks of the core cache may generate MemCancel packets. 1=Probes may not generate MemCancel packets.
7	**CPURdRspPassPW: CPU read response PassPW**. Read-write. Reset: 0. 1=Read responses to core-generated reads are allowed to pass posted writes. 0=Core responses do not pass posted writes. This bit is not expected to be set. This bit may only be set during the boot process.
6	**CPUReqPassPW: CPU request PassPW**. Read-write. Reset: 0. 1=Core-generated requests are allowed to pass posted writes. 0=Core requests do not pass posted writes. This bit is not expected to be set. This bit may only be set during the boot process.
5	Reserved.
4	**DisMTS: disable memory controller target start**. Read-write. Reset: 0. BIOS: 1. 1=Disables use of TgtStart. TgtStart is used to improve scheduling of back-to-back ordered transactions by indicating when the first transaction is received and ordered at the memory controller.
3	**DisWrDwP: disable write doubleword probes**. Read-write. Reset: 0. BIOS: 0. 1=Disables generation of probes for core-generated, WrSized doubleword commands.
2	**DisWrBP: disable write byte probes**. Read-write. Reset: 0. BIOS: 0. 1=Disables generation of probes for core-generated, WrSized byte commands.
1	**DisRdDwP: disable read doubleword probe**. Read-write. Reset: 0. BIOS: 0. 1=Disables generation of probes for coregenerated, RdSized doubleword commands.
0	**DisRdBP: disable read byte probe**. Read-write. Reset: 0. BIOS: 0. 1=Disables generation of probes for core-generated, RdSized byte commands.

D18F0x6C Link Initialization Control

Bits	Description
31	Reserved.
30	**RlsLnkFullTokCntImm**: **release upstream full token count immediately**. Read-write. Cold reset: 0. BIOS: 1 after buffer counts have been programmed. 1=Apply buffer counts programmed in D18F0x[F0,D0,B0,90] and D18F0x[F4,D4,B4,94] immediately without requiring warm reset. Once this bit is set, additional changes to the buffer counts only take effect upon warm reset.

29	Reserved.
28	**RlsIntFullTokCntImm: release internal full token count immediately**. Read-write. Cold reset: 0. BIOS: 1 after buffer counts have been programmed. 1=Apply buffer counts programmed in D18F3x6C, D18F3x70, D18F3x74, D18F3x78, D18F3x7C, D18F3x140, D18F3x144, D18F3x1[54,50,4C,48], D18F3x17C, and D18F3x1A0 immediately without requiring warm reset. Once this bit is set, additional changes to the buffer counts only take effect upon warm reset.
27	**ApplyIsocModeEnNow**. Read-write. Cold reset: 0. BIOS: 1 after RlsLnkFullTokCntImm and RlsIntFullTokCntImm have been set. 1=Apply the programmed value in D18F0x[E4,C4,A4,84][IsocEn] immediately without requiring warm reset. This bit may only be set if RlsLnkFullTokCntImm and RlsIntFullTokCntImm are set and isochronous buffers have been allocated. IF (ApplyIsocModeEnNow) THEN (D18F3x1[54,50,4C,48][IsocPreqTok0] > 0).
26:24	Reserved.
23	Reserved.
22:21	Reserved.
20	Reserved.
19:16	Reserved.
15:12	Reserved.
11	Reserved.
10:9	**BiosRstDet[2:1]: BIOS reset detect bits[2:1]**. See: BiosRstDet[0].
8	Reserved.
7	Reserved.
6	**InitDet: CPU initialization command detect**. Read-write. Reset: 0. This bit may be used by software to distinguish between an INIT and a warm or cold reset by setting it to a 1 before an initialization event is generated. This bit is cleared by RESET_L but not by an INIT command.
5	**BiosRstDet[0]: BIOS reset detect bit[0]**. Read-write. Cold reset: 0. BiosRstDet[2:0] = {BiosRstDet[2:1], BiosRstDet[0]}. May be used to distinguish between a reset event generated by the BIOS versus a reset event generated for any other reason by setting one or more of the bits to a 1 before initiating a BIOS-generated reset event.
4	**ColdRstDet: cold reset detect**. Read-write. Cold reset: 0. This bit may be used to distinguish between a cold versus a warm reset event by setting the bit to a 1 before an initialization event is generated.
3:2	Reserved.
1	Reserved.
0	**RouteTblDis: routing table disable**. Read-write. Reset: 1. BIOS: 0.

D18F0x[E4,C4,A4,84] Link Control

Table 114: Register Mapping for D18F0x[E4,C4,A4,84]

Register	Function
D18F0x84	ONION Link
D18F0xA4	ONIONPlus Link
D18F0x[E4,C4]	Reserved

This register is derived from the link control register defined in the link specification.

Bits	Description
31:16	Reserved.
15	**Addr64BitEn: 64-bit address packet enable**. Read-write. Cold reset: 0. 1=Requests to addresses greater than FF_FFFF_FFFFh are supported by this IO link. 0=Requests to addresses greater than FF_FFFF_FFFFh are master aborted as if the end of chain was reached. BIOS is required to ensure that the link-specification-defined "64 Bit Address Feature" bit in the device on the other side of the link is set prior to setting this bit. For coherent links, this bit is unused. D18F0x68[CHtExtAddrEn] is required to be set if this bit is set for any IO link. The link specification indicates that this bit is cleared by a warm reset; therefore this bit may be in a different state than an IO device on the other side of the link after a warm reset; care should be taken by BIOS to place devices on both sides of the link in the same state after a warm reset, before any packets to the high-order addresses enabled by this bit are generated.
14:13	Reserved.
12	**IsocEn: isochronous flow-control mode enable**. Read-write. Cold reset: 0. BIOS: 1 if the link is an ONION Link. This bit is set to place the link into isochronous flow-control mode (IFCM), as defined by the link specification. 1=IFCM. 0=Normal flow-control mode. See D18F0x6C[ApplyIsocMo-deEnNow].
11:6	Reserved.
5	Reserved.
4	**LinkFail: link failure**. Read; set-by-hardware; write-1-to-clear. Cold reset: 0. This bit is set high by the hardware if a Sync flood is received by the link. See 2.15.1.9.1 [Common Diagnosis Information].
3:0	Reserved.

D18F0x[EC,CC,AC,8C] Link Feature Capability

This register is derived from the link feature capability register defined in the link specification. Unless otherwise specified: 0=The feature is not supported; 1=The feature is supported.

Table 115: Register Mapping for D18F0x[EC,CC,AC,8C]

Register	Function
D18F0x8C	ONION Link
D18F0xAC	ONIONPlus Link
D18F0x[EC,CC]	Reserved

Bits	Description
31:6	Reserved.
5	**UnitIdReOrderDis: UnitID reorder disable**. Read-write. Reset: 0. 1=Upstream reordering for different UnitIDs is not supported; i.e., all upstream packets are ordered as if they have the same UnitID. 0=Reordering based on UnitID is supported.
4	Reserved. Reset: 1.
3:2	Reserved.
1	Reserved. Reset: 1.
0	Reserved. Reset: 1.

D18F0x[F0,D0,B0,90] Link Base Channel Buffer Count

Read-write; Reset-applied.

Table 116: Register Mapping for D18F0x[F0,D0,B0,90]

Register	Function
D18F0x90	ONION Link
D18F0xB0	ONIONPlus Link
D18F0x[F0,D0]	Reserved

D18F0x[F0,D0,B0,90] and D18F0x[F4,D4,B4,94] specify the *hard-allocated* link flow-control buffer counts in each virtual channel available to the transmitter at the other end of the link; it also provides the *free buffers* that may be used by any of the virtual channels, as needed. Base channel buffers are specified in D18F0x[F0,D0,B0,90]; isochronous buffer counts (if in IFCM) are specified in D18F0x[F4,D4,B4,94]. For all fields that specify buffer counts in D18F0x[F0,D0,B0,90] and D18F0x[F4,D4,B4,94]; If the link is ganged, then the number of buffers allocated is 2 times the value of the field; If the link is unganged, then the number of buffers allocated is the value of the field.

The cold or warm reset value is determined by whether the link initializes, whether the link is IO/coherent, whether the link is ganged/unganged, and whether the settings are locked by LockBc. Out of cold reset, the processor allocates a minimal number of buffers that is smaller than the default values in the register. BIOS must use D18F0x6C[RlsLnkFullTokCntImm] for the values in the register to take effect. This is necessary even if the values are unchanged from the default values.

The hard-allocated buffer counts are transmitted to the device at the other end of the link in buffer release messages after link initialization. The remaining buffers are held in the free list (specified by FreeData and FreeCmd) used to optimize buffer usage. When a transaction is received, if a free-list buffer is available, it is used for storage instead of one of the hard allocated buffers; as a result, a buffer release (for one of the hard allocated buffers used by the incoming request) can be immediately sent back to the device at the other end of the link without waiting for the transaction to be routed beyond the flow-control buffers.

Table 117: Link Buffer Definitions

Term	Definition
LpbSize	Link Packet Command Buffer size. LpbSize = 48.
LpbdSize	Link Packet Data Buffer size. LpbdSize = 32.
LcsSize	Link Command Scheduler size. LcsSize = 48.

Buffer allocation rules:

- The total number of command buffers allocated in the base and isochronous registers of a link cannot exceed LpbSize:
  - (D18F0x[B0,90][NpReqCmd] + D18F0x[B0,90][PReq] + D18F0x[B0,90][RspCmd] + D18F0x[B0,90][ProbeCmd] + D18F0x[B0,90][FreeCmd] + D18F0x[B4,94][IsocNpReqCmd] + D18F0x[B4,94][IsocPReq] + D18F0x[B4,94][IsocRspCmd]) <= LpbSize.
- The total number of data buffers allocated in the base and isochronous registers of a link cannot exceed LpbdSize:
  - (D18F0x[B0,90][NpReqData] + D18F0x[B0,90][RspData] + D18F0x[B0,90][PReq] + D18F0x[B0,90][FreeData] + D18F0x[B4,94][IsocPReq] + D18F0x[B4,94][IsocNpReqData] + D18F0x[B4,94][IsocRspData]) <= LpbdSize.
- The total number of hard allocated command buffers cannot exceed LcsSize.
  - (D18F0x[B0,90][ProbeCmd] + D18F0x[B0,90][RspCmd] + D18F0x[B0,90][PReq] + D18F0x[B0,90][NpReqCmd] + D18F0x[B4,94][IsocRspCmd] + D18F0x[B4,94][IsocPReq] + D18F0x[B4,94][IsocNpReqCmd]) <= LcsSize.
- BIOS must set up non-zero counts (and adjust the base channel counts accordingly) prior to enabling IFCM.
- If an IOMMU is present in the system, D18F0x[F4,D4,B4,94][IsocNpReqCmd] must be non-zero for all enabled links.
- If an IOMMU is present in the system, D18F0x[E4,C4,A4,84][IsocEn] must be enabled for the ONION link.

Bits	Description
31	**LockBc: lock buffer count register**. Cold reset: 0. BIOS: 1. 1=The buffer count registers, D18F0x[F0,D0,B0,90] and D18F0x[F4,D4,B4,94] are locked such that warm resets do not place the registers back to their default value. Setting this bit does not prevent the buffer counts from being updated after a warm reset based on the value of the buffer counts before the warm reset. 0=Upon warm reset, the buffer count registers return to their default value after the link initializes regardless of the value before the warm reset.
30	**PReq[3]: posted request command and data buffer count [3]**. IF (LockBc) THEN Cold reset: 0. ELSE Reset: 0. ENDIF. BIOS: IF (REG==D18F0x90) THEN 1. ELSE 0. ENDIF. See: PReq[2:0].

29:28	**NpReqData[3:2]: non-posted request data buffer count [3:2]**. IF (LockBc) THEN Cold reset: 00b. ELSE Reset: 00b. ENDIF. BIOS: IF (REG==D18F0x90) THEN 00b. ELSE 11b. ENDIF. See: NpReqData[1:0].
27:25	**FreeData: free data buffer count**. IF (D18F0x[F0,D0,B0,90][LockBc]) THEN Cold reset: 0. ELSE Reset: 0. ENDIF. BIOS: IF (REG==D18F0x90) THEN 3. ELSE 1. ENDIF.
24:20	**FreeCmd: free command buffer count**. IF (D18F0x[F0,D0,B0,90][LockBc]) THEN Cold reset: 0. ELSE Reset: 0. ENDIF. BIOS: IF (REG==D18F0x90) THEN 01h. ELSE 00h. ENDIF.
19:18	**RspData: response data buffer count**. IF (LockBc) THEN Cold reset: 1. ELSE Reset: 1. ENDIF. BIOS: IF (REG==D18F0x90) THEN 1. ELSE 0. ENDIF.
17:16	**NpReqData[1:0]: non-posted request data buffer count [1:0]**. NpReqData[3:0] = {NpReqData[3:2], NpReqData[1:0]}. IF (LockBc) THEN Cold reset: 01b. ELSE Reset: 01b. ENDIF. BIOS: IF (REG==D18F0x90) THEN 01b. ELSE 11b. ENDIF.
15:12	**ProbeCmd: probe command buffer count**. IF (LockBc) THEN Cold reset: 0h. ELSE Reset: 0h. ENDIF. BIOS: 0h.
11:8	**RspCmd: response command buffer count**. IF (LockBc) THEN Cold reset: 1h. ELSE Reset: 1h. ENDIF. BIOS: IF (REG==D18F0x90) THEN 2h. ELSE 0h. ENDIF.
7:5	**PReq[2:0]: posted request command and data buffer count [2:0]**. PReq[3:0] = {PReq[3], PReq[2:0]}. Specifies the number of posted command and posted data buffers allocated. IF (LockBc) THEN Cold reset: 110b. ELSE Reset: 110b. ENDIF. BIOS: IF (REG==D18F0x90) THEN 010b. ELSE 000b. ENDIF.
4:0	**NpReqCmd: non-posted request command buffer count**. IF (LockBc) THEN Cold reset: 09h. ELSE Reset: 09h. ENDIF. BIOS: IF (REG==D18F0x90) THEN 0Ah. ELSE 18h. ENDIF.

D18F0x[F4,D4,B4,94] Link Isochronous Channel Buffer Count

Read-write; Reset-applied. See D18F0x[F0,D0,B0,90].

Table 118: Register Mapping for D18F0x[F4,D4,B4,94]

Register	Function

Table 118: Register Mapping for D18F0x[F4,D4,B4,94]

D18F0x94	ONION Link
D18F0xB4	ONIONPlus Link
D18F0x[F4,D4]	Reserved

Bits	Description
31:29	Reserved.
28:27	**IsocRspData: isochronous response data buffer count**. IF (D18F0x[F0,D0,B0,90][LockBc]) THEN Cold reset: 0. ELSE Reset: 0. ENDIF. BIOS: 0.
26:25	**IsocNpReqData: isochronous non-posted request data buffer count**. IF (D18F0x[F0,D0,B0,90][LockBc]) THEN Cold reset: 0. ELSE Reset: 0. ENDIF. BIOS: IF (REG==D18F0x94) THEN 1. ELSE 0. ENDIF.
24:22	**IsocRspCmd: isochronous response command buffer count**. IF (D18F0x[F0,D0,B0,90][LockBc]) THEN Cold reset: 0. ELSE Reset: 0. ENDIF. BIOS: 0.
21:19	**IsocPReq: isochronous posted request command and data buffer count**. IF (D18F0x[F0,D0,B0,90][LockBc]) THEN Cold reset: 0. ELSE Reset: 0. ENDIF. This specifies the number of isochronous posted command and posted data buffers allocated. BIOS: 0.
18:16	**IsocNpReqCmd: isochronous non-posted request command buffer count**. IF (D18F0x[F0,D0,B0,90][LockBc]) THEN Cold reset: 0. ELSE Reset: 0. ENDIF. BIOS: IF (REG==D18F0x94) THEN 1. ELSE 0. ENDIF.
15:8	**SecBusNum: secondary bus number**. Reset: 0. Specifies the configuration-space bus number of the IO link. When configured as a coherent link, this register has no meaning. This field should match the corresponding D18F1x[1DC:1D0,EC:E0][BusNumBase], unless D18F1x[1DC:1D0,EC:E0][DevCmpEn]=1, in which case this field should be 00h).
7:0	Reserved.

D18F0x[F8,D8,B8,98] Link Type

Table 119: Register Mapping for D18F0x[F8,D8,B8,98]

Register	Function
D18F0x98	ONION Link
D18F0xB8	ONIONPlus Link
D18F0x[F8,D8]	Reserved

Bits	Description
31:6	Reserved.
5	**PciEligible**. Read-only. Reset: 1.
4:3	Reserved.
2	Reserved.

1	Reserved.
0	Reserved.

D18F0x[11C,118,114,110] Link Clumping Enable

Reset: 0000_0000h. D18F0x[11C,118,114,110] are associated with the whole link if it is ganged or sublink 0 if it is unganged; If the node does not support a link, then the corresponding register addresses become reserved.

Table 120: Register Mapping for D18F0x[11C,118,114,110]

Register	Function
D18F0x110	ONION Link
D18F0x114	ONIONPlus Link
D18F0x11[C:8]	Reserved

These registers specify how UnitIDs of upstream non-posted requests may be clumped per the link specification. The processor does not clump requests that it generates in the downstream direction.

Bits	Description
31:1	**ClumpEn**. Read-write. Each bit of this register corresponds to a link UnitID number. E.g., bit [2] corresponds to UnitID 02h, etc. 1=The specified UnitID is ordered in the same group as the specified UnitID - 1. For example, if this register is programmed to 0000_00C0h, then UnitIDs 7h, 6h, and 5h are all ordered as if they are part of the same UnitID. This is used to allow more than 32 tags to be assigned to a single stream for the purposes of ordering.
0	Reserved.

D18F0x150 Link Global Retry Control

Cold reset: 0000_0000h.

Bits	Description
31:0	Reserved.

D18F0x168 Extended Link Transaction Control

Read-write.

Bits	Description
31:21	Reserved.
20	**XcsSecPickerDstNcHt**. Reset: 0. BIOS: 1.
19	Reserved.
18	Reserved.
17:15	Reserved.
14:12	Reserved.
11:0	Reserved.

D18F0x16C Link Global Extended Control

Reset: 0000_0000h.

Bits	Description
31:0	Reserved.

D18F0x[18C:170] Link Extended Control

These registers provide control for each link. They are mapped to the links as follows:

Table 121: Register Mapping for D18F0x[18C:170]

Register	Function
D18F0x170	ONION Link
D18F0x174	ONIONPlus Link
D18F0x1[8C:78]	Reserved

Reset: 0000_0001h.

Bits	Description
31:0	Reserved.

D18F0x1A0 Link Initialization Status

Table 122: Onion Definitions

Term	Definition
OnionPlus	OnionPlus link detected. OnionPlus = (D18F0x1A0[OnionPlusCap]).

Bits	Description
31	**InitStatusValid: initialization status valid**. Read-only; Updated-by-hardware. Reset: 0. 1=Indicates that the rest of the information in this register is valid for all links; each link is either not connected or the initialization is complete.
30:28	Reserved.
27:24	**OnionPlusCap**.Read-only; Updated-by-hardware. Reset: 0h. 1=OnionPlus capable link detected. Bit — Description [0] — Link 0 [1] — Link 1 [2:3] — Reserved
23:4	Reserved.
3:2	**InitComplete1: initialization complete for link 1**. See: InitComplete0.
1:0	**InitComplete0: initialization complete for link 0**. Read-only; Updated-by-hardware. Reset: 00b. Bits — Description 00b — Internal northbridge link has not completed initialization. 10b-01b — Reserved. 11b — Internal northbridge link has completed initialization.

D18F0x1DC Core Enable

Reset: 0000_0000h.

Bits	Description
31:16	Reserved.
15:1	**CpuEn: core enable**. Read-write. This field is used to enable each of the cores after a reset. 1=Enable the core to start fetching and executing code from the boot vector. The most significant bit [N] is indicated by CpuCoreNum, as defined in section 2.4.4 [Processor Cores and Downcoring]. All bits greater than N are reserved. Bit — Description [0] — Core 1 enable [5:1] — Core <BIT+1> enable [6] — Core 7 enable [15:3] — Reserved.
0	Reserved.

3.10 Device 18h Function 1 Configuration Registers

See 3.1 [Register Descriptions and Mnemonics]. See 2.7 [Configuration Space].

D18F1x00 Device/Vendor ID

Bits	Description
31:16	**DeviceID: device ID**. Read-only. Value: 141Bh.
15:0	**VendorID: vendor ID**. Read-only. Value: 1022h.

D18F1x08 Class Code/Revision ID

Bits	Description
31:8	**ClassCode**. Read-only. Value: 06_0000h. Provides the host bridge class code as defined in the PCI specification.
7:0	**RevID: revision ID**. Read-only. Value: 00h. Processor revision. 00h=A0.

D18F1x0C Header Type

Reset: 0080_0000h.

Bits	Description
31:0	**HeaderTypeReg**. Read-only. These bits are fixed at their default values. The header type field indicates that there are multiple functions present in this device.

D18F1x[17C:140,7C:40] DRAM Base/Limit

The following sets of registers specify the DRAM address ranges:

Table 123: Register Mapping for D18F1x[17C:140,7C:40]

Function	Base Low	Limit Low	Base High	Limit High
Range 0	D18F1x40	D18F1x44	D18F1x140	D18F1x144
Reserved	D18F1x48, D18F1x[7:5][8,0]	D18F1x4C, D18F1x[7:5][C,4]	D18F1x148, D18F1x1[7:5][8,0]	D18F1x14C, D18F1x1[7:5][C,4]

Transaction addresses that are within the specified base/limit range are routed to the DstNode. See 2.8.2 [NB Routing].

DRAM mapping rules:
F1x0XX registers provide the low address bits. F1x1XX registers provide the high address bits.

- Transaction addresses are within the defined range if:
  {DramBase[47:24], 00_0000h} <= address[47:0] <= {DramLimit[47:24], FF_FFFFh}.
- DRAM regions must not overlap each other.
- Accesses to addresses that map to both DRAM, as specified by the DRAM base and limit registers (F1x[1, 0][7C:40]), and MMIO, as specified by D18F1x[2CC:2A0,1CC:180,BC:80], are routed to MMIO only.

- Programming of the DRAM address maps must be consistent with the Memory-Type Range Registers (MTRRs) and the top of memory registers, MSRC001_001A and MSRC001_001D. CPU accesses only hit within the DRAM address maps if the corresponding MTRR is of type DRAM. Accesses from IO links are routed based on the DRAM base and limit registers (F1x[1, 0][7C:40]) only.
- The appropriate RE or WE bit(s) must be set. When initializing a base/limit pair, the BIOS must write the [limit] register before either the RE or WE bit is set. When changing a base/limit pair that is already enabled, the BIOS should clear RE and WE before changing the address range.
- See 2.8.2.1.1 [DRAM and MMIO Memory Space].

When memory hoisting is enabled in a node via D18F1x2[1,0][8,0][LgcyMmioHoleEn], the corresponding BaseAddr/LimitAddr should be configured to account for the memory hoisted above the hole. See 2.9.12 [Memory Hoisting].

D18F1x[7:4][8,0] DRAM Base Low

IF (D18F2x118[LockDramCfg]) THEN Read-only. ELSE Read-write. ENDIF. Reset: 0000_0000h.

Table 124: Register Mapping for D18F1x[7:4][8,0]

Register	Function
D18F1x40	Range 0
D18F1x48	Reserved
D18F1x[7:5][8,0]	Reserved

Bits	Description
31:16	**DramBase[39:24]: DRAM base address register bits[39:24]**. DramBase[47:24] = {D18F1x1[7:4][8,0][DramBase[47:40]], D18F1x[7:4][8,0][DramBase[39:24]]}.
15:2	Reserved.
1	**WE: write enable**. 1=Writes to this address range are enabled.
0	**RE: read enable**. 1=Reads to this address range are enabled.

D18F1x1[7:4][8,0] DRAM Base High

Table 125: Register Mapping for D18F1x1[7:4][8,0]

Register	Function
D18F1x140	Range 0
D18F1x148	Reserved
D18F1x1[7:5][8,0]	Reserved

Bits	Description
31:8	Reserved.
7:0	**DramBase[47:40]: DRAM base address register bits[47:40]**. See: D18F1x[7:4][8,0][DramBase[39:24]].

D18F1x[7:4][C,4] DRAM Limit Low

IF (D18F2x118[LockDramCfg]) THEN Read-only. ELSE Read-write. ENDIF.

Table 126: Register Mapping for D18F1x[7:4][C,4]

Register	Function
D18F1x44	Range 0
D18F1x4C	Reserved
D18F1x[7:5][C,4]	Reserved

Bits	Description
31:16	**DramLimit[39:24]: DRAM limit address register bits[39:24]**. Reset: FCFFh. DramLimit[47:24] = {D18F1x1[7:4][C,4][DramLimit[47:40]], D18F1x[7:4][C,4][DramLimit[39:24]]}.
15:11	Reserved.
10:8	Reserved.
7:3	Reserved.
2:0	**DstNode: destination Node ID**. Reset: 000b. Specifies the node that a packet is routed to if it is within the address range.

D18F1x1[7:4][C,4] DRAM Limit High

IF (D18F2x118[LockDramCfg]) THEN Read-only. ELSE Read-write. ENDIF.

Table 127: Register Mapping for D18F1x1[7:4][C,4]

Register	Function
D18F1x144	Range 0
D18F1x14C	Reserved
D18F1x1[7:5][C,4]	Reserved

Bits	Description
31:8	Reserved.
7:0	**DramLimit[47:40]: DRAM limit address register bits[47:40]**. Reset: 00h. See D18F1x[7:4][C,4][DramLimit[39:24]].

D18F1x[2CC:2A0,1CC:180,BC:80] MMIO Base/Limit

These registers, The memory mapped IO base and limit registers D18F1x[2CC:2A0,1CC:180,BC:80] specify the mapping from memory addresses to the corresponding node and IO link for MMIO transactions. Address ranges are specified by upto 16 sets of base/limit registers.

Table 128: Register Mapping for D18F1x[2CC:2A0,1CC:180,BC:80]

Function	MMIO Base Low	MMIO Limit Low	MMIO Base/Limit High
Range 0	D18F1x80	D18F1x84	D18F1x180
Range 1	D18F1x88	D18F1x8C	D18F1x184
Range 2	D18F1x90	D18F1x94	D18F1x188
Range 3	D18F1x98	D18F1x9C	D18F1x18C
Range 4	D18F1xA0	D18F1xA4	D18F1x190
Range 5	D18F1xA8	D18F1xAC	D18F1x194
Range 6	D18F1xB0	D18F1xB4	D18F1x198
Range 7	D18F1xB8	D18F1xBC	D18F1x19C
Range 8	D18F1x1A0	D18F1x1A4	D18F1x1C0
Range 9	D18F1x1A8	D18F1x1AC	D18F1x1C4
Range 10	D18F1x1B0	D18F1x1B4	D18F1x1C8
Range 11	D18F1x1B8	D18F1x1BC	D18F1x1CC
Reserved	D18F1x2[B8,B0,A8,A0]	D18F1x2[BC,B4,AC,A4]	D18F1x2[CC,C8,C4,C0]

Transaction addresses that are within the specified base/limit range are routed to the node specified by DstNode and the link specified by DstLink. See 2.8.2 [NB Routing].

MMIO mapping rules:

- Transaction addresses are within the defined range if:
  {MMIOBase[47:16], 0000h} <= address[47:0] <= {MMIOLimit[47:16], FFFFh}.
- MMIO regions must not overlap each other.
- Accesses to addresses that map to both DRAM, as specified by the DRAM base and limit registers (see D18F1x[17C:140,7C:40]), and MMIO, as specified by the memory mapped IO base and limit registers (F1x[BC:80]), are routed to MMIO only.
- Programming of the MMIO address maps must be consistent with the Memory-Type Range Registers (MTRRs) and the top of memory registers, MSRC001_001A and MSRC001_001D. CPU accesses only hit within the MMIO address maps if the corresponding MTRR is of type IO. Accesses from IO links are routed based on D18F1x[2CC:2A0,1CC:180,BC:80].
- The appropriate RE or WE bit(s) must be set. When initializing a base/limit pair, the BIOS must write the limit register before either the RE or WE bit is set. When changing a base/limit pair that is already enabled, the BIOS should clear RE and WE before changing the address range.
- Scenarios in which the address space of multiple MMIO ranges target the same IO device is supported.
- See 2.8.2.1.1 [DRAM and MMIO Memory Space].

D18F1x[2B:1A,B:8][8,0] MMIO Base Low

Table 129: Register Mapping for D18F1x[2B:1A,B:8][8,0]

Register	Function
D18F1x80	Range 0
D18F1x88	Range 1
D18F1x90	Range 2
D18F1x98	Range 3
D18F1xA0	Range 4

Table 129: Register Mapping for D18F1x[2B:1A,B:8][8,0]

D18F1xA8	Range 5
D18F1xB0	Range 6
D18F1xB8	Range 7
D18F1x1A0	Range 8
D18F1x1A8	Range 9
D18F1x1B0	Range 10
D18F1x1B8	Range 11
D18F1x2[B:A][8,0]	Reserved

Bits	Description
31:8	**MMIOBase[39:16]: MMIO base address register bits[39:16]**. Read-write. Reset: 0. MMIOBase[47:16] = {D18F1x[2CC:2C0,1CC:1C0,19C:180][MMIOBase[47:40]], MMIO-Base[39:16]}.
7:4	Reserved.
3	**Lock**. Read-write. Reset: 0. 1=The memory mapped IO base and limit registers (D18F1x[2CC:2A0,1CC:180,BC:80]) are read-only (including this bit). WE or RE in this register must be set in order for this to take effect.
2	Reserved.
1	**WE: write enable**. Read-write. Reset: 0. 1=Writes to this address range are enabled.
0	**RE: read enable**. Read-write. Reset: 0. 1=Reads to this address range are enabled.

D18F1x[2B:1A,B:8][C,4] MMIO Limit Low

Table 130: Register Mapping for D18F1x[2B:1A,B:8][C,4]

Register	Function
D18F1x84	Range 0
D18F1x8C	Range 1
D18F1x94	Range 2
D18F1x9C	Range 3
D18F1xA4	Range 4
D18F1xAC	Range 5
D18F1xB4	Range 6
D18F1xBC	Range 7
D18F1x1A4	Range 8
D18F1x1AC	Range 9
D18F1x1B4	Range 10
D18F1x1BC	Range 11
D18F1x2[BC,B4,AC,A4]	Reserved

Bits	Description
31:8	**MMIOLimit[39:16]: MMIO limit address register bits[39:16]**. Read-write. Reset: 0. MMIOLimit[47:16] = {D18F1x[2CC:2C0,1CC:1C0,19C:180][MMIOLimit[47:40]], MMIOLimit[39:16]}.
7	**NP: non-posted**. Read-write. Reset: 0. 1=CPU write requests to this MMIO range are passed through the non-posted channel. This may be used to force writes to be non-posted for MMIO regions which map to the legacy ISA/LPC bus, or in conjunction with D18F0x68[DsNpReqLmt] in order to allow downstream CPU requests to be counted and thereby limited to a specified number. This latter use of the NP bit may be used to avoid loop deadlock scenarios in systems that implement a region in an IO device that reflects downstream accesses back upstream. See the link summary of deadlock scenarios for more information. 0=CPU writes to this MMIO range use the posted channel. This bit does not affect requests that come from IO links (the virtual channel of the request is specified by the IO request). If two MMIO ranges target the same IO device and the NP bit is set differently in both ranges, unexpected transaction ordering effects are possible. In particular, using PCI- and IO-link-defined producer-consumer semantics, if a producer (e.g., the processor) writes data using a non-posted MMIO range followed by a flag to a posted MMIO range, then it is possible for the device to see the flag updated before the data is updated.
6	**DstSubLink: destination sublink**. Read-write. Reset: 0. When a link is unganged, this bit specifies the destination sublink of the link specified by the memory mapped IO base and limit registers F1x[BC:80][DstLink]. 0=The destination link is sublink 0. 1=The destination link is sublink 1. If the link is ganged, then this bit must be low.
5:4	**DstLink: destination link ID**. Read-write. Reset: 0. For transactions within this MMIO range, this field specifies the destination IO link number of the destination node. Bits — Description 00b — Link 0 01b — Link 1 10b — Link 2 11b — Link 3
3	Reserved.
2:0	**DstNode: destination node ID bits**. Read-write. Reset: 0. For transactions within this MMIO range, this field specifies the destination node ID.

D18F1x[2CC:2C0,1CC:1C0,19C:180] MMIO Base/Limit High

Table 131: Register Mapping for D18F1x[2CC:2C0,1CC:1C0,19C:180]

Register	Function
D18F1x180	Range 0
D18F1x184	Range 1
D18F1x188	Range 2
D18F1x18C	Range 3
D18F1x190	Range 4
D18F1x194	Range 5
D18F1x198	Range 6

Table 131: Register Mapping for D18F1x[2CC:2C0,1CC:1C0,19C:180]

D18F1x19C	Range 7
D18F1x1C0	Range 8
D18F1x1C4	Range 9
D18F1x1C8	Range 10
D18F1x1CC	Range 11
D18F1x2[CC:C0]	Reserved

Bits	Description
31:24	Reserved.
23:16	**MMIOLimit[47:40]: MMIO limit address register bits[47:40]**. See: D18F1x[2B:1A,B:8][C,4][MMIOLimit[39:16]].
15:8	Reserved.
7:0	**MMIOBase[47:40]: MMIO base address register bits[47:40]**. See: D18F1x[2B:1A,B:8][8,0][MMIOBase[39:16]].

D18F1x[DC:C0] IO-Space Base/Limit

The IO-space base and limit registers, D18F1x[DC:C0], specify the mapping from IO addresses to the corresponding node and IO link for transactions resulting from x86-defined IN and OUT instructions. IO address ranges are specified by upto 8 sets of base/limit registers. The first set is F1xC0 and F1xC4, the second set is F1xC8 and F1xCC, and so forth. Transaction addresses that are within the specified base/limit range are routed to the node specified by DstNode and the link specified by DstLink. See 2.8.2 [NB Routing].

IO mapping rules:

- IO-space transaction addresses are within the defined range if: {IOBase[24:12], 000h} <= address <= {IOLimit[24:12], FFFh} and as specified by the IE bit; or if the address is in the range specified by the VE bits.
- IO regions must not overlap each other.
- The appropriate RE or WE bit(s) must be set.
- See 2.8.2.1.2 [IO Space].

D18F1x[1F:1E,D:C][8,0] IO-Space Base

Table 132: Register Mapping for D18F1x[1F:1E,D:C][8,0]

Register	Function
D18F1xC0	Range 0
D18F1xC8	Range 1
D18F1xD0	Range 2
D18F1xD8	Range 3
D18F1x1[F:E][8,0]	Reserved

Bits	Description
31:25	Reserved.

24:12	**IOBase[24:12]: IO base address register bits[24:12]**. Read-write. Reset: 0.
11:6	Reserved.
5	**IE: ISA enable**. Read-write. Reset: 0. 1=The IO-space address window is limited to the first 256 B of each 1 KB block specified; this only applies to the first 64 KB of IO space. 0=The PCI IO window is not limited in this way.
4	**VE: VGA enable**. Read-write. Reset: 0. 1=Include IO-space transactions targeting the VGA-compatible address space within the IO-space window of this base/limit pair. These include IO accesses in which address bits[9:0] range from 3B0h to 3BBh or 3C0h to 3DFh (address bits[15:10] are not decoded); this only applies to the first 64 KB of IO space; i.e., address bits[24:16] must be low). 0=IO-space transactions targeting VGA-compatible address ranges are not added to the IO-space window. This bit should only ever be set in one register. The MMIO range associated with the VGA enable bit in the PCI specification is not included in the VE bit definition; to map this range to an IO link, see D18F1xF4 [VGA Enable]. When D18F1xF4[VE] is set, the state of this bit is ignored.
3:2	Reserved.
1	**WE: write enable**. Read-write. Reset: 0. 1=Writes to this IO-space address range are enabled.
0	**RE: read enable**. Read-write. Reset: 0. 1=Reads to this IO-space address range are enabled.

D18F1x[1F:1E,D:C][C,4] IO-Space Limit

Table 133: Register Mapping for D18F1x[1F:1E,D:C][C,4]

Register	Function
D18F1xC4	Range 0
D18F1xCC	Range 1
D18F1xD4	Range 2
D18F1xDC	Range 3
D18F1x1[F:E][C,4]	Reserved

Bits	Description
31:25	Reserved.
24:12	**IOLimit[24:12]: IO limit address register bits[24:12]**. Read-write. Reset: 0.
11:7	Reserved.
6	**DstSubLink: destination sublink**. Read-write. Reset: 0. When a link is unganged, this bit specifies the destination sublink of the link specified by F1x[DC:C0][DstLink]. 0=The destination link is sublink 0. 1=The destination link is sublink 1. If the link is ganged, then this bit must be low.
5:4	**DstLink: destination link ID**. Read-write. Reset: 0. For transactions within this IO-space range, this field specifies the destination IO link number of the destination node. Bits — Description 00b — Link 0 01b — Link 1 10b — Link 2 11b — Link 3
3	Reserved.
2:0	**DstNode: destination node ID bits**. Read-write. Reset: 0. For transactions within this IO-space range, this field specifies the destination node ID.

D18F1x[1DC:1D0,EC:E0] Configuration Map

D18F1x[1DC:1D0,EC:E0] specify the mapping from configuration address to the corresponding node and IO link. Configuration address ranges are specified by upto 8 pairs of base/limit registers. Transaction addresses that are within the specified base/limit range are routed to the node specified by DstNode and the link specified by DstLink. See 2.8.2 [NB Routing].

Table 134: Register Mapping for D18F1x[1DC:1D0,EC:E0]

Register	Function
D18F1xE0	Range 0
D18F1xE4	Range 1
D18F1xE8	Range 2
D18F1xEC	Range 3
D18F1x1[DC:D0]	Reserved

Configuration space mapping rules:

- Configuration addresses (to"BusNo" and "Device" as specified by IOCF8 [IO-Space Configuration Address] in the case of IO accesses or 2.7 [Configuration Space] in the case of MMIO accesses) are within the defined range if:
  ({BusNumBase[7:0]} <= BusNo <= {BusNumLimit[7:0]}) & (DevCmpEn==0); or
  ({BusNumBase[4:0]} <= Device <= {BusNumLimit[4:0]}) & (DevCmpEn==1) & (BusNo == 00h).
- Configuration regions must not overlap each other.
- The appropriate RE or WE bit(s) must be set.
- See 2.8.2.1.3 [Configuration Space].

Bits	Description
31:24	**BusNumLimit[7:0]: bus number limit bits[7:0]**. Read-write. Reset: 0.
23:16	**BusNumBase[7:0]: bus number base bits[7:0]**. Read-write. Reset: 0.
15:3	Reserved.
2	**DevCmpEn: device number compare mode enable**. Read-write. Reset: 0. 1=A device number range rather than a bus number range is used to specify the configuration-space window (see above).
1	**WE: write enable**. Read-write. Reset: 0. 1=Writes to this configuration-space address range are enabled.
0	**RE: read enable**. Read-write. Reset: 0. 1=Reads to this configuration-space address range are enabled.

D18F1xF0 DRAM Hole Address

IF (D18F2x118[LockDramCfg]) THEN Read-only. ELSE Read-write. ENDIF. Same-for-all. Reset: 0000_0000h. See 2.9.12 [Memory Hoisting].

Bits	Description
31:24	**DramHoleBase[31:24]: DRAM hole base address**. Specifies the base address of the IO hole, below the 4GB address level, that is used in memory hoisting. Normally, DramHoleBase >= MSRC001_001A[TOM[31:24]].
23:16	Reserved.

15:7	**DramHoleOffset[31:23]: DRAM hole offset address**. When D18F1x2[1,0][8,0][LgcyMmioHoleEn]==1, this offset is subtracted from the physical address of certain accesses in forming the normalized address.
6:3	Reserved.
2	Reserved.
1	**DramMemHoistValid: dram memory hoist valid**. 1=Memory hoisting for the address range is enabled. 0=Memory hoisting is not enabled. This bit should be set if any D18F1x2[1,0][8,0][LgcyMmioHoleEn]==1 or DramHoleBase != 0.
0	**DramHoleValid: dram hole valid**. 1=Memory hoisting is enabled in the node. 0=Memory hoisting is not enabled. This bit should be set in the node that owns the DRAM address space that is hoisted above the 4 GB address level. See DramHoleBase.

D18F1xF4 VGA Enable

Reset: 0000_0000h.

Bits	Description
31:15	Reserved.
14	**DstSubLink: destination sublink**. Read-write. When a link is unganged, this bit specifies the destination sublink of the link specified by D18F1xF4[DstLink]. 0=The destination link is sublink 0. 1=The destination link is sublink 1. If the link is ganged, then this bit must be low.
13:12	**DstLink: destination link ID**. Read-write. For transactions within the D18F1xF4[VE]-defined ranges, this field specifies the destination IO link number of the destination node. Bits — Description 00b — Link 0 01b — Link 1 10b — Link 2 11b — Link 3
11:7	Reserved.
6:4	**DstNode: destination node ID**. Read-write. For transactions within the D18F1xF4[VE]-defined range, this field specifies the destination node ID.
3	**Lock**. Read-write. 1=All the bits in this register (D18F1xF4) are read-only (including this bit).
2	Reserved.
1	**NP: non-posted**. Read-write. 1=CPU write requests to the D18F1xF4[VE]-defined MMIO range are passed through the non-posted channel. 0=CPU writes may be posted.
0	**VE: VGA enable**. Read-write. 1=Transactions targeting the VGA-compatible address space are routed and controlled as specified by this register. The VGA-compatible address space is: (1) the MMIO range A_0000h through B_FFFFh; (2) IO-space accesses in which address bits[9:0] range from 3B0h to 3BBh or 3C0h to 3DFh (address bits[15:10] are not decoded; this only applies to the first 64 KB of IO space; i.e., address bits[24:16] must be low). 0=Transactions targeting the VGA-compatible address space are not affected by the state of this register. When this bit is set, the state of D18F1xF4[VE] is ignored.

D18F1x10C DCT Configuration Select

Reset: 0000_0000h.

Bits	Description
31:8	Reserved.
7	**DctCfgBcEn: Dct config write broadcast enable**. Read-write. 1=For a logical CSR write to D18F2x98_dct[3:0] or D18F2x9C_dct[3:0], all enabled DCTs receive the config data. 0=Only the DCT specified with DctCfgSel receives the config data of a config write. For a logical CSR read, DctCfgBcEn=x and the DCT with DctCfgSel supplies the read data.
6	Unused.
5:4	**NbPsSel: NB P-state configuration select**. Read-write. Specifies the set of DCT P-state registers to which accesses are routed. Bits — Description 00b — NB P-state 0 01b — NB P-state 1 10b — NB P-state 2 11b — NB P-state 3 The following registers must be programmed for each NB P-state enabled by D18F5x16[C:0][NbPstateEn]: • D18F2x210_dct[3:0]_nbp[3:0][MaxRdLatency]. • D18F2x210_dct[3:0]_nbp[3:0][DataTxFifoWrDly]. • D18F2x210_dct[3:0]_nbp[3:0][RdPtrInit].
3	**MemPsSel: Memory P-state configuration select**. Read-write. Specifies the set of DCT controller registers to which accesses are routed. This register works independently of NbPsSel. 0=Memory P-state 0. 1=Memory P-state 1. See 2.5.7.1 [Memory P-states] and 2.9.3 [DCT Configuration Registers].
2:0	**DctCfgSel: DRAM controller configuration select**. Read-write. Specifies DCT controller to which accesses are routed. See 2.9.3 [DCT Configuration Registers]. Bits — Description 000b — DCT 0 001b — DCT 1 010b — DCT 2 011b — DCT 3

D18F1x120 DRAM Base System Address

IF (D18F2x118[LockDramCfg]) THEN Read-only. ELSE Read-write. ENDIF. Cold reset: 0000_0000h. D18F1x120 and D18F1x124 are required to specify the base and limit system address range of the DRAM connected to the local node.

DRAM accesses to the local node with physical address Addr[47:0] that are within the following range are directed to the DCTs:

{DramBaseAddr[47:27], 000_0000h} <= Addr[47:0] <= {DramLimitAddr[47:27], 7FF_FFFFh};

DRAM accesses to the local node that are outside of this range are master aborted.

The address of the DRAM transaction is normalized before passing it to the DCTs by subtracting DramBaseAddr.
This range is also used to specify the range of DRAM covered by the scrubber (see D18F3x58 and D18F3x5C).

Bits	Description
31:21	Reserved.
20:0	**DramBaseAddr[47:27]**.

D18F1x124 DRAM Limit System Address

IF (D18F2x118[LockDramCfg]) THEN Read-only. ELSE Read-write. ENDIF. See D18F1x120 [DRAM Base System Address].

Bits	Description
31:24	Reserved.
23:21	Reserved.
20:0	**DramLimitAddr[47:27]**. Cold reset: 1F_FFFFh.

D18F1x2[1C:00] DRAM Controller Base/Limit

The DRAM controller base and limit registers define a DRAM controller address range and specify the mapping of physical DRAM addresses to a DCT as selected by DctSel or DctIntLvEn. The following base/limit register pairs specify the address ranges:

Table 135: Register Mapping for D18F1x2[1C:00]

Function	Base Address	Limit Address
Range 0	D18F1x200	D18F1x204
Range 1	D18F1x208	D18F1x20C
Range 2	D18F1x210	D18F1x214
Range 3	D18F1x218	D18F1x21C

BIOS should observe the following DCT configuration requirements:
- DRAM addresses are within the defined range if:
  {DctBaseAddr[47:27], 000b, 00_0000h} <= address[47:0] <= {DctLimitAddr[47:27], 111b, FF_FFFFh}.
- DCT base/limit address ranges must not overlap each other.
- A maximum of two address ranges may be mapped to a single DCT.

Hoisting. When memory hoisting is enabled viaLegacyMmioHoleEn, the corresponding DctBaseAddr/DctLimitAddr should be configured to account for the memory hoisted above the hole. A contiguous memory hole should only be mapped by one DctBaseAddr/DctLimitAddr pair. See 2.9.12 [Memory Hoisting].

Channel interleaving. A DRAM address range may be mapped to one DCT as a continuous region, or it may be interleaved between DCTs. See 2.9.11.2 [Channel Interleaving].

D18F1x2[1,0][8,0] DRAM Controller Base

IF (D18F2x118[LockDramCfg]) THEN Read-only. ELSE Read-write. ENDIF. Reset: 0000_0000h.

Table 136: Register Mapping for D18F1x2[1,0][8,0]

Register	Function
D18F1x200	Range 0
D18F1x208	Range 1
D18F1x210	Range 2
D18F1x218	Range 3

Bits	Description
31:11	**DctBaseAddr[47:27]: DRAM controller base address [47:27]**. Read-write. Specifies the base physical address bits for this address range.
10:7	Reserved.
6:4	**DctSel: DRAM controller select**. Read-write. Specifies the DCT mapped to this address range. Ignored if (D18F1x2[1,0][C,4][DctIntLvEn] != 0). Bits Definition 011b-000b DCT <*DctSel*> 111b-100b Reserved
3	**DctOffsetEn: DRAM controller offset enable**. Read-write. BIOS: See 2.9.12.2 [DctSelBaseOffset Programming]. 1=Add the offset specified by D18F1x2[4C:40][DctHighAddrOffset] to accesses in this address range in forming the normalized address. 0=Addition of the offset is not enabled.
2	Reserved.
1	**LgcyMmioHoleEn: legacy mmio hole enable**. Read-write. BIOS: See 2.9.12 [Memory Hoisting]. 1=Enable memory hoisting for this address range. BIOS sets this bit for an address range that spans the 4GB boundary and contains a hole for addresses used by MMIO. 0=Memory hoisting is not enabled.
0	**DctAddrVal: DRAM controller address valid**. Read-write. 1=Specifies this address range is valid and enabled. 0=This address range is not enabled.

D18F1x2[1,0][C,4] DRAM Controller Limit

IF (D18F2x118[LockDramCfg]) THEN Read-only. ELSE Read-write. ENDIF. Reset: 0000_0000h.

Table 137: Register Mapping for D18F1x2[1,0][C,4]

Register	Function
D18F1x204	Range 0
D18F1x20C	Range 1
D18F1x214	Range 2
D18F1x21C	Range 3

Bits	Description
31:11	**DctLimitAddr[47:27]: DRAM controller limit address bits [47:27]**. Read-write. Specifies the limit physical address bits for this address range.
10:4	Reserved.
3:0	**DctIntLvEn: DRAM controller interleave enable**. Read-write. BIOS: See 2.9.11.2 [Channel Interleaving]. 1=DCT participates in channel interleaving for this address range. Bit Definition [0] DCT 0 [1] DCT 1 [2] DCT 2 [3] DCT 3

D18F1x2[4C:40] DRAM Controller High Address Offset Register

IF (D18F2x118[LockDramCfg]) THEN Read-only. ELSE Read-write. ENDIF. Reset: 0000_0000h.

Table 138: Register Mapping for D18F1x2[4C:40]

Register	Function
D18F1x240	DCT 0
D18F1x244	DCT 1
D18F1x248	DCT 2
D18F1x24C	DCT 3

Bits	Description
31:23	Reserved.
22:11	**DctHighAddrOffset[38:27]: DRAM controller high address offset**. When D18F1x2[1,0][8,0][DctOffsetEn]==1, specifies the offset added by the DCT in forming the normalized address for that range. When a DCT is mapped by two ranges, this offset places the normalized address above those mapped by a previous D18F1x2[1C:00] address range. Reserved if D18F1x2[1,0][8,0][DctOffsetEn]!=1.
10:0	Reserved.

3.11 Device 18h Function 2 Configuration Registers

See 3.1 [Register Descriptions and Mnemonics]. See 2.7 [Configuration Space].

D18F2x00 Device/Vendor ID

Bits	Description
31:16	**DeviceID: device ID**. Read-only. Value: 141Ch.
15:0	**VendorID: vendor ID**. Read-only. Value: 1022h.

D18F2x08 Class Code/Revision ID

Reset: 0600_0000h.

Bits	Description
31:8	**ClassCode**. Read-only. Provides the host bridge class code as defined in the PCI specification.
7:0	**RevID: revision ID**. Read-only.

D18F2x0C Header Type

Reset: 0080_0000h.

Bits	Description
31:0	**HeaderTypeReg**. Read-only. These bits are fixed at their default values. The header type field indicates that there multiple functions present in this device.

D18F2x[5C:40]_dct[3:0] DRAM CS Base Address

See 2.9.3 [DCT Configuration Registers].

These registers along with D18F2x[6C:60]_dct[3:0] [DRAM CS Mask], translate DRAM request addresses (to a DRAM controller) into DRAM chip selects. Supported DIMM sizes are specified in D18F2x80_dct[3:0] [DRAM Bank Address Mapping]. For more information on the DRAM controllers, see 2.9 [DRAM Controllers (DCTs)].

For each chip select, there is a DRAM CS Base Address register. For each CS pair there is a DRAM CS Mask Register. For each CS pair, an even CS must be populated if the odd CS is populated. If a chipselect is populated in the system it must be indicated to the DCT by setting one of the mutually exclusive {CSEnable, TestFail} configuration bits.

Table 139: DIMM, Chip Select, and Register Mapping

Base Address Registers	Mask Register	Logical DIMM	Chip Select[1]
D18F2x40_dct[x]	F2x60	0	MEMCS[x]_L[0]
D18F2x44_dct[x]			MEMCS[x]_L[1]

Table 139: DIMM, Chip Select, and Register Mapping

Base Address Registers	Mask Register	Logical DIMM	Chip Select[1]
D18F2x48_dct[x]	F2x64	1	MEMCS[x]_L[2]
D18F2x4C_dct[x]			MEMCS[x]_L[3]
D18F2x[5C:50]_dct[x]	F2x6[C,8]	Reserved	
1. See 2.9.4 [DDR Pad to Processor Pin Mapping]			

The DRAM controller operates on the normalized physical address of the DRAM request. The normalized physical address includes all of the address bits that are supported by a DRAM controller. See 2.8 [Northbridge (NB)].

Each base address register specifies the starting normalized address of the block of memory associated with the chip select. Each mask register specifies the additional address bits that are consumed by the block of memory associated with the chip selects. If both chip selects of a DIMM are used, they must be the same size; in this case, a single mask register covers the address space consumed by both chip selects.

Lower-order address bits are provided in the base address and mask registers, as well. These allow memory to be interleaved between chip selects, such that contiguous physical addresses map to the same DRAM page of multiple chip selects. See 2.9.11.1 [Chip Select Interleaving]. The hardware supports the use of lower-order address bits to interleave chip selects if (1) the each chip select of the memory system spans the same amount of memory and (2) the number of chip selects of the memory system is a power of two.

BIOS is required to assign the largest DIMM chip-select range to the lowest normalized address of the DRAM controller. As addresses increase, the chip-select size is required to remain constant or decrease. This is necessary to keep DIMM chip-select banks on aligned address boundaries, regardless as to the amount of address space covered by each chip select.

For each normalized address for requests that enters a DRAM controller, a ChipSelect[i] is asserted if:

```
CSEnable[i] &
( {(InputAddr[38:27]   & ~AddrMask[i][38:27]),
        (InputAddr[21:11]   & ~AddrMask[i][21:11])} ==
       {(BaseAddr[i][38:27] & ~AddrMask[i][38:27]),
        (BaseAddr[i][21:11]  & ~AddrMask[i][21:11])} );
```

Bits	Description
31	Reserved.
30:19	**BaseAddr[38:27]: normalized physical base address bits [38:27]**. IF (D18F2x118[LockDramCfg]) THEN Read-only. ELSE Read-write. ENDIF. Reset: 0.
18:16	Reserved.
15:5	**BaseAddr[21:11]: normalized physical base address bits [21:11]**. IF (D18F2x118[LockDramCfg]) THEN Read-only. ELSE Read-write. ENDIF. Reset: 0.
4	Reserved.

3	**OnDimmMirror: on-DIMM mirroring (ODM) enabled**. IF (D18F2x118[LockDramCfg]) THEN Read-only. ELSE Read-write. ENDIF. Reset: 0. 1=Address and bank bits are swapped by hardware for MRS commands sent to this chip select. This mode accounts for routing on the DIMM. Hardware bit swapping does not occur for commands sent via D18F2x7C_dct[3:0][SendMrsCmd] when D18F2x7C_dct[3:0][EnDramInit]==0. This bit is expected to be set for the odd numbered rank of unbuffered DDR3 DIMMs if SPD byte 63 indicates that address mapping is mirrored. The following bits are swapped when enabled: • BA0 and BA1. • A3 and A4. • A5 and A6. • A7 and A8.
2	**TestFail: memory test failed**. IF (D18F2x118[LockDramCfg]) THEN Read-only. ELSE Read-write. ENDIF. Reset: 0. Set by BIOS to indicate that a rank is present but has failed memory training or a memory consistency test, indicating that the memory is bad or unused.
1	Reserved.
0	**CSEnable: chip select enable**. IF (D18F2x118[LockDramCfg]) THEN Read-only. ELSE Read-write. ENDIF. Reset: 0.

D18F2x[6C:60]_dct[3:0] DRAM CS Mask

See 2.9.3 [DCT Configuration Registers]. See D18F2x[5C:40]_dct[3:0].

Bits	Description
31	Reserved.
30:19	**AddrMask[38:27]: normalized physical address mask bits [38:27]**. IF (D18F2x118[LockDramCfg]) THEN Read-only. ELSE Read-write. ENDIF. Reset: 0.
18:16	Reserved.
15:5	**AddrMask[21:11]: normalized physical address mask bits [21:11]**. IF (D18F2x118[LockDramCfg]) THEN Read-only. ELSE Read-write. ENDIF. Reset: 0.
4	Reserved.
3:2	Reserved.
1:0	Reserved.

D18F2x78_dct[3:0] DRAM Control

See 2.9.3 [DCT Configuration Registers].

Bits	Description
31	Reserved.
30:18	Reserved.
17	**AddrCmdTriEn: address command tristate enable**. Read-write. Reset: 0. BIOS: See 2.9.9.4. 1=Tristate the address, command, and bank buses when a Deselect command is issued.

16	Reserved.
15	Reserved.
14:11	Reserved.
10:8	**DramType: DRAM type**. Read-write. Reset: 7h. Specifies the type of DRAM devices which are connected to this DCT. Bits — Description 000b — DDR3 001b — Reserved 010b — Reserved 011b — Reserved 110b-100b — Reserved 111b — Undefined
7:5	Reserved.
4	**PtrInitReq: fifo pointer initialization request**. Read; write-1-only; cleared-when-done. Reset: 0. BIOS: See 2.9.9.7. 1=The DCT performs transmit and receive fifo pointer initialization. This bit is cleared by hardware after the initialization completes.
3	**DccPgSsBusDis: Dcc powergate sourcesynchronous bus disable**. Read-write. Reset: 0. BIOS: 0. 1=Disable powergating the ss channel when the Dcc is powergated. 0=Dcc powergate also power-gates ss channel.
2	**GsyncDis: G-sync bus disable**. Read-write. Reset: 1. BIOS: See Table 35. 0=Enable the G-sync bus communication between phys and the PLL. 1=G-sync bus is masked.
1	Reserved.
0	**ChanVal: DRAM channel valid**. Read-write. Reset: 0. BIOS: See 2.9.9.7. 1=Communication between the DCT and DRAM phy is enabled and the DCT exits direct response mode. 0=Communi-cation between the DCT and phy is disabled and direct response mode is enabled.

D18F2x7C_dct[3:0] DRAM Initialization

Reset: 0000_0000h. See 2.9.3 [DCT Configuration Registers].

For Ddr3Mode, BIOS can directly control the DRAM initialization sequence using this register. To do so, BIOS sets EnDramInit to start DRAM initialization. BIOS should then complete the initialization sequence specified in the appropriate JEDEC specification. After completing the sequence, BIOS clears EnDramInit to complete DRAM initialization. BIOS should not assert LDTSTOP_L while EnDramInit is set. Setting more than one of the command bits in this register (SendControlWord, SendMrsCmd, and SendAutoRefresh) at a time results in undefined behavior.

Bits	Description
31	**EnDramInit: enable DRAM initialization**. Read-write. 1=Place the DRAM controller in the BIOS-controlled DRAM initialization mode. The DCT deasserts CKE when this bit is set. BIOS must wait until D18F2x98_dct[3:0][DctAccessDone] == 1 before programming AssertCke=1. BIOS must clear this bit after DRAM initialization is complete. BIOS must not set this bit on a DCT with no attached DIMMs.
30	Reserved.
29	**SendZQCmd: send ZQ command**. Read; write-1-only; cleared-by-hardware. 1=The DCT sends the ZQ calibration command with either all even or all odd chip selects active. The first command targets even chip selects. Subsequent commands alternate between even and odd chip selects. This bit is cleared by the hardware after the command completes. This bit is valid only when EnDramInit=1.
28	**AssertCke: assert CKE**. Read-write. Setting this bit causes the DCT to assert the CKE pins. This bit cannot be used to deassert the CKE pins. If the link between the DCT and the phy is not connected (D18F2x78_dct[3:0][PtrInitReq] has not previously been set), then this bit has no effect on the pin state until it is connected with PtrInitReq.
27	Reserved.
26	**SendMrsCmd: send MRS command**. Read; write-1-only; cleared-by-hardware. 1=The DCT sends the MRS commands defined by the MrsAddress and MrsBank fields of this register to the chip selects defined in D18F2xA8_dct[3:0][MrsCtrlWordCS]. This bit is cleared by hardware after the command completes.
25	**SendAutoRefresh: send auto refresh command**. Read; write-1-only; cleared-by-hardware. 1=The DCT sends an auto refresh command. This bit is cleared by hardware after the command completes.
24	**DeassertCke: deassert CKE**. Read; write-1-only; cleared-by-hardware. Setting this bit causes the DCT to deassert the CKE pins. This bit cannot be used to assert the CKE pins. If the link between the DCT and the phy is not connected (D18F2x78_dct[3:0][PtrInitReq] has not previously been set), then this bit has no effect on the pin state until it is connected with PtrInitReq. DeassertCke register bit is cleared by hardware immediately after the register write completes.
23:22	**MrsChipSel: MRS command chip select**. Read-write. Specifies which DRAM chip select is used for MRS commands. Defined only if (~EnDramInit | ~D18F2x90_dct[3:0][UnbuffDimm]); otherwise MRS commands are sent to all chip selects. Bits — Description 00b — MRS command is sent to CS0 01b — MRS command is sent to CS1 10b — MRS command is sent to CS2 11b — MRS command is sent to CS3
21:18	**MrsBank[3:0]: bank address for MRS commands**. Read-write. Specifies the data driven on the DRAM bank pins for MRS commands. MrsBank[3] is Reserved.
17:0	**MrsAddress[17:0]: address for MRS commands**. Read-write. Specifies the data driven on the DRAM address pins for MRS commands.

D18F2x80_dct[3:0] DRAM Bank Address Mapping

IF (D18F2x118[LockDramCfg]) THEN Read-only. ELSE Read-write. ENDIF. Reset: 0000_0000h. See 2.9.3 [DCT Configuration Registers]. These fields specify DIMM configuration information. These fields are required to be programmed based on the DRAM device size and with information of the DIMM. Table 140 shows the bit numbers for each position.

Bits	Description
31:16	Reserved.
15:8	Reserved.
7:4	**DimmAddrMap1: DIMM 1 address map**.
3:0	**DimmAddrMap0: DIMM 0 address map**.

Table 140: DDR3 DRAM Address Mapping

Bits	CS Size	Device size, width	Bank			Address																
			2	1	0		15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
0000b		Reserved				Row																
						Col																
0001b	256MB	512Mb, x16	15	14	13	Row	x	x	x	x	17	16	27	26	25	24	23	22	21	20	19	18
						Col	x	x	x	x	x	AP	12	11	10	9	8	7	6	5	4	3
0010b	512MB	512Mb, x8	15	14	13	Row	x	x	x	17	16	28	27	26	25	24	23	22	21	20	19	18
		1Gb, x16				Col	x	x	x	x	x	AP	12	11	10	9	8	7	6	5	4	3
0011b		Reserved				Row																
						Col																
0100b		Reserved				Row																
						Col																
0101b	1GB	1Gb, x8	15	14	13	Row	x	x	17	16	29	28	27	26	25	24	23	22	21	20	19	18
		2Gb, x16				Col	x	x	x	x	x	AP	12	11	10	9	8	7	6	5	4	3
0110b		Reserved																				
0111b	2GB	2Gb, x8	15	14	13	Row	x	17	16	30	29	28	27	26	25	24	23	22	21	20	19	18
		4Gb, x16				Col	x	x	x	x	x	AP	12	11	10	9	8	7	6	5	4	3
1000b		Reserved																				
1001b		Reserved																				
1010b	4GB	4Gb, x8	15	14	13	Row	17	16	31	30	29	28	27	26	25	24	23	22	21	20	19	18
		8Gb, x16				Col	x	x	x	x	x	AP	12	11	10	9	8	7	6	5	4	3
1011b	8GB	8Gb, x8	16	15	14	Row	17	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18
						Col	x	x	x	x	13	AP	12	11	10	9	8	7	6	5	4	3
1111b-1100b		Reserved																				

D18F2x84_dct[3:0] DRAM MRS

Reset: 0000_0005h. See 2.9.3 [DCT Configuration Registers].

<table>
<tr><td>Bits</td><td>Description</td></tr>
<tr><td>31:24</td><td>Reserved.</td></tr>
<tr><td>23</td><td>PchgPDModeSel: precharge power down mode select. Read-write. BIOS: 1. Specifies how a chip select enters and exits power down mode. This mode is enabled by D18F2x94_dct[3:0][PowerDownEn] and its behavior varies based on the setting of D18F2x94_dct[3:0][PowerDownMode]and MR0[PPD] in D18F2x2E8_dct[3:0]_mp[1:0][MxMr0].
<table>
<tr><td>PowerDownMode</td><td>PchgPDModeSel</td><td>MR0[PPD]</td><td>Description</td></tr>
<tr><td>0b</td><td>0b</td><td>0b</td><td>Full channel slow exit (DLL off)</td></tr>
<tr><td>0b</td><td>0b</td><td>1b</td><td>Full channel fast exit (DLL on)</td></tr>
<tr><td>0b</td><td>1b</td><td>xb</td><td>Full channel dynamic fast exit/slow exit</td></tr>
<tr><td>1b</td><td>0b</td><td>0b</td><td>Reserved</td></tr>
<tr><td>1b</td><td>0b</td><td>1b</td><td>Partial channel fast exit (DLL on)</td></tr>
<tr><td>1b</td><td>1b</td><td>xb</td><td>Partial channel dynamic fast exit/slow exit</td></tr>
</table>
See D18F2x248_dct[3:0]_mp[1:0][Txpdll, Txp]. In dynamic fast exit/slow exit power down mode, the DCT dynamically issues MRS command(s) to the DRAM to specify the powerdown mode; the DCT specifies fast exit mode when chip selects on one of the CKEs has recently been active; it specifies deep power down when chip selects on all CKEs have been idle. PchgPDModeSel=0 && MR0[PPD]=1 fast exit modes are reserved if S3 is also supported .</td></tr>
<tr><td>22:2</td><td>Reserved.</td></tr>
<tr><td>1:0</td><td>BurstCtrl: burst length control. Read-write. BIOS: 01b. Specifies the number of sequential beats of DQ related to one read or write command. Requests from the processor are always 64-byte-length. Requests generated by D18F2x250_dct[3:0] are always 64-byte-length. Requests from GMC may be 32-byte or 64-byte-length. Software must ensure that GMC requests are disabled to configure the controller and drams for 8-beat burst length (e.g. during training). If this mode is changed, software must issue a mode-register set command to MR0 of the drams to place them in the same mode.
<table>
<tr><td>Bits</td><td>Description</td></tr>
<tr><td>00b</td><td>8 beats</td></tr>
<tr><td>01b</td><td>Dynamic 4 or 8 beats</td></tr>
<tr><td>11b-10b</td><td>Reserved</td></tr>
</table></td></tr>
</table>

D18F2x88_dct[3:0] DRAM Timing Low

Reset: 3F00_0000h. See 2.9.3 [DCT Configuration Registers].

<table>
<tr><td>Bits</td><td>Description</td></tr>
<tr><td>31:30</td><td>Reserved.</td></tr>
<tr><td>29:24</td><td>MemClkDis: MEMCLK disable. Read-write. 1=Disable the MEMCLK. 0=Enable MEMCLK. All enabled clocks should be 0; all no-connect and unused clocks should be 1.
<table>
<tr><td>Bit</td><td>Pad</td></tr>
<tr><td>[0]</td><td>MEMCLK_H[0]</td></tr>
<tr><td>[1]</td><td>MEMCLK_H[1]</td></tr>
<tr><td>[2]</td><td>MEMCLK_H[2]</td></tr>
<tr><td>[3]</td><td>MEMCLK_H[3]</td></tr>
<tr><td>[4]</td><td>MEMCLK_H[4]</td></tr>
<tr><td>[5]</td><td>MEMCLK_H[5]</td></tr>
</table></td></tr>
<tr><td>23:0</td><td>Reserved.</td></tr>
</table>

D18F2x8C_dct[3:0] DRAM Timing High

See 2.9.3 [DCT Configuration Registers].

Bits	Description
31:19	Reserved.
18	**DisAutoRefresh: disable automatic refresh**. Read-write. Reset: 0. BIOS: See 2.9.9.4. 1=Automatic refresh is disabled.
17:16	**Tref: refresh rate**. Read-write. Reset: 0. BIOS: See 2.9.9.3. This specifies the average time between refresh requests to all DRAM devices. Bits Description 00b Undefined behavior. 01b Reserved 10b Every 7.8 us 11b Every 3.9 us
15:0	Reserved.

D18F2x90_dct[3:0] DRAM Configuration Low

See 2.9.3 [DCT Configuration Registers].

Bits	Description
31:28	**IdleCycLimit: idle cycle limit**. Read-write. Reset: 8h. BIOS: 8h. Specifies the number of MEMCLK cycles an idle page is open before it is closed if DynPageCloseEn==0. This field is ignored if DynPageCloseEn==1. Bits Description 0h 8 clocks Fh-1h <IdleCycLimit>*16 clocks
27	**DisDllShutdownSR: disable DLL shutdown in self-refresh mode**. Read-write. Reset: 1. 1=Disable the power saving features of shutting down DDR phy DLLsduring DRAM self refresh and memory P-states. 0=Shutdown DLLs during DRAM self refresh and allow memory P-state transitions. Setting this bit does not effect the current memory P-state.Setting this bit for the DCT master channel of a DCT pair controls both DCTs of the pair. Setting this bit for the DCT which is not the master channel has no effect.
26	Reserved.
25	**PendRefPaybackS3En: pending refresh payback S3 enable**. Read-write. Reset: 0. BIOS: 1. Specifies the S3 refresh payback behavior when PendRefPayback=0. 1=Pending refreshes are paid back on S3 entry. 0=Pending refreshes are not paid back on S3 entry.
24	**StagRefEn: Stagger Refresh Enable**. Read-write. Reset: 0. BIOS: 1. 1=The DRAM controller arbitrates refreshes among chip selects based on the Tstag value. See D18F2x228_dct[3:0]. 0=DCT arbitrates among chip selects using the Trfc value.
23	**ForceAutoPchg: force auto precharging**. Read-write. Reset: 0. BIOS: See 2.9.9.4. 1=Force auto-precharge cycles with every read or write command.

22:21	**IdleCycLowLimit: idle cycle low limit**. Read-write. Reset: 0. Specifies the number of MEMCLK cycles a page is allowed to be open before it may be closed by the dynamic page close logic. This field is ignored if D18F2x90_dct[3:0][DynPageCloseEn] == 0. Bits Description 00b 16 clocks 01b 32 clocks 10b 64 clocks 11b 96 clocks
20	**DynPageCloseEn: dynamic page close enable**. Read-write. Reset: 0. See 2.9.9.4 [DCT Specific Configuration]. 1=The DRAM controller dynamically determines when to close open pages based on the history of that particular page and D18F2x90_dct[3:0][IdleCycLowLimit]. 0=Any open pages not auto-pre-charged by the DRAM controller are automatically closed after IdleCycLimit clocks of inactivity.
19	**DimmEccEn: DIMM ECC enable**. Read-write. Reset: 0. 1=ECC checking is capable of being enabled for all DIMMs on the DRAM controller by D18F3x44[DramEccEn]. This bit should not be set unless all populated DIMMs support ECC check bits. 0=ECC checking is disabled on the DRAM controller.
18	**PendRefPayback: pending refresh payback**. Read-write. Reset: 0. BIOS: 0. 1=The DRAM controller executes all pending refresh commands before entering the self refresh state. 0=The controller enters the self refresh state regardless of the number of pending refreshes; applies to any self refresh entry if PendRefPaybackS3En=0, else any non-S3 self refresh entry.
17	**EnterSelfRef: enter self refresh command**. Read, write-1-only; cleared-by-hardware. Reset: 0. 1=The DRAM controller places the DRAMs into self refresh mode. The DRAM interface is tristated 1 MEMCLK after the self refresh command is issued to the DRAMs. Once entered, the DRAM interface must remain in self refresh mode for a minimum of 5 MEMCLKs. This bit is read as a 1 while the enter-self-refresh command is executing; it is read as 0 at all other times.
16	**UnbuffDimm: unbuffered DIMM**. Read-write or read-only, depending on the product. Reset: Product-specific. 1=The DRAM controller is connected to unbuffered DIMMs. 0=Reserved.
15:12	Reserved.
11	Reserved.
10	Reserved.
9	Reserved.
8	Reserved.
7	Reserved.
6	Reserved.
5	Reserved.

4	Reserved.
3	Reserved.
2	Reserved.
1	**ExitSelfRef: exit self refresh (after suspend to RAM or for DRAM training) command**. Read, write-1-only; cleared-by-hardware. Reset: 0. Writing a 1 to this bit causes the DRAM controller to bring the DRAMs out of self refresh mode. It also causes the DRAM controller to issue ZQCL and MRS MR0 commands. This command should be executed by BIOS when returning from the suspend to RAM state, after the DRAM controller configuration registers are properly initialized, or when self refresh is used during DRAM training. This bit is read as a 1 while the exit-self-refresh command is executing; it is read as 0 at all other times. This bit should not be set if the DCT is disabled.
0	Reserved.

D18F2x94_dct[3:0] DRAM Configuration High

See 2.9.3 [DCT Configuration Registers].

Bits	Description
31	**DphyMemPsSelEn**. Read-write. Reset: 1h. BIOS: 0. 1=The DCT uses D18F1x10C[MemPsSel] to configure DctOffset[24] to the phy while the value that software writes to DctOffset[24] is ignored. 0=Software determines DctOffset[24]. BIOS must clear this bit for proper operation.
30:29	Reserved.
28:24	**DcqBypassMax: DRAM controller queue bypass maximum**. Read-write. Reset: 00h. BIOS: 2.9.9.4. The DRAM controller arbiter normally allows transactions to pass other transactions in order to optimize DRAM bandwidth. This field specifies the maximum number of times that the oldest memory-access request in the DRAM controller queue may be bypassed before the arbiter decision is overridden and the oldest memory-access request is serviced instead. Bits — Description 00h — No bypass; the oldest request is never bypassed. 1Fh-01h — The oldest request may be bypassed no more than <DcqBypassMax> time.
23	**ProcOdtDis: processor on-die termination disable**. Read-write. Reset: 0.1=The processor-side on-die termination is disabled. 0=Processor-side on-die termination enabled. Changes to this bit must be performed prior to setting MemClkFreqVal.
22	**BankSwizzleMode: bank swizzle mode**. Read-write. Reset: 0. BIOS:2.9.9.4. 1=Remaps the DRAM device bank address bits as a function of normalized physical address bits. Each of the bank address bits, as specified in D18F2x80_dct[3:0], are remapped as follows: • Define X as a bank address bit (e.g., X=15 if the bank bit is specified to be address bit [15]). • Define S(n) as the state of address bit [n], (0 or 1), and B as the remapped bank address bit. Then, Ddr3Mode: B= S(X) ^ S(X + 3) ^ S(X + 6); for an 8-bank DRAM. For example, encoding 02h of Table 140 would be remapped from Bank[2:0]={A15, A14, A13} to the following: Bank[2:0] = {A15^A18^A21, A14^A17^A20, A13^A16^A19}.

21	**FreqChgInProg: frequency change in progress**. Read-only. Reset: 0. 1=A MEMCLK frequency change is in progress. The DDR phyasserts this bit when it is in the process of locking the PLL.BIOS should not program the phy registers while this bit is set. 0=DRAM-interface commands can be sent to the phy.
20	**SlowAccessMode: slow access mode (a.k.a. 2T mode)**. Read-write. Reset: 0. 1=One additional MEMCLK of setup time is provided on all DRAM address and control signals (not including CS, CKE, and ODT); i.e., these signals are driven for two MEMCLK cycles rather than one. 0=DRAM address and control signals are driven for one MEMCLK cycle. 2T mode may be needed in order to meet electrical requirements of certain DIMM speed and loading configurations. If memory P-states are enabled then BIOS must set this bit if 2T timing is recommended for either memory P-state.
19	Reserved.
18	Reserved.
17	Reserved.
16	**PowerDownMode: power down mode**. Read-write. Reset: 0. BIOS: 1. Specifies how a chip select or group of chip selects enters power down mode when enabled by D18F2x94_dct[3:0][PowerDownEn]. A chip select enters power down mode when the DCT deasserts the CKE pin. The command and address signals tristate one MEMCLK after CKE deasserts. The DCT behavior varies based on the setting of D18F2x84_dct[3:0][PchgPDModeSel]. See also Table 139 [DIMM, Chip Select, and Register Mapping]. 0=Channel CKE control mode; the DRAM channel is placed in power down mode when all chip selects associated with the channel are idle; CKE pins for the channel operate in lock step in terms of placing the channel in power down mode. 1=Chip select CKE control mode; the chip select group controlled by a CKE pinis placed in power down mode when all chip selects associated with the pin are idle.
15	**PowerDownEn: power down mode enable**. Read-write. Reset: 0. BIOS: 1. 1=Power down mode is enabled. Only precharge power down mode is supported, not active power down mode. See PowerDownMode, D18F2x84_dct[3:0][PchgPDModeSel], D18F2xA8_dct[3:0][PrtlChPDEnhEn, AggrPDEn, PDPhyPSDis], and D18F2x248_dct[3:0]_mp[1:0][PchgPDEnDelay].
14	**DisDramInterface: disable the DRAM interface**. Read-write. Reset: 0. 1=The DRAM controller is disabled and the DRAM interface is placed into a low power state. This bit must be set if there are no DIMMs connected to the DCT.
13	Reserved.
12	Reserved.

11:10	**ZqcsInterval: ZQ calibration short interval**. Read-write. Reset: 00b. This field specifies the programmable interval for the controller to send out the DRAM ZQ calibration short command. Bits Description 00b ZQ calibration short command is disabled 01b 64 ms 10b 128 ms 11b 256 ms
9:8	Reserved.
7	**MemClkFreqVal: memory clock frequency valid**. Read-write. Reset: 0. System BIOS should set this bit after setting up D18F2x94_dct[3:0][MemClkFreq] to the proper value. This indicates to the DRAM controller that it may start driving internal channel clocks corresponding to MEMCLK to the proper frequency. This bit should not be set if the DCT is disabled. BIOS must change each DCT's operating frequency in order.
6:5	Reserved.
4:0	**MemClkFreq: memory clock frequency**. Read-write. Reset: 000b. Specifies the frequency and rate of the DRAM interface (MEMCLK). See: Table 141 [Valid Values for Memory Clock Frequency Value Definition]. The rate is twice the frequency. See D18F5x84[DdrMaxRate] and D18F5x84[DdrMaxRateEnf]. See MemClkFreqVal.

Table 141: Valid Values for Memory Clock Frequency Value Definition

Bits	Description
01h-00h	Reserved
02h	200 MHz. (400 MT/s)
03h	Reserved
04h	333 MHz. (667 MT/s)
05h	Reserved
06h	400 MHz. (800 MT/s)
09h-07h	Reserved
0Ah	533 MHz. (1066 MT/s)
0Dh-0Bh	Reserved
0Eh	667 MHz. (1333 MT/s)
11h-0Fh	Reserved
12h	800 MHz. (1600 MT/s)
15h-13h	Reserved
16h	933 MHz. (1866 MT/s)
19h-17h	Reserved
1Ah	1066 MHz. (2133 MT/s)
1Eh-1Bh	Reserved
1Fh	1200 MHz. (2400 MT/s)

D18F2x98_dct[3:0] DRAM Controller Additional Data Offset

Reset: 8000_0000h. See 2.9.3 [DCT Configuration Registers].

Each DCT includes an array of registers that are used primarily to control DRAM-interface electrical parameters. Access to these registers is accomplished as follows:

- Reads (without auto-increment):

1. Write the register number to D18F2x98_dct[3:0][DctOffset] with D18F2x98_dct[1:0][DctAccessWrite, DctOffsetAutoIncEn]={0,0}.
2. Read the register contents from D18F2x9C_dct[3:0].

Writes (without auto-increment):

1. Write all 32 bits of register data to D18F2x9C_dct[3:0] (individual byte writes are not supported).
2. Write the register number to D18F2x98_dct[3:0][DctOffset] with D18F2x98_dct[3:0][DctAccessWrite, DctOffsetAutoIncEn]={1,0}.
   - The data will be delivered to the phy similar to a posted memory-write, and the write will complete without any further action. However, to ensure that the contents of the array register write have been delivered to the phy, software issues a subsequent configuration register read or write to any register in the northbridge. For example, reading D18F2x98_dct[3:0] will accomplish this.

- Reads (with auto-increment):

1. Write the first register number to D18F2x98_dct[3:0][DctOffset] with D18F2x98_dct[1:0][DctAccessWrite, DctOffsetAutoIncEn]={0,1}.
2. Read the register contents from D18F2x9C_dct[3:0].
3. Repeat step 2 as needed for each additional array register read.
4. Program D18F2x98_dct[3:0][DctOffsetAutoIncEn]=0.

Writes (with auto-increment):

1. Write the first register number to D18F2x98_dct[3:0][DctOffset] with D18F2x98_dct[3:0][DctAccessWrite, DctOffsetAutoIncEn]={1,1}.
2. Write all 32 bits of register data to D18F2x9C_dct[3:0] .
3. Repeat step 2 as needed for each additional array register write.
4. Program D18F2x98_dct[3:0][DctOffsetAutoIncEn]=0.

Bits	Description
31	Reserved.
30	**DctAccessWrite: DRAM controller read/write select**. Read-write. 0=Specifies a read access. 1=Specifies a write access.
29	**DctOffsetAutoIncEn: DCT offset auto-increment enable**. Read-write. 1=Specifies that subsequent accesses will cause the DCT to increment the DctOffset field by one after the access. When in this mode, the DCT will generate accesses to the phy registers with sequential accesses only to the data port (D18F2x9C_dct[3:0]). 0=DctOffset is not incremented after each access.
28:0	**DctOffset: DRAM controller offset**. Read-write.

D18F2x9C_dct[3:0] DRAM Controller Additional Data Port

See D18F2x98_dct[3:0] for register access information. See 2.9.3 [DCT Configuration Registers]. Address: D18F2x98_dct[3:0][DctOffset].

Bits	Description
31:0	**Data**.

D18F2x9C_x00[F,3:0]0_0009_dct[3:0] High Addr Mode

Cold reset: 0000_0000h. See 2.9.4.1 for chiplet to pad mapping.

Table 142: Index Mapping for D18F2x9C_x00[F,3:0]0_0009_dct[3:0]

Address Bits	Valid Values	Name
D18F2x98_dct[3:0][23:20]	[3:0]	CAD chiplet
D18F2x98_dct[3:0][23:20]	Fh	CAD chiplet [3:0]

Bits	Description
31:1	Reserved.
0	**HiAddrMode: High Addressing Mode**. Read-write. 1=If (Ddr3Mode) ODT[3] and CS_L[7:6] are address bits with address timing.

D18F2x9C_x0000_000E_dct[3:0] Global Control Slave

Cold reset: 0000_0001h.

Bits	Description
31:1	Reserved.
0	**G5_Mode: GDDR5 Mode.** Read-write. 1=Combo phy slave chip is in GDDR5 mode. 0=Combo phy slave chip is in DDR3 mode. See section 2.9 for product support.

D18F2x9C_x0[3,1:0][F,3:0]0_0014_dct[3:0] Dll Lock Maintenance

Cold reset: 0000_0000h. See 2.9.4.1 for chiplet to pad mapping.

Table 143: Index Mapping for D18F2x9C_x0[3,1:0][F,3:0]0_0014_dct[3:0]

Address Bits	Valid Values	Name
D18F2x98_dct[3:0][23:20]	[3:0]	CAD chiplet
D18F2x98_dct[3:0][23:20]	Fh	CAD chiplet [3:0]
D18F2x98_dct[3:0][25:24]	[1:0]	Memory Pstate
D18F2x98_dct[3:0][25:24]	3h	Memory Pstate [1:0]

Bits	Description
31:8	Reserved.

7:4	**DllPumpPeriod: Dll charge pump period**. Read-write. BIOS: 3h. Specifies the number of DLL relocks required to keep the receive DLLs locked for the period where there is no traffic.
3:0	**MaxDurDllNoLock: Max duration Dll no-lock**. Read-write. BIOS: See 2.9.9.9. Specifies the number of PCLK cycles that occur before the phy DLLs relock. A DLL relock occurs every 2^(MaxDurDllNoLock+1) if there are no reads or writes during the period. 0=DLL power saving(standby) disabled. If MaxDurDllNoLock!=0 (standby is enabled), D18F2x9C_x00[F,3:0]0_0078_dct[3:0][DllResetRelock] must be set to 1 prior to writing this register and then D18F2x9C_x00[F,3:0]0_0078_dct[3:0][DllResetRelock] must be cleared after the register write.

D18F2x9C_x00F0_0015_dct[3:0] Vref Byte

Cold reset: 0000_0000h.

Bits	Description
31:4	Reserved.
3:0	**VrefFilt: Vref filter.** Read-write. BIOS: 0. This field adjusts noise coupling on to VrefOut and adjusts the input resistance.

D18F2x9C_x0[3,1:0][F,3:0]0_[F,3:0]028_dct[3:0] CAD RdPtrOffset

Cold reset: 0000_0000h. See 2.9.4.1 for chiplet and group (TG) to pin mapping.

Table 144: Index Mapping for D18F2x9C_x0[3,1:0][F,3:0]0_[F,3:0]028_dct[3:0]

Address Bits	Valid Values	Name
D18F2x98_dct[3:0][15:12]	[3:0]	Timing Group
D18F2x98_dct[3:0][15:12]	Fh	Timing Group [3:0]
D18F2x98_dct[3:0][23:20]	[3:0]	CAD chiplet
D18F2x98_dct[3:0][23:20]	Fh	CAD chiplet [3:0]
D18F2x98_dct[3:0][25:24]	[1:0]	Memory Pstate
D18F2x98_dct[3:0][25:24]	3h	Memory Pstate [1:0]

Bits	Description
31:6	Reserved.
5:0	**TxRdPtrOffset: Tx Read Pointer Offset**. Read-write. BIOS: See 2.9.9.2.6. The amount of time (specified in units of 2UI) that is added to the read pointer of the Tx command-FIFO for reading out commands.

D18F2x9C_x00[F,3:0]0_[F,3:0][8,3:0]2E_dct[3:0] RdPtrInitVal

Cold reset: 0000_0000h. See 2.9.4.1 for chiplet and group (TG) to pin mapping.

Table 145: Index Mapping for D18F2x9C_x00[F,3:0]0_[F,3:0][8,3:0]2E_dct[3:0]

Address Bits	Valid Values	Name
D18F2x98_dct[3:0][11:8]	[3:0]	NbPstate
D18F2x98_dct[3:0][11:8]	8h	NbPstate PMU
D18F2x98_dct[3:0][15:12]	[3:0]	Timing Group

Table 145: Index Mapping for D18F2x9C_x00[F,3:0]0_[F,3:0][8,3:0]2E_dct[3:0]

D18F2x98_dct[3:0][15:12]	Fh	Timing Group [3:0]
D18F2x98_dct[3:0][23:20]	[3:0]	CAD chiplet
D18F2x98_dct[3:0][23:20]	Fh	CAD chiplet [3:0]

Bits	Description
31:6	Reserved.
5:0	**RdPtrInitVal: Read Pointer Initial Value**. Read-write. BIOS: See 2.9.9.2.6. Specifies RdPtr initial value for the transmit command-FIFOs.

D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0] CAD Tx Impedance

Cold reset: 0000_0FFFh. BIOS: See 2.9.9.2.4. See 2.9.4.1 for chiplet to pad and 2.9.4 for pad to pin mapping.

Table 146: Address Mapping for D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0]

Address	Description
PciCfgDevFunc[11:0]	182h
PciCfgOffset[11:0]	09Ch
D18F2x98_dct[3:0][31:28]	0h
D18F2x98_dct[3:0][27:24]	**mp: memory P-state selector**. Value / Name / Description 1h-0h / 1h-0h / Memory P-state <Value> 3h / Broadcast / Broadcast to Memory P-states [1:0]
D18F2x98_dct[3:0][23:20]	**chiplet: chiplet selector**. Value / Name / Description 3h-0h / 3-0 / Chiplet <Value> Fh / Broadcast / Broadcast to chiplets [8:0]
D18F2x98_dct[3:0][19:16]	0h
D18F2x98_dct[3:0][15:12]	**pad: pad selector**. Value / Name / Description Bh-0h / Bh-0h / pad <Value> Fh / Broadcast / Broadcast to pad pads [B:0]
D18F2x98_dct[3:0][11:0]	041h
D18F1x10C[DctCfgSel]	**dct: DCT controller select**. Value / Name / Description 011b-000b / 3h-0h / DCT <Value>

Bits	Description
31:12	Reserved.

11:6	**DrvStrenP: PMOS driver output impedance**. Read-write. BIOS: See 2.9.9.2.4. Specifies the pull-down output driver impedance. See DrvStrenN for field description.
5:0	**DrvStrenN: NMOS driver output impedance**. Read-write. BIOS: See 2.9.9.2.4. Specifies the pul-lup output driver impedance. Bits Description 00h disabled 01h 120 ohms 03h 60 ohms 07h 40 ohms 0Fh 30 ohms 1Fh 24 ohms 3Fh 20 ohms

D18F2x9C_x00[F,3:0]0_[F,B:0]04A_dct[3:0] Rx Control 1

Cold reset: 0000_0080h. See 2.9.4.1 for chiplet to pad and 2.9.4 for pad to pin mapping.

Table 147: Index Mapping for D18F2x9C_x00[F,3:0]0_[F,B:0]04A_dct[3:0]

Address Bits	Valid Values	Name
D18F2x98_dct[3:0][15:12]	[B:0]	pad
D18F2x98_dct[3:0][15:12]	Fh	pad[B:0]
D18F2x98_dct[3:0][23:20]	[3:0]	CAD chiplet
D18F2x98_dct[3:0][23:20]	Fh	CAD chiplet [3:0]

Bits	Description
31:9	Reserved.
8	**BiasBypassEn: Bias bypass enable**. Read-write. BIOS: 0.
7	**PowerDownRcvr: Power down receiver**. Read-write. BIOS: See 2.9.9.9. 1=Power down the receiver.
6:4	**MajorMode: Major mode**. Read-write. BIOS: See 2.9.9.2. Specifies operating mode of the phy logic. Bits Description 000b DDR3 111b-001b Reserved
3:0	Reserved.

D18F2x9C_x00[F,3:0]0_[F,B:0]04E_dct[3:0] TxControlDq

Cold reset: 0000_0013h. See 2.9.4.1 for chiplet to pad and 2.9.4 for pad to pin mapping.

Table 148: Index Mapping for D18F2x9C_x00[F,3:0]0_[F,B:0]04E_dct[3:0]

Address Bits	Valid Values	Name
D18F2x98_dct[3:0][15:12]	[B:0]	pad
D18F2x98_dct[3:0][15:12]	Fh	pad[B:0]
D18F2x98_dct[3:0][23:20]	[3:0]	CAD chiplet
D18F2x98_dct[3:0][23:20]	Fh	CAD chiplet [3:0]

Bits	Description
31:13	Reserved.
12	**EQEnable: Equalization enable**. Read-write. BIOS: 0.
11	**DrvPwrGateEn: Powergate driver enable**. Read-write. BIOS: 1.
10:0	Reserved.

D18F2x9C_x00[F,3:0]0_[F,B:0]05F_dct[3:0] CAD Tx Slew Rate

Cold reset: 0000_03FFh. BIOS: See 2.9.9.2.4. See 2.9.4.1 for chiplet to pad mapping and 2.9.4 for pad to pin mapping.

Table 149: Index Mapping for D18F2x9C_x00[F,3:0]0_[F,B:0]05F_dct[3:0]

Address Bits	Valid Values	Name
D18F2x98_dct[3:0][15:12]	[B:0]	pad
D18F2x98_dct[3:0][15:12]	Fh	pad[B:0]
D18F2x98_dct[3:0][23:20]	[3:0]	CAD chiplet
D18F2x98_dct[3:0][23:20]	Fh	CAD chiplet [3:0]

Bits	Description
31:6	Reserved.
5:3	**TxPreN: NMOS predriver code**. Read-write. BIOS: See 2.9.9.2.7. Specifies the falling edge slew rate of the transmit pad. 000b=Slowest slew rate. 111b=Fastest slew rate.
2:0	**TxPreP: PMOS predriver code**. Read-write. BIOS: See 2.9.9.2.7. Specifies the rising edge slew rate of the transmit pad. 000b=Slowest slew rate. 111b=Fastest slew rate.

D18F2x9C_x00[F,3:0]0_0077_dct[3:0] DllPowerdown

Cold reset: 0000_0000h. BIOS: See 2.9.9.9. See 2.9.4.1 for chiplet to pad mapping and see 2.9.4 for pad to pin mapping.

Table 150: Address Mapping for D18F2x9C_x00[F,3:0]0_0077_dct[3:0]

Address	Description
PciCfgDevFunc[11:0]	182h
PciCfgOffset[11:0]	09Ch
D18F2x98_dct[3:0][31:24]	00h
D18F2x98_dct[3:0][23:20]	**chiplet: chiplet selector**. Value / Name / Description 3h-0h / 3-0 / Chiplet <Value> Fh / Broadcast / Broadcast to chiplets [3:0]
D18F2x98_dct[3:0][19:12]	10h
D18F2x98_dct[3:0][19:0]	00077h
D18F1x10C[DctCfgSel]	**dct: DCT controller select**. Value / Name / Description 011b-000b / 3h-0h / DCT <Value>

Bits	Description
31:11	Reserved.
10:6	**DllPowerDownTx: Dll powerdown Tx**. Read-write.
5	**DllPowerDownXCLK: Dll powerdown XCLK**. Read-write.
4	Reserved.
3:1	**DllPowerDownPI: Dll powerdownPI**. Read-write.
0	**DllPowerDown: Dll powerdown**. Read-write.

D18F2x9C_x00[F,3:0]0_0078_dct[3:0] DllControl

Cold reset: 0000_0000h. See 2.9.4.1 for chiplet to pad mapping and see 2.9.4 for pad to pin mapping.

Table 151: Address Mapping for D18F2x9C_x00[F,3:0]0_0078_dct[3:0]

Address	Description
PciCfgDevFunc[11:0]	182h
PciCfgOffset[11:0]	09Ch
D18F2x98_dct[3:0][31:24]	00h
D18F2x98_dct[3:0][23:20]	**chiplet: chiplet selector**. Value: 3h-0h, Name: 3-0, Description: Chiplet <Value> Value: Fh, Name: Broadcast, Description: Broadcast to chiplets [3:0]
D18F2x98_dct[3:0][19:12]	10h
D18F2x98_dct[3:0][19:0]	00078h
D18F1x10C[DctCfgSel]	**dct: DCT controller select**. Value: 011b-000b, Name: 3h-0h, Description: DCT <Value>

Bits	Description
31:8	Reserved.
7	**DllResetRelock: Dll reset relock**. Read-write. 1=Reset the DLL. 0=Relock the DLL. This bit must be set for 20 ns and then cleared anytime a forced relock of the DLL is required.
6:0	Reserved.

D18F2x9C_x0[3,1:0][F,3:0]0_[F,3:0]081_dct[3:0] Tx Delay

Cold reset: 0000_0000h. BIOS: See 2.9.9.2.10. This register controls the timing of the address, command, chip select, ODT and clock enable pins with respect to memory clock. See 2.9.4.1 for chiplet/timing group to pad and 2.9.4 for pad to pin mapping.

Table 152: Index Mapping for D18F2x9C_x0[3,1:0][F,3:0]0_[F,3:0]081_dct[3:0]

Address Bits	Valid Values	Name
D18F2x98_dct[3:0][15:12]	[3:0]	Timing Group
D18F2x98_dct[3:0][15:12]	Fh	Timing Group [3:0]

Table 152: Index Mapping for D18F2x9C_x0[3,1:0][F,3:0]0_[F,3:0]081_dct[3:0]

D18F2x98_dct[3:0][23:20]	[3:0]	CAD chiplet
D18F2x98_dct[3:0][23:20]	Fh	CAD chiplet [3:0]
D18F2x98_dct[3:0][25:24]	[1:0]	Memory Pstate
D18F2x98_dct[3:0][25:24]	3h	Memory Pstate [1:0]

Bits	Description
31:5	Reserved.
4:0	**TxFineDly: Tx fine delay**. Read-write. Specifies the time that the address/command signals are delayed from the default setup time, in increments of 1/32 UI.

D18F2x9C_x00[F,8:0]1_0000_dct[3:0] VariousChicken

Cold reset: 0000_0000h. BIOS: See 2.9.9.9.

Table 153: Index Mapping for D18F2x9C_x00[F,8:0]1_0000_dct[3:0]

Address Bits	Valid Values	Name
D18F2x98_dct[3:0][23:20]	[8:0]	Data chiplet
D18F2x98_dct[3:0][23:20]	Fh	Data chiplet [8:0]

Bits	Description
31:3	Reserved.
2	**DByteEnable: data byte enable**. Read-write. Controls whether this DBYTE is enabled. If this DBYTE is not enabled, it receives no clocks and remains in reset. 1=Disable this DBYTE. 0=Enable this DBYTE.
1:0	Reserved.

D18F2x9C_x0001_000E_dct[3:0] Global Control Slave

Cold reset: 0000_0001h.

Bits	Description
31:1	Reserved.
0	**G5_Mode: GDDR5 Mode.** Read-write. 1=Combo phy slave chip is in GDDR5 mode. 0=Combo phy slave chip is in DDR3 mode. See section 2.9 for product support.

D18F2x9C_x0[3,1:0][F,8:0]1_0014_dct[3:0] Dll Lock Maintenance

Cold reset: 0000_0037h. See 2.9.4.1 for chiplet to pin mapping.

Table 154: Index Mapping for D18F2x9C_x0[3,1:0][F,8:0]1_0014_dct[3:0]

Address Bits	Valid Values	Name

Table 154: Index Mapping for D18F2x9C_x0[3,1:0][F,8:0]1_0014_dct[3:0]

D18F2x98_dct[3:0][23:20]	[8:0]	Data chiplet
D18F2x98_dct[3:0][23:20]	Fh	Data chiplet [8:0]
D18F2x98_dct[3:0][27:24]	[1:0]	Memory Pstate
D18F2x98_dct[3:0][27:24]	3h	Memory Pstate [1:0]

Bits	Description
31:8	Reserved.
7:4	**DllPumpPeriod: Dll charge pump period**. Read-write. BIOS: 3h. Specifies the number of DLL relocks required to keep the receive DLLs locked for the period where there is no traffic.
3:0	**MaxDurDllNoLock: Max duration Dll no-lock**. Read-write. BIOS: See 2.9.9.9. Specifies the number of PCLK cycles that occur before the phy DLLs relock. A DLL relock occurs every 2^(MaxDurDllNoLock+1) if there are no reads or writes during the period. 0=DLL power saving(standby) disabled. If MaxDurDllNoLock!=0 (standby is enabled), D18F2x9C_x00[F,8:0]1_0[F,2:0]78_dct[3:0][DllResetRelock] must be set to 1 prior to writing this register and then D18F2x9C_x00[F,8:0]1_0[F,2:0]78_dct[3:0][DllResetRelock] must be cleared after the register write.

D18F2x9C_x00F1_0015_dct[3:0] Vref Byte

Cold reset: 0000_0000h.

Bits	Description
31:4	Reserved.
3:0	**VrefFilt: Vref filter.** Read-write. BIOS: 0. This field adjusts noise coupling on to VrefOut and adjusts the input resistance.

D18F2x9C_x00[F,8:0]1_0016_dct[3:0] Proc Odt Timing

Cold reset: 0000_1244h. See 2.9.4.1 for chiplet to pin mapping.

Table 155: Index Mapping for D18F2x9C_x00[F,8:0]1_0016_dct[3:0]

Address Bits	Valid Values	Name
D18F2x98_dct[3:0][23:20]	[8:0]	Data chiplet
D18F2x98_dct[3:0][23:20]	Fh	Data chiplet [8:0]

Bits	Description
31:16	Reserved.
15	**ProcOdtOn: Proc ODT on**. Read-write. BIOS: IF (Gddr5Mode) THEN 1. ELSE 0. ENDIF.1=Controller always enables ODT when not driving. If Gddr5Mode this may be used as G5ParkOdt.
14	**ProcOdtOff: Proc ODT off**. Read-write. BIOS: 0. 1=Controller never enables ODT unless ProcOdtOn=1.
13:11	**POdtStartDelayDqs: Proc ODT start delay DQS**. Read-write. BIOS: 2h. Controls the ODT turn on delay for DQS during reads. Bits — Delay 100b-000b — <2*POdtStartDelayDqs> UI 110b-101b — Reserved 111 — Uses RxTraffic to turn-on at the earliest possible time and stays enabled for duration of DLL operation
10:8	**POdtStartDelayDq: Proc ODT start delay DQ**. Read-write. BIOS: 2h. Controls the ODT turn on delay for DQ during reads. Bits — Delay 100b-000b — <2*POdtStartDelayDq> UI 110b-101b — Reserved 111 — Uses RxTraffic to turn-on at the earliest possible time and stays enabled for duration of DLL operation

7:4	**POdtWidthDqs: Proc ODT width DQS**. Read-write. BIOS: 4h. Controls the duration of ODT for DQS during reads. Bits Duration 0100b-0000b <10+(2*POdtWidthDqs)> UI 1111b-0101b Reserved
3:0	**POdtWidthDq: Proc ODT width DQ**. Read-write. BIOS: 4h. Controls the duration of ODT for DQ during reads. Bits Duration 0100b-0000b <8+(2*POdtWidthDq)> UI 1111b-0101b Reserved

D18F2x9C_x00[F,8:0]1_001C_dct[3:0] Dynamic PowerDown

Cold reset: 0000_0001h. BIOS: See 2.9.9.9. See 2.9.4.1 for chiplet to pin mapping.

Table 156: Index Mapping for D18F2x9C_x00[F,8:0]1_001C_dct[3:0]

Address Bits	Valid Values	Name
D18F2x98_dct[3:0][23:20]	[8:0]	Data chiplet
D18F2x98_dct[3:0][23:20]	Fh	Data chiplet [8:0]

Bits	Description
31:1	Reserved.
0	**DynPowerDown: Dynamic Power Down**. Read-write. 1=Analog circuitry is turned off.

D18F2x9C_x0[3,1:0][F,8:0]1_0028_dct[3:0] DATA RdPtrOffset

Cold reset: 0000_018Ah. See 2.9.4.1 for chiplet to pin mapping.

Table 157: Index Mapping for D18F2x9C_x0[3,1:0][F,8:0]1_0028_dct[3:0]

Address Bits	Valid Values	Name
D18F2x98_dct[3:0][23:20]	[8:0]	Data chiplet
D18F2x98_dct[3:0][23:20]	Fh	Data chiplet [8:0]
D18F2x98_dct[3:0][25:24]	[1:0]	Memory Pstate
D18F2x98_dct[3:0][25:24]	3h	Memory Pstate [1:0]

Bits	Description
31:11	Reserved.
10:6	**TxRdPtrOffset: Tx Read Pointer Offset**. Read-write. BIOS: See 2.9.9.2.6. The amount of time (specified in units of 2UI) that is added to the read pointer of the Tx FIFO for reading out Tx data from the Tx data-FIFO.
5:0	**RxRdPtrOffset: Rx Read Pointer Offset**. Read-write. BIOS: See 2.9.9.2.6. The amount of time (specified in units of 2UI) that is added to the read pointer of the Tx FIFO for reading out received data from the Rx data-FIFO.

D18F2x9C_x0[3,1:0][F,8:0]1_0029_dct[3:0] Dll Early Traffic Offset

Cold reset: 0000_0000h. BIOS: See 2.9.9.9. See 2.9.4.1 for chiplet to pin mapping.

Table 158: Index Mapping for D18F2x9C_x0[3,1:0][F,8:0]1_0029_dct[3:0]

Address Bits	Valid Values	Name
D18F2x98_dct[3:0][23:20]	[8:0]	Data chiplet
D18F2x98_dct[3:0][23:20]	Fh	Data chiplet [8:0]
D18F2x98_dct[3:0][27:24]	[1:0]	Memory Pstate
D18F2x98_dct[3:0][27:24]	3h	Memory Pstate [1:0]

Bits	Description
31:11	Reserved.
10:6	**TxTrafficOffset: Rx stagger postamble**. Read-write. Specifies the amount of time that TxEarlyTraffic will be asserted prior to TxEn, unit=2*UI.
5:0	**RxTrafficOffset: Rx stagger preamble**. Read-write. Specifies the amount of time that RxEarlyTraffic will be asserted prior to RxEn, unit=2*UI.

D18F2x9C_x0[3,1:0][F,8:0]1_002A_dct[3:0] Rx Dll Standby Stagger Config

Cold reset: 0000_0000h. BIOS: See 2.9.9.9. See 2.9.4.1 for chiplet to pin mapping.

Table 159: Index Mapping for D18F2x9C_x0[3,1:0][F,8:0]1_002A_dct[3:0]

Address Bits	Valid Values	Name
D18F2x98_dct[3:0][23:20]	[8:0]	Data chiplet
D18F2x98_dct[3:0][23:20]	Fh	Data chiplet [8:0]
D18F2x98_dct[3:0][27:24]	[1:0]	Memory Pstate
D18F2x98_dct[3:0][27:24]	3h	Memory Pstate [1:0]

Bits	Description
31:12	Reserved.
11:6	**RxStggrPost: Rx stagger postamble**. Read-write. Specifies the duration Rx Dlls remain locked after read request (RxEn), unit=4*UI.
5:0	**RxStggrAnte: Rx stagger preamble**. Read-write. Specifies the duration Rx Dlls remain locked after RxEarlyTraffic, unit=4*UI.

D18F2x9C_x0[3,1:0][F,8:0]1_002B_dct[3:0] Tx Dll Standby Stagger Config

Cold reset: 0000_0000h. BIOS: See 2.9.9.9. See 2.9.4.1 for chiplet to pin mapping.

Table 160: Index Mapping for D18F2x9C_x0[3,1:0][F,8:0]1_002B_dct[3:0]

Address Bits	Valid Values	Name
D18F2x98_dct[3:0][23:20]	[8:0]	Data chiplet
D18F2x98_dct[3:0][23:20]	Fh	Data chiplet [8:0]
D18F2x98_dct[3:0][27:24]	[1:0]	Memory Pstate
D18F2x98_dct[3:0][27:24]	3h	Memory Pstate [1:0]

Bits	Description
31:10	Reserved.
9:5	**TxStggrPost: Tx stagger postamble**. Read-write. Specifies the duration Tx Dlls remain locked after write request (TxEn), unit=4*UI.
4:0	**TxStggrAnte: Tx stagger preamble**. Read-write. Specifies the duration Tx Dlls remain locked after TxEarlyTraffic, unit=4*UI.

D18F2x9C_x0[3,1:0][F,8:0]1_002C_dct[3:0] Rx Pad Traffic Early Offset

Cold reset: 0000_0000h. BIOS: See 2.9.9.9. See 2.9.4.1 for chiplet to pin mapping.

Table 161: Index Mapping for D18F2x9C_x0[3,1:0][F,8:0]1_002C_dct[3:0]

Address Bits	Valid Values	Name
D18F2x98_dct[3:0][23:20]	[8:0]	Data chiplet
D18F2x98_dct[3:0][23:20]	Fh	Data chiplet [8:0]
D18F2x98_dct[3:0][27:24]	[1:0]	Memory Pstate
D18F2x98_dct[3:0][27:24]	3h	Memory Pstate [1:0]

Bits	Description
31:6	Reserved.
5:0	**RxPadTrafficOffset: Rx pad traffic offset**. Read-write. Specifies the duration RxPadEarlyTraffic will be asserted prior to RxEn, unit=2*UI.

D18F2x9C_x00[F,8:0]1_0[8,3:0]2E_dct[3:0] DATA RdPtrInitVal

Cold reset: 0000_0000h. See 2.9.4.1 for chiplet to pin mapping.

Table 162: Index Mapping for D18F2x9C_x00[F,8:0]1_0[8,3:0]2E_dct[3:0]

Address Bits	Valid Values	Name
D18F2x98_dct[3:0][11:8]	[3:0]	NbPstate
D18F2x98_dct[3:0][11:8]	8h	NbPstate PMU
D18F2x98_dct[3:0][23:20]	[8:0]	Data chiplet
D18F2x98_dct[3:0][23:20]	Fh	Data chiplet [8:0]

Bits	Description
31:7	Reserved.
6:2	**RdPtrInitVal[6:2]: Rd pointer initial value[6:2]**. Read-write. BIOS: See 2.9.9.2.6. Specifies RdPtr initial value for the transmit FIFOs. Each RdPtrInitVal[6:0] is in units of UI. Software may write entire RdPtrInitVal[6:0] field.
1:0	**RdPtrInitVal[1:0]: Rd pointer initial value[1:0]**. RAZ. BIOS: See 2.9.9.2.6. Specifies RdPtr initial value for the transmit FIFOs. Each RdPtrInitVal[6:0] is in units of UI. Software may write entire RdPtrInitVal[6:0] field.

D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]041_dct[3:0] DATA Tx Impedance

Cold reset: 0000_3FFFh. See 2.9.4.1 for chiplet to pin mapping.

Table 163: Address Mapping for D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]041_dct[3:0]

Address	Description
PciCfgDevFunc[11:0]	182h
PciCfgOffset[11:0]	09Ch
D18F2x98_dct[3:0][31:28]	0h
D18F2x98_dct[3:0][27:24]	**mp: memory P-state selector**. See: Table 146 [Address Mapping for D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0]].
D18F2x98_dct[3:0][23:20]	**chiplet: chiplet selector**. Value / Name / Description 8h-0h / 8-0 / Chiplet <Value> Fh / Broadcast / Broadcast to chiplets [8:0]
D18F2x98_dct[3:0][19:16]	1h
D18F2x98_dct[3:0][15:12]	**Txpad: Tx pad selector**. See: Table 146 [Address Mapping for D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0]].
D18F2x98_dct[3:0][11:0]	041h
D18F1x10C[DctCfgSel]	**dct: DCT controller select**. See: Table 146 [Address Mapping for D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0]].

Bits	Description
31:14	Reserved.

13:7	**DrvStrenN: NMOS driver output impedance**. Read-write. BIOS: See 2.9.9.2.5. Specifies the pull-up output driver impedance.
6:0	**DrvStrenP: PMOS driver output impedance**. Read-write. BIOS: See 2.9.9.2.5. Specifies the pull-down output driver impedance. Bits Description Bits Description 00h disabled 01h 480 ohms 34h 48 ohms 04h 240 ohms 35h 43.6 ohms 05h 160 ohms 70h 40 ohms 0Ch 120 ohms 71h 36.9 ohms 0Dh 96 ohms 74h 34.3 ohms 0Fh 80 ohms 75h 32 ohms 15h 68 ohms 7Ch 30 ohms 30h 60 ohms 7Dh 28.2 ohms 31h 53.3 ohms 7Fh 26.7 ohms

D18F2x9C_x0[3,1:0][F,8:0]1_[F,7:0]043_dct[3:0] DATA Rcv Majormode

Cold reset: 0000_xxxxh. See 2.9.4.1 for chiplet to pin mapping.

Table 164: Address Mapping for D18F2x9C_x0[3,1:0][F,8:0]1_[F,7:0]043_dct[3:0]

Address	Description
PciCfgDevFunc[11:0]	182h
PciCfgOffset[11:0]	09Ch
D18F2x98_dct[3:0][31:28]	0h
D18F2x98_dct[3:0][27:24]	**mp: memory P-state selector**. See: Table 146 [Address Mapping for D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0]].
D18F2x98_dct[3:0][23:20]	**chiplet: chiplet selector**. Value Name Description 8h-0h 8-0 Chiplet <Value> Fh Broadcast Broadcast to chiplets [8:0]
D18F2x98_dct[3:0][19:16]	1h
D18F2x98_dct[3:0][15:12]	**bit: pad selector**. Value Name Description 7h-0h 7-0 Bit <Value> Fh Broadcast Broadcast to bits [7:0]
D18F2x98_dct[3:0][11:0]	043h
D18F1x10C[DctCfgSel]	**dct: DCT controller select**. See: Table 146 [Address Mapping for D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0]].

Bits	Description
31:3	Reserved.
2:0	**MajorMode: Rx Major mode**. Read-write. BIOS: See 2.9.9.9 Bits: Description 000b: DDR3 normal 011b-001b: Reserved 100b: DDR3 low power 111b-101b: Reserved

D18F2x9C_x0[3,1:0][F,8:0]1_[F,7:0]045_dct[3:0] DATA VrefNom

Cold reset: 0000_xxxxh. See 2.9.4.1 for chiplet to pin mapping.

Table 165: Address Mapping for D18F2x9C_x0[3,1:0][F,8:0]1_[F,7:0]045_dct[3:0]

Address	Description
PciCfgDevFunc[11:0]	182h
PciCfgOffset[11:0]	09Ch
D18F2x98_dct[3:0][31:28]	0h
D18F2x98_dct[3:0][27:24]	**mp: memory P-state selector**. See: Table 146 [Address Mapping for D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0]].
D18F2x98_dct[3:0][23:20]	**chiplet: chiplet selector**. Value: Name: Description 8h-0h: 8-0: Chiplet <Value> Fh: Broadcast: Broadcast to chiplets [8:0]
D18F2x98_dct[3:0][19:16]	1h
D18F2x98_dct[3:0][15:12]	**bit: pad selector**. Value: Name: Description 7h-0h: 7-0: Bit <Value> Fh: Broadcast: Broadcast to bits [7:0]
D18F2x98_dct[3:0][11:0]	045h
D18F1x10C[DctCfgSel]	**dct: DCT controller select**. See: Table 146 [Address Mapping for D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0]].

Bits	Description
31:7	Reserved.
6:0	**VrefDnom: Rx Vref nominal**. Read-write. BIOS: 40h.

D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]046_dct[3:0] DATA Tx EQ HI Impedance

Cold reset: 0000_0000h. See 2.9.4.1 for chiplet to pin mapping.

Table 166: Address Mapping for D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]046_dct[3:0]

Address	Description
PciCfgDevFunc[11:0]	182h
PciCfgOffset[11:0]	09Ch
D18F2x98_dct[3:0][31:28]	0h
D18F2x98_dct[3:0][27:24]	**mp: memory P-state selector**. See: Table 146 [Address Mapping for D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0]].
D18F2x98_dct[3:0][23:20]	**chiplet: chiplet selector**. See: Table 163 [Address Mapping for D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]041_dct[3:0]].
D18F2x98_dct[3:0][19:16]	1h
D18F2x98_dct[3:0][15:12]	**Txpad: Tx pad selector**. See: Table 146 [Address Mapping for D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0]].
D18F2x98_dct[3:0][11:0]	046h
D18F1x10C[DctCfgSel]	**dct: DCT controller select**. See: Table 146 [Address Mapping for D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0]].

Bits	Description
31:14	Reserved.
13:7	**EQStrenHiN: Equalization HI NMOS driver output impedance**. Read-write. BIOS: See 2.9.9.2.10. Specifies the pulldown output driver impedance during Hi de-emphasis .
6:0	**EQStrenHiP: Equalization HI PMOS driver output impedance**. Read-write. BIOS: See 2.9.9.2.10. Specifies the pullup output driver impedance during Hi de-emphasis .

D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]047_dct[3:0] DATA Tx EQ LO Impedance

Cold reset: 0000_0000h. See 2.9.4.1 for chiplet to pin mapping.

Table 167: Address Mapping for D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]047_dct[3:0]

Address	Description
PciCfgDevFunc[11:0]	182h
PciCfgOffset[11:0]	09Ch
D18F2x98_dct[3:0][31:28]	0h
D18F2x98_dct[3:0][27:24]	**mp: memory P-state selector**. See: Table 146 [Address Mapping for D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0]].
D18F2x98_dct[3:0][23:20]	**chiplet: chiplet selector**. See: Table 163 [Address Mapping for D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]041_dct[3:0]].
D18F2x98_dct[3:0][19:16]	1h
D18F2x98_dct[3:0][15:12]	**Txpad: Tx pad selector**. See: Table 146 [Address Mapping for D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0]].
D18F2x98_dct[3:0][11:0]	047h
D18F1x10C[DctCfgSel]	**dct: DCT controller select**. See: Table 146 [Address Mapping for D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0]].

Bits	Description
31:14	Reserved.
13:7	**EQStrenLoN: Equalization LO NMOS driver output impedance**. Read-write. BIOS: See 2.9.9.2.10. Specifies the pulldown output driver impedance during Lo de-emphasis .
6:0	**EQStrenLoP: Equalization LO PMOS driver output impedance**. Read-write. BIOS: See 2.9.9.2.10. Specifies the pullup output driver impedance during Lo de-emphasis .

D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]048_dct[3:0] DATA Tx EQ Boost Impedance

Cold reset: 0000_0000h. See 2.9.4.1 for chiplet to pin mapping.

Table 168: Address Mapping for D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]048_dct[3:0]

Address	Description
PciCfgDevFunc[11:0]	182h
PciCfgOffset[11:0]	09Ch
D18F2x98_dct[3:0][31:28]	0h
D18F2x98_dct[3:0][27:24]	**mp: memory P-state selector**. See: Table 146 [Address Mapping for D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0]].
D18F2x98_dct[3:0][23:20]	**chiplet: chiplet selector**. See: Table 163 [Address Mapping for D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]041_dct[3:0]].
D18F2x98_dct[3:0][19:16]	1h
D18F2x98_dct[3:0][15:12]	**Txpad: Tx pad selector**. See: Table 146 [Address Mapping for D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0]].
D18F2x98_dct[3:0][11:0]	047h
D18F1x10C[DctCfgSel]	**dct: DCT controller select**. See: Table 146 [Address Mapping for D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0]].

Bits	Description
31:14	Reserved.
13:7	**BoostStrenN: Equalization Boost driver output impedance**. Read-write. BIOS: See 2.9.9.2.10. Specifies the boost impedance during rise or fall data bit times.
6:0	**BoostStrenP: Equalization Boost driver output impedance**. Read-write. BIOS: See 2.9.9.2.10. Specifies the boost impedance during rise or fall data bit times.

D18F2x9C_x00[F,8:0]1_[F,B:0]04A_dct[3:0] DqDqs Rx Control

Cold reset: 0000_0200h. See 2.9.4.1 for chiplet to pin mapping.

Table 169: Index Mapping for D18F2x9C_x00[F,8:0]1_[F,B:0]04A_dct[3:0]

Address Bits	Valid Values	Name

Table 169: Index Mapping for D18F2x9C_x00[F,8:0]1_[F,B:0]04A_dct[3:0]

D18F2x98_dct[3:0][15:12]	[B:0]	Rx pad
D18F2x98_dct[3:0][15:12]	Fh	Rx pad [B:0]
D18F2x98_dct[3:0][23:20]	[8:0]	Data chiplet
D18F2x98_dct[3:0][23:20]	Fh	Data chiplet [8:0]

Bits	Description
31:10	Reserved.
9	**DisableFCPeaking: Disable FC Peaking**. Read-write. 1=Disable inductive-peaking for the folded-cascode gain stage of the DQ receiver.
8	**BiasBypassEn**. Read-write. See: D18F2x9C_x00[F,3:0]0_[F,B:0]04A_dct[3:0][8].
7	**PowerDownRcvr**. Read-write. See: D18F2x9C_x00[F,3:0]0_[F,B:0]04A_dct[3:0][7].
6:4	**MajorMode**. Read-write. See: D18F2x9C_x00[F,3:0]0_[F,B:0]04A_dct[3:0][6:4].
3:0	**FineDlyCtrl: Fine delay control**. Read-write. Specifies an untimed amount of delay that the DATA (includes both DQ and DQS/WCK) chiplet signals are delayed from the default setup time, in addition to the per-group DLL RxDly. When applied to a CSR for a data strobe pad, then this has the equivelent functionality of legacy receiver enable delay. When applied to a CSR for a DQ pad, then this has the equivelent functionality of legacy read DQS delay. Bits Description 0h Minimum delay 9h Maximum delay Fh-Ah Reserved

D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]04D_dct[3:0] DATA Rx Impedance

Cold reset: 0000_0000h. See 2.9.4.1 for chiplet to pad and pad to pin mapping.

Table 170: Address Mapping for D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]04D_dct[3:0]

Address	Description
PciCfgDevFunc[11:0]	182h
PciCfgOffset[11:0]	09Ch
D18F2x98_dct[3:0][31:28]	0h
D18F2x98_dct[3:0][27:24]	**mp: memory P-state selector**. See: Table 146 [Address Mapping for D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0]].
D18F2x98_dct[3:0][23:20]	**chiplet: chiplet selector**. See: Table 163 [Address Mapping for D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]041_dct[3:0]].
D18F2x98_dct[3:0][19:16]	1h
D18F2x98_dct[3:0][15:12]	**Rxpad: Rx pad selector**. See: Table 146 [Address Mapping for D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0]].
D18F2x98_dct[3:0][11:0]	04Dh
D18F1x10C[DctCfgSel]	**dct: DCT controller select**. See: Table 146 [Address Mapping for D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0]].

Bits	Description
31:8	Reserved.
7:4	**ODTStrenN: ODT strength NMOS**. Read-write. BIOS: See 2.9.9.2.5. Specifies the ODT impedance when in thevinin termination mode. See ODTStrenP for field description.
3:0	**ODTStrenP: ODT strength PMOS**. Read-write. BIOS: See 2.9.9.2.5. Specifies the ODT impedance when in thevinin termination mode. Note legacy ProcOdt values are given in Thevenin. Bits — Description 0h — disabled 1h — 480 ohms 4h — 240 ohms 5h — 160 ohms Ch — 120 ohms Dh — 96 ohms Fh — 80 ohms

D18F2x9C_x00[F,8:0]1_[F,B:0]04E_dct[3:0] TxControlDq

Cold reset: 0000_0013h. See 2.9.4.1 for chiplet to pin mapping.

Table 171: Index Mapping for D18F2x9C_x00[F,8:0]1_[F,B:0]04E_dct[3:0]

Address Bits	Valid Values	Name
D18F2x98_dct[3:0][15:12]	[B:0]	pad
D18F2x98_dct[3:0][15:12]	Fh	pad [B:0]
D18F2x98_dct[3:0][23:20]	[8:0]	Data chiplet
D18F2x98_dct[3:0][23:20]	Fh	Data chiplet [8:0]

Bits	Description
31:13	Reserved.
12	**EQEnable: Equalization enable**. Read-write. BIOS: 0.
11	**DrvPwrGateEn: Powergate driver enable**. Read-write. BIOS: 1.
10:0	Reserved.

D18F2x9C_x00[F,8:0]1_[F,B:0]051_dct[3:0] DqDqsRcvCntrl3

Cold reset: 0000_0052h. See 2.9.4.1 for chiplet to pad mapping and 2.9.4 for pad to pin mapping.

Table 172: Address Mapping for D18F2x9C_x00[F,8:0]1_[F,B:0]051_dct[3:0]

Address	Description
PciCfgDevFunc[11:0]	182h
PciCfgOffset[11:0]	09Ch
D18F2x98_dct[3:0][31:24]	00h
D18F2x98_dct[3:0][23:20]	**chiplet: chiplet selector**. See: Table 163 [Address Mapping for D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]041_dct[3:0]].

Table 172: Address Mapping for D18F2x9C_x00[F,8:0]1_[F,B:0]051_dct[3:0]

D18F2x98_dct[3:0][19:16]	1h
D18F2x98_dct[3:0][15:12]	**Rxpad: Rx pad selector**. See: Table 146 [Address Mapping for D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0]].
D18F2x98_dct[3:0][11:0]	05Fh
D18F1x10C[DctCfgSel]	**dct: DCT controller select**. See: Table 146 [Address Mapping for D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0]].

Bits	Description
31:9	Reserved.
8	**RxPadStandbyEn: Rx pad standby enable**. Read-write. BIOS: 1. 1=Enables standby power savings for the receiver.
7:0	Reserved.

D18F2x9C_x00[F,8:0]1_[F,B:0]05F_dct[3:0] DATA Tx Slew Rate

Cold reset: 0000_03BFh. See 2.9.4.1 for chiplet to pad mapping and 2.9.4 for pad to pin mapping.

Table 173: Address Mapping for D18F2x9C_x00[F,8:0]1_[F,B:0]05F_dct[3:0]

Address	Description
PciCfgDevFunc[11:0]	182h
PciCfgOffset[11:0]	09Ch
D18F2x98_dct[3:0][31:24]	00h
D18F2x98_dct[3:0][23:20]	**chiplet: chiplet selector**. See: Table 163 [Address Mapping for D18F2x9C_x0[3,1:0][F,8:0]1_[F,B:0]041_dct[3:0]].
D18F2x98_dct[3:0][19:16]	1h
D18F2x98_dct[3:0][15:12]	**Txpad: Tx pad selector**. See: Table 146 [Address Mapping for D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0]].
D18F2x98_dct[3:0][11:0]	05Fh
D18F1x10C[DctCfgSel]	**dct: DCT controller select**. See: Table 146 [Address Mapping for D18F2x9C_x0[3,1:0][F,3:0]0_[F,B:0]041_dct[3:0]].

Bits	Description
31:7	Reserved.
6	**G5Mode: Gddr5 mode**. Read-write. BIOS: See 2.9.9.2. 1=Driver is in GDDR5 mode. 0=Driver is in DDR3 mode. See 2.9 for product support.
5:3	**TxPreN: NMOS predriver calibration code**. Read-write. BIOS: See 2.9.9.2.7. Specifies the falling edge slew rate of the transmit pad. 000b=Slowest slew rate. 111b=Fastest slew rate.
2:0	**TxPreP: PMOS predriver calibration code**. Read-write. BIOS: See 2.9.9.2.7. Specifies the rising edge slew rate of the transmit pad. 000b=Slowest slew rate. 111b=Fastest slew rate.

D18F2x9C_x00[F,8:0]1_0[F,2:0]77_dct[3:0] DllPowerdown

Cold reset: 0000_0000h. See 2.9.4.1 for chiplet to pad mapping and see 2.9.4 for pad to pin mapping.

Table 174: Address Mapping for D18F2x9C_x00[F,8:0]1_0[F,2:0]77_dct[3:0]

Address	Description
PciCfgDevFunc[11:0]	182h
PciCfgOffset[11:0]	09Ch
D18F2x98_dct[3:0][31:24]	00h
D18F2x98_dct[3:0][23:20]	**chiplet: chiplet selector**. Value / Name / Description 8h-0h / 8-0 / Chiplet <Value> Fh / Broadcast / Broadcast to chiplets [8:0]
D18F2x98_dct[3:0][19:12]	10h
D18F2x98_dct[3:0][11:8]	**pad: pad selector**. Value / Name / Description 0h / 0h / DQ[3:0] pads 1h / 1h / DQ[7:4], MEMDQSDM[0] pads 2h / 2h / MEMDQS_H[0][1] pad Fh / All / all pads (groups[2:0])
D18F2x98_dct[3:0][7:0]	78h
D18F1x10C[DctCfgSel]	**dct: DCT controller select**. Value / Name / Description 011b-000b / 3h-0h / DCT <Value>

1. MEMDQS_H[0] is the positive polarity strobe pad for a x8 device. MEMDQSDM[0] is the data mask pin used in x8 or x16 devices.

Bits	Description
31:11	Reserved.
10:6	**DllPowerDownTx: Dll power down transmitter**. Read-write.
5	**DllPowerDownXCLK: Dll power down XCLK**. Read-write.
4:1	Reserved.
0	**DllPowerDown: Dll power down**. Read-write.

D18F2x9C_x00[F,8:0]1_0[F,2:0]78_dct[3:0] DllControl

Cold reset: 0000_0000h. See 2.9.4.1 for chiplet to pad mapping and see 2.9.4 for pad to pin mapping.

Table 175: Address Mapping for D18F2x9C_x00[F,8:0]1_0[F,2:0]78_dct[3:0]

Address	Description
PciCfgDevFunc[11:0]	182h
PciCfgOffset[11:0]	09Ch
D18F2x98_dct[3:0][31:24]	00h

Table 175: Address Mapping for D18F2x9C_x00[F,8:0]1_0[F,2:0]78_dct[3:0]

D18F2x98_dct[3:0][23:20]	**chiplet: chiplet selector**. Value / Name / Description 8h-0h / 8-0 / Chiplet <Value> Fh / Broadcast / Broadcast to chiplets [8:0]
D18F2x98_dct[3:0][19:12]	10h
D18F2x98_dct[3:0][11:8]	**pad: pad selector**. Value / Name / Description 0h / 0h / DQ[3:0] pads 1h / 1h / DQ[7:4], MEMDQSDM[0] pads 2h / 2h / MEMDQS_H[0][1] pad Fh / All / all pads (groups[2:0])
D18F2x98_dct[3:0][7:0]	78h
D18F1x10C[DctCfgSel]	**dct: DCT controller select**. Value / Name / Description 011b-000b / 3h-0h / DCT <Value>

1. MEMDQS_H[0] is the positive polarity strobe pad for a x8 device. MEMDQSDM[0] is the data mask pin used in x8 or x16 devices.

Bits	Description
31:8	Reserved.
7	**DllResetRelock: Dll reset relock**. Read-write. 1=Reset the DLL. 0=Relock the DLL. This bit must be set for 20 ns and then cleared anytime a forced relock of the DLL is required.
6:0	Reserved.

D18F2x9C_x0[F,1:0][F,8:0]1_[F,9:0][F,3:0]80_dct[3:0] Rx Delay

Cold reset: 0000_0040h. See 2.9.4.1 for chiplet to pad mapping and see 2.9.4 for pad to pin mapping.

Table 176: Address Mapping for D18F2x9C_x0[F,1:0][F,8:0]1_[F,9:0][F,3:0]80_dct[3:0]

Address	Description
PciCfgDevFunc[11:0]	182h
PciCfgOffset[11:0]	09Ch
D18F2x98_dct[3:0][31:28]	0h
D18F2x98_dct[3:0][27:24]	**mp: memory P-state selector**. Value / Name / Description 1h-0h / 1h-0h / Memory P-state <Value> Fh / Broadcast / Broadcast to Memory P-states [1:0]
D18F2x98_dct[3:0][23:20]	**chiplet: chiplet selector**. Value / Name / Description 8h-0h / 8-0 / Chiplet <Value> Fh / Broadcast / Broadcast to chiplets [8:0]
D18F2x98_dct[3:0][19:16]	1h

Table 176: Address Mapping for D18F2x9C_x0[F,1:0][F,8:0]1_[F,9:0][F,3:0]80_dct[3:0]

D18F2x98_dct[3:0][15:12]	**pad: pad selector**. Value / Name / Description 0h / 0h / DQ[3:0] pads 1h / 1h / DQ[7:4] pads 2h / 2h / MEMDQS_H[0][2] pad Fh / All / all pads (k group[3:0])
D18F2x98_dct[3:0][11:8]	**dimm: dimm selector**. Value / Name / Description 3h-0h / 3h-0h / dimm <Value> Fh / Broadcast / Broadcast to all dimms [3:0]
D18F2x98_dct[3:0][7:0]	80h
D18F1x10C[DctCfgSel]	**dct: DCT controller select**. Value / dct / Description 011b-000b / 3h-0h / DCT <dct>

1. If D18F2xA8_dct[3:0][PerRankTimingEn]=1 then each CSR addressed with DIMM controls the corresponding numbered chipselect, up to four total chipselects.
2. MEMDQS_H[0] is the positive polarity strobe pad for a x8 device.

Bits	Description
31:8	Reserved.
7:0	**RxDly: Rx delay**. Read-write. BIOS: See 2.9.9.2.10. Specifies the time that the DATA (includes both DQ and DQS/WCK) chiplet signals are delayed from the default setup time, in increments of 1/32UI. When applied to a CSR for a data strobe pad, then this has the equivelent functionality of legacy receiver enable delay. When applied to a CSR for a DQ pad, then this has the equivelent functionality of legacy read DQS delay.

D18F2x9C_x0[F,1:0][F,8:0]1_[F,9:0][F,3:0]81_dct[3:0] Tx Delay

Cold reset: 0000_0000h. See 2.9.4.1 for chiplet to pad mapping and see 2.9.4 for pad to pin mapping.

Table 177: Address Mapping for D18F2x9C_x0[F,1:0][F,8:0]1_[F,9:0][F,3:0]81_dct[3:0]

Address	Description
PciCfgDevFunc[11:0]	182h
PciCfgOffset[11:0]	09Ch
D18F2x98_dct[3:0][31:28]	0h
D18F2x98_dct[3:0][27:24]	**mp: memory P-state selector**. Value / Name / Description 1h-0h / 1h-0h / Memory P-state <Value> Fh / Broadcast / Broadcast to Memory P-states [1:0]
D18F2x98_dct[3:0][23:20]	**chiplet: chiplet selector**. Value / Name / Description 8h-0h / 8-0 / Chiplet <Value> Fh / Broadcast / Broadcast to chiplets [8:0]
D18F2x98_dct[3:0][19:16]	1h

Table 177: Address Mapping for D18F2x9C_x0[F,1:0][F,8:0]1_[F,9:0][F,3:0]81_dct[3:0]

D18F2x98_dct[3:0][15:12]	**pad: pad selector**. Value / Name / Description 0h / 0h / DQ[3:0] pads 1h / 1h / DQ[7:4], MEMDQSDM[0] pads 2h / 2h / MEMDQS_H[0][2] pad Fh / All / all pads (k group[3:0])
D18F2x98_dct[3:0][11:8]	**dimm: dimm selector**. Value / Name / Description[1] 3h-0h / 3h-0h / dimm <Value> Fh / Broadcast / Broadcast to all dimms [3:0]
D18F2x98_dct[3:0][7:0]	81h
D18F1x10C[DctCfgSel]	**dct: DCT controller select**. Value / Name / Description 011b-000b / 3h-0h / DCT <Value>

1. If D18F2xA8_dct[3:0][PerRankTimingEn]=1 then each CSR addressed with DIMM controls the corresponding numbered chipselect, up to four total chipselects.
2. MEMDQS_H[0] is the positive polarity strobe pad for a x8 device. MEMDQSDM[0] is the data mask pin used in x8 or x16 devices.

Bits	Description
31:8	Reserved.
7:0	**TxDly: Tx delay**. Read-write. BIOS: See 2.9.9.2.10. Specifies the time that the DATA (includes both DQ and DQS/WCK) chip signals are delayed from the default setup time, in increments of 1/32 UI. When applied to a CSR for a write strobe pad, then this has the equivelent functionality of legacy write DQS delay. When applied to a CSR for a DQ pad, then this has the equivelent functionality of legacy write data delay.

D18F2x9C_x0002_0000_dct[3:0] Pll MemoryPstate0

Cold reset: 0000_0400h.

Table 178: Index Mapping for PllMultDiv Value Definition

Bits	Data Rate
0603h	667 MT/s
0D01h	1333 MT/s
1000h	1600 MT/s
1203h	1866 MT/s
1501h	2133 MT/s
1800h	2400 MT/s
2000h	3200 MT/s
2200h	3400 MT/s
Note: “Memory-Clock” frequency is one-half of the data rate for DDR3.	

Bits	Description
31:16	Reserved.
15:0	**PllMultDiv: Pll multiplier divider**. Read-write. BIOS: 2.9.9.2.3. Specifies the DRAM bus data rate for DDR3 memory P-state 0, by way of phy Pll multiplier and divider. See Table 178.

D18F2x9C_x0002_0001_dct[3:0] Pll MemoryPstate1

Cold reset: 0000_0400h.

Bits	Description
31:16	Reserved.
15:0	**PllMultDiv: Pll multiplier divider**. Read-write. BIOS: 2.9.9.2.3. Specifies the DRAM bus data rate for memory P-state 1 by way of phy Pll multiplier and divider. See Table 178.

D18F2x9C_x0002_0004_dct[3:0] Mailbox Protocol Shadow

Cold reset: 0000_0007h.

Bits	Description
31:3	Reserved.
2	**Us2Rdy: Upstream 2 Ready.** Read-only. This bit is a read-only copy of D18F2x9C_x0002_0035_dct[3:0][Rdy].
1	**UsRdy: Upstream Ready.** Read-only. This bit is a read-only copy of D18F2x9C_x0002_0033_dct[3:0][Rdy].
0	Reserved.

D18F2x9C_x0002_000B_dct[3:0] Power State Command

Cold reset: 0000_0002h.

Bits	Description
31:16	Reserved.
15:14	**CmdType: Command Type.** Read-write. Bits — Description 00b — Change to PS0 or PS1 01b — NbPstate Update 10b — Phase Align 11b — Null, update register values only
13:10	Reserved.
9:8	**NbPstate: Nb Pstate.** Read-write.
7:5	Reserved.
4	**EnterS3: Enter S3.** Read-write. 1=PHY removes the MemReset control from DCT interface in preparation of S3 state transition. Only valid with LP2 command.

3	Reserved.
2:0	**PhyPowerState: Phy Power State**. Read-write. Specifies the phy power state to transition to when this register is written. Bits Description 000b PS0 001b PS1 011b-010b Reserved 100b LP2 111b-101b Reserved

D18F2x9C_x0002_000E_dct[3:0] Global Control

Cold reset: 0000_0003h.

Bits	Description
31:2	Reserved.
1	**PhyDisable: Phy Disable.** Read-write. BIOS: 2.9.9.2. 1=Phy is disabled. 0=Phy is enabled.
0	**G5_Mode: GDDR5 Mode.** Read-write. 1=Combo phy master chip is in GDDR5 mode. 0=Combo phy master chip is in DDR3 mode. The phy writes this value to all slave chiplet instances during a configuration write to D18F2x9C_x0002_000B_dct[3:0]. See section 2.9 for product support.

D18F2x9C_x00F2_0015_dct[3:0] Vref Byte

Cold reset: 0000_0000h.

Bits	Description
31:4	Reserved.
3:0	**VrefFilt: Vref filter.** Read-write. BIOS: 0. This field adjusts noise coupling on to VrefOut and adjusts the input resistance.

D18F2x9C_x0002_0032_dct[3:0] US Mailbox 1 Message

Cold reset: 0000_0000h.

Bits	Description
31:16	Reserved.
15:0	**Message: Message.** Read-write. This field specifies the encoded message received.

D18F2x9C_x0002_0033_dct[3:0] US Mailbox 1 Protocol

Cold reset: 0000_0001h.

Bits	Description
31:1	Reserved.
0	**Rdy: Ready.** Read-write. 1=The US Mailbox 1 is ready for a data transfer from the PMU to the mailbox; the PMU may write to D18F2x9C_x0002_0032_dct[3:0][Message]. 0=PMU may not write to D18F2x9C_x0002_0032_dct[3:0][Message].

D18F2x9C_x0002_0034_dct[3:0] US Mailbox 2 Message

Cold reset: 0000_0000h.

Bits	Description
31:16	Reserved.
15:0	**Message: Message.** Read-write. This field specifies the data received.

D18F2x9C_x0002_0035_dct[3:0] US Mailbox 2 Protocol

Cold reset: 0000_0001h.

Bits	Description
31:1	Reserved.
0	**Rdy: Ready.** Read-write. 1=The US Mailbox 2 is ready for a data transfer from the PMU to the mailbox; the PMU may write to D18F2x9C_x0002_0034_dct[3:0][Message]. 0=PMU may not write to D18F2x9C_x0002_0034_dct[3:0][Message].

D18F2x9C_x0002_005B_dct[3:0] D3_EVNTMERR

Cold reset: 0000_003Fh.

Bits	Description
31:4	Reserved.
3	**D3MERR_RxEn: MEMERR receiver enable.** Read-write. BIOS:0. 1=Enable receiver for MEMERR pad.
2:1	Reserved.
0	**D3EVNT_RxEn: EVENT_L receiver enable.** Read-write. BIOS: 1. 1=Enable receiver for EVENT_L pad.

D18F2x9C_x0002_005F_dct[3:0] Misc Phy Status

Cold reset: 0000_000xh.

Bits	Description
31:2	Reserved.
1	**PORMemReset: POR MemReset.** Read-only. 1=Previous cold reset was a power-up event (accompanied by ramping VDDIO). 0=Previous cold reset was associated with S3 (VDDIO was already supplied).
0	**DctSane: Dct Sane.** Read-only; updated-by-hardware. 1=Software provides the logic state of Memreset_L to drive as specified by D18F2x9C_x0002_0060_dct[3:0][MemReset]. 0=MemReset_L logic state is provided by the complement of PORMemReset. This bit is set by hardware after the first write to D18F2x9C_x0002_000B_dct[3:0].

D18F2x9C_x0002_0060_dct[3:0] Memreset Control

Cold reset: 0000_0000h.

Bits	Description
31:1	Reserved.
0	**MemReset_L.** Read-write. BIOS: See 2.9.9.5. 1=MemReset_L pin is driven inactive when D18F2x9C_x0002_005F_dct[3:0][DctSane]=1. 0=MemReset_L pin is driven active when D18F2x9C_x0002_005F_dct[3:0][DctSane]=1.

D18F2x9C_x0[1:0]02_0080_dct[3:0] PMU CLK Divider

Cold reset: 0000_0008h.

Table 179: Index Mapping for D18F2x9C_x0[1:0]02_0080_dct[3:0]

Address Bits	Valid Values	Name
D18F2x98_dct[3:0][27:24]	0h	memory Pstate 0
D18F2x98_dct[3:0][27:24]	1h	memory Pstate 1

Bits	Description
31:4	Reserved.
3:0	**PMUClkDiv: PMU CLK divider.** Read-write. BIOS: 2.9.9.2.3. Specifies the divider from PCLK to the PMU input clock. PCLK frequency is the same as the data rate (See D18F2x9C_x0002_0000_dct[3:0][PllMultDiv] and D18F2x9C_x0002_0001_dct[3:0][PllMultDiv]). This must be programmed so the PMU operates no faster than 533 MHz. Software should program this to the smallest divider which meets this condition for best training results. For example, if the data rate is 5Gb/s (PllMultDiv==3200h) then PMUClkDiv=divide by 10 (the PMU runs at 500 MHz). If for example, the data rate is 667Mb/s (PllMultDiv==0603h) then PMUClkDiv=divide by 2 (the PMU runs at 333 MHz). When training is complete and the PMU is in reset, it is recommended that BIOS program this to PMU CLK = CPU RefClk. Bits — Description 0000b — divide by 1 0001b — divide by 2 0010b — divide by 4 0011b — divide by 6 0100b — divide by 8 0101b — divide by 10 0111b — PMU CLK turned off 1111b-1000b — PMU CLK = CPU Refclk

D18F2x9C_x0002_0087_dct[3:0] Disable Calibration

Cold reset: 0000_0014h.

Bits	Description
31:2	Reserved.

1	**DisAutoComp: Disable automatic compensation**. Read-write. BIOS: 2.9.9.2.5. 1=Disable automatic updates of Tx and POdt targets. If Ddr3Mode each 64-bit channel has one calibrator and one disable bit. If Gddr5Mode two 32-bit channels have one calibrator and one disable bit located in the master channel.
0	**DisPredriverCal: Disable predriver calibration**. Read-write. BIOS: 2.9.9.2.5. 1=Disable automatic updates of predriver targets. If Ddr3Mode each 64-bit channel has one calibrator and one disable bit. If Gddr5Mode two 32-bit channels have one calibrator and one disable bit located in the master channel.

D18F2x9C_x0002_0088_dct[3:0] CalRate

Cold reset: 0000_0083h.

Bits	Description
31:9	Reserved.
8	**CalOdtNeverLock: Calibration init Odt no-lock mode**. Read-write. BIOS: 2.9.9.2.5.
7	**CalInitMode: Calibration init mode**. Read-write. BIOS: 2.9.9.2.5.
6	Reserved.
5	**CalOnce: Calibration run one time**. Read-write. BIOS: 2.9.9.2.5. 1=Run one time. 0=Run continuously.
4	**CalRun: Calibration run**. Read-write. BIOS: 2.9.9.2.5.
3:0	**CalInterval: Calibration interval**. Read-write. BIOS: 2.9.9.2.5.

D18F2x9C_x0002_0089_dct[3:0] PllLockTime

Cold reset: 0000_00C8h.

Bits	Description
31:16	Reserved.
15:0	**PllLockTime: Pll lock time**. Read-write. BIOS: 2.9.9.2.3. Specifies the number of 5ns periods the phy waits for PLLs to lock during a frequency change.

D18F2x9C_x0002_0093_dct[3:0] PllRegWaitTime

Cold reset: 0000_0023h.

Bits	Description
31:16	Reserved.
15:0	**PllRegWaitTime: PLL regulator wait time.** Read-write. BIOS: 2.9.9.2.3. Specifies the number of 5 ns periods the phy waits for the PLL to become stable when coming out of PLL regulator off power down mode.

D18F2x9C_x0002_0097_dct[3:0] CalBusy

Cold reset: 0000_0000h.

Bits	Description
31:1	Reserved.
0	**CalBusy: Calibration busy.** Read-only.

D18F2x9C_x0002_0098_dct[3:0] Cal Misc 2

Cold reset: 0000_0204h.

Bits	Description
31:14	Reserved.
13	**CalG5D3: Calibrate G5 D3.** Read-write. BIOS: (D18F2x9C_x00[F,3:0]0_[F,B:0]04A_dct[3:0][MajorMode[0]]). 1=Calibrator performs the GDDR5 sequence. 0=Calibrator performs the DDR3 sequence. See section 2.9 for product support.
12:11	**CalCmptrResTrim: Calibration comparator resistance trim.** Read-write. BIOS: 2.9.9.2.2. Specifies input comparator voltage. This should be programmed consistent with I/O voltage. Bits — Cal Cmptr voltage 00b — 1.50V 01b — 1.35V 10b — 1.25V 11b — Reserved
10:0	Reserved.

D18F2x9C_x0002_0099_dct[3:0] PMU Reset

Cold reset: 0000_0001h.

Bits	Description
31:7	Reserved.
6	**SRAM_SD: PMU SRAM Shutdown.** Read-write. BIOS: 2.9.9.9. 1=Power down PMU SRAM.
5:4	Reserved.
3	**PmuReset: PMU Reset.** Read-write. BIOS: 2.9.9.2. 1=Places the phy microcontroller unit (PMU) in reset. 0=Starts clocks and removes the reset signal to the PMU.
2:1	Reserved.
0	**PmuStall: PMU Stall.** Read-write. BIOS: 2.9.9.2. 1=Places the phy microcontroller unit (PMU) in a clock gated stall state. 0=Starts clocks and resume execution at current instruction pointer.

D18F2x[B,0]9C_x0005_[5BFF:4000]_dct[3:0] PMU IC SRAM

Cold reset: 0000_0000h.
This is a word-addressable address space.
Software must write a pair of words into PMU SRAM, starting with an numbered index, in order for a write to be properly latched. E.g. writing to SRAM index 0 and then index 1 will result in two data words being written to SRAM; writing to index 0 only or index 1 only will result in no data being written to SRAM. If writing an even numbered word-sized block of SRAM then no additional writes are necessary. If writing with random access and software loses track of how many words were written, then it should assume the write was not latched and re-write utilizing a pair of accesses as stated above. It is not recommended to interrupt two consecutive writes with an intervening read operation.

Bits	Description
31:16	Reserved.
15:0	**PMUFirmwareSRAM: PMU Firmware SRAM.** Read-write. BIOS: 2.9.9.2.9.

D18F2x9C_x0005_[0BFF:0000]_dct[3:0] PMU SRAM Message Block

Cold reset: 0000_0000h.
This is a word-addressable address space. The lower 256 bytes of SRAM in the data portion of the address map is the SRAMMsgBlk. The remaining portion of the 6KB of SRAM is used by the system.
Software must write a pair of words into PMU SRAM, starting with an even numbered index, in order for a write to be properly latched. E.g. writing to SRAM index 0 and then index 1 will result in two data words being written to SRAM; writing to only an even index will result in no data written to SRAM; writing to only an odd index will result in arbitrary data written to the memory addressed by the corresponding even index (destroying the prior contents) but the odd index will be written with the intended data. If writing an even numbered word-sized block of SRAM aligned on an even index then no additional writes are necessary. If writing with random access and software loses track of how many words were written, then it should assume the write was not latched and re-write utilizing a pair of accesses as stated above. It is not recommended to interrupt two consecutive writes with an intervening read operation.

Bits	Description
31:16	Reserved.
15:0	**SRAMMsgBlk: SRAMMsgBlk**. Read-write. BIOS: 2.9.9.2.9.

D18F2x9C_x00F4_00E[7:0]_dct[3:0] Odt Pattern

Cold reset: 0000_0000h.

Bits	Description
31:8	Reserved.
7:4	**OdtRdPatCs: Odt read pattern Cs[7:0].** Read-write. BIOS: See D18F2x[234:230]_dct[3:0]. This register specifies the ODT[3:0] pin pattern during a read to chipselect [7:0]. It is used by the PMU during initial training for DDR3 mode and does not need to be saved and restored for S3.
3:0	**OdtWrPatCs: Odt write pattern Cs[7:0].** Read-write. BIOS: See D18F2x[23C:238]_dct[3:0]. This register specifies the ODT[3:0] pin pattern during a write to chipselect [7:0]. It is used by the PMU during initial training for DDR3 mode and does not need to be saved and restored for S3.

D18F2x9C_x00F4_00FD_dct[3:0] Phy CKE control

Cold reset: 0000_0000h.

Bits	Description
31:8	Reserved.
7:4	**AcsmCkeEnb[3:0]: ACSM CKE enable[3:0].** Read-write. 1=If AcsmCkeOride==1 then CKE is asserted active. 0=If AcsmCkeOride==1 then CKE is deasserted.
3:0	**AcsmCkeOride[3:0]: ACSM CKE override[3:0].** Read-write. 1=When the DCT is not connected, PMU overrides the ACSM output values, allowing directly programmability with AcsmCkeEnb. 0=When the DCT is not connected, the ACSM determines CKE output values.

D18F2x9C_x0007_0015_dct[3:0] Lane to CRC Map0

Cold reset: 0000_0000h.

Bits	Description
31:12	Reserved.
11:9	**CrcLaneMap3: Crc lane map 3.** Read-write. Map lane 3 to CRC input.
8:6	**CrcLaneMap2: Crc lane map 2.** Read-write. Map lane 2 to CRC input.
5:3	**CrcLaneMap1: Crc lane map 1.** Read-write. Map lane 1 to CRC input.
2:0	**CrcLaneMap0: Crc lane map 0.** Read-write. Map lane 0 to CRC input.

D18F2x9C_x0007_0016_dct[3:0] Lane to CRC Map1

Cold reset: 0000_0000h.

Bits	Description
31:12	Reserved.
11:9	**CrcLaneMap7: Crc lane map 7.** Read-write. Map lane 7 to CRC input.
8:6	**CrcLaneMap6: Crc lane map 6.** Read-write. Map lane 6 to CRC input.
5:3	**CrcLaneMap5: Crc lane map 5.** Read-write. Map lane 5 to CRC input.
2:0	**CrcLaneMap4: Crc lane map 4.** Read-write. Map lane 4 to CRC input.

D18F2x9C_x0009_0000_dct[3:0] ABIT Enable

Cold reset: 0000_0000h.

Bits	Description
31:1	Reserved.
0	**ABitEn: ABIT enable.** Read-write. 1=ABIT chiplet is enabled. The ABIT chiplet is used to extend the number of address/command bits controlled by the phy while having separate granular control from existing ABYTE chips. 0=ABIT chiplet is powered down. Chip still responds to CSR accesses.

D18F2x9C_x0009_000E_dct[3:0] Global Control Slave

Cold reset: 0000_0001h.

Bits	Description
31:1	Reserved.
0	**G5_Mode: GDDR5 Mode.** Read-write. 1=Combo phy slave chip is in GDDR5 mode. 0=Combo phy slave chip is in DDR3 mode. See section 2.9 for product support.

D18F2x9C_x0009_004A_dct[3:0] Rx Control 1

Cold reset: 0000_0080h. See 2.9.4.1 for chiplet to pad and 2.9.4 for pad to pin mapping. D18F2x98_dct[3:0][15:12] selects the pad number.

Bits	Description
31:9	Reserved.
8	**BiasBypassEn: Bias bypass enable**. Read-write. BIOS: 0.

7	**PowerDownRcvr: Power down receiver**. Read-write. BIOS: See 2.9.9.9. 1=Power down the receiver.
6:4	**MajorMode: Major mode**. Read-write. BIOS: See 2.9.9.2. Specifies operating mode of the phy logic. Bits Description 000b DDR3 111b-001b Reserved
3:0	Reserved.

D18F2x9C_x00FF_000D_dct[3:0] Phy Clock Control

Cold reset: 0000_0000h.

Bits	Description
31:1	Reserved.
0	**PhyClkCtl: Phy Clock Control.** Read-write. BIOS: See 2.9.9.7. 1=Do not stop bus clocks when control is handed off between the DCT and the PMU. This is used to pass from normal operating mode to periodic phase training without glitching bus clocks.

D18F2xA4 DRAM Controller Temperature Throttle

See 2.9.3 [DCT Configuration Registers].
See 2.9.14 [DRAM On DIMM Thermal Management and Power Capping].

<table>
<tr><th>Bits</th><th>Description</th></tr>
<tr><td>31:24</td><td>Reserved.</td></tr>
<tr><td>23:20</td><td>BwCapCmdThrottleMode: bandwidth capping command throttle mode. Read-write. Reset: 0. Specifies the command throttle mode when BwCapEn=1. The DCT throttles commands over a rolling window of 100 clock cycles, maintaining the average throttling as specified by this field.

<table>
<tr><th>Bits</th><th>Description</th></tr>
<tr><td>0000b</td><td>Command throttling is disabled</td></tr>
<tr><td>0001b</td><td>Throttle commands by 30%</td></tr>
<tr><td>0010b</td><td>Throttle commands by 40%</td></tr>
<tr><td>0011b</td><td>Throttle commands by 50%</td></tr>
<tr><td>0100b</td><td>Throttle commands by 55%</td></tr>
<tr><td>0101b</td><td>Throttle commands by 60%</td></tr>
<tr><td>0110b</td><td>Throttle commands by 65%</td></tr>
<tr><td>0111b</td><td>Throttle commands by 70%</td></tr>
<tr><td>1000b</td><td>Throttle commands by 75%</td></tr>
<tr><td>1001b</td><td>Throttle commands by 80%</td></tr>
<tr><td>1010b</td><td>Throttle commands by 85%</td></tr>
<tr><td>1011b</td><td>Throttle commands by 90%</td></tr>
<tr><td>1100b</td><td>Throttle commands by 95%</td></tr>
<tr><td>1101b</td><td>Reserved</td></tr>
<tr><td>1110b</td><td>Throttle commands as specified by CmdThrottleMode</td></tr>
<tr><td>1111b</td><td>Reserved</td></tr>
</table>
Throttling should not be enabled until after DRAM initialization (D18F2x110[DramEnable]==1) and training (see 2.9.9.6 [DRAM Training]) are complete.</td></tr>
<tr><td>19:16</td><td>Reserved.</td></tr>
<tr><td>15</td><td>Reserved.</td></tr>
</table>

14:12	**CmdThrottleMode: command throttle mode**. Read-write. Reset: 0. BIOS: See 2.9.9.6 [DRAM Training]. Specifies the command throttle mode when ODTSEn==1 and the EVENT_L pin is asserted. The DCT throttles commands over a rolling window of 100 clock cycles, maintaining the average throttling as specified by this field. Bits — Description 000b — Command throttling is disabled. 001b — Throttle commands by 30%. 010b — Throttle commands by 50%. 011b — Throttle commands by 60%. 100b — Throttle commands by 70%. 101b — Throttle commands by 80%. 110b — Throttle commands by 90%. 111b — Place the DRAM devices in powerdown mode (see D18F2x94_dct[3:0][PowerDownMode]) when EVENT_L is asserted. This mode is not valid if D18F2x94_dct[3:0][PowerDownEn]==0. Throttling should not be enabled until after DRAM initialization (D18F2x110[DramEnable]==1) and training are complete. See also BwCapEn.
11	**BwCapEn: bandwidth capping enable**. Read-write. Reset: 0. 1=The memory command throttle mode specified by BwCapCmdThrottleMode is applied. This bit is used by software to enable command throttling independent of the state of the EVENT_L pin. If this bit is set, ODTSEn=1, and the EVENT_L pin is asserted, the larger of the two throttle percentages specified by CmdThrottleMode and BwCapCmdThrottleMode is used.
10:9	Reserved.
8	**ODTSEn: on DIMM temperature sensor enable**. Read-write. Reset: 0. BIOS: See 2.9.9.6 [DRAM Training]. Enables the monitoring of the EVENT_L pin and indicates whether the on DIMM temperature sensors of the DIMMs on a channel are enabled. 0=Disabled. 1=Enabled. While the EVENT_L pin is asserted, the controller (a) doubles the refresh rate (if Tref=7.8 us), and (b) throttles the address bus utilization as specified by CmdThrottleMode[2:0].
7:0	Reserved.

D18F2xA8_dct[3:0] DRAM Controller Miscellaneous 2

See 2.9.3 [DCT Configuration Registers].

Bits	Description
31	**PerRankTimingEn: per rank timing enable**. Read-write. Reset: 0. BIOS: 0. Specifies the mapping between chip selects and a set of programmable timing delays. 1=Each chip select is controlled by a set of timing delays. A maximum of 4 chip selects are supported per channel. 0=Each chip select pair is controlled by a set timing delays.
30	Reserved.
29	**RefChCmdMgtDis: refresh channel command management disable**. Read-write; Same-for-all. Reset: 0. 1=DCTs issue refresh commands independently. 0=DCTs stagger the issue of refresh commands.

28	**FastSelfRefEntryDis: fast self refresh entry disable**. Read-write; Same-for-all. Reset: 1. BIOS: ~D18F2x1B4[FlushWrOnS3StpGnt]. 1=DCT pushes outstanding transactions to memory prior to entering self refresh. 0=DCT enters self refresh immediately unless instructed to push outstanding transactions to memory by D18F2x11C[FlushWrOnStpGnt] or D18F2x1B4[FlushWrOnS3StpGnt].
27:26	Reserved.
25:24	Reserved.
23	Reserved.
22	**PrtlChPDEnhEn: partial channel power down enh enable**. Read-write. Reset: 0. BIOS: 0. Selects the channel idle hysteresis for fast exit/slow exit mode changes when (D18F2x94_dct[3:0][PowerDownMode] & D18F2x84_dct[3:0][PchgPDModeSel]). 1=Hysteresis specified by D18F2x244_dct[3:0][PrtlChPDDynDly]. 0=256 clock hysteresis.
21	**AggrPDEn: aggressive power down enable**. Read-write. Reset: 0. BIOS: 1. 1=The DCT places the DRAM devices in precharge power down mode when pages are closed as specified by D18F2x248_dct[3:0]_mp[1:0][AggrPDDelay]. 0=The DCT places the DRAM devices in precharge power down mode when pages are closed as specified by D18F2x90_dct[3:0][DynPageCloseEn].
20	**BankSwap: swap bank address**. Read-write. Reset: 0. BIOS: See BIOS: See 2.9.9.6 [DRAM Training]. 1=Swap the DRAM bank address bits. IF ((D18F2x110[BankSwapAddr8En]) && D18F2x110[DctSelIntLvAddr]==100b) THEN normalized address bits (7+n):8 are swapped with normalized address bits used for bank address (See D18F2x80_dct[3:0]) ELSE normalized address bits [(8+n):9] are swapped with normalized address bits used for bank address; n is the number of bank address bits for the chip select. For example, if D18F2x110[DctSelIntLvAddr]==100b and D18F2x80_dct[3:0][DimmAddrMap]==0111b, then normalized address bits [10:8] are swapped with normalized address bits [15:13]. This swap happens before D18F2x94_dct[3:0][BankSwizzleMode] is applied.
19	**PDPhyPSDis: power down phy power save disable**. Read-write. Reset: 0. BIOS: 1. 1=Disable phy clock gating during precharge power down (phy LP1 power state). 0=Enable phy clock gating during precharge power down to save power. BIOS must set this bit prior to setting D18F2x94_dct[3:0][PowerDownEn]=1, or before enabling the controller.
18	Reserved.
17:16	Reserved.
15:8	**MrsCtrlWordCS[7:0]: MRS and control word chip select**. Read-write. Reset: 0. Specifies the target chip selects used for MRS or control word programming. See D18F2x7C_dct[3:0][SendMrsCmd, SendControlWord]. When used in conjunction with D18F2x7C_dct[3:0][SendMrsCmd], defined only if (~D18F2x7C_dct[3:0][EnDramInit] | ~D18F2x90_dct[3:0][UnbuffDimm]); otherwise, MRS commands are sent to all chip selects. Bit — Description [0] — CS0 is asserted [1] — CS1 is asserted [2] — CS2 is asserted [3] — CS3 is asserted [4] — CS4 is asserted [5] — CS5 is asserted [6] — CS6 is asserted [7] — CS7 is asserted
7:6	Reserved.
5	Reserved.

4	Reserved.
3:2	Reserved.
1:0	Reserved.

D18F2xAC DRAM Controller Temperature Status

Cold reset: 0000_0000h.

Bits	Description
31:8	Reserved.
7	Reserved.
6	**MemTempHot3: Memory temperature hot, DCT3**. See: MemTempHot0.
5	Reserved.
4	**MemTempHot2: Memory temperature hot, DCT2**. See: MemTempHot0.
3	Reserved.
2	**MemTempHot1: Memory temperature hot, DCT1**. See: MemTempHot0.
1	Reserved.
0	**MemTempHot0: Memory temperature hot, DCT0**. Read; Write-1-to-clear. 1=The EVENT_L pin was asserted indicating the memory temperature exceeded the normal operating limit; the DCT may be throttling the interface to aid in cooling. See D18F2xA4.

D18F2xF8 P-state Power Information 1

Read-only.

Bits	Description
31:24	**PwrValue3: P3 power value**. See PwrValue0. Value: Product-specific.
23:16	**PwrValue2: P2 power value**. See PwrValue0. Value: Product-specific.
15:8	**PwrValue1: P1 power value**. See PwrValue0. Value: Product-specific.
7:0	**PwrValue0: P0 power value**. PwrValue and PwrDiv together specify the expected power draw of a single core in P0 and 1/NumCores of the Northbridge in the NB P-state as specified by MSRC001_00[6B:64][NbPstate]. NumCores is defined to be the number of cores per node at cold reset. Value: Product-specific. PwrDiv — Description 00b — PwrValue / 1 W, Range: 0 to 255 W 01b — PwrValue / 10 W, Range: 0 to 25.5 W 10b — PwrValue / 100 W, Range: 0 to 2.55 W 11b — Reserved

D18F2xFC P-state Power Information 2

Read-only.

Bits	Description
31:24	Reserved.

23:22	**PwrDiv7: P7 power divisor**. See D18F2xF8[PwrValue0]. Value: Product-specific.
21:20	**PwrDiv6: P6 power divisor**. See D18F2xF8[PwrValue0]. Value: Product-specific.
19:18	**PwrDiv5: P5 power divisor**. See D18F2xF8[PwrValue0]. Value: Product-specific.
17:16	**PwrDiv4: P4 power divisor**. See D18F2xF8[PwrValue0]. Value: Product-specific.
15:14	**PwrDiv3: P3 power divisor**. See D18F2xF8[PwrValue0]. Value: Product-specific.
13:12	**PwrDiv2: P2 power divisor**. See D18F2xF8[PwrValue0]. Value: Product-specific.
11:10	**PwrDiv1: P1 power divisor**. See D18F2xF8[PwrValue0]. Value: Product-specific.
9:8	**PwrDiv0: P0 power divisor**. See D18F2xF8[PwrValue0]. Value: Product-specific.
7:0	**PwrValue4: P4 power value**. See D18F2xF8[PwrValue0]. Value: Product-specific.

D18F2x104 P-state Power Information 3

Read-only.

Bits	Description
31:24	Reserved.
23:16	**PwrValue7: P7 power value**. See D18F2xF8[PwrValue0]. Value: Product-specific.
15:8	**PwrValue6: P6 power value**. See D18F2xF8[PwrValue0]. Value: Product-specific.
7:0	**PwrValue5: P5 power value**. See D18F2xF8[PwrValue0]. Value: Product-specific.

D18F2x110 DRAM Controller Select Low

Reset: 0000_0000h.

Bits	Description
31:11	Reserved.
10	**MemCleared: memory cleared**. Read-only; updated-by-hardware. 1=Memory has been cleared since the last warm reset. This bit is set by MemClrInit. See MemClrInit.
9	**MemClrBusy: memory clear busy**. Read-only; updated-by-hardware. 1=The memory clear operation in either of the DCTs is in progress. Reads or writes to DRAM while the memory clear operation is in progress result in undefined behavior.
8	**DramEnable: DRAM enabled**. Read-only. 1=All of the used DCTs are initialized (see 2.9.9.5 [DRAM Device Initialization and Training]) or have exited from self refresh (D18F2x90_dct[3:0][ExitSelfRef] transitions from 1 to 0).

7:6	**DctSelIntLvAddr[1:0]: DRAM controller select channel interleave address bit [1:0]**. IF (D18F2x118[LockDramCfg]) THEN Read-only. ELSE Read-write. ENDIF. DctSelIntLvAddr = {D18F2x114[DctSelIntLvAddr[2]], D18F2x110[DctSelIntLvAddr[1:0]]}. BIOS: 100b. Specifies how interleaving is selected between the DCTs. IF (POPCNT(DctIntLvEn) == 2) THEN Bits Description 011b-000b Reserved 100b Address bit [8] 101b Address bit [9] 111b-110b Reserved ELSEIF (POPCNT(DctIntLvEn) == 4) THEN Bits Description 011b-000b Reserved 100b Address bit [9:8] 101b Address bit [10:9] 111b-110b Reserved ENDIF.
5	**DctDatIntLv: DRAM controller data interleave enable**. IF (D18F2x118[LockDramCfg]) THEN Read-only. ELSE Read-write. ENDIF. BIOS: D18F3x44[DramEccEn]. 1=DRAM data bits from every two consecutive 64-bit DRAM lines are interleaved in the ECC calculation such that a dead bit of a DRAM device is correctable.
4	Reserved.
3	**MemClrInit: memory clear initialization**. IF (D18F2x118[LockDramCfg]) THEN Read-only. ELSE Read-write. ENDIF. 1=The node writes 0s to all locations of system memory attached to the node and sets the MemCleared bit. The status of the memory clear operation can be determined by reading the MemClrBusy and MemCleared bits. This command is ignored if MemClrBusy==1 when the command is received. DramEnable must be set before setting MemClrInit. The memory prefetcher must be disabled by setting D18F2x11C[PrefIoDis] and D18F2x11C[PrefCpuDis] before memory clear initialization and then can be re-enabled when MemCleared==1. Channel intereleaving and memory hole remapping must be disabled before setting MemClrInit. See D18F1x2[1,0][C,4][DctIntLvEn] and D18F1x2[1,0][8,0][LgcyMmioHoleEn]. Software must temporarily configure each channel with a Base/Limit register pair, initiate memory clear, then reprogram these to the desired configuration when memory clear is complete.
2	**BankSwapAddr8En: Bank swap to address bit 8 enable**. Read-write. BIOS: (D18F2xA8_dct[3:0][BankSwap] && D18F2x110[DctSelIntLvAddr]==100b). See D18F2xA8_dct[3:0][BankSwap].
1:0	Reserved.

D18F2x114 DRAM Controller Select High

IF (D18F2x118[LockDramCfg]) THEN Read-only. ELSE Read-write. ENDIF. Reset: 0000_0000h.

Bits	Description
31:10	Reserved.

9	**DctSelIntLvAddr[2]: DRAM controller select channel interleave address bit [2]**. See D18F2x110[DctSelIntLvAddr[1:0]].
8:0	Reserved.

D18F2x118 Memory Controller Configuration Low

Fields in this register (bits[17:0]) indicate priority of request types. Variable priority requests enter the memory controller as medium priority and are promoted to high priority if they have not been serviced in the time specified by MctVarPriCntLmt. This feature may be useful for isochronous IO traffic. If isochronous traffic is specified to be high priority, it may have an adverse effect on the bandwidth and performance of the devices associated with the other types of traffic. However, if isochronous traffic is specified as medium priority, the processor may not meet the isochronous bandwidth and latency requirements. The variable priority allows the memory controller to optimize DRAM transactions until isochronous traffic reaches a time threshold and must be serviced more quickly.

Bits	Description
31:28	**MctVarPriCntLmt: variable priority time limit**. Read-write. Reset: 0000b. BIOS: 0001b. Bits / Description / Bits / Description 0000b 80ns 1000b 720ns 0001b 160ns 1001b 800ns 0010b 240ns 1010b 880ns 0011b 320ns 1011b 960ns 0100b 400ns 1100b 1040ns 0101b 480ns 1101b 1120ns 0110b 560ns 1110b 1200ns 0111b 640ns 1111b 1280ns
27	Reserved.
26:24	**McqHiPriByPassMax: memory controller high priority bypass max**. Read-write. Reset: 100b. Specifies the number high-priority operations that are allowed before yielding to medium or low-priority operations. 000b is reserved.
23	Reserved.
22:20	**McqMedPriByPassMax: memory controller medium bypass low priority max**. Read-write. Reset: 100b. Specifies the number of medium-priority operations that are allowed before yielding to low-priority operations. 000b is reserved.

19	**LockDramCfg**. Write-1-only. Reset: 0. BIOS: See 2.9.13 [DRAM CC6/PC6 Storage], 2.5.3.2.3.3 [Core C6 (CC6) State]. The following registers are read-only if LockDramCfg==1; otherwise the access type is specified by the register: • D18F1xF0 [DRAM Hole Address] • D18F2x[5C:40]_dct[3:0] [DRAM CS Base Address] • D18F2x[6C:60]_dct[3:0] [DRAM CS Mask] • D18F2x80_dct[3:0] [DRAM Bank Address Mapping] • D18F2x110 [DRAM Controller Select Low] • D18F2x114 [DRAM Controller Select High] • D18F2x250_dct[3:0] [DRAM Loopback and Training Control] • D18F4x128[CoreStateSaveDestNode] • D18F1x[17C:140,7C:40] [DRAM Base/Limit] • D18F1x120 [DRAM Base System Address] • D18F1x124 [DRAM Limit System Address] • D18F2x118[CC6SaveEn]
18	**CC6SaveEn**. IF (D18F2x118[LockDramCfg]) THEN Read-only. ELSE Read-write. ENDIF. Reset: 0. 1=CC6 save area is enabled. See 2.5.3.2.7 [BIOS Requirements for Initialization]. BIOS: (D18F4x118[PwrGateEnCstAct0] | D18F4x118[PwrGateEnCstAct1] | D18F4x11C[PwrGateEnCstAct2]).
17:16	**MctPriScrub: scrubber priority**. Read-write. Reset: 00b. Bits — Description 00b — Medium 01b — Reserved 10b — High 11b — Variable
15:14	**MctPriTrace: trace-mode request priority**. Read-write. Reset: 10b. See: MctPriCpuRd. This must be set to 10b.
13:12	**MctPriIsoc: display refresh read priority**. Read-write. Reset: 10b. See: MctPriCpuRd.
11:10	**MctPriWr: default write priority**. Read-write. Reset: 01b. See: MctPriCpuRd.
9:8	**MctPriDefault: default non-write priority**. Read-write. Reset: 00b. See: MctPriCpuRd.
7:6	**MctPriIsocWr: IO write with the isochronous bit set priority**. Read-write. Reset: 00b. See: MctPriCpuRd. This does not apply to isochronous traffic that is classified as display refresh.
5:4	**MctPriIsocRd: IO read with the isochronous bit set priority**. Read-write. Reset: 10b. See: MctPriCpuRd. This does not apply to isochronous traffic that is classified as display refresh.
3:2	**MctPriCpuWr: CPU write priority**. Read-write. Reset: 01b. See: MctPriCpuRd.
1:0	**MctPriCpuRd: CPU read priority**. Read-write. Reset: 00b. Bits — Description 00b — Medium 01b — Low 10b — High 11b — Variable

D18F2x11C Memory Controller Configuration High

The two main functions of this register are to control write bursting and memory prefetching.

Write bursting. DctWrLimit and MctWrLimit specify how writes may be burst from the MCT intothe DCT to improve DRAM efficiency. When the number of writes in the MCT reaches the value specified in Mct-WrLimit, then they are all burst to the DCTs at once. Prior to reaching the watermark, a limited number of writes can be passed to the DCTs (specified by DctWrLimit), tagged as low priority, for the DCTs to complete when otherwise idle. Rules regarding write bursting:

- Write bursting mode only applies to low-priority writes. Medium and high priority writes are not withheld from the DCTs for write bursting.
- If write bursting is enabled, writes stay in the MCQ until the threshold specified by MctWrLimit is reached.
- Once the threshold is reached, all writes in MCQ are converted to medium priority.
- Any write in MCQ that matches the address of a subsequent access is promoted to either medium priority or the priority of the subsequent access, whichever is higher.
- DctWrLimit only applies to low-priority writes.

Memory prefetching. The MCT prefetcher detects stride patterns in the stream of requests and then, for predictable stride patterns, generates prefetch requests. A stride pattern is a pattern of requests through system memory that are the same number of cachelines apart. The prefetcher supports strides of -4 to +4 cachelines, which can include alternating patterns (e.g. +1, +2, +1, +2), and can prefetch 1, 2, 3, 4, or 5 cachelines ahead, depending on the confidence. In addition, a fixed stride mode (non-alternating) may be used for IO requests which often have fixed stride patterns. This mode bypasses the stride predictor such that CPU-access stride predictions are not adversely affected by IO streams.

The MCT tracks several stride patterns simultaneously. Each of these has a confidence level associated with it that varies as follows:

- Each time a request is received that matches the stride pattern, the confidence level increases by one.
- Each time a request is received within +/- 4 cachelines of the last requested cacheline in the pattern that does not match the pattern, then the confidence level decreases by one.
- When the confidence level reaches the saturation point specified by PrefConfSat, then it no-longer increments.

Each request that is not within +/- 4 cachelines of the last requested cacheline line of all the stride patterns tracked initiates a new stride pattern by displacing one of the existing least-recently-used stride patterns.

The memory prefetcher uses an adaptive prefetch scheme to adjust the prefetch distance based upon the buffer space available for prefetch request data. The adaptive scheme counts the total number of prefetch requests and the number of prefetch requests that cannot return data because of buffer availability. After every 16 prefetch requests, the prefetcher uses the following rules to adjust the prefetch distance:

- If the ratio of prefetch requests that cannot return data to total prefetch requests is greater than or equal to D18F2x1B0[AdapPrefMissRatio] then the prefetch distance is reduced by D18F2x1B0[AdapPrefNegativeStep].
- If the ratio of prefetch requests that cannot return data to total prefetch requests is less than D18F2x1B0[AdapPrefMissRatio] then the prefetch distance is increased by D18F2x1B0[AdapPrefPositiveStep].
- If the adjusted prefetch distance is greater than the prefetch distance defined for the current confidence level, the prefetch distance for the current confidence level is used.

The adaptive prefetch scheme supports fractional prefetch distances by alternating between two whole number prefetch distances. For example a prefetch distance of 1.25 causes a prefetch distance sequence of: 1, 1, 1, 2, 1, 1, 1, 2.

Bits	Description
31	**MctScrubEn: MCT scrub enable**. Read-write. Reset: 0. 1=Enables periodic flushing of prefetches and writes based on the DRAM scrub rate. This is used to ensure that prefetch and write data aging is not so long that soft errors accumulate and become uncorrectable. When enabled, each DRAM scrub event causes a single prefetch to be de-allocated (the oldest one) and all queued writes to be flushed to DRAM.
30	**FlushWr: flush writes command**. Read; write-1-only; cleared-by-hardware. Reset: 0. Setting this bit causes write bursting to be canceled and all outstanding writes to be flushed to DRAM. This bit is cleared when all writes are flushed to DRAM.
29	**FlushWrOnStpGnt: flush writes on stop-grant**. Read-write. Reset: 0. BIOS: ~D18F2x1B4[FlushWrOnS3StpGnt]. 1=Causes write bursting to be canceled and all outstanding writes to be flushed to DRAM when in the stop-grant state.
28	Reserved.
27:25	**PrefThreeConf: prefetch three-ahead confidence**. Read-write. Reset: 100b. BIOS: 110b. Confidence level required in order to prefetch three cachelines ahead (same encoding as PrefTwoConf below).
24:22	**PrefTwoConf: prefetch two-ahead confidence**. Read-write. Reset: 011b. BIOS: 011b. Confidence level required in order to prefetch two cachelines ahead. Bits — Description 000b — 0 110b-001b — [PrefTwoConf*2] 111b — 14
21:20	**PrefOneConf: prefetch one-ahead confidence**. Read-write. Reset: 10b. BIOS: 10b. Confidence level required in order to prefetch one ahead (0 through 3).
19:18	**PrefConfSat: prefetch confidence saturation**. Read-write. Reset: 00b. BIOS: 00b. Specifies the point at which prefetch confidence level saturates and stops incrementing. Bits — Description 00b — 15 01b — 7 10b — 3 11b — Reserved
17:16	**PrefFixDist: prefetch fixed stride distance**. Read-write. Reset: 00b. Specifies the distance to prefetch ahead if in fixed stride mode. 00b=1 cacheline; 01b=2 cachelines; 10b=3 cachelines; 11b=4 cachelines.
15	**PrefFixStrideEn: prefetch fixed stride enable**. Read-write. Reset: 0. 1=The prefetch stride for all requests (CPU and IO) is fixed (non-alternating).
14	**PrefIoFixStrideEn: Prefetch IO fixed stride enable**. Read-write. Reset: 0. 1=The prefetch stride for IO requests is fixed (non-alternating).
13	**PrefIoDis: prefetch IO-access disable**. Read-write. Reset: 1. BIOS: 0. 1=Disables IO requests from triggering prefetch requests.
12	**PrefCpuDis: prefetch CPU-access disable**. Read-write. Reset: 1. BIOS: 0. 1=Disables CPU requests from triggering prefetch requests.
11:7	**MctPrefReqLimit: memory controller prefetch request limit**. Read-write. Reset: 1Eh. BIOS: 1Dh. Specifies the maximum number of outstanding prefetch requests allowed. See D18F3x78 for restrictions on this field.

6:2	**MctWrLimit: memory controller write-burst limit**. Read-write. Reset: 1Fh. BIOS: 0Ah. Specifies the number of writes in the memory controller queue before they are burst into the DCTs. Bits: Description 00h: 32 1Dh-01h: [32-MctWrLimit] 1Eh: 2 1Fh: Write bursting disabled
1:0	**DctWrLimit: DRAM controller write limit**. Read-write. Reset: 00b. BIOS: 01b. Specifies the maximum number of writes allowed in the DCT queue when write bursting is enabled, prior to when the number of writes in MCQ exceeds the watermark specified by MctWrLimit. Bits: Description 00b: 0 01b: 2 10b: 4 11b: 8

D18F2x1B0 Extended Memory Controller Configuration Low

The main function of this register is to control the memory prefetcher. See D18F2x11C [Memory Controller Configuration High] about the adaptive prefetch scheme.

Table 180: BIOS Recommendations for D18F2x1B[4:0]

Condition	D18F2x1B0	D18F2x1B4	
DdrRate	DcqBwThrotWm	DcqBwThrotWm1	DcqBwThrotWm2
667	0h	3h	4h
800	0h	3h	5h
1066	0h	4h	6h
1333	0h	5h	8h
1600	0h	6h	9h
1866	0h	7h	Ah
2133	0h	8h	Ch

Bits	Description
31:28	**DcqBwThrotWm: dcq bandwidth throttle watermark**. Read-write. Reset: 3h. BIOS: Table 180. Specifies the number of outstanding DRAM read requests before new DRAM prefetch requests and speculative prefetch requests are throttled. 0h=Throttling is disabled. Legal values are 0h through Ch. Programming this field to a non-zero value disables D18F2x1B4[DcqBwThrotWm1, DcqBwThrotWm2].
27:25	**PrefFiveConf: prefetch five-ahead confidence**. Read-write. Reset: 110b. BIOS: 111b. Confidence level required in order to prefetch five cachelines ahead. Bits: Description 000b: 0 110b-001b: [PrefFiveConf*2] 111b: 14

24:22	**PrefFourConf: prefetch four-ahead confidence**. Read-write. Reset: 101b. BIOS: 111b. Confidence level required in order to prefetch four cachelines ahead. Bits Description 000b 0 110b-001b [PrefFourConf*2] 111b 14
21	Reserved.
20	**DblPrefEn: double prefetch enable**. Read-write. Reset: 0. 1=The memory prefetcher only generates prefetch requests when it is able to generate a pair of prefetch requests to consecutive cache lines.
19:18	Reserved.
17:13	Reserved. Reset: 11100b.
12	**EnSplitDctLimits: split DCT write limits enable**. Read-write. Reset: 0. BIOS: 1. 1=The number of writes specified by D18F2x11C[DctWrLimit, MctWrLimit] is per DCT. 0=The number of writes specified by D18F2x11C[DctWrLimit, MctWrLimit] is for the even[0,2] or odd[1,3] DCT channels. 0=The number of writes specified by D18F2x11C[DctWrLimit, MctWrLimit] is total writes independent of DCT. Setting this bit also affects the encoding of D18F2x11C[DctWrLimit].
11	**DisIoCohPref: disable coherent prefetched for IO**. Read-write. Reset: 0. 1=Probes are not generated for prefetches generated for reads from IO devices.
10:8	**CohPrefPrbLmt: coherent prefetch probe limit**. Read-write. Reset: 000b. BIOS: 000b. Specifies the maximum number of probes that can be outstanding for memory prefetch requests. Bits Description 000b Probing disabled for memory prefetch requests 111b-001b Reserved.
7:6	Reserved.
5:4	**AdapPrefNegativeStep: adaptive prefetch negative step**. Read-write. Reset: 00b. BIOS: 00b. Specifies the step size that the adaptive prefetch scheme uses when decreasing the prefetch distance. Bits Description 00b 2/16 01b 4/16 10b 8/16 11b 16/16
3:2	**AdapPrefPositiveStep: adaptive prefetch positive step**. Read-write. Reset: 00b. BIOS: 00b. Specifies the step size that the adaptive prefetch scheme uses when increasing the prefetch distance. Bits Description 00b 1/16 01b 2/16 10b 4/16 11b 8/16
1:0	**AdapPrefMissRatio: adaptive prefetch miss ratio**. Read-write. Reset: 00b. BIOS: 01b. Specifies the ratio of prefetch requests that do not have data buffer available to the total number of prefetch requests at which the adaptive prefetch scheme begins decreasing the prefetch distance. Bits Description 00b 1/16 01b 2/16 10b 4/16 11b 8/16

D18F2x1B4 Extended Memory Controller Configuration High Register

Bits	Description
31	**FlushOnMmioWrEn: flush on mmio write enable**. Read-write. Reset: 0. 1=Any CPU-sourced MMIO write that matches D18F1x[2CC:2A0,1CC:180,BC:80] causes the memory controller data buffers to be flushed to memory.
30:28	**S3SmafId: S3 SMAF id**. Read-write. Reset: 100b. SMAF encoding of D18F3x[84:80] corresponding to the ACPI S3 state when FlushWrOnS3StpGnt==1. Reserved when FlushWrOnS3StpGnt==0.
27	**FlushWrOnS3StpGnt: flush write on S3 stop grant**. Read-write. Reset: 0. BIOS: 1. 1=Write bursting is canceled and all outstanding writes are flushed to DRAM when in the stop-grant state and the SMAF code is equal to S3SmafId, indicating entry into the ACPI S3 state. See D18F2xA8_dct[3:0][FastSelfRefEntryDis], D18F2x11C[FlushWrOnStpGnt].
26	**EnSplitMctDatBuffers: enable split MCT data buffers**. Read-write. Reset: 0. BIOS: 1. 1=Enable resource allocation into the split buffer resources BIOS must program this bit before any DRAM memory accesses are issued from the processor.
25	**SmuCfgLock: SMU configuration lock**. Read-write; updated-by-hardware. Reset: 0. This field should never be cleared by software. The following registers are read-only if LockSmuCfg=1; otherwise the access type is specified by the register: • D18F4x15C [Core Performance Boost Control] • D18F5x12C [Clock Power/Timing Control 4] • D18F5x170 [Northbridge P-state Control] • D18F5x188 [Clock Power/Timing Control 5] • D18F5x170 [Northbridge P-state Control]
24:23	Reserved.
22	**SpecPrefDisWm1: speculative prefetch disable watermark 1**. Read-write. Reset: 0. 0=Disable speculative prefetches at the DcqBwThrotWm2 limit. 1=Disable speculative prefetches at the DcqBwThrotWm1 limit. See also D18F2x1B0[SpecPrefDis].
21	**RegionAlloWm2: region prefetch allocate watermark 2**. Read-write. Reset: 0. See DemandAlloWm2.
20	**RegionPropWm2: region prefetch propagate watermark 2**. Read-write. Reset: 0. See DemandPropWm2.
19	**StrideAlloWm2: stride prefetch allocate watermark 2**. Read-write. Reset: 1. See DemandAlloWm2.
18	**StridePropWm2: stride prefetch propagate watermark 2**. Read-write. Reset: 1. See DemandPropWm2.
17	**DemandAlloWm2: demand request allocate watermark 2**. Read-write. Reset: 1. Specifies the behavior from the DcqBwThrotWm1 limit to the DcqBwThrotWm2 limit. 0=Requests do not allocate a new entry. 1=Requests allocate a new entry; defined only if (DemandAlloWm1 & DemandPropWm2).
16	**DemandPropWm2: demand request propagate watermark 2**. Read-write. Reset: 1. Specifies the behavior from the DcqBwThrotWm1 limit to the DcqBwThrotWm2 limit. 0=Requests do not update existing entries. 1=Requests update existing entries; defined only if (DemandPropWm1==1).
15	**RegionAlloWm1: region prefetch allocate watermark 1**. Read-write. Reset: 0. See DemandAlloWm1.

14	**RegionPropWm1: region prefetch propagate watermark 1**. Read-write. Reset: 1. See DemandPropWm1.
13	**StrideAlloWm1: stride prefetch allocate watermark 1**. Read-write. Reset: 1. See DemandAlloWm1.
12	**StridePropWm1: stride prefetch propagate watermark 1**. Read-write. Reset: 1. See DemandPropWm1.
11	**DemandAlloWm1: demand request allocate watermark 1**. Read-write. Reset: 1. Specifies the behavior prior to the DcqBwThrotWm1 limit. 0=Requests do not allocate a new entry. 1=Requests allocate a new entry; defined only if (DemandPropWm1==1).
10	**DemandPropWm1: demand request propagate watermark 1**. Read-write. Reset: 1. Specifies the behavior prior to the DcqBwThrotWm1 limit. 0=Requests do not update existing entries. 1=Requests update existing entries.
9:5	**DcqBwThrotWm2: DCQ bandwidth throttle watermark 2**. Read-write. Reset: 06h. BIOS: Table 180. Specifies a prefetch throttling watermark based on the number of outstanding DRAM read requests. This field is reserved when D18F2x1B0[DcqBwThrotWm] != 0. When throttling is enabled, if the number of outstanding DRAM read requests exceeds DcqBwThrotWm2 both request allocate and propagate are blocked and new prefetches are disabled. When throttling is enabled, DcqBwThrotWm2 should be programmed to a value greater than DcqBwThrotWm1. 0h=Throttling is disabled. Legal values are 0h through 18h.
4:0	**DcqBwThrotWm1: DCQ bandwidth throttle watermark 1**. Read-write. Reset: 03h. BIOS: Table 180. Specifies a prefetch throttling watermark based on the number of outstanding DRAM read requests. This field is reserved when D18F2x1B0[DcqBwThrotWm] != 0. 0h=Throttling is disabled. Legal values are 0h through 18h.

D18F2x1BC_dct[3:0] DRAM CKE to CS Map

Reset: 0000_AA55h. See 2.9.3 [DCT Configuration Registers].

Table 181: Field Mapping for D18F2x1BC_dct[3:0]

Register	Bits			
	31:24	23:16	15:8	7:0
D18F2x1BC_dct[3:0]	CKE3	CKE2	CKE1	CKE0

Table 182: BIOS Recommendations for D18F2x1BC_dct[3:0]

Condition:		D18F2x1BC_dct[3:0]
Package	NumDimmSlots	
FP3	1, 2	08040201h

Bits	Description
31:24	**CSMapCKE: CS map CKE**. See: D18F2x1BC_dct[3:0][7:0].
23:16	**CSMapCKE: CS map CKE**. See: D18F2x1BC_dct[3:0][7:0].

15:8	**CSMapCKE: CS map CKE**. See: D18F2x1BC_dct[3:0][7:0].
7:0	**CSMapCKE: CS map CKE**. Read-write. BIOS: See Table 182 [BIOS Recommendations for D18F2x1BC_dct[3:0]]. Maps the CS to CKE relationship. 1=This CKE is associated with the listed chip select. 0=This CKE is not associated with the listed chip select. Only even CKEs may be assigned to even CSes. Only odd CKEs may be assigned to odd CSes. Bit — Description [0] — CS0 [1] — CS1 [2] — CS2 [3] — CS3 [7:4] — Reserved

D18F2x200_dct[3:0]_mp[1:0] DDR3 DRAM Timing 0

Reset: 0F05_0505h. See 2.9.3 [DCT Configuration Registers].

Bits	Description
31:30	Reserved.
29:24	**Tras: row active strobe**. Read-write. BIOS: See 2.9.9.3 [SPD ROM-Based Configuration]. Specifies the minimum time in memory clock cycles from an activate command to a precharge command, both to the same chip select bank. Bits — Description 07h-00h — Reserved 2Ah-08h — <Tras> clocks 3Fh-2Bh — Reserved
23:21	Reserved.
20:16	**Trp: row precharge time**. Read-write. BIOS: See 2.9.9.3 [SPD ROM-Based Configuration]. Specifies the minimum time in memory clock cydes from a precharge command to an activate command or auto refresh command, both to the same bank. Bits — Description 04h-00h — Reserved 13h-05h — <Trp> clocks 1Fh-14h — Reserved
15:13	Reserved.
12:8	**Trcd: RAS to CAS delay**. Read-write. BIOS: See 2.9.9.3 [SPD ROM-Based Configuration]. Specifies the time in memory clock cycles from an activate command to a read/write command, both to the same bank. Bits — Description 04h-00h — Reserved 13h-05h — <Trcd> clocks 1Fh-14h — Reserved

7:5	Reserved.
4:0	**Tcl: CAS latency**. Read-write. BIOS: See 2.9.9.3 [SPD ROM-Based Configuration]. Specifies the time in memory clock cycles from the CAS assertion for a read cycle until data return (from the perspective of the DRAM devices). Bits Description 04h-00h Reserved 13h-05h <Tcl> clocks 1Fh-14h Reserved

D18F2x204_dct[3:0]_mp[1:0] DDR3 DRAM Timing 1

Reset: 0400_040Bh. See 2.9.3 [DCT Configuration Registers].

Bits	Description
31:28	Reserved.
27:24	**Trtp: read CAS to precharge time**. Read-write. BIOS: See 2.9.9.3 [SPD ROM-Based Configuration]. Specifies the earliest time in memory clock cycles a page can be closed after having been read. Satisfying this parameter ensures read data is not lost due to a premature precharge. Bits Description 3h-0h Reserved Bh-4h <Trtp> clocks Fh-Ch Reserved
23:22	Reserved.
21:16	**FourActWindow: four bank activate window**. Read-write. BIOS: See 2.9.9.3 [SPD ROM-Based Configuration]. Specifies the rolling tFAW window in memory clock cycles during which no more than 4 banks in an 8-bank device are activated. Bits Description 00h No tFAW window restriction 05h-01h Reserved 2Ch-06h [FourActWindow] clocks 3Fh-2Dh Reserved
15:12	Reserved.
11:8	**Trrd: row to row delay (or RAS to RAS delay)**. Read-write. BIOS: See 2.9.9.3 [SPD ROM-Based Configuration]. Specifies the minimum time in memory clock cycles between activate commands to different chip select banks. Bits Description 0h Reserved 9h-1h <Trrd> clocks Fh-Ah Reserved

7:6	Reserved.
5:0	**Trc: row cycle time.** Read-write. BIOS: See 2.9.9.3 [SPD ROM-Based Configuration]. Specifies the minimum time in memory clock cycles from and activate command to another activate command or an auto refresh command, all to the same chip select bank. Bits: Description 09h-00h: Reserved 3Ah-0Ah: <Trc> clocks 3Fh-3Bh: Reserved

D18F2x208_dct[3:0] DDR3 DRAM Timing 2

See 2.9.3 [DCT Configuration Registers].

Bits	Description
31:27	Reserved.
26:24	**Trfc3: auto refresh row cycle time for CS 6 and 7**. See: Trfc0.
23:19	Reserved.
18:16	**Trfc2: auto refresh row cycle time for CS 4 and 5**. See: Trfc0.
15:11	Reserved.
10:8	**Trfc1: auto refresh row cycle time for CS 2 and 3**. See: Trfc0.
7:3	Reserved.
2:0	**Trfc0: auto refresh row cycle time for CS 0 and 1**. Read-write. Reset: 100b. BIOS: 2.9.9.3 [SPD ROM-Based Configuration]. Specifies the minimum time from a refresh command to the next valid command, except NOP or DES. The recommended programming of this register varies based on DRAM density and speed. Bits: Description 000b: Reserved 001b: 90 ns 010b: 110 ns 011b: 160 ns 100b: 300 ns 101b: 350 ns 111b-110b: Reserved

D18F2x20C_dct[3:0]_mp[1:0] DDR3 DRAM Timing 3

See 2.9.3 [DCT Configuration Registers].

Bits	Description
31:18	Reserved.
17:16	**WrDqDqsEarly: DQ and DQS write early**. Read-write. Reset: 0. Specifies the DQ and DQS launch timing for write commands relative to the Tcwl MEMCLK. Bits: Description 00b: 0 MEMCLK early 01b: 0.5 MEMCLK early 10b: Reserved 11b: Reserved

15:12	Reserved.
11:8	**Twtr: internal DRAM write to read command delay**. Read-write. Reset: 4h. BIOS: See 2.9.9.3 [SPD ROM-Based Configuration]. Specifies the minimum number of memory clock cycles from a write operation to a read operation, both to the same chip select. This is measured from the rising clock edge following last non-masked data strobe of the write to the rising clock edge of the next read command. Bits: Description 3h-0h: Reserved Bh-4h: <Twtr> clocks Fh-Ch: Reserved
7:5	Reserved.
4:0	**Tcwl: CAS write latency.** Read-write. Reset: 05h. BIOS: See 2.9.9.3 [SPD ROM-Based Configuration]. Specifies the number of memory clock cycles from internal write command to first write data in at the DRAM. Bits: Description 04h-00h: Reserved 0Ah-05h: <Tcwl> clocks 1Fh-0Bh: Reserved

D18F2x210_dct[3:0]_nbp[3:0] DRAM NB P-state

See 2.9.3 [DCT Configuration Registers]. For D18F2x210_dct[3:0]_nbp[x], x=D18F1x10C[NbPsSel]; see D18F1x10C[NbPsSel].

Bits	Description
31:22	**MaxRdLatency: maximum read latency**. Read-write. Reset: 000h. BIOS: See 2.9.9.6 [DRAM Training]. Specifies the maximum round-trip latency in the system from the processor to the DRAM devices and back. The DRAM controller uses this to help determine when the first two beats of incoming DRAM read data can be safely transferred to the NCLK domain. The time includes the asynchronous and synchronous latencies. Bits: Description 000h: 0 NCLKs 3FEh-001h: <MaxRdLatency> NCLKs 3FFh: 1023 NCLKs
21:19	Reserved.
18:16	**DataTxFifoWrDly: data transmit FIFO write delay**. Read-write. Reset: 0. Specifies the DCT to phy write data FIFO delay. Bits: Description 000b: 0 MEMCLK 001b: 0.5 MEMCLK 010b: 1.0 MEMCLK 011b: 1.5 MEMCLKs 100b: 2.0 MEMCLKs 101b: 2.5 MEMCLKs 110b: 3.0 MEMCLKs 111b: Reserved
15:0	Reserved.

D18F2x214_dct[3:0]_mp[1:0] DDR3 DRAM Timing 4

Reset: 0001_0202h.

Bits	Description
31:20	Reserved.
19:16	**TwrwrSdSc: write to write timing same DIMM same chip select**. Read-write. BIOS: See 2.9.9.4.1.2 [TwrwrSdSc, TwrwrSdDc, TwrwrDd (Wr->Wr Timing)]. Specifies the minimum number of cycles from the last clock of virtual CAS of the first write-burst operation to the clock in which CAS is asserted for a following write-burst operation. Bits — Description 0h — Reserved 1h — 1 clock Ah-2h — <TwrwrSdSc> clocks Bh — 11 clocks Fh-Ch — Reserved
15:12	Reserved.
11:8	**TwrwrSdDc: write to write timing same DIMM different chip select**. See: TwrwrDd.
7:4	Reserved.
3:0	**TwrwrDd: write to write timing different DIMM**. Read-write. BIOS: See 2.9.9.4.1.2 [TwrwrSdSc, TwrwrSdDc, TwrwrDd (Wr->Wr Timing)]. Specifies the minimum number of cycles from the last clock of virtual CAS of the first write-burst operation to the clock in which CAS is asserted for a following write-burst operation. Bits — Description 1h-0h — Reserved Bh-2h — <TwrwrDd> clocks Fh-Ch — Reserved

D18F2x218_dct[3:0]_mp[1:0] DDR3 DRAM Timing 5

Reset: 0103_0203h. See 2.9.3 [DCT Configuration Registers].

Bits	Description
31:30	**TrdrdBan: read to read timing ban**. Read-write. BIOS: See 2.9.9.4.1 [DDR3 Turnaround Parameters]. Bans the traffic for the specified cases where the number of cycles from the last clock of virtual CAS of a first read-burst operation to the clock in which CAS is asserted for a following read-burst operation. Bits — Description 00b — Ban disabled, traffic allowed as specified by TrdrdSdSc, TrdrdSdDc, TrdrdDd. 01b — Ban Trdrd traffic at 2 MEMCLKs. 10b — Ban Trdrd traffic at 2 and 3 MEMCLKs. 11b — Reserved
29:28	Reserved.

27:24	**TrdrdSdSc: read to read timing same DIMM same chip select**. Read-write. BIOS: See 2.9.9.4.1.1 [TrdrdBan, TrdrdSdSc, TrdrdSdDc, and TrdrdDd (Rd->Rd Timing)]. Specifies the minimum number of cycles from the last clock of virtual CAS of a first read-burst operation to the clock in which CAS is asserted for a following read-burst operation. Bits Description 0h Reserved Bh-1h <TrdrdSdSc> clocks Fh-Ch Reserved
23:20	Reserved.
19:16	**TrdrdSdDc: read to read timing same DIMM different chip select**. See: TrdrdDd.
15:12	Reserved.
11:8	**Twrrd: write to read DIMM termination turnaround.** Read-write. BIOS: See 2.9.9.4.1.3 [Twrrd (Write to Read DIMM Termination Turn-around)]. Specifies the minimum number of cycles from the last clock of virtual CAS of the first write-burst operation to the clock in which CAS is asserted for a following read-burst operation, both to different chip selects. Bits Description 0h Reserved Bh-1h <Twrrd> clocks Fh-Ch Reserved
7:4	Reserved.
3:0	**TrdrdDd: read to read timing different DIMM**. Read-write. BIOS: See 2.9.9.4.1.1 [TrdrdBan, TrdrdSdSc, TrdrdSdDc, and TrdrdDd (Rd->Rd Timing)]. Specifies the minimum number of cycles from the last clock of virtual CAS of a first read-burst operation to the clock in which CAS is asserted for a following read-burst operation. Bits Description 1h-0h Reserved Bh-2h <TrdrdDd> clocks Fh-Ch Reserved

D18F2x21C_dct[3:0]_mp[1:0] DDR3 DRAM Timing 6

Reset: 0004_0300h. See 2.9.3 [DCT Configuration Registers].

Bits	Description
31:21	Reserved.
20:16	**TrwtWB: read to write turnaround for opportunistic write bursting.** Read-write. BIOS: TrwtTO + 1. Specifies the minimum number of clock cycles from the last clock of virtual CAS of a first read-burst operation to the clock in which CAS is asserted for a following write-burst operation. Bits Description 02h-00h Reserved 1Ch-03h <TrwtWB> clocks 1Fh-1Dh Reserved
15:13	Reserved.

12:8	**TrwtTO: read to write turnaround.** Read-write. BIOS: See 2.9.9.4.1.4 [TrwtTO (Read-to-Write Turnaround for Data, DQS Contention)]. Specifies the minimum number of clock cycles from the last clock of virtual CAS of a first read-burst operation to the clock in which CAS is asserted for a following write-burst operation. Bits Description 01h-00h Reserved 1Bh-02h <TrwtTO> clocks 1Fh-1Ch Reserved
7:0	Reserved.

D18F2x220_dct[3:0] DDR3 DRAM Timing 7

Reset: 0000_0C04h. See 2.9.3 [DCT Configuration Registers].

Bits	Description
31:13	Reserved.
12:8	**Tmod: mode register command delay.** Read-write. BIOS: See 2.9.9.3 [SPD ROM-Based Configuration]. Specifies the minimum time in memory clock cycles from an MRS command to another non-MRS command (excluding NOP and DES), all to the same chip select. Bits Description 01h-00h Reserved 14h-02h <Tmod> clocks 1Fh-15h Reserved
7:4	Reserved.
3:0	**Tmrd: mode register command cycle time.** Read-write. BIOS: See 2.9.9.3 [SPD ROM-Based Configuration]. Specifies the minimum time in memory clock cycles from an MRS command to another MRS command, all to the same chip select. Bits Description 1h-0h Reserved 8h-2h <Tmrd> clocks Fh-9h Reserved

D18F2x224_dct[3:0] DDR3 DRAM Timing 8

Reset: 0000_0408h. See 2.9.3 [DCT Configuration Registers].

Bits	Description
31:11	Reserved.
10:8	**Tzqcs: Zq short cal command delay.** Read-write. BIOS: See 2.9.9.3 [SPD ROM-Based Configuration]. Specifies the minimum time in memory clock cycles from a ZQCS command to any other command (excluding NOP and DES) on the channel. Bits Description Bits Description 000b Reserved 100b 64 clocks 001b 16 clocks 101b 80 clocks 010b 32 clocks 110b 96 clocks 011b 48 clocks 111b Reserved

7:4	Reserved.
3:0	**Tzqoper: Zq long cal command delay.** Read-write. BIOS: See 2.9.9.3 [SPD ROM-Based Configuration]. Specifies the minimum time in memory clock cycles from a ZQCL command to any other command (excluding NOP and DES) on the channel. Bits: Description 0000b: Reserved 0001b: 32 clocks 0010b: 64 clocks 0011b: 96 clocks 0100b: 128 clocks 0101b: 160 clocks 0110b: 192 clocks 0111b: 224 clocks 1000b: 256 clocks 1001b: 288 clocks 1010b: 320 clocks 1011b: 352 clocks 1100b: 384 clocks 1111b-1101b: Reserved

D18F2x228_dct[3:0] DDR3 DRAM Timing 9

See 2.9.3 [DCT Configuration Registers].

Bits	Description
31:24	Reserved.
23:16	Reserved.
15:8	**Tstag1: auto refresh stagger time for logical DIMM 1**. See: Tstag0.
7:0	**Tstag0: auto refresh stagger time for logical DIMM 0**. Read-write. Reset: 00h. BIOS: MAX(D18F2x204_dct[3:0]_mp[1:0][Trrd], CEIL(D18F2x204_dct[3:0]_mp[1:0][FourActWindow]/4)). Specifies the number of clocks between auto refresh commands to different ranks of a DIMM when D18F2x90_dct[3:0][StagRefEn]=1. Bits: Description 00h: 0 clocks FEh-01h: <Tstag0> clocks FFh: 255 clocks

D18F2x22C_dct[3:0]_mp[1:0] DDR3 DRAM Timing 10

Reset: 0000_000Ch. See 2.9.3 [DCT Configuration Registers].

Bits	Description
31:24	Reserved.
23:13	Reserved.
12:8	Reserved.

7:5	Reserved.
4:0	**Twr: write recovery**. Read-write. BIOS: See 2.9.9.3. Specifies the minimum time from the last data write until the chip select bank precharge. Bits — Description 04h-00h — Reserved 08h-05h — 8 to 5 clocks 09h — Reserved 0Ah — 10 clocks 0Bh — Reserved 0Ch — 12 clocks 0Dh — Reserved 0Eh — 14 clocks 0Fh — Reserved 10h — 16 clocks 11h — Reserved 12h — 18 clocks 1Fh-13h — Reserved

D18F2x[234:230]_dct[3:0] DDR3 DRAM Read ODT Pattern [High:Low]

Reset: 0000_0000h. See 2.9.3 [DCT Configuration Registers]. This register is used by BIOS to specify the state of the ODT pins during DDR reads. F2x230 is used to control chip selects 0-3. F2x234 is used to control chip selects 4-7.

Table 183: Field Mapping for D18F2x[234:230]_dct[3:0]

Register	Bits			
	27:24	19:16	11:8	3:0
D18F2x230_dct[3:0]	CS3	CS2	CS1	CS0
D18F2x234_dct[3:0]	CS7	CS6	CS5	CS4

See 2.9.9.3.1 [DRAM ODT Pin Control] for more information.

Bits	Description
31:28	Reserved.
27:24	**RdOdtPatCs73: read ODT pattern chip select [7,3]**. See: RdOdtPatCs40.
23:20	Reserved.
19:16	**RdOdtPatCs62: read ODT pattern chip select [6,2]**. See: RdOdtPatCs40.
15:12	Reserved.
11:8	**RdOdtPatCs51: read ODT pattern chip select [5,1]**. See: RdOdtPatCs40.
7:4	Reserved.
3:0	**RdOdtPatCs40: read ODT pattern chip select [4,0]**. Read-write. Specifies the state of ODT[3:0] pins when a read occurs to the specified chip select.

D18F2x[23C:238]_dct[3:0] DDR3 DRAM Write ODT Pattern [High:Low]

Reset: 0000_0000h. See 2.9.3 [DCT Configuration Registers]. This register is used by BIOS to specify the state of the ODT pins during DDR writes. F2x238 is used to control chip selects 0-3. F2x23C is used to control chip selects 4-7.

Table 184: Field Mapping for D18F2x[23C:238]_dct[3:0]

Register	Bits			
	27:24	19:16	11:8	3:0
D18F2x238_dct[3:0]	CS3	CS2	CS1	CS0
D18F2x23C_dct[3:0]	CS7	CS6	CS5	CS4

See 2.9.9.3.1 [DRAM ODT Pin Control] for more information.

Bits	Description
31:28	Reserved.
27:24	**WrOdtPatCs73: write ODT pattern chip select [7,3]**. See: WrOdtPatCs40.
23:20	Reserved.
19:16	**WrOdtPatCs62: write ODT pattern chip select [6,2]**. See: WrOdtPatCs40.
15:12	Reserved.
11:8	**WrOdtPatCs51: write ODT pattern chip select [5,1]**. See: WrOdtPatCs40.
7:4	Reserved.
3:0	**WrOdtPatCs40: write ODT pattern chip select [4,0]**. Read-write. Specifies the state of ODT[3:0] pins when a write occurs to the specified chip select.

D18F2x240_dct[3:0]_mp[1:0] DDR3 DRAM ODT Control

Reset: 0000_0000h. See 2.9.3 [DCT Configuration Registers].

Bits	Description
31:15	Reserved.
14:12	**WrOdtOnDuration: write ODT on duration.** Read-write. BIOS: 6. Specifies the number of memory clock cycles that ODT is asserted for writes. Bits — Description 5h-0h — Reserved 7h-6h — <WrOdtOnDuration> clocks
11	Reserved.
10:8	**WrOdtTrnOnDly: Write ODT Turn On Delay.** Read-write. BIOS: 0. Specifies the number of memory clock cycles that ODT assertion is delayed relative to write CAS. Bits — Description 0h — 0 clocks 7h-1h — <WrOdtTrnOnDly> clocks, Reserved if (WrOdtOnDuration=0)

7:4	**RdOdtOnDuration: Read ODT On Duration.** Read-write. BIOS: 6. Specifies the number of memory clock cycles that ODTis asserted for an eight-beat read burst. The controller will shorten the ODT pulse duration by two clock cycles if the burst is chopped. Bits Description 5h-0h Reserved 9h-6h <RdOdtOnDuration> clocks Fh-Ah Reserved
3:0	**RdOdtTrnOnDly: Read ODT Turn On Delay.** Read-write. BIOS: MAX(0, D18F2x200_dct[3:0]_mp[1:0][Tcl] - D18F2x20C_dct[3:0]_mp[1:0][Tcwl]). Specifies the number of clock cycles that ODT assertion is delayed relative to read CAS. Bits Description 0h 0 clocks Fh-1h <RdOdtTrnOnDly> clocks, Reserved if (RdOdtOnDuration=0)

D18F2x244_dct[3:0] DRAM Controller Miscellaneous 3

Reset: 0000_0000h. See 2.9.3 [DCT Configuration Registers].

Bits	Description
31:8	Reserved.
7:4	Reserved.
3:0	**PrtlChPDDynDly: partial channel power down dynamic delay**. Read-write. BIOS: 4h. Specifies the channel idle hysteresis for fast exit/slow exit mode changes when D18F2xA8_dct[3:0][PrtlChPDEnhEn]==1. Bits Description 0h 0 clocks 7h-1h <PrtlChPDDynDly*32> clocks 8h 256 clocks Fh-9h Reserved

D18F2x248_dct[3:0]_mp[1:0] DRAM Power Management 0

Reset: 0000_0A03h. See 2.9.3 [DCT Configuration Registers].

Bits	Description
31	Reserved.
30	Reserved.
29:24	**AggrPDDelay: aggressive power down delay**. Read-write. BIOS: 20h. Specifies a hysteresis count from the last DRAM activity for the DCT to close pages prior to precharge power down. Reserved if D18F2xA8_dct[3:0][AggrPDEn]==0. See PchgPDEnDelay and D18F2x94_dct[3:0][PowerDownEn]. Bits Description 00h 64 clocks 01h 1 clock 3Eh-02h <AggrPDDelay> clocks 3Fh 63 clocks
23:22	Reserved.

21:16	**PchgPDEnDelay: precharge power down entry delay**. Read-write. BIOS: IF (D18F2xA8_dct[3:0][AggrPDEn]) THEN (MaxRxCmdDelay + 5). ELSE 00h. ENDIF. (See 2.9.9.2.11 for information on MaxRxCmdDelay). Specifies the power down entry delay. If D18F2xA8_dct[3:0][AggrPDEn]==0, this delay behaves as a hysteresis. This field must satisfy the minimum power down entry delay requirements. See also D18F2x94_dct[3:0][PowerDownEn]. PchgPDEnDelay == 0 || PchgPDEnDelay >= MaxRxCmdDelay + 5. See 2.9.9.2.11 for information on MaxRxCmdDelay. Bits: Description 00h: 64 clocks 01h: 1 clock 3Eh-02h: <PchgPDEnDelay> clocks 3Fh: 63 clocks
15:13	Reserved.
12:8	**Txpdll: exit DLL and precharge powerdown to command delay**. Read-write. Specifies the minimum time that the DCT waits to issue a command after exiting precharge powerdown mode if the DLL was also disabled. Reserved if !Ddr3Mode. Bits: Description 09h-00h: Reserved 1Dh-0Ah: <Txpdll> clocks 1Fh-1Eh: Reserved
7:4	Reserved.
3:0	**Txp: exit precharge PD to command delay**. Read-write. Specifies the minimum time that the DCT waits to issue a command after exiting precharge powerdown mode. Bits: Description 2h-0h: Reserved 8h-3h: <Txp> clocks Fh-9h: Reserved

D18F2x24C_dct[3:0] DDR3 DRAM Power Management 1

Reset: 0214_0803h.See 2.9.3 [DCT Configuration Registers].

Bits	Description
31:30	Reserved.
29:24	**Tcksrx: clock stable to self refresh exit delay**. Read-write. Specifies the minimum time in memory clock cycles that the DCT waits to assert CKE after clock frequency is stable. Bits: Description 01h-00h: Reserved 0Eh-02h: <Tcksrx> clocks 3Fh-0Fh: Reserved
23:22	Reserved.

21:16	**Tcksre: self refresh to command delay**. Read-write. Specifies the minimum time in memory clock cycles that the DCT waits to remove external clocks after entering self refresh or powerdown. Bits Description 04h-00h Reserved 27h-05h <Tcksre> clocks 3Fh-28h Reserved
15:14	Reserved.
13:8	**Tckesr: self refresh to command delay**. Read-write. Specifies the minimum time in memory clock cycles that the DCT waits to issue a command after entering self refresh. Bits Description 01h-00h Reserved 2Bh-02h <Tckesr> clocks 3Fh-2Ch Reserved
7:4	Reserved.
3:0	**Tpd: minimum power down entry to exit**. Read-write. Specifies minimum time in memory clock cycles for powerdown entry to exit timing. Bits Description 0h Reserved Ah-1h <Tpd> clocks Fh-Bh Reserved

D18F2x250_dct[3:0] DRAM Loopback and Training Control

Reset: 0000_0000h. See 2.9.3 [DCT Configuration Registers]. See 2.9.10 [Continuous Pattern Generation].

Bits	Description
31:21	Reserved.
20:17	Reserved.
16	Reserved.
15	Reserved.
14	Reserved.
13	**LfsrRollOver: LFSR roll over**. IF (D18F2x118[LockDramCfg]) THEN Read-only. ELSE Read-write. ENDIF. Specifies the behavior of DataPrbsSeed and the data comparison logic if the generated address wraps around to equal D18F2x25[8,4]_dct[3:0][TgtAddress]. 0=The PRBS will not be re-seeded. 1=The PRBS will be re-seeded.
12	**CmdSendInProg: command in progress**. Read-only; updated-by-hardware. 0=DCT is idle. 1=DCT is busy.
11	**SendCmd: send command**. IF (D18F2x118[LockDramCfg]) THEN Read-only. ELSE Read-write. ENDIF. 0=Stop command generation. 1=Begin command generation as specified in CmdTgt, Cmd-Type, and D18F2x260_dct[3:0][CmdCount]. BIOS must set this field to a 0 after acommand series is completed. Reserved if ~CmdTestEnable.
10	**TestStatus: test status**. Read-only. 0=Command generation is in progress. 1=Command generation has completed. Reserved if ~(SendCmd & (D18F2x260_dct[3:0][CmdCount] > 0 | StopOnErr)).

9:8	**CmdTgt: command target**. IF (D18F2x118[LockDramCfg]) THEN Read-only. ELSE Read-write. ENDIF. Specifies the SendCmd command target address mode. See D18F2x25[8,4]_dct[3:0]. Bits: Description 00b: Issue commands to address Target A 01b: Issue alternating commands to address Target A and Target B 11b-10b: Reserved
7:5	**CmdType: command type**. IF (D18F2x118[LockDramCfg]) THEN Read-only. ELSE Read-write. ENDIF. Specifies the SendCmd command type. Bits: Description 000b: Read 001b: Write 010b: Alternating write and read 111b-011b: Reserved
4	**StopOnErr: stop on error**. IF (D18F2x118[LockDramCfg]) THEN Read-only. ELSE Read-write. ENDIF. Specifies the DCT behavior if a data comparison error occurs. 1=Stop command generation. 0=Continue command generation. If StopOnErr==1, BIOS must program ResetAllErr=1 when programming SendCmd=1.
3	**ResetAllErr: reset all errors**. IF (D18F2x118[LockDramCfg]) THEN Read-only. ELSE Read; write-1-only; cleared-by-hardware. ENDIF. 1=Clear error status bits and error counters in D18F2x264_dct[3:0], D18F2x268_dct[3:0], and D18F2x26C_dct[3:0].
2	**CmdTestEnable: command test enable**. IF (D18F2x118[LockDramCfg]) THEN Read-only. ELSE Read-write. ENDIF. 0=Disable the command generation mode. 1=Enable the command generation mode. See SendCmd. Software must disable data scrambling before using this logic to generate patterns. See D18F2xB60_dct[3:0][DataScrambleEn].
1:0	Reserved.

D18F2x25[8,4]_dct[3:0] DRAM Target [B, A] Base

Reset: 0000_0000h. See 2.9.3 [DCT Configuration Registers]. See 2.9.10 [Continuous Pattern Generation].

Table 185: Register Mapping for D18F2x25[8,4]_dct[3:0]

Register	Function
D18F2x254_dct[3:0]	Target A
D18F2x258_dct[3:0]	Target B

Bits	Description
31:27	Reserved.
26:24	**TgtChipSelect: target chip select**. Read-write. Specifies the chip select. Bits: Description 111b-000b: CS<TgtChipSelect>
23:20	**TgtBank: target bank [3:0]**. Read-write. Specifies the bank address. If Ddr3Mode then TgtBank[3] is ignored.
19:16	Reserved.

15:10	**TgtAddress[15:10]: target address [15:10]**. Read-write. Specifies the upper column address bits [15:10]. Software must always program bit [10] and bit [12] equal to 0.
9:0	**TgtAddress[9:0]: target address [9:0]**. Read-write. Specifies the column address bits [9:0]. The address sequencing in a command series occurs as follows: TgtAddress[9:3] is incremented by one with wrap around. The increment occurs after each command if D18F2x250_dct[3:0][CmdType] == 00xb or if (D18F2x250_dct[3:0][CmdType] == 010b and D18F2x250_dct[3:0][CmdTgt] == 01b). The increment occurs after each command pair if (D18F2x250_dct[3:0][CmdType] == 010b and D18F2x250_dct[3:0][CmdTgt] == 00b).

D18F2x25C_dct[3:0] DRAM Command 0

Reset: 0000_0001h. See 2.9.3 [DCT Configuration Registers]. See 2.9.10 [Continuous Pattern Generation].

Bits	Description
31:22	**BubbleCnt2: bubble count 2**. See: BubbleCnt. Specifies the number of NOP commands inserted after the last clock of virtual CAS of each read-burst operation in alternating write and read mode. Defined only if (D18F2x250_dct[3:0][CmdType] == 010b); otherwise reserved.
21:12	**BubbleCnt: bubble count**. Read-write. Specifies the number of NOP commands inserted after the last clock of virtual CAS of the last command of the command stream specified by CmdStreamLen. Bits — Description 000h — 0 command bubbles 3FEh-001h — <BubbleCnt> command bubbles 3FFh — 3FFh command bubbles
11:9	Reserved.
8	**CmdTimingEn: command timing enable**. Read-write. 1=Forces DCT to schedule commands initiated by D18F2x250_dct[3:0][SendCmd] to adhere to the same DRAM timing parameters as normal traffic. 0=Commands initiated by D18F2x250_dct[3:0][SendCmd] ignore DRAM timing parameters.
7:0	**CmdStreamLen: command stream length**. Read-write. Specifies the number of commands generated before BubbleCnt bubbles are inserted. Bits — Description 00h — Reserved 01h — 1 command FEh-02h — <CmdStreamLen> commands; defined only if ~(D18F2x250_dct[3:0][CmdType]==010b) FFh — 255 commands; defined only if ~(D18F2x250_dct[3:0][CmdType]==010b)

D18F2x260_dct[3:0] DRAM Command 1

Reset: 0000_0000h. See 2.9.3 [DCT Configuration Registers]. See 2.9.10 [Continuous Pattern Generation].

Bits	Description
31:21	Reserved.
20:0	**CmdCount: command count**. Read-write. Specifies the maximum number of commands to generate when D18F2x250_dct[3:0][SendCmd]==1. See also D18F2x250_dct[3:0][StopOnErr]. Bits — Description 00_0000h — Infinite commands. 1F_FFFFh-00_0001h — <CmdCount> commands

D18F2x264_dct[3:0] DRAM Status 0

Reset: 0000_0000h. See 2.9.3 [DCT Configuration Registers]. See 2.9.10 [Continuous Pattern Generation].

Bits	Description
31:25	**ErrDqNum: error DQ number**. Read-only. Indicates the DQ bit of the first error occurrence when D18F2x264_dct[3:0][ErrCnt] > 0. Cleared by D18F2x250_dct[3:0][ResetAllErr]. Bits: Description 3Fh-00h: Data[<ErrDqNum>] 47h-40h: ECC[7:0] 7Fh-48h: Reserved
24:0	**ErrCnt: error count**. Read; set-by-hardware; write-1-to-clear. Specifies a saturating counter indicating the number of DQ bit errors detected. Counts a maximum of 1 error per bit-lane per each bit-time. Status is accumulated until cleared by D18F2x250_dct[3:0][ResetAllErr]. Errors can be masked on per-bit basis by programming D18F2x274_dct[3:0], D18F2x278_dct[3:0], and D18F2x27C_dct[3:0]. Bits: Description 000_0000h: 0 errors 1FF_FFFDh-000_0001h: <ErrCnt> errors 1FF_FFFEh: 1FF_FFFEh errors 1FF_FFFFh: 1FF_FFFFh or more errors

D18F2x268_dct[3:0] DRAM Status 1

Reset: 0000_0000h. See 2.9.3 [DCT Configuration Registers]. See 2.9.10 [Continuous Pattern Generation].

Bits	Description
31:20	Reserved.
19:0	**NibbleErrSts: nibble error status**. Read-only. Indicates error detection status on a per nibble basis when D18F2x264_dct[3:0][ErrCnt] > 0. Status is accumulated until cleared by D18F2x250_dct[3:0][ResetAllErr]. Bit: Description [15:0]: Data[<(NibbleErrSts*4)+3>:<NibbleErrSts*4>] [16]: ECC[3:0] [17]: ECC[7:4] [19:18]: Reserved

D18F2x26C_dct[3:0] DRAM Status 2

Reset: 0000_0000h. See 2.9.3 [DCT Configuration Registers]. See 2.9.10 [Continuous Pattern Generation].

Bits	Description

31:18	Reserved.
17:0	**NibbleErr180Sts: nibble error 180 status**. Read-only. Indicates error detection status on a per nibble basis when D18F2x264_dct[3:0][ErrCnt] > 0, comparing read data against data shifted 1-bit time earlier. Status is accumulated until cleared by D18F2x250_dct[3:0][ResetAllErr]. Bit Description [15:0] Data[<(NibbleErr180Sts]*4)+3>:<NibbleErr180Sts*4>] [16] ECC[3:0] [17] ECC[7:4]

D18F2x270_dct[3:0] DRAM PRBS

See 2.9.3 [DCT Configuration Registers]. See 2.9.10 [Continuous Pattern Generation].

Bits	Description
31	Reserved.
30:24	Reserved.
23:19	Reserved.
18:0	**DataPrbsSeed: data PRBS seed**. Read-write. Reset: 7FFFFh. Specifies the seed value used for creating pseudo random traffic on the data bus. This register must be written with a non-zero seed value.

D18F2x274_dct[3:0] DRAM DQ Mask Low

See D18F1x10C[DctCfgSel]. See 2.9.3 [DCT Configuration Registers]. See 2.9.10 [Continuous Pattern Generation].

Bits	Description
31:0	**DQMask[31:0]: DQ mask**. Read-write. DQMask[63:0] = {D18F2x278_dct[3:0][DQMask[63:32]], DQMask[31:0]}. Reset: 0000_0000_0000_0000h. 1=The corresponding DQ bit will not be compared. 0=The corresponding DQ bit will be compared. See D18F2x264_dct[3:0][ErrCnt]. Bit Description [0] Data[0] [62:1] Data[<DQMask>] [63] Data[63]

D18F2x278_dct[3:0] DRAM DQ Mask High

Bits	Description
31:0	**DQMask[63:32]: DQ mask**. See: D18F2x274_dct[3:0][DQMask[31:0]].

D18F2x27C_dct[3:0] DRAM ECC and EDC Mask

Reset: 0000_0000h. See 2.9.3 [DCT Configuration Registers]. See 2.9.10 [Continuous Pattern Generation].

Bits	Description
31:20	Reserved.

19:16	Reserved.
15:8	Reserved.
7:0	**EccMask: ECC mask**. Read-write. 1=The corresponding ECC DQ bit will not be compared. 0=The corresponding ECC DQ bit will be compared. See D18F2x264_dct[3:0][ErrCnt]. Bit Description [0] ECC[0] [6:1] ECC[<EccMask>] [7] ECC[7].

D18F2x28C_dct[3:0] DRAM Command 2

Reset: 0000_0000h. See 2.9.3 [DCT Configuration Registers]. See 2.9.10 [Continuous Pattern Generation]. This register may only be used when D18F2x250_dct[3:0][CmdTestEnable]=1.

Bits	Description
31	**SendActCmd: send activate command**. Read; write-1-only; cleared-by-hardware. 1=The DCT sends an activate command as specified by ChipSelect, Bank, and Address. This bit is cleared by hardware after the command completes.
30	**SendPchgCmd: send precharge all command**. Read; write-1-only; cleared-by-hardware. The DCT sends a precharge command based on CmdAddress[10]. This bit is cleared by hardware after the command completes. 0=Command has completed. 1=If (CmdAddress[10]==1) then send a precharge all command as specified by CmdChipSelect; If (CmdAddress[10]==0) then send a precharge command as specified by CmdChipSelect, CmdBank.
29:22	**CmdChipSelect: command chip select**. Read-write. Specifies the chip select. Bit Description [7:0] CS<CmdChipSelect>
21:18	**CmdBank: command bank [3:0]**. Read-write. Specifies the bank address. Bits Description 7h-0h Bank<CmdBank> Fh-8h Reserved.
17:0	**CmdAddress: command address [17:0]**. Read-write. Specifies the row address.

D18F2x290_dct[3:0] DRAM Status 3

Reset: 0000_0000h. See 2.9.3 [DCT Configuration Registers]. See 2.9.10 [Continuous Pattern Generation].

Bits	Description
31:27	Reserved.
26:24	**ErrBeatNum: error beat number**. Read-only. Indicates the data beat of the first error occurrence in the command reported by ErrCmdNum when D18F2x264_dct[3:0][ErrCnt] > 0 and D18F2x260_dct[3:0][CmdCount] > 0. Cleared by D18F2x250_dct[3:0][ResetAllErr]. Bits Description 7h-0h <ErrBeatNum> beat

23:21	Reserved.
20:0	**ErrCmdNum: error command number**. Read-only. Indicates the command number of the first error occurrence when D18F2x264_dct[3:0][ErrCnt] > 0 and D18F2x260_dct[3:0][CmdCount] > 0. Cleared by D18F2x250_dct[3:0][ResetAllErr]. Bits Description 1F_FFFFh-00_0000h <ErrCmdNum> command

D18F2x294_dct[3:0] DRAM Status 4

See 2.9.3 [DCT Configuration Registers]. See 2.9.10 [Continuous Pattern Generation].

Bits	Description
31:0	**DQErr[31:0]: DQ error**. Read-only. DQErr[63:0] = {D18F2x298_dct[3:0][DQErr[63:32]], DQErr[31:0]}. Reset: 0000_0000_0000_0000h. Indicates error detection status on a per bit basis when D18F2x264_dct[3:0][ErrCnt] > 0. Status is accumulated until cleared by D18F2x250_dct[3:0][ResetAllErr]. Bit Description [0] Data[0] [62:1] Data[<DQErr>] [63] Data[63]

D18F2x298_dct[3:0] DRAM Status 5

Bits	Description
31:0	**DQErr[63:32]: DQ error**. See: D18F2x294_dct[3:0][DQErr[31:0]].

D18F2x29C_dct[3:0] DRAM Status 6

Reset: 0000_0000h. See 2.9.3 [DCT Configuration Registers]. See 2.9.10 [Continuous Pattern Generation].

Bits	Description
31:20	Reserved.
19:16	Reserved.
15:8	Reserved.
7:0	**EccErr: ECC error**. Read-only. Indicates ECC error detection status on a per bit basis when D18F2x264_dct[3:0][ErrCnt] > 0. Status is accumulated until cleared by D18F2x250_dct[3:0][ResetAllErr]. Bit Description [0] ECC[0] [6:1] ECC[<EccErr>] [7] ECC[7]

D18F2x2E0_dct[3:0] Memory P-state Control and Status

See 2.9.3 [DCT Configuration Registers].

Bits	Description
31	Reserved.
30	**FastMstateDis: fast M-state change disable**. Read-write. Reset: 0. 1=The DCT changes MEMCLK frequency only after the NCLK frequency has changed. 0=The DCT changes MEMCLK frequency while the Northbridge changes NCLK.
29	Reserved.
28:24	**M1MemClkFreq: M1 memory clock frequency**. Read-write. Reset: 00h. Specifies the frequency of the DRAM interface (MEMCLK) for memory P-state 1. See Table 141 [Valid Values for Memory Clock Frequency Value Definition]. The hardware enforces D18F5x84[DdrMaxRateEnf] when writes to this field occur. See D18F5x84[DdrMaxRate] and D18F5x84[DdrMaxRateEnf]. BIOS must also program D18F2x9C_x0002_0001_dct[3:0][PllMultDiv] for M1.
23	Reserved.
22:20	**MxMrsEn: Mx Mrs enable**. Read-write. Reset:0. 1=The DCT writes to the DRAM MR after a memory P-state change. 0=The DCT does not write to the DRAM MR. Bit — Description, MR value [0] — MR0, D18F2x2E8_dct[3:0]_mp[1:0][MxMr0] [1] — MR1, D18F2x2E8_dct[3:0]_mp[1:0][MxMr1] [2] — MR2, D18F2x2EC_dct[3:0]_mp[1:0][MxMr2]
19:1	Reserved.
0	**CurMemPstate: current memory P-state**. Reset: 0. Read-only; updated-by-hardware. Specifies the current memory P-state. 0=M0. 1=M1.

D18F2x2E8_dct[3:0]_mp[1:0] MRS Buffer

See 2.9.3 [DCT Configuration Registers].

Bits	Description
31:16	**MxMr1: Mx MR1**. Read-write. Reset: 0000h. Specifies the value written to DRAM MR1 after a memory P-state change. If the M1 value is the same as the M0 value, then BIOS should optimize P-state switching latency by programming D18F2x2E0_dct[3:0][MxMrsEn]=0.
15:0	**MxMr0: Mx MR0**. Read-write. Reset: 0000h. Specifies the value written to DRAM MR0 after a memory P-state change. If the M1 value is the same as the M0 value, then BIOS should optimize P-state switching latency by programming D18F2x2E0_dct[3:0][MxMrsEn]=0.

D18F2x2EC_dct[3:0]_mp[1:0] MRS Buffer

See 2.9.3 [DCT Configuration Registers].

Bits	Description
31:16	Reserved.
15:0	**MxMr2: Mx MR2**. Read-write. Reset: 0000h. Specifies the value written to DRAM MR2 after a memory P-state change. If the M1 value is the same as the M0 value, then BIOS should optimize P-state switching latency by programming D18F2x2E0_dct[3:0][MxMrsEn]=0.

D18F2x2F0_dct[3:0]_mp[1:0] DRAM Controller Misc 3

See 2.9.3 [DCT Configuration Registers].

Bits	Description
31:1	Reserved.
0	**EffArbDis: Efficient arbitration disable**. Read-write. Reset: 0. BIOS: 0. 0=The DCT optimizes the arbitration phases to improve performance under certain traffic conditions whenever the NCLK to MEMCLK ratio is less than 2:1. 1=The DCT arbitrates normally, at all NCLK:MEMCLK ratios.

D18F2x400_dct[3:0] GMC to DCT Control 0

Reset: 0000_0000h. See 2.9.3 [DCT Configuration Registers].
The GMC to DCT interface controls how DRAM bus resources are allocated and arbitrated between the MCT and the GMC. A token is the unit of available resource and is equivalent to a DCQ entry. A minimum count ensures a number of available DCQ entries. A token limit for MCT or GMC ensures resources are not all allocated to the GMC, or MCT respectively. Limits are configured bimodal: for normal GMC traffic and for when urgent (nominally display refresh) GMC traffic is occurring.
D18F2x400_dct[3:0][MctTokenLimit] == D18F2x404_dct[3:0][UrMctTokenLimit].

Bits	Description
31:16	Reserved.
15:12	Reserved.
11:8	**GmcTokenLimit: GMC token limit**. Read-write. BIOS: 4h. Limit of outstanding GMC tokens. Bits: Description Fh-0h: <GmcTokenLimit> tokens
7:4	Reserved.
3:0	**MctTokenLimit: MCT token limit**. Read-write. BIOS: 4h. Limit of outstanding MCT tokens. Bits: Description Fh-0h: <MctTokenLimit> tokens

D18F2x404_dct[3:0] GMC to DCT Control 1

Reset: 0000_0000h. See 2.9.3 [DCT Configuration Registers].

Bits	Description
31	**UrgentTknDis: Urgent token disable**. Read-write. BIOS: 0. 0=When urgent GMC traffic is requested, override the programmed values in D18F2x400_dct[3:0] and force the token scheme to heavily weight towards graphics by using the programmable token limits in D18F2x404_dct[3:0]. 1=Token scheme remains at the previously programmed non-urgent token limits in D18F2x400_dct[3:0] regardless of urgent GMC traffic.
30:28	Reserved.
27:24	**UrGmcMinTokens: Display refresh GMC minimum tokens**. Read-write. BIOS: 4. Urgent mode minimum number of tokens assigned to the GMC. Bits: Description Fh-0h: <UrGmcMinTokens> tokens

23:21	Reserved.
20:16	**UrGmcTokenLimit: Display refresh GMC token limit**. Read-write. BIOS: 04h. Urgent mode limit of outstanding GMC tokens. Bits Description 10h-0h <UrGmcTokenLimit> tokens 1Fh-11h Reserved
15:12	Reserved.
11:8	**UrMctMinTokens: Display refresh MCT minimum tokens**. Read-write. BIOS: 4. Urgent mode minimum number of tokens assigned to the MCT. Bits Description Fh-0h <UrMctMinTokens> tokens
7:5	Reserved.
4:0	**UrMctTokenLimit: Display refresh MCT token limit**. Read-write. BIOS: 04h. Urgent mode limit of outstanding MCT tokens. Bits Description 10h-0h <UrMctTokenLimit> tokens 1Fh-11h Reserved

D18F2x408_dct[3:0] GMC to DCT Control 2

See 2.9.3 [DCT Configuration Registers].

Bits	Description
31:29	Reserved.
28:24	**CpuElevPrioPeriod: Cpu elevate priority period**. Read-write. Reset: 0.BIOS: Ch. Specifies the hysteresis of how often a new MCT read can be elevated to high priority if no other MCT reads currently exist in the DCQ. If CpuElevPrioPeriod==0, MCT will continuously elevate the priority of a new lone MCT read to high. Reserved if CpuElevPrioDis==1. Since this field controls internal timing in the NCLK domain, external bus equivalence is approximate. Bits Description 00h hysteresis counter disabled 1Fh-01h <CpuElevPrioPeriod*32> MEMCLKs
23:3	Reserved.
2	**NonP0UrgentTknDis: non-P0 urgent token disable**. Read-write. Reset: 0. BIOS: 0. 0=Switch from normal GMC traffic token scheme defined by D18F2x400_dct[3:0] to urgent GMC traffic token scheme defined by D18F2x404_dct[3:0] when all processors are not in software P0 state. 1=Use normal GMC traffic token scheme when all processors are not in software P0 state.
1	**TokenAllocSelect: Token allocation select**. Read-write. Reset: 0. BIOS: 0. 0=When both the MCT and GMC have less than their maximum outstanding tokens, tokens are allocated by alternating between each. 1= When both the MCT and GMC have less than their maximum outstanding tokens, tokens are allocated to whichever has less (DCQ entries + current outstanding).
0	**CpuElevPrioDis: Cpu elevate priority disable**. Read-write. Reset: 0. BIOS: 0. 1=Reads from MCT arbitrate with GMC traffic normally. 0=Elevate the priority of a new MCT read to high if no other MCT reads currently exist in the DCQ. This can alleviate CPU stalls during very long graphics requests.

D18F2x420_dct[3:0] GMC to DCT FIFO Config 1

See 2.9.3 [DCT Configuration Registers].

Bits	Description
31:12	Reserved.
11:8	Reserved.
7:4	Reserved.
3:0	Reserved.

D18F2xB60_dct[3:0] DRAM Control 0

Reset: 0000_3010h.

Bits	Description
31:1	Reserved.
0	**DataScrambleEn: data scramble enable**. Read-write; Same-for-all. 1=Data scrambling enabled. Data stored in the DRAM will be scrambled. 0=Data scrambling disabled. This register must have the same value for all DCT's. This bit is valid for Ddr3Mode. BIOS should set this bit prior to any memory write transactions to DRAM not generated by the DCT pattern generation logic. See D18F2x250_dct[3:0][CmdTestEnable] for additional pattern generation requirements.

D18F2xB64_dct[3:0] Data Scramble Key

Reset: 0000_0000h. See 2.9.3 [DCT Configuration Registers].

Bits	Description
31:0	**DatScrambleKey: data scramble key.** Read-write; Same-for-all. Specifies the key value used for data scrambling. This bit is valid for Ddr3Mode.

3.12 Device 18h Function 3 Configuration Registers

See 3.1 [Register Descriptions and Mnemonics]. See 2.7 [Configuration Space].

D18F3x00 Device/Vendor ID

Bits	Description
31:16	**DeviceID: device ID**. Read-only. Value: 141Dh.
15:0	**VendorID: vendor ID**. Read-only. Value: 1022h.

D18F3x04 Status/Command

Bits	Description
31:16	**Status**. Read-only. Reset: 0000h, except bit[20]. Bit[20] is set to indicate the existence of a PCI-defined capability block, if one exists.
15:0	**Command**. Read-only. Reset: 0000h.

D18F3x08 Class Code/Revision ID

Bits	Description
31:8	**ClassCode**. Read-only. Reset: 06_0000h. Provides the host bridge class code as defined in the PCI specification.
7:0	**RevID: revision ID**. Read-only. Reset: 00h.

D18F3x0C Header Type

Reset: 0080_0000h.

Bits	Description
31:0	**HeaderTypeReg**. Read-only. These bits are fixed at their default values. The header type field indicates that there are multiple functions present in this device.

D18F3x34 Capability Pointer

Bits	Description
31:8	Reserved.
7:0	**CapPtr**. Read-only. Value: F0h. Points to D18F3xF0 to provide capability.

D18F3x40 MCA NB Control

MSR0000_0410[31:0] is an alias of D18F3x40. See MSR0000_0410[31:0].

Bits	Description
31	**McaCpuDatErrEn: Compute Unit data error**. Read-write. Reset: 0. 1=Enables MCA reporting of CPU data errors sent to the NB.
30	Unused.
29:28	Unused.
27	Unused.
26	**NbArrayParEn: northbridge array parity error reporting enable**. Read-write. Reset: 0. 1=Enables reporting of parity errors in the NB arrays.
25	**UsPwDatErrEn: upstream data error enable**. Read-write. Reset: 0. 1=Enables MCA reporting of upstream posted writes in which the EP bit is set.
24:18	Unused.
17	**CpPktDatEn: completion packet error reporting enable**. Read-write. Reset: 0. 1=Enables MCA reporting of completion packets with the EP bit set.
16	**NbIntProtEn: northbridge internal bus protocol error reporting enable**. Read-write. Reset: 0. 1=Enables MCA reporting of protocol errors detected on the northbridge internal bus. When possible, this enable should be cleared before initiating a warm reset to avoid logging spurious errors due to RESET_L signal skew.
15:13	Unused.
12	**WDTRptEn: watchdog timer error reporting enable**. Read-write. Reset: 0. 1=Enables MCA reporting of watchdog timer errors. The watchdog timer checks for NB system accesses for which a response is expected but no response is received. See D18F3x44 [MCA NB Configuration] for information regarding configuration of the watchdog timer duration. This bit does not affect operation of the watchdog timer in terms of its ability to complete an access that would otherwise cause a system hang. This bit only affects whether such errors are reported through MCA.
11	**AtomicRMWEn: atomic read-modify-write error reporting enable**. Read-write. Reset: 0. 1=Enables MCA reporting of atomic read-modify-write (RMW) commands received from an IO link. Atomic RMW commands are not supported. An atomic RMW command results in a link error response being generated back to the requesting IO device. The generation of the link error response is not affected by this bit.
10	Unused.
9	**TgtAbortEn: target abort error reporting enable**. Read-write. Reset: 0. 1=Enables MCA reporting of target aborts to a link. The NB returns an error response back to the requestor with any associated data all 1s independent of the state of this bit.
8	**MstrAbortEn: master abort error reporting enable**. Read-write. Reset: 0. 1=Enables MCA reporting of master aborts to a link. The NB returns an error response back to the requestor with any associated data all 1s independent of the state of this bit.
7:6	Unused.
5	**SyncPktEn: link sync packet error reporting enable**. Read-write. Reset: 0. 1=Enables MCA reporting of link-defined sync error packets detected on link. The NB floods its outgoing link with sync packets after detecting a sync packet on the incoming link independent of the state of this bit.

4:2	Unused.
1	**UECCEn: uncorrectable ECC error reporting enable**. Read-write. Reset: 0. 1=Enables MCA reporting of DDR3 DRAM uncorrectable ECC errors which are detected in the NB. In some cases data may be forwarded to the core prior to checking ECC in which case the check takes place in one of the other error reporting banks.
0	**CECCEn: correctable ECC error reporting enable**. Read-write. Reset: 0. 1=Enables MCA reporting of DDR3 DRAM correctable ECC errors which are detected in the NB.

D18F3x44 MCA NB Configuration

See D18F3x180 [Extended NB MCA Configuration].

Bits	Description
31	**NbMcaLogEn: northbridge MCA log enable**. Read-write. Reset: 0. 1=Enables logging (but not reporting) of NB MCA errors even if MCA is not globally enabled.
30	**SyncFloodOnDramAdrParErr: sync flood on DRAM address parity error**. Read-write. Reset: 0. BIOS: 1. 1=Enable Sync flood on detection of a DRAM address parity error.
29	**DisMstAbortCpuErrRsp: master abort CPU error response disable**. Read-write. Reset: 0. 1=Disables master abort reporting through the CPU MCA error-reporting banks; Suppresses sending of RDE to CPU; Does not log any MCA information in the NB.
28	**DisTgtAbortCpuErrRsp: target abort CPU error response disable**. Read-write. Reset: 0. 1=Disables target abort reporting through the CPU MCA error-reporting banks; Suppresses sending of RDE to CPU; Does not log any MCA information in the NB.
27	**NbMcaToMstCpuEn: machine check errors to master CPU only**. Read-write. Reset: 0. BIOS: 1. 1=NB MCA errors in CMP device are only reported to the node base core (NBC), and the NB MCA registers in MSR space (MSR0000_0410, MSR0000_0411, MSR0000_0412, MSR0000_0413, MSRC000_0408, and MSRC001_0048) are only accessible from the NBC; reads of these MSRs from other cores return 0's and writes are ignored. This allows machine check handlers running on different cores to avoid coordinating accesses to the NB MCA registers. This field does not affect PCI-defined configuration space accesses to these registers, which are accessible from all cores. See 3.1 [Register Descriptions and Mnemonics] for a description of MSR space and 3 [Registers] for PCI-defined configuration space. 0=NB MCA errors may be reported to the core that originated the request, if applicable and known, and the NB MCA registers in MSR space are accessible from any core. Note: • When the CPU which originated the request is known, it is stored in MSR0000_0411[ErrCoreId], regardless of the setting of NbMcaToMstCpuEn. See Table 234 for errors where ErrCoreId is known. • If IO originated the request, then the error is reported to the NBC, regardless of the setting of NbMcaToMstCpuEn.
26	**FlagMcaCorrErr: correctable error MCA exception enable**. Read-write. Reset: 0. 1=Raise a machine check exception for correctable and deferred machine check errors which are enabled in D18F3x40.
25	**DisPciCfgCpuErrRsp: PCI configuration CPU error response disable**. Read-write. Reset: 0. 1=Disables generation of an error response to the core on detection of a master abort, target abort, or data error condition, and disables logging and reporting through the MCA error-reporting banks for PCI configuration accesses. For NB WDT errors on PCI configuration accesses, this prevents sending an error response to the core, but does not affect logging and reporting of the NB WDT error. See D18F3x180[DisPciCfgCpuMstAbortRsp], which applies only to master aborts.

24	**IoRdDatErrEn: IO read data error log enable**. Read-write. Reset: 0. 1=Enables MCA logging and reporting of errors on transactions from IO devices upon detection of a target abort, master abort, or data error condition. 0=Errors on transactions from IO devices are not logged in MCA, although error responses to the requesting IO device may still be generated.
23	**ChipKillEccCap: chip-kill ECC mode**. Read-only; updated-by-hardware. Reset: 0. 1=Chipkill ECC mode capable; ECC checking is based on x8 ECC symbols (D18F3x180[EccSymbolSize]) and can be used for chipkill. 0=Chipkill ECC mode not capable; ECC checking is based on two interleaved, unganged 64/8-bit data/ECC lines and x4 ECC symbols and cannot be used for chipkill. See 2.15.2 [DRAM ECC Considerations].
22	**DramEccEn: DRAM ECC enable**. Read-write. Reset: 0. 1=Enables ECC check/correct mode. 0=ECC check/correct mode disabled, Data-poisoning is not supported.This bit must be set in order for ECC checking/correcting by the NB to be enabled. If set, ECC is checked and correctable errors are corrected irrespective of whether machine check ECC reporting is enabled. The hardware only allows values to be programmed into this field which are consistent with the ECC capabilities of the device as specified in D18F3xE8 [Northbridge Capabilities]. Attempts to write values inconsistent with the capabilities results in this field not being updated. This bit does not affect ECC checking in the north-bridge arrays.
21	**SyncFloodOnAnyUcErr: sync flood on any UC error**. Read-write. Reset: 0. BIOS: 1. 1=Enable Sync flood of all links with sync packets on detection of any NB MCA error that is uncorrectable, including northbridge array errors and link protocol errors.
20	**SyncFloodOnWDT: sync flood on watchdog timer error**. Read-write. Reset: 0. BIOS: 1. 1=Enable Sync flood of all links with sync packets on detection of a watchdog timer error.
19:18	**GenSubLinkSel: sublink select for CRC error generation**. Read-write. Reset: 0. Selects the sub-link of a link selectedby GenLinkSel to beused for CRC error injectionthrough GenCrcErrByte0 and GenCrcErrByte1. When the link is ganged, GenSubLinkSel must be 00b. When the link is unganged, the following values indicate which sublink is selected: Bits — Description 00b — Sublink 0 01b — Sublink 1 10b — Reserved 11b — Reserved
17	**GenCrcErrByte1: generate CRC error on byte lane 1**. Read-write. Reset: 0. 1=For ganged links (see GenSubLinkSel), a CRC error is injected on byte lane 1 of the link specified by GenLinkSel. For ganged links in retry mode or unganged links, this field is reserved, and GenCrcErrByte0 must be used. The data carried by the link is unaffected. This bit is cleared after the error has been generated.
16	**GenCrcErrByte0: generate CRC error on byte lane 0**. Read-write. Reset: 0. 1=Causes a CRC error to be injected on byte lane 0 of the link specified by GenLinkSel and the sublink specified by Gen-SubLinkSel. The data carried by the link is unaffected. This bit is cleared after the error has been gen-erated.

15:14	**GenLinkSel: link select for CRC error generation**. Read-write. Reset: 00b. Selects the link to be used for CRC error injection through GenCrcErrByte1/GenCrcErrByte0. Bits: Description 00b: link 0 01b: link 1 10b: link 2 11b: link 3
13:12	**WDTBaseSel: watchdog timer time base select**. Read-write. Reset: 0. Selects the time base used by the watchdog timer. The counter selected by WDTCntSel determines the maximum count value in the time base selected by WDTBaseSel. Bits: Description 00b: 1.31 ms 01b: 1.28 us 10b: Reserved. 11b: Reserved.
11:9	**WDTCntSel[2:0]: watchdog timer count select bits[2:0]**. Read-write. Reset: 0. Selects the count used by the watchdog timer. WDTCntSel = {D18F3x180[WDTCntSel[3]], D18F3x44[WDTCntSel[2:0]]}. The counter selected by WDTCntSel determines the maximum count value in the time base selected by WDTBaseSel. WDTCntSel is encoded as: Bits: Description 0000b: 4095 0001b: 2047 0010b: 1023 0011b: 511 0100b: 255 0101b: 127 0110b: 63 0111b: 31 1000b: 8191 1001b: 16383 1111b-1010b: Reserved Because WDTCntSel is split between two registers, care must be taken when programming WDTCntSel to ensure that a reserved value is never used by the watchdog timer or undefined behavior could result.
8	**WDTDis: watchdog timer disable**. Read-write. Cold reset: 0. 1=Disables the watchdog timer. The watchdog timer is enabled by default and checks for NB system accesses for which a response is expected and where no response is received. If such a condition is detected the outstanding access is completed by generating an error response back to the requestor. An MCA error may also be generated if enabled in D18F3x40 [MCA NB Control].
7	**IoErrDis: IO error response disable**. Read-write. Reset: 0. 1=Disables setting either Error bit in link response packets to IO devices on detection of a target or master abort error condition.
6	**CpuErrDis: CPU error response disable**. Read-write. Reset: 0. BIOS: 1. 1=Disables generation of a read data error response to the core on detection of a target or master abort error condition.
5	**IoMstAbortDis: IO master abort error response disable**. Read-write. Reset: 0. 1=Signals target abort instead of master abort in link response packets to IO devices on detection of a master abort error condition.When IoMstAbortDis and D18F3x180[ChgMstAbortToNoErr] are both set, D18F3x180[ChgMstAbortToNoErr] takes precedence.

4	**SyncPktPropDis: sync packet propagation disable**. Read-write. Reset: 0. 1=Disables flooding of all outgoing links with sync packets when a sync packet is detected on an incoming link. Sync packets are propagated by default.
3	**SyncPktGenDis: sync packet generation disable**. Read-write. Reset: 0. 1=Disables flooding of all outgoing links with sync packets when a CRC error is detected on an incoming link. By default, sync packet generation for CRC errors is controlled through D18F0x[E4,C4,A4,84] [Link Control].
2	**SyncFloodOnDramUcEcc: sync flood on uncorrectable DRAM ECC error**. Read-write. Reset: 0. BIOS: 1. 1=Enable Sync flood of all links with sync packets on detection of an uncorrectable DRAM ECC error.
1	**CpuRdDatErrEn: CPU read data error log enable**. Read-write. Reset: 0. 1=Enables reporting of read data errors (master aborts and target aborts) for data destined for the CPU on this node. This bit should be clear if read data error logging is enabled for the remaining error reporting blocks in the CPU. Logging the same error in more than one block may cause a single error event to be treated as a multiple error event and cause the CPU to enter shutdown.
0	Reserved.

D18F3x48 MCA NB Status Low

Bits	Description
31:0	MSR0000_0411[31:0] is an alias of D18F3x48. See MSR0000_0411.

D18F3x4C MCA NB Status High

Bits	Description
31:0	MSR0000_0411[63:32] is an alias of D18F3x4C. See MSR0000_0411.

D18F3x50 MCA NB Address Low

Bits	Description
31:0	MSR0000_0412[31:0] is an alias of D18F3x50. See MSR0000_0412[31:0].

D18F3x54 MCA NB Address High

Bits	Description
31:0	MSR0000_0412[63:32] is an alias of D18F3x54. See MSR0000_0412[63:32].

D18F3x58 Scrub Rate Control

This register specifies the ECC sequential scrubbing rate for lines of memory and cache. See 2.8.3 [Memory Scrubbers]. Scrub rates are a platform consideration. See 2.15.1.8 [Scrub Rate Considerations].

Bits	Description
31:29	Reserved.

28:24	Reserved.
23:5	Reserved.
4:0	**DramScrub: DRAM scrub rate**. Read-write. Reset: 0_0000b. Specifies time between 64 B scrub events. See D18F3x5C and D18F3x60. Bits / Description / Bits / Description 00h Disable sequential scrubbing — 10h 1.31 ms 01h 40 ns[1] — 11h 2.62 ms 02h 80 ns[1] — 12h 5.24 ms 03h 160 ns[1] — 13h 10.49 ms 04h 320 ns[1] — 14h 20.97 ms 05h 640 ns — 15h 42 ms 06h 1.28 us — 16h 84 ms 07h 2.56 us — 1Eh-17h Reserved 08h 5.12 us — 1Fh Reserved 09h 10.2 us 0Ah 20.5 us 0Bh 41.0 us 0Ch 81.9 us 0Dh 163.8 us 0Eh 327.7 us 0Fh 655.4 us Note: 1. This setting is not supported except as a DRAM scrub rate when no other memory accesses are being performed.

D18F3x5C DRAM Scrub Address Low

In addition to sequential DRAM scrubbing, the DRAM scrubber has a redirect mode for scrubbing DRAM locations accessed during normal operation. This is enabled by setting D18F3x5C[ScrubReDirEn]. When a DRAM read is generated by any agent other than the DRAM scrubber, correctable ECC errors are corrected as the data is passed to the requestor, but the data in DRAM is not corrected if redirect scrubbing mode is disabled. In scrubber redirect mode, correctable errors detected during normal DRAM read accesses redirect the scrubber to the location of the error. After the scrubber corrects the location in DRAM, it resumes scrubbing from where it left off. DRAM scrub address registers are not modified by the redirect scrubbing mode. Sequential scrubbing and scrubber redirection can be enabled independently or together. ECC errors detected by the scrubber are logged in the MCA registers (See D18F3x40 [MCA NB Control]).

Bits	Description
31:6	**ScrubAddr[31:6]: DRAM scrubber address bits[31:6]**. Read-write; updated-by-hardware. ScrubAddr[47:6] = {D18F3x60[ScrubAddr[47:32]], ScrubAddr[31:6]}. Reset: 0. ScrubAddr points to a DRAM cacheline in physical address space. BIOS should initialize the scrubber address register to the base address of the node specified by D18F1x[17C:140,7C:40] [DRAM Base/Limit] prior to enabling sequential scrubbing through D18F3x58[DramScrub]. When sequential scrubbing is enabled: it starts at the address that the scrubber address registers are initialized to; it increments through address space and updates the scrubber address registers as it does so; when the scrubber reaches the DRAM limit address specified by D18F1x[17C:140,7C:40], it wraps around to the base address. Reads of the scrubber address registers provide the next cacheline to be scrubbed.

5:1	Reserved.
0	**ScrubReDirEn: DRAM scrubber redirect enable**. Read-write. Reset: 0. If a correctable error is discovered from a non-scrubber DRAM read, then the data is corrected before it is returned to the requestor; however, the DRAM location may be left in a corrupted state (until the next time the scrubber address counts up to that location, if sequential scrubbing is enabled through D18F3x58[DramScrub]). 1=Enables the scrubber to immediately scrub any address in which a correctable error is discovered. This bit and sequential scrubbing can be enabled independently or together; if both are enabled, the scrubber jumps from the scrubber address to where the correctable error was discovered, scrubs that location, and then jumps back to where it left off; the scrubber address register is not affected during scrubber redirection.

D18F3x60 DRAM Scrub Address High

Bits	Description
31:16	Reserved.
15:0	**ScrubAddr[47:32]: DRAM scrubber address bits[47:32]**. See: D18F3x5C[ScrubAddr[31:6]]. Reset: 0.

D18F3x64 Hardware Thermal Control (HTC)

See 2.10.3.1 [PROCHOT_L and Hardware Thermal Control (HTC)]. If D18F3xE8[HtcCapable]==0 then this register is reserved.

Bits	Description
31	Reserved.
30:28	**HtcPstateLimit: HTC P-state limit select**. Read-write. Reset: Product-specific. Specifies the P-state limit of all cores when in the HTC-active state. This field uses hardware P-state numbering and is not changed on a write if the value written is greater than D18F3xDC[HwPstateMaxVal] or less than D18F4x15C[NumBoostStates]. See 2.10.3.1 [PROCHOT_L and Hardware Thermal Control (HTC)] and 2.5.3.1.1.2 [Hardware P-state Numbering] .
27:24	**HtcHystLmt: HTC hysteresis**. Read-write. Reset: Product-specific. The processor exits the HTC-active state when (Tctl < (HtcTmpLmt - HtcHystLmt). Bits — Description 0h — 0 1h — 0.5 Eh-2h — <HtcHystLmt*0.5> Fh — 7.5
23	**HtcSlewSel: HTC slew-controlled temperature select**. Read-write. Reset: 0. 1=HTC logic is driven by the slew-controlled temperature, Tctl, specified in D18F3xA4 [Reported Temperature Control]. 0=HTC logic is driven by the measured control temperature with no slew controls.
22:16	**HtcTmpLmt: HTC temperature limit**. Read-write. Reset: Product-specific. The processor enters the HTC-active state when Tctl reaches or exceeds the temperature limit defined by this register. Bits — Description 00h — 52 01h — 52.5 7Eh-02h — <(HtcTmpLmt*0.5) + 52> 7Fh — 115.5

15:8	Reserved.
7	**PslApicLoEn: P-state limit lower value change APIC interrupt enable**. Read-write. Reset: 0. PslApicLoEn and PslApicHiEn enable interrupts using APIC330 [LVT Thermal Sensor] of each core when the active P-state limit in MSRC001_0061[CurPstateLimit] changes. PslApicLoEn enables the interrupt when the limit value becomes lower (indicating higher performance). PslApicHiEn enables the interrupt when the limit value becomes higher (indicating lower performance). 1=Enable interrupt.
6	**PslApicHiEn: P-state limit higher value change APIC interrupt enable**. Read-write. Reset: 0. See PslApicLoEn.
5	**HtcActSts: HTC-active status**. Read; set-by-hardware; write-1-to-clear. Reset: 0. This bit is set by hardware when the processor enters the HTC-active state. It is cleared by writing a 1 to it.
4	**HtcAct: HTC-active state**. Read-only; updated-by-hardware. Reset: X. 1=The processor is currently in the HTC-active state. 0=The processor is not in the HTC-active state.
3:1	Reserved.
0	**HtcEn: HTC enable**. Read-write. Reset: 0. BIOS: IF (D18F3x64[HtcTmpLmt]==0) THEN 0. ELSE 1. ENDIF. 1=HTC is enabled; the processor is capable of entering the HTC-active state.

D18F3x68 Software P-state Limit

See 2.10.3.2 [Software P-state Limit Control]. If D18F3xE8[HtcCapable]==0 then this register is reserved.

Bits	Description
31	Reserved.
30:28	**SwPstateLimit: software P-state limit select**. Read-write. Reset: Product-specific. Specifies a P-state limit for all cores. Uses hardware P-state numbering; see 2.5.3.1.1.2 [Hardware P-state Numbering]. Not changed on a write if the value written is greater than D18F3xDC[HwPstateMaxVal] or less than D18F4x15C[NumBoostStates]. See SwPstateLimitEn.
27:6	Reserved.
5	**SwPstateLimitEn: software P-state limit enable**. Read-write. Reset: 0. 1=SwPstateLimit is enabled.
4:0	Reserved.

D18F3x6C Data Buffer Count

Out of cold reset, the processor allocates a minimal number of buffers that is smaller than the default values in the register. BIOS must use D18F0x6C[RlsLnkFullTokCntImm] for the values in the register to take effect. This is necessary even if the values are unchanged from the default values.

- To ensure deadlock free operation the following minimum buffer allocations are required:
  - D18F3x6C[UpRspDBC] >= 1.
  - D18F3x6C[DnReqDBC] >= 1.
  - D18F3x6C[UpReqDBC] >= 1.
  - D18F3x6C[DnRspDBC] >= 1.
- If D18F0x[E4,C4,A4,84][IsocEn]=1: IsocRspDBC >= 1.
- The total number of data buffers allocated in this register and D18F3x7C must satisfy the following equation:
  - D18F3x6C[UpReqDBC] + D18F3x6C[UpRspDBC] + D18F3x6C[DnReqDBC] + D18F3x6C[DnRspDBC] + D18F3x6C[IsocRspDBC] + (IF (D18F3x7C[Sri2XbarFreeRspDBC]==0)

THEN (D18F3x7C[Sri2XbarFreeXreqDBC]*2) ELSE D18F3x7C[Sri2XbarFreeXreqDBC] ENDIF) + D18F3x7C[Sri2XbarFreeRspDBC] <= 16.

Bits	Description
31	Reserved.
30:28	**IsocRspDBC: isochronous response data buffer count**. Read-write. Cold reset: 3. BIOS: 1.
27:19	Reserved.
18:16	**UpRspDBC: upstream response data buffer count**. Read-write. Cold reset: 2. BIOS: 1.
15	Reserved.
14:8	Reserved.
7:6	**DnRspDBC: downstream response data buffer count**. Read-write. Cold reset: 2. BIOS: 1.
5:4	**DnReqDBC: downstream request data buffer count**. Read-write. Cold reset: 1. BIOS: 1.
3	Reserved.
2:0	**UpReqDBC: upstream request data buffer count**. Read-write. Cold reset: 2. BIOS: 2.

D18F3x70 SRI to XBAR Command Buffer Count

Out of cold reset, the processor allocates a minimal number of buffers that is smaller than the default values in the register. BIOS must use D18F0x6C[RlsLnkFullTokCntImm] for the values in the register to take effect. This is necessary even if the values are unchanged from the default values.

- To ensure deadlock free operation the following minimum buffer allocations are required:
  - D18F3x70[UpRspCBC] >= 1.
  - D18F3x70[UpPreqCBC] >= 1.
  - D18F3x70[DnPreqCBC] >= 1.
  - D18F3x70[UpReqCBC] >= 1.
  - D18F3x70[DnReqCBC] >= 1.
  - D18F3x70[DnRspCBC] >= 1.
- If any of the D18F0x[E4,C4,A4,84][IsocEn] bits are set:
  IsocReqCBC >= 1 IsocRspCBC >= 1
- If D18F0x[E4,C4,A4,84][IsocEn]==1 and isochronous posted requests may be generated by the system:
  IsocPreqCBC >= 1
- The total number of SRI to XBAR commandbuffers allocated in this register and D18F3x7C must satisfy the following equation:
  - D18F3x70[IsocRspCBC] + D18F3x70[IsocPreqCBC] + D18F3x70[IsocReqCBC] + D18F3x70[UpRspCBC] + D18F3x70[DnPreqCBC] + D18F3x70[UpPreqCBC] + D18F3x70[DnReqCBC] + D18F3x70[DnRspCBC] + D18F3x70[UpReqCBC] + D18F3x7C[Sri2XbarFreeRspCBC] + D18F3x7C[Sri2XbarFreeXreqCBC] <= 48.

Bits	Description
31	Reserved.
30:28	**IsocRspCBC: isoc response command buffer count**. Read-write. Cold reset: 1. BIOS: 1.
27	Reserved.
26:24	**IsocPreqCBC: isoc posted request command buffer count**. Read-write. Cold reset: 1. BIOS: 0.
23	Reserved.
22:20	**IsocReqCBC: isoc request command buffer count**. Read-write. Cold reset: 1. BIOS: 1.
19	Reserved.

18:16	**UpRspCBC: upstream response command buffer count**. Read-write. Cold reset: 1. BIOS: 7.
15	Reserved.
14:12	**DnPreqCBC: downstream posted request command buffer count**. Read-write. Cold reset: 2. BIOS: 1.
11	Reserved.
10:8	**UpPreqCBC: upstream posted request command buffer count**. Read-write. Cold reset: 1. BIOS: 1.
7:6	**DnRspCBC: downstream response command buffer count**. Read-write. Cold reset: 1. BIOS: 1.
5:4	**DnReqCBC: downstream request command buffer count**. Read-write. Cold reset: 1. BIOS: 1.
3	Reserved.
2:0	**UpReqCBC: upstream request command buffer count**. Read-write. Cold reset: 3. BIOS: 7.

D18F3x74 XBAR to SRI Command Buffer Count

Cold reset: 0007_1111h. Out of cold reset, the processor allocates a minimal number of buffers that is smaller than the default values in the register. BIOS must use D18F0x6C[RlsLnkFullTokCntImm] for the values in the register to take effect. This is necessary even if the values are unchanged from the default values.

Table 186: Buffer Definitions

Term	Definition
SpqSize	Probe command queue size. SpqSize = 20.
SrqSize	SRQ (XBAR command and probe response to SRI) queue size. SrqSize = 52.
PrbRsp	SRQ entries hard allocated to probe responses. PrbRsp = 4.
MpbcSize	MPB command buffer size. MpbcSize = 48.
McqSize	MCT command queue size. McqSize = 72.

- To ensure deadlock free operation the following minimum buffer allocations are required:
  - D18F3x74[ProbeCBC] >= 2.
  - D18F3x74[UpReqCBC] >= 1.
  - D18F3x74[UpPreqCBC] >= 1.
  - (IsocReqCBC + IsocPreqCBC + DRReqCBC) <= 31.
  - (IsocReqCBC + IsocPreqCBC + DRReqCBC) <= (McqSize - 16).
- If any of D18F0x[E4,C4,A4,84][IsocEn] bits are set, then IsocReqCBC >= 1.
- If any of the D18F0x[E4,C4,A4,84][IsocEn] bits are set and isochronous posted requests may be generated by the system:
  IsocPreqCBC >= 1
- The total number of XBAR to SRI commandbuffers allocated in this register and D18F3x7C must satisfy the following equation:
  - D18F3x74[UpReqCBC] + D18F3x74[UpPreqCBC] + D18F3x74[DnReqCBC] +

D18F3x74[DnPreqCBC] + D18F3x74[IsocReqCBC] + D18F3x74[IsocPreqCBC] + D18F3x74[DRReqCBC] + D18F3x7C[Xbar2SriFreeListCBC] + (D18F3x1A0[CpuCmdBufCnt] * NumOfCompUnits) + D18F3x1A0[CpuToNbFreeBufCnt] + PrbRsp <= SrqSize

- The total number of SPQ (probe command) buffers allocated must satisfy the following equation:
  - (D18F3x17C[SPQPrbFreeCBC] + D18F3x74[ProbeCBC]) <= SpqSize.

Bits	Description
31:28	**DRReqCBC: display refresh request command buffer count**. Read-write.
27	Reserved.
26:24	**IsocPreqCBC: isochronous posted request command buffer count**. Read-write. BIOS: 1.
23:20	**IsocReqCBC: isochronous request command buffer count**. Read-write. BIOS: 1.
19:16	**ProbeCBC: probe command buffer count**. Read-write. BIOS: Ch. Bits: Description 0h: 0 buffers Ch-1h: <ProbeCBC> buffers Fh-Dh: Reserved.
15	Reserved.
14:12	**DnPreqCBC: downstream posted request command buffer count**. Read-write. BIOS: 0.
11	Reserved.
10:8	**UpPreqCBC: upstream posted request command buffer count**. Read-write. BIOS: 1.
7	Reserved.
6:4	**DnReqCBC: downstream request command buffer count**. Read-write. BIOS: 0.
3	Reserved.
2:0	**UpReqCBC: upstream request command buffer count**. Read-write. BIOS: 1.

D18F3x78 MCT to XBAR Buffer Count

Cold Reset: 0024_0519h. Out of cold reset, the processor allocates a minimal number of buffers that is smaller than the default values in the register. BIOS must use D18F0x6C[RlsLnkFullTokCntImm] for the values in the register to take effect. This is necessary even if the values are unchanged from the default values.

- To ensure deadlock free operation the following minimum buffer allocations are required:
  ProbeCBC >= 1 RspCBC >= 1 RspDBC >= 2
  RspDBC >= D18F2x11C[MctPrefReqLimit]+2
- The total number of command buffers allocated in this register must satisfy the following equation:
  (D18F3x78[ProbeCBC] + D18F3x78[RspCBC]) <= MpbcSize.

Bits	Description
31:22	Reserved.
21:16	**RspDBC: response data buffer count**. Read-write. BIOS: 20h Bits / Description 01h-00h: Reserved 02h: 2 Buffers 1Fh-03h: <RspDBC> Buffers 20h: 32 Buffers 3Fh-21h: Reserved
15:13	Reserved.
12:8	**ProbeCBC: probe command buffer count**. Read-write. BIOS: 11h.
7:6	Reserved.
5:0	**RspCBC: response command buffer count**. Read-write. BIOS: 1Fh.

D18F3x7C Free List Buffer Count

Cold Reset: 0003_660Ch. Out of cold reset, the processor allocates a minimal number of buffers that is smaller than the default values in the register. BIOS must use D18F0x6C[RlsLnkFullTokCntImm] for the values in the register to take effect. This is necessary even if the values are unchanged from the default values. See D18F3x6C and D18F3x70.

- To ensure deadlock free operation the following minimum buffer allocations are required:
  - IF (D18F3x7C[Sri2XbarFreeRspCBC]==0) THEN (D18F3x7C[Sri2XbarFreeXreqCBC]>2).
  - IF (D18F3x7C[Sri2XbarFreeRspCBC]!=0) THEN (D18F3x7C[Sri2XbarFreeRspCBC]>2).
  - IF (D18F3x7C[Sri2XbarFreeRspDBC]==0) THEN (D18F3x7C[Sri2XbarFreeXreqDBC]>2).
  - IF (D18F3x7C[Sri2XbarFreeRspDBC]!=0) THEN (D18F3x7C[Sri2XbarFreeRspDBC]>2).
  - D18F3x7C[Xbar2SriFreeListCBC] >= (D18F3x1A0[CpuToNbFreeBufCnt] * NumOfCompUnits) + 2.

Bits	Description
31	Reserved.
30:28	**Xbar2SriFreeListCBInc: XBAR to SRI free list command buffer increment**. Read-write. This field is use to add buffers to the free list pool if they are reclaimed from hard allocated entries without having to go through warm reset. This field may only be programmed after buffers have been allocated and released via D18F0x6C[RlsLnkFullTokCntImm].
27:23	Reserved.
22:20	**Sri2XbarFreeRspDBC: SRI to XBAR free response data buffer count**. Read-write. BIOS: 0.
19:16	**Sri2XbarFreeXreqDBC: SRI to XBAR free request and posted request data buffer count**. Read-write. BIOS: 5h. If Sri2XbarFreeRspDBC=0h, then these buffers are shared between requests, responses and posted requests and the number of buffers allocated is two times the value of this field.

15:12	**Sri2XbarFreeRspCBC: SRI to XBAR free response command buffer count**. Read-write. BIOS: 0h.
11:8	**Sri2XbarFreeXreqCBC: SRI to XBAR free request and posted request command buffer count**. Read-write. BIOS: Eh. If Sri2XbarFreeRspCBC=0h, then these buffers are shared between requests, responses and posted requests and the number of buffers allocated is two times the value of this field.
7:6	Reserved.
5:0	**Xbar2SriFreeListCBC: XBAR to SRI free list command buffer count**. Read-write. BIOS: 2Ah.

D18F3x[84:80] ACPI Power State Control

This block consists of eight identical 8-bit registers, one for each System Management Action Field (SMAF) code associated with STPCLK assertion commands from the link. Refer to the descriptions below for the associated ACPI state and system management actions for each of the 8 SMAF codes. The SmafAct fields specify the system management actions taken when the corresponding SMAF code is received. For instance, a SMAF code of 5 results in the power management actions specified by SmafAct5. Some ACPI states and associated SMAF codes may not be supported in certain conditions. See 2.5 [Power Management] for which states are supported.

When a link STPCLK assertion command is received by the processor, the power management commands specified by the register with the corresponding SMAF code are invoked. When the STPCLK deassertion command is received by the processor, the processor returns into the operational state.

In multi-node systems, these registers should be programmed identically in all nodes.

Table 187: SMAF Action Definition

Register	SmafAct	ACPI state	Description
D18F3x84[31:24]	SmafAct7	C1	Initiated when a Halt instruction is executed by processor. This does not involve the interaction with the SMC, therefore the SMC is required to never send STPCLK assertion commands with SMAF=7h.
D18F3x84[23:16]	SmafAct6	S4/S5	Initiated by a processor access to the ACPI-defined PM1_CNTa register.
D18F3x84[15:8]	SmafAct5	Throttling	Occurs based upon SMC hardware-initiated throttling. AMD recommends using PROCHOT_L for thermal throttling and not implementing stop clock based throttling.
D18F3x84[7:0]	SmafAct4	S3	Initiated by a processor access to the ACPI-defined PM1_CNTa register.
D18F3x80[31:24]	SmafAct3	S1	Initiated by a processor access to the ACPI-defined PM1_CNTa register.
D18F3x80[23:16]	SmafAct2	-	
D18F3x80[15:8]	SmafAct1	C1E, or Link init.	Initiated by an access to the ACPI-defined P_LVL3 register.
D18F3x80[7:0]	SmafAct0	C2	Initiated by a processor access to the ACPI-defined P_LVL2 register.

D18F3x80 ACPI Power State Control Low

Reset: 0000_0000h. Read-write.

<table>
<tr><th>Bits</th><th>Description</th></tr>
<tr><td>31:29</td><td>ClkDivisorSmafAct3. See: ClkDivisorSmafAct0.</td></tr>
<tr><td>28:27</td><td>Reserved.</td></tr>
<tr><td>26</td><td>NbGateEnSmafAct3. See: NbGateEnSmafAct0.</td></tr>
<tr><td>25</td><td>NbLowPwrEnSmafAct3. See: NbLowPwrEnSmafAct0.</td></tr>
<tr><td>24</td><td>CpuPrbEnSmafAct3. See: CpuPrbEnSmafAct0.</td></tr>
<tr><td>23:21</td><td>ClkDivisorSmafAct2. See: ClkDivisorSmafAct0.</td></tr>
<tr><td>20:19</td><td>Reserved.</td></tr>
<tr><td>18</td><td>NbGateEnSmafAct2. See: NbGateEnSmafAct0.</td></tr>
<tr><td>17</td><td>NbLowPwrEnSmafAct2. See: NbLowPwrEnSmafAct0.</td></tr>
<tr><td>16</td><td>CpuPrbEnSmafAct2. See: CpuPrbEnSmafAct0.</td></tr>
<tr><td>15:13</td><td>ClkDivisorSmafAct1. See: ClkDivisorSmafAct0.</td></tr>
<tr><td>12:11</td><td>Reserved.</td></tr>
<tr><td>10</td><td>NbGateEnSmafAct1. See: NbGateEnSmafAct0.</td></tr>
<tr><td>9</td><td>NbLowPwrEnSmafAct1. See: NbLowPwrEnSmafAct0.</td></tr>
<tr><td>8</td><td>CpuPrbEnSmafAct1. See: CpuPrbEnSmafAct0.</td></tr>
<tr><td>7:5</td><td>ClkDivisorSmafAct0: clock divisor. Read-write.
Specifies the core clock frequency while in the low-power state. This divisor is relative to the current FID frequency, or:
• 100 MHz * (10h + MSRC001_00[6B:64][CpuFid[5:0]]) of the current P-state specified by MSRC001_0063[CurPstate].
If MSRC001_00[6B:64][CpuDid] of the current P-state indicates a divisor that is deeper than specified by this field, then no frequency change is made when entering the low-power state associated with this register.
<table>
<tr><th>Bits</th><th>Description</th><th>Bits</th><th>Description</th></tr>
<tr><td>000b</td><td>/1</td><td>100b</td><td>/16</td></tr>
<tr><td>001b</td><td>/2</td><td>101b</td><td>/128</td></tr>
<tr><td>010b</td><td>/4</td><td>110b</td><td>/512</td></tr>
<tr><td>011b</td><td>/8</td><td>111b</td><td>Turn off clocks</td></tr>
</table>
</td></tr>
<tr><td>4:3</td><td>Reserved.</td></tr>
</table>

2	**NbGateEnSmafAct0: Northbridge gate enable**. Read-write. This bit does not control hardware. NbLowPwrEn is required to be set if this bit is set.
1	**NbLowPwrEnSmafAct0: Northbridge low-power enable**. Read-write. 1=The NB clock is ramped down to the divisor specified by D18F3xD4[NbClkDiv] and DRAM is placed into self-refresh mode when LDTSTOP_L is asserted while in the low-power state.
0	**CpuPrbEnSmafAct0: CPU direct probe enable**. Read-write. Specifies how probes are handled while in the low-power state. 0=When the probe request comes into the NB, the core clock is brought up to the COF (based on the current P-state), all outstanding probes are completed, the core waits for a hysteresis time based on D18F3xD4[ClkRampHystSel], and then the core clock is brought down to the frequency specified by ClkDivisor. 1=The core clock does not change frequency; the probe is handled at the frequency specified by ClkDivisor; this may only be set if: • ClkDivisor specifies a divide-by 1, 2, 4, 8, or 16 and NbCof <= 3.2 GHz • ClkDivisor specifies a divide-by 1, 2, 4, or 8 and NbCof >= 3.4 GHz This bit also specifies functionality of the timer used for cache flushing during halt. See D18F3xDC[CacheFlushOnHaltTmr]. • If ((D18F3x84[CpuPrbEnSmafAct7]==0) && (D18F3xDC[IgnCpuPrbEn]==0)), only the time when the core is halted and has its clocks ramped up to service probes is counted. • If ((D18F3x84[CpuPrbEnSmafAct7]==1) or (D18F3xDC[IgnCpuPrbEn]==1)), all of the time the core is halted is counted.

D18F3x84 ACPI Power State Control High

Reset: 0000_0000h. Read-write.

Bits	Description
31:29	**ClkDivisorSmafAct7**. See: D18F3x80[ClkDivisorSmafAct0].
28:27	Reserved.
26	**NbGateEnSmafAct7**. See: D18F3x80[NbGateEnSmafAct0].
25	**NbLowPwrEnSmafAct7**. See: D18F3x80[NbLowPwrEnSmafAct0].
24	**CpuPrbEnSmafAct7**. See: D18F3x80[CpuPrbEnSmafAct0].
23:21	**ClkDivisorSmafAct6**. See: D18F3x80[ClkDivisorSmafAct0].
20:19	Reserved.
18	**NbGateEnSmafAct6**. See: D18F3x80[NbGateEnSmafAct0].
17	**NbLowPwrEnSmafAct6**. See: D18F3x80[NbLowPwrEnSmafAct0].
16	**CpuPrbEnSmafAct6**. See: D18F3x80[CpuPrbEnSmafAct0].
15:13	**ClkDivisorSmafAct5**. See: D18F3x80[ClkDivisorSmafAct0].
12:11	Reserved.
10	**NbGateEnSmafAct5**. See: D18F3x80[NbGateEnSmafAct0].
9	**NbLowPwrEnSmafAct5**. See: D18F3x80[NbLowPwrEnSmafAct0].
8	**CpuPrbEnSmafAct5**. See: D18F3x80[CpuPrbEnSmafAct0].
7:5	**ClkDivisorSmafAct4**. See: D18F3x80[ClkDivisorSmafAct0]. BIOS: 111b.
4:3	Reserved.

2	**NbGateEnSmafAct4**. See: D18F3x80[NbGateEnSmafAct0].
1	**NbLowPwrEnSmafAct4**. See: D18F3x80[NbLowPwrEnSmafAct0]. BIOS: 1.
0	**CpuPrbEnSmafAct4**. See: D18F3x80[CpuPrbEnSmafAct0].

D18F3x88 NB Configuration 1 Low (NB_CFG1_LO)

Bits	Description
31:0	MSRC001_001F[31:0] is an alias of D18F3x88. See MSRC001_001F.

D18F3x8C NB Configuration 1 High (NB_CFG1_HI)

Bits	Description
31:0	MSRC001_001F[63:32] is an alias of D18F3x8C. See MSRC001_001F.

D18F3xA0 Power Control Miscellaneous

Bits	Description
31	**CofVidProg: COF and VID of P-states programmed**. Read-only. Reset: Product-specific. 1=Out of cold reset, the VID, FID, and DID values of the P-state registers specified by MSRC001_0071[StartupPstate] and D18F5x174[StartupNbPstate] have been applied to the processor. 0=Out of cold reset, the boot VID is applied to all processor power planes, the NB clock plane is set to 800 MHz (with a FID of 00h=800 MHz and a DID of 0b) and core CPU clock planes are set to 800 MHz (with a FID of 00h=1.6 GHz and a DID of 1h). Registers containing P-state information such as FID, DID, and VID values are valid out of cold reset independent of the state of D18F3xA0[CofVidProg]. BIOS must transition the processor to a valid P-state out of cold reset when D18F3xA0[CofVidProg]=0. See 2.5.3.1.6 [BIOS Requirements for Core P-state Initialization and Transitions].
30:28	Reserved.
27:16	**ConfigId: Configuration identifier**. Read-only. Reset: Product-specific. Specifies the configuration ID associated with the product.
15	Reserved.
14	**Svi2HighFreqSel: SVI2 high frequency select**. Read-write. Cold reset: 0. BIOS: 1. 0=3.4 MHz. 1=20 MHz. Writes to this field take effect at the next SVI command boundary. If 20 MHz is supported by the VRM, BIOS should program this to 1 prior to any VID transitions. Once this bit is set, it should not be cleared until the next cold reset.
13:11	**PllLockTime: PLL synchronization lock time**. Read-write. Reset: 0. BIOS: 001b. If a P-state change occurs that applies a new FID to the PLL, this field specifies the time required for the PLL to lock to the new frequency. Bits / Description / Bits / Description 000b 1 us 100b 8 us 001b 2 us 101b 16 us 010b 3 us 110b Reserved 011b 4 us 111b Reserved

10	Reserved.
9	Reserved.
8	**PsiVid[7]**. Read-write. Reset: 0. BIOS: 2.5.1.3.1.1. See PsiVid[6:0].
7	**PsiVidEn: PSI_L VID enable**. Read-write. Reset: 0. BIOS: 2.5.1.3.1.1. This bit specifies how PSI_L is controlled. This signal may be used by the voltage regulator to improve efficiency while in reduced power states. 1=Control over the PSI_L signal is as specified by the PsiVid field of this register. 0=PSI_L is always high. See 2.5.1.3.1 [PSIx_L Bit].
6:0	**PsiVid[6:0]: PSI_L VID threshold**. Read-write. Reset: 0. BIOS: 2.5.1.3.1.1. PsiVid[7:0] = {PsiVid[7], PsiVid[6:0]}. When enabled by PsiVidEn, PsiVid[7:0] specifies the threshold value of the VID code generated by the processor, which in turn determines the state of PSI0_L. When the VID code generated by the processor is less than PsiVid[7:0] (i.e., the VID code is specifying a higher voltage level than the PsiVid-specified voltage level), then PSI0_L is high; when the VID code is greater than or equal to PsiVid[7:0], PSI0_L is driven low. See 2.5.1.3.1 [PSIx_L Bit].

D18F3xA4 Reported Temperature Control

The slew rate controls in this register are used to filter processor temperature measurements. Separate controls are provided for a measured temperaturethat is higher or lower than Tctl. The per-step timer counts as long as the measured temperature stays either above or below Tctl. Each time the measured temperature changes to the other side of Tctl, the step timer resets, and Tctl is not changed. If, for example, step times are enabled in both directions, Tctl=62.625, and the measured temperature keeps jumping quickly between 62.5 and 63.0, then (assuming the step times are long enough) Tctl would not change. However, once the measured temperature settles on one side of Tctl, Tctl can step toward the measured temperature. If the difference of measured temperature minus Tctl is greater than the value set by MaxTmpDiffUp, then Tctl is set equal to the measured temperature. See 2.10 [Thermal Functions].

<table>
<tr><th>Bits</th><th>Description</th></tr>
<tr><td>31:21</td><td>CurTmp: current temperature.
IF (D18F3xA4[CurTmpTjSel]==11b) THEN Read-write. ELSE Read-only; updated-by-hardware. ENDIF. Reset: X. Provides the current control temperature, Tctl, after the slew-rate controls have been applied.
RangeUnajusted = (D18F3xA4[CurTmpTjSel]!=11b).
<table>
<tr><th>Bits</th><th>RangeUnajusted</th><th>Description</th></tr>
<tr><td>000h</td><td>0</td><td>-49</td></tr>
<tr><td>001h</td><td>0</td><td>-48.875</td></tr>
<tr><td>7FEh-002h</td><td>0</td><td><(CurTmp*0.125)-49></td></tr>
<tr><td>7FFh</td><td>0</td><td>206.875</td></tr>
<tr><td>000h</td><td>1</td><td>0</td></tr>
<tr><td>001h</td><td>1</td><td>0.125</td></tr>
<tr><td>7FEh-002h</td><td>1</td><td><CurTmp*0.125></td></tr>
<tr><td>7FFh</td><td>1</td><td>255.875</td></tr>
</table></td></tr>
<tr><td>20</td><td>Reserved.</td></tr>
<tr><td>19:18</td><td>Reserved.</td></tr>
</table>

17:16	**CurTmpTjSel: Current temperature select**. Read-write. Reset: 00. These bits may be used for diagnostic software. Bits Description 00b CurTmp provides the read-only Tctl value. 01b Reserved. 10b Reserved. 11b CurTmp is a read-write register that specifies a value used to create Tctl. The two LSB's are read-only zero.
15:13	Reserved.
12:8	**PerStepTimeDn: per step time down**. Read-write. Cold reset: 18h. BIOS: 0Fh. Specifies the time that measured temperaturemust remain below Tctl before applying a 0.125 downward step. See: PerStepTimeUp.
7	**TmpSlewDnEn: temperature slew downward enable**. Read-write. Cold reset: 0. BIOS: 1. 1=Downward slewing enabled. 0=Downward slewing disabled.
6:5	**TmpMaxDiffUp: temperature maximum difference up**. Read-write. Cold reset: 00b. BIOS: 11b. Specifies the maximum difference, (measured temperature - Tctl), when Tctl immediatly updates to the measured temperature. Bits Description 00b 0.0 (disable upward slew) 01b 1.0 10b 3.0 11b 9.0
4:0	**PerStepTimeUp: per 1/8th degree step time up**. Read-write. Cold reset: 00h. BIOS: 0Fh. Specifies the time that measured temperaturemust remain above Tctl before applying a 0.125 upward step. Bits Definition 1Fh-00h <(PerStepTimeUp[2:0] + 1) * 10^PerStepTimeUp[4:3]> ms, ranging from 1 ms to 8000 ms.

D18F3xA8 Pop Up and Down P-states

Bits	Description
31:29	**PopDownPstate**. Read-write. Reset: D18F3xDC[HwPstateMaxVal]. BIOS: D18F3xDC[HwPstateMaxVal]. Specifies the pop-down P-state number. This field uses hardware P-state numbering. See 2.5.3.2.3.3 [Core C6 (CC6) State].
28:0	Reserved.

D18F3xB8 NB Array Address

Reset: XXXX_XXXXh. D18F3xB8 [NB Array Address] and D18F3xBC [NB Array Data Port] provide a mechanism to inject errors into DRAM and data read from internal NB arrays.

D18F3xB8 should first be written with the target array and address within the array. Read and write accesses to D18F3xBC then access the target address within the target array.

Bits	Description
31:28	**ArraySelect**. Read-write. Selects the NB array to access. Bits — Description 7h-0h — Reserved 8h — D18F3xBC_x8 [DRAM ECC] Fh-9h — Reserved
27:10	Reserved.
9:0	**ArrayAddress**. Read-write. Selects the location to access within the selected array. This format of this field is a function of ArraySelect. ArraySelect — Description 007h-000h — Reserved. 008h — DRAM ECC. 3FFh-009h — Reserved.

D18F3xBC NB Array Data Port

See D18F3xB8 for register access information. Address: D18F3xB8[ArraySelect].

Bits	Description
31:0	**Data**.

D18F3xBC_x8 DRAM ECC

This register controls injection of errors in writes to DRAM. See 2.15.3.1 [DRAM Error Injection].

Bits	Description
31:29	Reserved.
28:20	**ErrInjEn: enable error injection to word**. Read-write. Reset: 0. Each bit in this field corresponds to a 16-bit DRAM word and enables injecting errors in that word. Bit — Description [0] — Data[15:0] [1] — Data[31:16] [2] — Data[47:32] [3] — Data[63:48] [4] — Data[79:64] [5] — Data[95:80] [6] — Data[111:96] [7] — Data[127:112] [8] — ECC[15:0]
19	Reserved.
18	**DramErrEn**. Read-write. Reset: 0. 1=Errors are continually injected on DRAM writes. The error injection takes place only on DRAM write accesses and should be initiated by a non-cacheable store. Errors continue to be injected on writes until this bit is cleared to a 0 by software.

17	**EccWrReq**. Read; write-1-only; cleared-by-hardware. Reset: 0. 1=Error is injected on DRAM write at the bits enabled by ErrInjEn and EccVector. A single error injection takes place on the next DRAM write access and should be initiated by a non-cacheable store. This bit is cleared by hardware after the write.
16	**EccRdReq**. Read; write-1-only; cleared-by-hardware. Reset: 0. 1=Indicates a DRAM ECC read is requested. The read takes place on the next DRAM read access and should be initiated by a non-cacheable load. The ECC bits read from DRAM are stored in EccVector. This bit is cleared by hardware after the read.
15:0	**EccVector: error injection vector**. Read-write. Reset: X. When used in conjunction with EccWrReq, each bit of EccVector enables injecting errors to the corresponding bit within each word enabled by ErrInjEn. When used in conjunction with EccRdReq, EccVector holds the contents of the DRAM ECC bits after the read.

D18F3xD4 Clock Power/Timing Control 0

Bits	Description
31	**NbClkDivApplyAll**. Read-write. Cold reset: 0. BIOS: 1. See NbClkDiv.
30:28	**NbClkDiv: NB clock divisor**. Read-write. Cold reset: Product-specific. BIOS: 100b. Specifies the NB CLK divisor associated with D18F3x80/D18F3x84[NbLowPwrEn]. This divisor is applied while LDTSTOP_L is asserted if the corresponding core CLK divisor, D18F3x80/D18F3x84[ClkDivisor], is set to "turn off clocks" or if NBClkDivApplyAll=1; otherwise, the divisor specified by D18F3x80/D18F3x84[ClkDivisor] is applied. This divisor is relative to the current NB FID frequency, or: 100 MHz * (4 + D18F5x16[C:0][NbFid[5:0]]). If D18F5x16[C:0][NbDid] of the current NB P-state indicates a divisor that is lower than specified by this field, then no NB frequency change is made when entering the low-power state associated with this register (i.e., if this field specifies a divide-by 1 and the DID is divide-by 2, then the divisor remains 2 while in the low-power state). This field is encoded as follows: Bits / Description / Bits / Description 000b / Divide-by 1 / 100b / Divide-by 16 001b / Divide-by 2 / 101b / Reserved 010b / Divide-by 4 / 110b / Reserved 011b / Divide-by 8 / 111b / Reserved

<table>
<tr><td>27:24</td><td>PowerStepUp. Read-write. Cold reset: 0000b. Specifiesthe rate at which blocks of compute unit and NB logic are gated on while the processor transitions from a quiescent state to an active state as part of a power management state transition. There are about 15 steps in this transition for each compute unit and about 5 steps for the NB for the PowerStepDown and PowerStepUp transitions. So the total transition time for a single compute unit is about 15 times the time specified by PowerStepDown and PowerStepUp and the transition time for the NB is about 5 times the time specified by PowerStep-Down and PowerStepUp. Use of longer transition times may help reduce voltage transients associated with power state transitions. The bits for PowerStepUp and PowerStepDown are encoded as follows:
<table>
<tr><th>Bits</th><th>Description</th><th>Bits</th><th>Description</th></tr>
<tr><td>0000b</td><td>Reserved. 10</td><td>00b</td><td>50 ns</td></tr>
<tr><td>0001b</td><td>Reserved. 10</td><td>01b</td><td>Reserved.</td></tr>
<tr><td>0010b</td><td>Reserved. 10</td><td>10b</td><td>Reserved.</td></tr>
<tr><td>0011b</td><td>100 ns</td><td>1011b</td><td>Reserved.</td></tr>
<tr><td>0100b</td><td>90 ns</td><td>1100b</td><td>Reserved.</td></tr>
<tr><td>0101b</td><td>80 ns</td><td>1101b</td><td>Reserved.</td></tr>
<tr><td>0110b</td><td>70 ns</td><td>1110b</td><td>Reserved.</td></tr>
<tr><td>0111b</td><td>60 ns</td><td>1111b</td><td>Reserved.</td></tr>
</table>
• If PowerStepDown or PowerStepUp are programmed to greater than 50 ns, then the value applied to the NB is clipped to 50 ns. The compute unit steps are not clipped.
• BIOS: 1000b.</td></tr>
<tr><td>23:20</td><td>PowerStepDown. Read-write. Cold reset: 0000b. BIOS: 1000b. This specifies the rate at which blocks of compute unit and NB logic are gated off while the processor transitions from an active state to a quiescent state as part of a power management state transition. Valid values are the same as those for PowerStepUp.</td></tr>
<tr><td>19:18</td><td>Reserved.</td></tr>
<tr><td>17:15</td><td>Reserved.</td></tr>
<tr><td>14</td><td>CacheFlushImmOnAllHalt: cache flush immediate on all halt. Read-write. Cold reset: 0. BIOS: 0. 1=Flush the caches immediately when all cores in a package have halted. The following condition must be true in order for the caches to be flushed:
• D18F4x118/D18F4x11C[CacheFlushEn]=1 for the corresponding C-state action field on all cores.</td></tr>
<tr><td>13</td><td>Reserved.</td></tr>
<tr><td>12</td><td>ClkRampHystCtl: clock ramp hysteresis control. Read-write. Cold reset: 0. Specifies the time base for ClkRampHystSel when (D18F4x128[CoreCstateMode] ? (D18F3x80/D18F3x84[CpuPrbEnSmafAct]=0) : (D18F4x118/D18F4x11C[CpuPrbEnCstAct]=0)). 0=320 ns. 1=1.28 us.</td></tr>
</table>

11:8	**ClkRampHystSel: clock ramp hysteresis select**. Read-write. Cold reset: 0h. BIOS: Fh. When the core(s) are in the stop-grant or halt state and a probe request is received, the core clock may need to be brought up to service the probe. • If (D18F4x128[CoreCstateMode] ? (D18F3x80/D18F3x84[CpuPrbEnSmafAct]=0) : (D18F4x118/D18F4x11C[CpuPrbEnCstAct]=0)) then this field specifies how long the core clock is left up to service additional probes before being brought back down. Each time a probe request is received, the hysteresis timer is reset such that the period of time specified by this field must expire with no probe request before the core clock is brought back down. The hysteresis time is encoded as (the time base specified by D18F3xD4[ClkRampHystCtl]) * (1 + ClkRampHystSel). • If (D18F4x128[CoreCstateMode] ? (D18F3x80/D18F3x84[CpuPrbEnSmafAct]=1) : (D18F4x118/D18F4x11C[CpuPrbEnCstAct]=1)) then this field specifies a fixed amount of time to allow for probes to be serviced after completing the transition of each core. If, for example, two cores enter stop-grant or halt at the same time, then (1) the first core would complete the transition to the low power state, (2) probe traffic would be serviced for the time specified by this field, (3) the second core would complete the transition to the low power state, and (4) probe traffic would be seviced for the time specified by this field (and afterwards, until the next power state transition). For this purpose, values range from 0h=40 ns to Fh=640 ns, encoded as 40 ns * (1 + ClkRampHystSel).
7:6	Reserved.
5:0	**MaxSwPstateCpuCof:maximum software P-state core COF.** Read-only. Cold reset: Product-specific. Specifies the maximum CPU COF supported by the processor in a software P-state. The maximum frequency is 100 MHz * MaxSwPstateCpuCof, if MaxSwPstateCpuCof is greater than zero; if MaxSwPstateCpuCof = 00h, then there is no frequency limit. Any attempt to change a software P-state CPU COF to a frequency greater than specified by this field is ignored. See2.5.3.1.1.1 [Software P-state Numbering] .

D18F3xD8 Clock Power/Timing Control 1

See 2.5.1.4 [Voltage Transitions].

Bits	Description
31:7	Reserved.
6:4	**VSRampSlamTime**. Read-write. Cold reset: 000b. BIOS: 100b. Specifies the time the processor waits for voltage transitions to complete before beginning an additional voltage change or a frequency change. Wait time = (VSRampSlamTime / 15mV) * ABS(destination voltage - current voltage). Bits / Description / Bits / Description 000b 5.00 us 100b 2.00 us 001b 3.75 us 101b 1.50 us 010b 3.00 us 110b 1.20 us 011b 2.40 us 111b 1.00 us
3:0	Reserved.

D18F3xDC Clock Power/Timing Control 2

Bits	Description
31:30	**NbsynPtrAdjPstate[2:1]: NB/core synchronization FIFO pointer adjust P-state[2:1]**. Read-write. Reset: Product-specific. See NbsynPtrAdj.
29:27	**NbsynPtrAdjLo: NB/core synchronization FIFO pointer adjust low**. Read-write. Cold reset: 000b. BIOS: IF (D18F5x260[ClkStretchEn] && D18F5x260[ClkStretchPercent]==1) THEN 011b. ELSIF (D18F5x260[ClkStretchEn] && D18F5x260[ClkStretchPercent]==2). THEN 011b. ELSE 101b. ENDIF. See NbsynPtrAdj.
26	**IgnCpuPrbEn: ignore CPU probe enable**. Read-write. Cold reset: 0. BIOS: 1. See D18F3x80/D18F3x84[CpuPrbEnSmafAct] and D18F4x118/D18F4x11C[CpuPrbEnCstAct].
25:19	**CacheFlushOnHaltTmr: cache flush on halt timer**. Read-write. Cold reset: 00h. BIOS: 32h. Specifies how long each core needs to stay in a C-state before it flushes its caches. See CacheFlushOnHaltCtl, D18F3x80/D18F3x84[CpuPrbEnSmafAct], and D18F4x118/D18F4x11C[CacheFlushTmrSel]. Bits: Description 00h: 5.12 us 7Fh-01h: (<CacheFlushOnHaltTmr> * 10.24us) - 5.12us <= Time <= <CacheFlushOnHaltTmr> * 10.24 us
18:16	**CacheFlushOnHaltCtl: cache flush on halt control**. Read-write. Cold reset: 000b. BIOS: 111b. Enables cache flush on halt when (CacheFlushOnHaltCtl != 0). Specifies what core clock divisor is used after the caches have been flushed. See D18F4x118/D18F4x11C[CacheFlushTmrSel]. Bits: Description 000b: Divide-by 1 001b: Divide-by 2 010b: Divide-by 4 011b: Divide-by 8 100b: Divide-by 16 101b: Reserved 110b: Reserved 111b: Turn off clocks See D18F3x[84:80] and D18F4x11[C:8] for clock divisor specifications that are in effect during a C-state before the caches have been flushed. See 2.5.3.2.3.1 [C-state Probes and Cache Flushing].
15	**NbsynPtrAdjPstate[0]: NB/core synchronization FIFO pointer adjust P-state[0]**. Read-write. Reset: Product-specific. See NbsynPtrAdj.

14:12	**NbsynPtrAdj: NB/core synchronization FIFO pointer adjust**. Read-write. Cold reset: 000b. BIOS: IF (D18F5x260[ClkStretchEn] && D18F5x260[ClkStretchPercent]==1) THEN 011b. ELSIF (D18F5x260[ClkStretchEn] && D18F5x260[ClkStretchPercent]==2). THEN 011b. ELSE 101b. ENDIF. Changes to this field take effect after any of the following events: • Warm reset. • At least one core on all compute units perform a P-state transition. • An NB P-state transition. There is a synchronization FIFO between the NB clock domain and core clock domains. At cold reset, the read pointer and write pointer for each of these FIFOs is positioned conservatively, such that FIFO latency may be greater than is necessary. NbsynPtrAdj and NbsynPtrAdjLo may be used to position the read pointer and write pointer of each FIFO closer to each other such that latency is reduced. Each increment of NbsynPtrAdj and NbsynPtrAdjLo represents one clock cycle of whichever is the slower clock (longer period) between the NB clock and the core clock. NbsynPtrAdj is used when the core P-state is less than or equal to NbsynPtrAdjPstate, otherwise NbsynPtrAdjLo is used. Values less than the recommended value are allowed; values greater than the recommended value are illegal. Bits — Description 6h-0h — Position the read pointer <NbsynPtrAdj, NbsynPtrAdjLo> clock cycles closer to the write pointer. 7h — Reserved
11	Reserved.
10:8	**HwPstateMaxVal: P-state maximum value**. Read-write. IF ((D18F3xE8[HtcCapable]==1) && (D18F3x64[HtcTmpLmt]!=0) && (D18F3x64[HtcPstateLimit] > HwPstateMaxVal)) THEN BIOS: D18F3x64[HtcPstateLimit]. ENDIF. Cold reset: specified by the reset state of MSRC001_00[6B:64][PstateEn]; the cold reset value is the highest P-state number corresponding to the MSR in which PstateEn is set (e.g., if MSRC001_0064 and MSRC001_0065 have this bit set and the others do not, then HwPstateMaxVal=1; if MSRC001_0064 has this bit set and the others do not, then HwPstateMaxVal=0). This specifies the highest P-state value (lowest performance state) supported by the hardware. This field must not be written to a value less (higher performance) than MSRC001_0071[CurPstateLimit]. See MSRC001_0061[PstateMaxVal]. This field uses hardware P-state numbering. See 2.5.3.1.1.2 [Hardware P-state Numbering].
7:0	Reserved.

D18F3xE4 Thermtrip Status

Bits	Description
31	**SwThermtp: software THERMTRIP**. Write-1-only; cleared-by-hardware. Reset: 0. Writing a 1 to this bit position induces a THERMTRIP event. This bit returns 0 when read. This is a diagnostic bit, and it should be used for testing purposes only.
30:6	Reserved.

5	**ThermtpEn: THERMTRIP enable**.Read-only.Reset: Product-specific. 1=The THERMTRIP state is supported. See 2.10.3.3 [THERMTRIP].
4	Reserved.
3	**ThermtpSense: THERMTRIP sense**. Read-only. Cold reset: 0. 1=The processor temperature exceeded the THERMTRIP value (regardless as to whether the THERMTRIP state is enabled). This bit is also set when the diagnostic bit SwThermtp==1.
2	Reserved.
1	**Thermtp: THERMTRIP**. Read-only. Cold reset: 0. 1=The processor has entered the THERMTRIP state.
0	Reserved.

D18F3xE8 Northbridge Capabilities

Read-only. Value: Product-specific. Unless otherwise specified, 1=The feature is supported by the processor; 0=The feature is not supported.

Bits	Description
31:29	Reserved.
28	**SUCCOR**. Read-only. See CPUID Fn8000_0007_EBX[SUCCOR]. Value: 0.
27:26	Reserved.
25	Reserved.
24	**MemPstateCap: memory P-state capable**.
23:20	Reserved.
19	**x2Apic: x2APIC capability**. Value: 0.
18:16	Reserved.
15	Reserved.
14	**MultVidPlane: multiple VID plane capable**. Value: 1.
13:12	Reserved.
11	Reserved.
10	**HtcCapable: HTC capable**. This affects D18F3x64 and D18F3x68.
9	**SvmCapable: SVM capable**.
8	**MctCap: memory controller (on the processor) capable**. Value: 1.
7:5	Reserved.
4	**ChipKill: chipkill ECC capable**.
3	**ECC: ECC capable**.
2	**EightNode: Eight-node multi-processor capable**.

1	**DualNode: Dual-node multi-processor capable**.
0	Reserved.

D18F3xF0 DEV Capability Header Register

The DEV secure loader function is configured through D18F3xF4 and D18F3xF8. The register number (i.e., the number that follows F8_x in the register mnemonic) is specified by D18F3xF4[DevFunction]. Access to this register is accomplished as follows:

- Reads: Write the register number to D18F3xF4[DevFunction]. Read the register contents from D18F3xF8.
- Writes: Write the register number to D18F3xF4[DevFunction]. Write the register contents to D18F3xF8.

IF (D18F3xE8[SvmCapable]==0) THEN

Bits	Description
31:0	Reserved.

ELSE

Bits	Description
31:0	Reserved.

ENDIF.

D18F3xF4 DEV Function Register

Reset: 0000_0000h. Reserved if (D18F3xE8[SvmCapable]==0).

Bits	Description
31:0	Reserved.

D18F3xF8 DEV Data Port

Reset: 0000_0000h. Address: D18F3xF4[DevFunction]. See D18F3xF0 for details about this port.

Bits	Description
31:0	Reserved.

D18F3xF8_x4 DEV Secure Loader Control Register

Reset: 0000_0000h.

Bits	Description
31:8	Reserved.
7:5	Reserved.
4:0	Reserved.

D18F3xFC CPUID Family/Model/Stepping

CPUID Fn0000_0001_EAX, CPUID Fn8000_0001_EAX are an alias of D18F3xFC.

Bits	Description
31:28	Reserved.
27:20	**ExtFamily: extended family**. Read-only. Value: 06h.
19:16	**ExtModel: extended model**. Read-only. Value: Product-specific.
15:12	Reserved.
11:8	**BaseFamily**. Read-only. Reset: Fh.
7:4	**BaseModel**. Read-only. Value: Product-specific.
3:0	**Stepping**. Read-only. Value: Product-specific.

D18F3x138 DCT0 Bad Symbol Identification

Bits	Description
31:0	Reserved.

D18F3x13C DCT1 Bad Symbol Identification

Bits	Description
31:0	Reserved.

D18F3x140 SRI to XCS Token Count

Out of cold reset, the processor allocates a minimal number of buffers that is smaller than the default values in the register. BIOS must use D18F0x6C[RlsLnkFullTokCntImm] for the values in the register to take effect. This is necessary even if the values are unchanged from the default values.

D18F3x140, D18F3x144, and D18F3x1[54,50,4C,48] specify the number of XCS (XBAR command scheduler) entries assigned to each virtual channel within each source port. See 2.8 [Northbridge (NB)]. The default totals are:

Buffer allocation rules:

- The totals of SRI, MCT and the links must not exceed the number of XCS entries. XcsSize = 52.
  - SUM(D18F3x140[UpReqTok, UpPreqTok, UpRspTok, DnReqTok, DnPreqTok, DnRspTok, IsocReqTok, IsocPreqTok, IsocRspTok, FreeTok]) + SUM(D18F3x144[ProbeTok, RspTok]) + SUM(D18F3x148[ReqTok0, PReqTok0, RspTok0, ProbeTok0, {FreeTok[3:2],FreeTok[1:0]}, IsocReqTok0, IsocPReqTok0, IsocRspTok0, ReqTok1, PReqTok1, RspTok1, ProbeTok1, IsocReqTok1, IsocPReqTok1, IsocRspTok1]) + SUM(D18F3x14C[ReqTok0, PReqTok0, RspTok0, ProbeTok0, {FreeTok[3:2],FreeTok[1:0]}, IsocReqTok0, IsocPReqTok0, IsocRspTok0, ReqTok1, PReqTok1, RspTok1, ProbeTok1, IsocReqTok1, IsocPReqTok1, IsocRspTok1]) <= XcsSize. See D18F3x1[54,50,4C,48].

The defaults for D18F3x140 and D18F3x1[54,50,4C,48]do not allocate any tokens in the isochronous channel. If isochronous flow control mode (IFCM) is enabled (D18F0x[E4,C4,A4,84][IsocEn]), then the XCS token counts must be changed.

- If IFCM is enabled, then D18F3x140[IsocReqTok, IsocRspTok] must each be non-zero. If isochronous posted requests may be generated in the system, then D18F3x140[IsocPreqTok] must also be non-zero.
- If an IOMMU is present, D18F3x1[54,50,4C,48][IsocReqTok] must be non-zero.

Bits	Description
31:25	Reserved.
24:20	**FreeTok: free tokens**. Read-write. Cold Reset: 0Ch. BIOS: Ch. The number of free tokens must always be greater than or equal to 2 to ensure deadlock free operation.
19:18	Reserved.
17:16	**IsocRspTok: isochronous response tokens**. Read-write. Cold Reset: 0. BIOS: 1.
15:14	**IsocPreqTok: isochronous posted request tokens**. Read-write. Cold Reset: 0. BIOS: 0.
13:12	**IsocReqTok: isochronous request tokens**. Read-write. Cold Reset: 0. BIOS: 1.
11:10	**DnRspTok: downstream response tokens**. Read-write. Cold Reset: 1. BIOS: 2.
9:8	**UpRspTok: upstream response tokens**. Read-write. Cold Reset: 3. BIOS: 1.
7:6	**DnPreqTok: downstream posted request tokens**. Read-write. Cold Reset: 1. BIOS: 1.
5:4	**UpPreqTok: upstream posted request tokens**. Read-write. Cold Reset: 1. BIOS: 1.
3:2	**DnReqTok: downstream request tokens**. Read-write. Cold Reset: 1. BIOS: 1.
1:0	**UpReqTok: upstream request tokens**. Read-write. Cold Reset: 3. BIOS: 3.

D18F3x144 MCT to XCS Token Count

See D18F3x140.

Bits	Description
31:8	Reserved.
7:4	**ProbeTok: probe tokens**. Read-write. Cold Reset: 7h. BIOS: 4h.
3:0	**RspTok: response tokens**. Read-write. Cold Reset: 7h. BIOS: Bh.

D18F3x1[54,50,4C,48] Link to XCS Token Count

See D18F3x140.

Table 188: Register Mapping for D18F3x1[54,50,4C,48]

Register	Function
D18F3x148	ONION Link
D18F3x14C	ONIONPlus Link
D18F3x1[54:50]	Reserved

Bits	Description
31:30	**FreeTok[3:2]: free tokens**. Read-write. Cold reset: 00b. BIOS: 0. See FreeTok[1:0].
29	Reserved.
28	**IsocRspTok1: isochronous response tokens sublink 1**. Read-write. Cold reset: 0. BIOS: 0.
27	Reserved.
26	**IsocPreqTok1: isochronous posted request tokens sublink 1**. Read-write. Cold reset: 0. BIOS: 0.
25	Reserved.
24	**IsocReqTok1: isochronous request tokens sublink 1**. Read-write. Cold reset: 0. BIOS: 0.
23:22	**ProbeTok1: probe tokens sublink 1**. Read-write. Cold reset: 0. BIOS: 0.
21:20	**RspTok1: response tokens sublink 1**. Read-write. Cold reset: 0. BIOS: 0.
19:18	**PReqTok1: posted request tokens sublink 1**. Read-write. Cold reset: 0. BIOS: 0.
17:16	**ReqTok1: request tokens sublink 1**. Read-write. Cold reset: 0. BIOS: 0.
15:14	**FreeTok[1:0]: free tokens**. Read-write. Cold reset: 00b. FreeTok[3:0] = {FreeTok[3:2], FreeTok[1:0]}. BIOS: IF (REG==D18F3x148) THEN 01b. ELSE 10b. ENDIF.
13:12	**IsocRspTok0: isochronous response tokens sublink 0**. Read-write. Cold reset: 0.BIOS: 0.
11:10	**IsocPreqTok0: isochronous posted request tokens sublink 0**. Read-write. Cold reset: 0. BIOS: IF (REG==D18F3x148) THEN 1. ELSE 0. ENDIF. See D18F0x6C[ApplyIsocModeEnNow].
9:8	**IsocReqTok0: isochronous request tokens sublink 0**. Read-write. Cold reset: 0. BIOS: IF (REG==D18F3x148) THEN 1. ELSE 0. ENDIF.

7:6	**ProbeTok0: probe tokens sublink 0**. Read-write. Cold reset: 2. BIOS: 0.
5:4	**RspTok0: response tokens sublink 0**. Read-write. Cold reset: 2. BIOS: IF (REG==D18F3x148) THEN 2. ELSE 0. ENDIF.
3:2	**PReqTok0: posted request tokens sublink 0**. Read-write. Cold reset: 2. BIOS: IF (REG==D18F3x148) THEN 2. ELSE 0. ENDIF.
1:0	**ReqTok0: request tokens sublink 0**. Read-write. Cold reset: 2. BIOS: IF (REG==D18F3x148) THEN 2. ELSE 3. ENDIF.

D18F3x160 NB Machine Check Misc (DRAM Thresholding) 0 (MC4_MISC0)

See 2.15.1 [Machine Check Architecture] for a general description of the machine check architecture.
See 2.15.1.7 [Error Thresholding]. D18F3x160 is associated with the DRAM error type. See MSR0000_0413.

Bits	Description
31	**Valid**. Read-only. Reset: 1.
30	**CntP: counter present**. Read-only. Reset: 1.
29	**Locked**. Read-only. Reset: 0.
28:24	Reserved.
23:20	**LvtOffset: LVT offset**. IF (Locked) THEN Read-only. ELSE Read-write. ENDIF. Reset: 0. BIOS: 1.
19	**CntEn: counter enable**. IF (Locked) THEN Read-only. ELSE Read-write. ENDIF. Reset: 0.
18:17	**IntType: interrupt type**. IF (Locked) THEN Read-only. ELSE Read-write. ENDIF. Cold reset: 0.
16	**Ovrflw: overflow.** IF (Locked) THEN Read-only; set-by-hardware. ELSE Read-write; set-by-hardware. ENDIF. Cold reset: 0.
15:12	Reserved.
11:0	**ErrCnt: error counter**. IF (Locked) THEN Read-only; updated-by-hardware. ELSE Read-write; updated-by-hardware. ENDIF. Cold reset: 0.

D18F3x168 NB Machine Check Misc (Link Thresholding) 1 (MC4_MISC1)

See 2.15.1.7 [Error Thresholding]. D18F3x168 is associated with the link error type. See MSRC000_0408.

Bits	Description
31	**Valid**. Read-only. Reset: 1.
30	**CntP: counter present**. Read-only. Reset: 1.
29	**Locked**. Read-only. Reset: 0.
28:24	Reserved.
23:20	**LvtOffset: LVT offset**. IF (Locked) THEN Read-only. ELSE Read-write. ENDIF. Reset: 0. BIOS: 1.
19	**CntEn: counter enable**. IF (Locked) THEN Read-only. ELSE Read-write. ENDIF. Reset: 0.
18:17	**IntType: interrupt type**. IF (Locked) THEN Read-only. ELSE Read-write. ENDIF. Cold reset: 0.
16	**Ovrflw: overflow.** IF (Locked) THEN Read-only; set-by-hardware. ELSE Read-write; set-by-hardware. ENDIF. Cold reset: 0.

15:12	Reserved.
11:0	**ErrCnt: error counter**. IF (Locked) THEN Read-only; updated-by-hardware. ELSE Read-write; updated-by-hardware. ENDIF. Cold reset: 0.

D18F3x17C Extended Freelist Buffer Count

Out of cold reset, the processor allocates a minimal number of buffers that is smaller than the default values in the register. BIOS must use D18F0x6C[RlsLnkFullTokCntImm] for the values in the register to take effect. This is necessary even if the values are unchanged from the default values.

Bits	Description
31:4	Reserved.
3:0	**SPQPrbFreeCBC: XBAR to SRI Probe command buffer freelist**. Cold Reset: 8h. Read-write. BIOS: 8h.

D18F3x180 Extended NB MCA Configuration

Reset: 0000_0000h. This register is an extension of D18F3x44 [MCA NB Configuration].

Bits	Description
31	Reserved.
30	Reserved.
29	**SyncFloodOnDramUncCrcErr**. Read-write. 1=Enable generation of Sync flood on DRAM Uncorrectable CRC Error.
28	**SyncFloodOnCC6DramUcErr**. Read-write. BIOS: 1. 1=Enable generation of Sync flood when an Uncorrectable ECC error occurs on C6 restore reads.
27	Reserved.
26	**ConvertUnCorToCorErrEn: convert uncorrectable error to correctable error enable**. Read-write. 1=The status of uncorrectable errors is changed to appear as correctable errors; MSR0000_0411[UC, PCC] are cleared and a machine check exception will not be raised. For uncorrectable ECC errors, MSR0000_0411[UECC] is cleared and MSR0000_0411[CECC] is set. This field is intended for debug observability.
25	**EccSymbolSize: ECC symbol size and code selection**. Read-write. BIOS: See 2.15.2 [DRAM ECC Considerations]. 0=x4 symbol size and code used. 1=Reserved.
24	**McaLogErrAddrWdtErr: log error address on WDT errors**. Read-write. BIOS: 1. 1=When a watchdog timeout error occurs (see MSR0000_0410[WDTRptEn]), the associated address is logged and MSR0000_0411[AddrV] is set. 0=When a watchdog timeout error occurs, NB state information is saved and MSR0000_0411[AddrV] is cleared. See D18F3x50 for details on saved information.
23	**SyncFloodOnDramTempErr**. Read-write. 1=Sync flood is generated on a DRAM temp Error.
22	Reserved.

21	**SyncFloodOnCpuLeakErr: sync flood on CPU leak error**. Read-write. BIOS: 1. 1=Enable Sync flood when one of the cores encounters an uncorrectable error which cannot be contained to the process on the core.
20	Reserved.
19	**PwP2pDatErrRmtPropDis: posted write for remote peer-to-peer data error propagation disable**. Read-write. 1=A peer-to-peer posted write with a data error is not propagated to the target IO link chain if the target IO link chain is not attached to the local node (the same node as the source IO link chain). Instead, the write is dropped by the host bridge. The state of this field is ignored if SyncFloodOnUsPwDatErr==1 or DatWrErrDeferEn==0.
18	**PwP2pDatErrLclPropDis: posted write for local peer-to-peer data error propagation disable**. Read-write. 1=A peer-to-peer posted write with a data error is not propagated to the target IO link chain if the target IO link chain is attached to the local node (the same node as the source IO link chain). Instead, the write is dropped by the host bridge. The state of this field is ignored if SyncFloodOnUsPwDatErr==1 or DatWrErrDeferEn==0.
17	**SyncFloodOnDeferErrToIO: convert deferred error for an IO link to sync flood enable**. Read-write. BIOS: 1. 1=A deferred error which targets an IO link device is turned into a Sync flood. • When DramErrDeferEn is set and the read response is for a DMA read with a data error, setting SyncFloodOnDeferErrToIO causes a Sync flood. • When DatWrErrDeferEn is set and the write is peer-to-peer, setting SyncFloodOnDeferErrToIO causes a Sync flood.
16	**DeferDatErrNcHtMcaEn: convert deferred error for an IO link to machine check exception enable**. IF (D18F3xE8[SUCCOR]) THEN Read-write. ELSE Read-only. ENDIF. 1=A deferred error which targets an IO link device is turned into a machine check exception. • When DramErrDeferEn is set and the read response is for a DMA read with a data error, setting DeferDatErrNcHtMcaEn causes an uncorrected error to be logged and a machine check exception to be generated. An error response is returned to the IO device irrespective of the setting of DeferDatErrNcHtMcaEn. • When DatWrErrDeferEn is set and the write is peer-to-peer, setting DeferDatErrNcHtMcaEn causes an uncorrected error to be logged and a machine check exception to be generated. An error indication is sent to the target IO device irrespective of the setting of DeferDatErrNcHtMcaEn.
15	Reserved.
14:11	Reserved.
10	Reserved.
9	**SyncFloodOnUCNbAry: sync flood on UC NB array error**. Read-write. BIOS: 1. 1=Enable Sync flood on detection of an UC error in an NB array.
8	**SyncFloodOnProtErr: sync flood on protocol error**. Read-write. BIOS: 1. 1=Enable Sync flood on detection of link protocol error, L3 protocol error, and probe filter protocol error.
7	**SyncFloodOnTgtAbortErr**. Read-write. BIOS: 1. 1=Enable Sync flood on generated or received link responses that indicate target aborts.
6	**SyncFloodOnDatErr**. Read-write. BIOS: 1. 1=Enable Sync flood on generated or received link responses that indicate data error.

5	**DisPciCfgCpuMstAbortRsp**. Read-write. BIOS: 1. 1=For master abort responses to CPU-initiated configuration accesses, disables MCA error reporting and generation of an error response to the core. It is recommended that this bit be set in order to avoid MCA exceptions being generated from master aborts for PCI configuration accesses, which are common during device enumeration.
4	**ChgMstAbortToNoErr**. Read-write. 1=Signal no errors instead of master abort in link response packets to IO devices on detection of a master abort condition. When ChgMstAbortToNoErr and D18F3x44[IoMstAbortDis] are both set, ChgMstAbortToNoErr takes precedence.
3	**ChgDatErrToTgtAbort**. Read-write. 1=Signal target abort instead of data error in link response packets to IO devices (for Gen1 link compatibility).
2	**WDTCntSel[3]: watchdog timer count select bit[3]**. Read-write. See D18F3x44[WDTCntSel].
1	**SyncFloodOnUsPwDatErr: sync flood on upstream posted write data error**. Read-write. BIOS: 1. 1=Enable Sync flood generation when an upstream posted write data error is detected.
0	**McaLogUsPwDatErrEn: MCA log of upstream posted write data error enable**. Read-write. BIOS: 1. 1=Enable logging of upstream posted write data errors in MCA (if NB MCA registers are appropriately enabled and configured).

D18F3x188 NB Configuration 2

Same-for-all.

Bits	Description
31:28	Reserved.
27	**DisCpuWrSzDw64ReOrd: disable streaming store reorder**. Read-write. Reset: 1. BIOS: 1. 1=Disable reordering of streaming store commands.
26:10	Reserved.
9	**DisL3HiPriFreeListAlloc**. Read-write. Reset: 0. BIOS: 1. 1=Disables normal SRQ entry scheme which gives higher priority to XBAR.
8:0	Reserved.

D18F3x190 Downcore Control

Cold reset: 0000_0000h. See 2.4.4 [Processor Cores and Downcoring] and 2.4.4.1 [Software Downcoring using D18F3x190[DisCore]].

Bits	Description
31:0	**DisCore**. Read-write; reset-applied. 0=Core enabled. 1=Core disabled. Bit — Description [0] — Core 0. [2:1] — Core <BIT>. [3] — Core 3. [31:4] — Reserved.

D18F3x1A0 Core Interface Buffer Count

Out of cold reset, the processor allocates a minimal number of buffers that is smaller than the default values in

the register. BIOS must use D18F0x6C[RlsLnkFullTokCntImm] for the values in the register to take effect. This is necessary even if the values are unchanged from the default values.

- The following buffer allocations rules must be satisfied:
  - CpuCmdBufCnt >= 2.

Bits	Description
31	Reserved.
30:26	**NbToCpuPrbLmt**. Read-write. Reset: 0Fh. BIOS: Ch. Maximum number of outstanding probes to the compute-unit. Bits: Description 02h-00h: Reserved. 0Fh-03h: Maximum of <NbToCpuPrbLmt> probes. 1Fh-10h: Reserved.
25:24	Reserved.
23:20	**NbToCpuDatReqLmt**. Read-write. Reset: Ch. Octoword outstanding per core limit. Bits: Description Ch-0h: Octoword outstanding per core limit. Fh-Dh: Reserved.
19	Reserved.
18:16	**CpuToNbFreeBufCnt**. Read-write. Cold Reset: 2h. BIOS: 3h. Provides the number of tokens which can released to each compute unit from the freelist pool. This field can be updated at any time by BIOS and does not require a warm reset to take effect.
15:12	Reserved. Cold reset: 4h.
11:10	Reserved.
9:4	Reserved.
3	Reserved.
2:0	**CpuCmdBufCnt: CPU to SRI command buffer count**. Read-write; reset-applied. Cold Reset: 2h. BIOS: 1h. Each compute unit is allocated the number of buffers specified by this field.

D18F3x1CC IBS Control

Reset: 0000_0000h. MSRC001_103A is an alias of D18F3x1CC. D18F3x1CC is programmed by BIOS; The OS reads the LVT offset from MSRC001_103A.

Bits	Description
31:9	Reserved.
8	**LvtOffsetVal: local vector table offset valid**. Read-write. BIOS: 1. 1=The offset in LvtOffset is valid. 0=The offset in LvtOffset is not valid and IBS interrupt generation is disabled.

7:4	Reserved.
3:0	**LvtOffset: local vector table offset**. Read-write. BIOS: 0h. Specifies the address of the IBS LVT entry in the APIC registers. See APIC[530:500]. Bits: Description 3h-0h: LVT address = <500h + LvtOffset<<4> Fh-4h: Reserved

D18F3x1FC Product Information Register 1

Bits	Description
31:22	Reserved.
21	**VddrLowVoltageSupport**.Value: Product-specific. 1=BIOS sets VDDR and VDDP voltage to 0.95V, limits DRAM rate to 1600, and limits PCIe to Gen2. 0=Default VDDR and VDDP voltages.
20:17	**DiDtCfg4**. Value: Product-specific. See MSRC001_1028[DiDtCfg4].
16	**DiDtCfg3**. Value: Product-specific. See MSRC001_1028[DiDtCfg3].
15:14	**DiDtCfg2**. Value: Product-specific. See MSRC001_1028[DiDtCfg2].
13:6	**DiDtCfg1**. Value: Product-specific. See MSRC001_1028[DiDtCfg1].
5:1	**DiDtCfg0**. Value: Product-specific. See MSRC001_1028[DiDtCfg0].
0	**DiDtMode**. Value: Product-specific. See MSRC001_1028[DiDtMode].

D18F3x200 Performance Mode Control Register

Bits	Description
31:8	Reserved.
7:4	**EnCpuSkidBufFull**. Read-write. Reset: 0. Enables optimal use of the CPU skid buffers, in the presence of multiple data movement requests from the same core.
3	**EnMcqPrbPickThrottle**. Read-write. Reset: 0. BIOS: 1. 1=Enabling throttling the MCQ to ensure the bypass path is taken by the probes instead of allocating in to the XCS.
2	**EnDctOddToNcLnkDatXfr**. Read-write. Reset: 0. BIOS: 1. 1=Enables direct transfer of data from odd-numbered DRAM channels (1,3,..) to non-coherent links on the local node.
1	**EnDctEvnToNcLnkDatXfr**. Read-write. Reset: 0. BIOS: 1. 1=Enables direct transfer of data from even-numbered DRAM channels (0,2,..) to non-coherent links on the local node.
0	Reserved.

D18F3x238 DCT2 Bad Symbol Identification

Bits	Description
31:0	Reserved.

D18F3x23C DCT3 Bad Symbol Identification

Bits	Description
31:0	Reserved.

D18F3x2B4 DCT and Fuse Power Gate Control

See 2.5.4.3 [Fuse Power Gating].

Bits	Description
31:27	Reserved.
26	**FusePwrStatus**. Read-only. Cold reset: 0. Specifies whether fuses are power-gated. 1=Fuses are powered. 0=Fuses are powered-down.
25:24	**PwrDnHyst**. Read-write. Cold reset: 00b. Specifies the minimum amount of time that must expire with no fuse power up events before fuse power gating is initiated. Bits — Description 00b — 10 us 01b — 32 us 10b — 128 us 11b — Reserved.
23:22	**PostPwrDnDelay**. Read-write. Cold reset: 00b. Specifies the amount of time between the completion of fuse power gating and the start of a new fuse power operation. Bits — Description 00b — 1 RefClk 01b — 64 RefClks 10b — 128 RefClks 11b — 256 RefClks
21:20	Reserved.
19:18	**PostPwrUpDelay**. Read-write. Cold reset: 00b. Specifies the amount of time between the completion of fuse power ungating and the start of a new fuse power operation. Bits — Description 00b — 1 RefClk 01b — Reserved. 10b — Reserved. 11b — Reserved.
17:16	**PrePwrUpDelay**. Read-write. Cold reset: 00b. Specifies the amount of time between a power up event and the start of fuse power ungating. Bits — Description 00b — 1 RefClk 01b — Reserved. 10b — Reserved. 11b — Reserved.

15:12	Reserved.
11:8	**DctClkGateEn**. Read-write. Cold reset: 0h. BIOS: 6h. 1=Enable DCT clock gating. 0=Disable DCT clock gating. [0]=DCT 0; ...; [3]=DCT 3. Once clock gating has been enabled, it cannot be disabled without a cold reset.
7:4	Reserved.
3:0	**DctPwrGateEn**. Read-write. Cold reset: 0h. BIOS: 6h. 1=Enable static DCT power gating. 0=Disable static DCT power gating. [0]=DCT 0; ...; [3]=DCT 3. There are two power islands in the DCT, one for DCT 0 and 3, and another for DCT 1 and 2. An island is only power gated if power gating is enabled for all DCTs on the power island. An island is physically power gated when the northbridge enters its NB C-state, and remain so if configured properly with DctPwrGateEn. For any given DCT, DctClkGateEn is required to be set prior to or in parallel with DctPwrGateEn being set.

3.13 Device 18h Function 4 Configuration Registers

See 3.1 [Register Descriptions and Mnemonics]. See 2.7 [Configuration Space].

D18F4x00 Device/Vendor ID

Bits	Description
31:16	**DeviceID: device ID**. Read-only. Value: 141Eh.
15:0	**VendorID: vendor ID**. Read-only. Value: 1022h.

D18F4x04 Status/Command

Bits	Description
31:16	**Status**. Read-only. Reset: 0000_0000_000X_0000b. Only Status[4] may be set to indicate the existence of a PCI-defined capability block. 0=No supported links are unganged. 1=At least one link may be unganged, in which case there is a capability block associated with sublink one of the link in this function.
15:0	**Command**. Read-only. Value: 0000h.

D18F4x08 Class Code/Revision ID

Reset: 0600_0000h.

Bits	Description
31:8	**ClassCode**. Read-only. Provides the host bridge class code as defined in the PCI specification.
7:0	**RevID: revision ID**. Read-only.

D18F4x0C Header Type

Reset: 0080_0000h.

Bits	Description
31:0	**HeaderTypeReg**. Read-only. These bits are fixed at their default values. The header type field indicates that there are multiple functions present in this device.

D18F4x34 Capabilities Pointer

Bits	Description
31:8	Reserved.
7:0	**CapPtr: capabilities pointer**. Read-only. Value: 00h.

D18F4x110 Sample and Residency Timers

Bits	Description
31:21	Reserved.
20:13	**MinResTmr: minimum residency timer**. IF D18F4x15C[BoostLock] THEN Read-only. ELSE Read-write. ENDIF. Cold reset: Product-specific. Specifies the minimum amount of time required between TDP-initiated P-state transitions. The minimum amount of time is defined as MinResTmr * CSampleTimer * 5.12us .
12	Reserved.
11:0	**CSampleTimer**. IF D18F4x15C[BoostLock] THEN Read-only. ELSE Read-write. Cold reset: 0. Specifies the value that the internal CSampleTimer counter must increment to before expiring. When the internal CSampleTimer counter expires, it is reset to 0. See 2.5.9 [Application Power Management (APM)].

D18F4x11[C:8] C-state Control

D18F4x11[C:8] consist of three identical 16-bit registers, one for each C-state Action Field (CAF) associated with an IO address that is read to enter C-states. Refer to 2.5.3.2 [Core C-states].

- D18F4x118[15:0] specifies the actions attempted by the core when software reads from the IO address specified by MSRC001_0073[CstateAddr].
- D18F4x118[31:16] specifies the actions attempted by the core when software reads from the IO address specified by MSRC001_0073[CstateAddr]+1.
- D18F4x11C[15:0] specifies the actions attempted by the core when software reads from the IO address specified by MSRC001_0073[CstateAddr]+2.

D18F4x118 C-state Control 1

Bits	Description
31:30	Reserved.
29	**SelfRefrEarly1**. Read-write. Reset: 0. See: SelfRefrEarly0. BIOS: 0.
28	**SelfRefr1**. Read-write. Reset: 0. See: SelfRefr0. BIOS: 1.
27	**NbClkGate1**. Read-write. Reset: 0. See: NbClkGate0. BIOS: 1.
26	**NbPwrGate1**. Read-write. Reset: 0. See: NbPwrGate0. IF (CPUID Fn8000_0001_EBX[PkgType] ==1) THEN BIOS: 0. ELSE BIOS: 1. ENDIF. See 2.5.4.2 [NB C-states].
25	**PwrOffEnCstAct1**. Read-write; updated-by-SMU. Reset: 0. See: PwrOffEnCstAct0. BIOS: 1.

24	**PwrGateEnCstAct1**. Read-write. Reset: 0. See: PwrGateEnCstAct0. BIOS: 1.
23:21	**ClkDivisorCstAct1**. Read-write. Reset: 0. See: ClkDivisorCstAct0. BIOS: 000b.
20	Reserved.
19:18	**CacheFlushTmrSelCstAct1**. Read-write. Reset: 0. See: CacheFlushTmrSelCstAct0. BIOS: 01b.
17	**CacheFlushEnCstAct1**. Read-write. Reset: 0. See: CacheFlushEnCstAct0. BIOS: 1.
16	**CpuPrbEnCstAct1**. Read-write. Reset: 0. See: CpuPrbEnCstAct0. BIOS: 1.
15:14	Reserved.
13	**SelfRefrEarly0: allow early self-refresh**. Read-write. Reset: 0. BIOS: 0. 1=Allow self-refresh while cores in PC1 or CC1 are waiting for the cache flush timer to expire. 0=Wait for cache flush timer to expire before allowing self-refresh. See 2.5.7.2 [DRAM Self-Refresh] and 2.5.3.2.3.1 [C-state Probes and Cache Flushing].
12	**SelfRefr0: self-refresh**. Read-write. Reset: 0. BIOS: 1. 1=Allow DRAM self-refresh while in NB C-states. 0=Prevent DRAM self-refresh while in NB C-states. NbClkGate0 must be equal to SelfRefr0. See 2.5.7.2 [DRAM Self-Refresh] and 2.5.4.2 [NB C-states].
11	**NbClkGate0: NB clock-gating**. Read-write. Reset: 0. BIOS: 1. 1=Allow clock-gating of the NB. 0=Prevent clock-gating of the NB. NbClkGate0 must be equal to SelfRefr0. See 2.5.4.2 [NB C-states].
10	**NbPwrGate0: NB power-gating**. Read-write. Reset: 0. IF (CPUID Fn8000_0001_EBX[PkgType] ==1) THEN BIOS: 0. ELSE BIOS: 1. ENDIF. See 2.5.4.2 [NB C-states]. 1=Allow power-gating of the NB. 0=Prevent power-gating of the NB. NbPwrGate0 can only be programmed to 1 if NbClkGate0 and SelfRefr0 are programmed to 1. See 2.5.4.2 [NB C-states].
9	**PwrOffEnCstAct0: power off enable**. Read-write; updated-by-SMU. Reset: 0. BIOS: 1. 1=Package power off enable. CacheFlushEnCstAct0 is required to be set if this bit is set. PwrGateEnCstAct0 is required to be set if this bit is set. See 2.5.3.2.3.4 [Package C6 (PC6) State].
8	**PwrGateEnCstAct0: power gate enable**. Read-write. Reset: 0. BIOS: 1. 1=Core power gating is enabled. CacheFlushEnCstAct0 is required to be set if this bit is set. See2.5.3.2.3.3 [Core C6 (CC6) State].

<table>
<tr><td>7:5</td><td>ClkDivisorCstAct0: clock divisor. Read-write. Reset: 0. Specifies the core clock frequency while in the low-power state before the caches are flushed. This divisor is relative to the current FID frequency, or:
• 100 MHz * (10h + MSRC001_00[6B:64][CpuFid]) of the current P-state specified by MSRC001_0063[CurPstate].
If MSRC001_00[6B:64][CpuDid] of the current P-state indicates a divisor that is deeper than specified by this field, then no frequency change is made when entering the low-power state associated with this register.
<table><tr><th>Bits</th><th>Description</th><th>Bits</th><th>Description</th></tr><tr><td>000b</td><td>/1</td><td>100b</td><td>/16</td></tr><tr><td>001b</td><td>/2</td><td>101b</td><td>Reserved</td></tr><tr><td>010b</td><td>/4</td><td>110b</td><td>Reserved</td></tr><tr><td>011b</td><td>/8</td><td>111b</td><td>Turn off clocks.</td></tr></table>See CacheFlushTmrSelCstAct0.</td></tr>
<tr><td>4</td><td>Reserved.</td></tr>
<tr><td>3:2</td><td>CacheFlushTmrSelCstAct0: cache flush timer select. Read-write. Reset: 00b. BIOS: 10b. Specifies the timer to use for cache flush.
<table><tr><th>Bits</th><th>Cache flush timer</th></tr><tr><td>00b</td><td>0 us</td></tr><tr><td>01b</td><td>D18F3xDC[CacheFlushOnHaltTmr]</td></tr><tr><td>10b</td><td>D18F4x128[CacheFlushTmr]</td></tr><tr><td>11b</td><td>Reserved</td></tr></table>Each compute unit has one timer that is shared by all cores within the compute-unit. D18F3xDC[CacheFlushOnHaltCtl] specifies the core clock divisor to use after the caches are flushed. Writing values greater than 10b result in 10b. See CacheFlushEnCstAct0 and CpuPrbEnCstAct0.</td></tr>
<tr><td>1</td><td>CacheFlushEnCstAct0: cache flush enable. Read-write. Reset: 0. BIOS: 1. 1=Cache flush enable. The cache flush timer starts counting when the C-state is entered. See CacheFlushTmrSelCstAct0 and 2.5.3.2.3.1 [C-state Probes and Cache Flushing].</td></tr>
<tr><td>0</td><td>CpuPrbEnCstAct0: core direct probe enable. Read-write. Reset: 0. BIOS: 1. Specifies how probes are handled while in the low-power state. 0=When the probe request comes into the NB, the core clock is brought up to the COF (based on the current P-state), all outstanding probes are completed, the core waits for a hysteresis time based on D18F3xD4[ClkRampHystSel], and then the core clock is brought down to the frequency specified by ClkDivisorCstAct0. 1=The core clock does not change frequency; the probe is handled at the frequency specified by ClkDivisorCstAct0; this may only be set if:
• ClkDivisorCstAct0 specifies a divide-by 1, 2, 4, 8, or 16 and NbCof <= 3.2 GHz
• ClkDivisorCstAct0 specifies a divide-by 1, 2, 4, or 8 and NbCof >= 3.4 GHz
This bit also specifies functionality of the timer used for cache flushing. See CacheFlushTmrSelCstAct0.
• If CpuPrbEnCstAct0==0 and D18F3xDC[IgnCpuPrbEn]==0, only the time when the core is in a non-C0 state and has its clocks ramped up to service probes is counted.
• If CpuPrbEnCstAct0==1 or D18F3xDC[IgnCpuPrbEn]==1, all of the time the core is in a non-C0 state is counted.</td></tr>
</table>

D18F4x11C C-state Control 2

Reset: 0000_0000h. Read-write.

Bits	Description
31:14	Reserved.
13	**SelfRefrEarly2**. See: D18F4x118[SelfRefrEarly0].
12	**SelfRefr2**. See: D18F4x118[SelfRefr0].
11	**NbClkGate2**. See: D18F4x118[NbClkGate0].
10	**NbPwrGate2**. Read-write. IF (CPUID Fn8000_0001_EBX[PkgType] ==1) THEN BIOS: 0. ELSE BIOS: 1. ENDIF. 1=Allow clock-gating of the NB. 0=Prevent clock-gating of the NB. NbClkGate2 must be equal to SelfRefr2. See 2.5.4.2 [NB C-states].
9	**PwrOffEnCstAct2**. See: D18F4x118[PwrOffEnCstAct0].
8	**PwrGateEnCstAct2**. See: D18F4x118[PwrGateEnCstAct0].
7:5	**ClkDivisorCstAct2**. See: D18F4x118[ClkDivisorCstAct0].
4	Reserved.
3:2	**CacheFlushTmrSelCstAct2**. See: D18F4x118[CacheFlushTmrSelCstAct0].
1	**CacheFlushEnCstAct2**. See: D18F4x118[CacheFlushEnCstAct0].
0	**CpuPrbEnCstAct2**. See: D18F4x118[CpuPrbEnCstAct0].

D18F4x124 C-state Interrupt Control

Bits	Description
31:0	Reserved.

D18F4x128 C-state Policy Control 1

Reset: 0080_0000h.

Bits	Description
31	**CstateMsgDis: C-state messaging disable**. Read-write. Specifies whether any messages are sent to the FCH when a core enters or exits a C-state. 0=Messages are sent. 1=Messages are not sent. See 2.5.3.2.4.1 [FCH Messaging].
30:25	Reserved.
24:23	**CacheFlushSucMonMispredictAct: cache flush success monitor mispredict action**. Read-write. Specifies the cache flush success monitor decrement when non-C0 residency is shorter than duration specified by CacheFlushSucMonTmrSel. Bits — Description 00b — reset counter to zero 01b — decrement by 1 10b — decrement by 2 11b — decrement by 3

22:21	**CacheFlushSucMonTmrSel: cache flush success monitor timer select**. Read-write. BIOS: 00b. Specifies the non-C0 duration used to increment the cache flush success monitor. Bits — Duration 00b — Use cache flush timer specified by D18F4x11[C:8] 01b — D18F3xDC[CacheFlushOnHaltTmr] 10b — D18F4x128[CacheFlushTmr] 11b — Reserved
20:18	**CacheFlushSucMonThreshold: cache flush success monitor threshold**. Read-write. BIOS: 101b. Flush the caches immediately if cache flushing is enabled and the cache flush success monitor count == CacheFlushSucMonThreshold. A value of 0 disables the cache flush success monitor. See D18F4x118/D18F4x11C[CacheFlushEn].
17:12	Reserved.
11:5	**CacheFlushTmr: cache flush timer**. Read-write. BIOS: 32h. Specifies how long each core needs to stay in a C-state before it flushes its caches. See D18F4x118/D18F4x11C[CacheFlushTmrSel]. Bits — Description 00h — <= 5.12 us 7Fh-01h — (<CacheFlushTmr> * 10.24us) - 5.12us <= Time <= <CacheFlushTmr> * 10.24 us
4:2	**HaltCstateIndex**. Read-write. Specifies the IO-based C-state that is invoked by a HLT instruction.
1	**CoreCstatePolicy**. Read-write. Specifies how the processor arbitrates voltage and frequency when different non-C0 C-state requests are received on each core in a compute unit. 0=Transition both cores to the shallower C-state request. 1=Transition both cores to the deeper C-state request. For instance, if core 0 gets a request to go to C2 and core 1 gets a request to go to C1, hardware looks at the setting of CoreCstatePolicy. If CoreCstatePolicy is programmed to 0, the processor sends both cores to C1. If CoreCstatePolicy is programmed to 1, the processor sends both cores to C2. BIOS should program this field to the same value in all nodes of a multi-node processor. See also 2.5.2.1 [Dependencies Between Cores].
0	Reserved.

D18F4x13C SMU P-state Control

Reset: 0000_0000h. Read-only; updated-by-SMU.

Bits	Description
31:4	Reserved.
3:1	**SmuPstateLimit**. Specifies the highest-performance P-state (lowest value) allowed. SmuPstateLimit is always bounded by MSRC001_0061[PstateMaxVal]. This field uses hardware P-state numbering. See MSRC001_0071[CurPstateLimit] and 2.5.3.1.1.2 [Hardware P-state Numbering].
0	**SmuPstateLimitEn**.

D18F4x15C Core Performance Boost Control

Bits	Description
31	**BoostLock**. Read-only. Reset: Product-specific. Specifies whether the following registers are Read-write, read-only, or have special requirements related to writability. See individual register definitions for details. • MSRC001_00[6B:64][CpuFid, CpuDid, CpuVid]. • D18F4x110[MinResTmr] • D18F4x15C[NumBoostStates]. • D18F4x16C[CstateCnt, CstateBoost]. • D18F4x250[NodeTdpLimit]. • D18F5xEC[LSCacThreshold, LSPstate, LSCpNum]
30:9	Reserved.
8	**CstatePowerEn: C-state power enable**. If D18F2x1B4[SmuCfgLock] THEN Read-only; updated-by-hardware. ELSE Read-write. ENDIF. Reset: 0. BIOS: 1.
7	**ApmMasterEn: APM master enable**. If D18F2x1B4[SmuCfgLock] THEN Read-only; updated-by-hardware. ELSE Read-write. ENDIF. Reset: 0. BIOS: IF(D18F4x15C[NumBoostStates]==0) THEN 0. ELSE 1. ENDIF. 1=Enables the ability to turn on features associated with APM when used in conjunction with the individual feature enable bits. See 2.5.9 [Application Power Management (APM)].
6:5	Reserved.
4:2	**NumBoostStates: number of boosted states**. IF (D18F4x15C[BoostLock] | ApmMasterEn | D18F2x1B4[SmuCfgLock]) THEN Read-only. ELSE Read-write. ENDIF. Reset: Product-specific. Specifies the number of P-states that are considered boosted P-states. See 2.5.9 [Application Power Management (APM)].
1:0	**BoostSrc: boost source**. IF D18F2x1B4[SmuCfgLock] THEN Read-only; updated-by-hardware. ELSE Read-write. ENDIF. Reset: 0. BIOS: 2.5.3.1.6. Specifies whether CPB is enabled or disabled. Bits — Description 00b — Boosting disabled 01b — Boosting enabled 10b — Reserved 11b — Reserved

D18F4x164 Fixed Errata

Bits	Description
31:0	**FixedErrata**. Value: Product-specific. See the Revision Guide for the definition of this field. See 1.2 [Reference Documents].

D18F4x16C APM TDP Control

Bits	Description
31:15	Reserved.
14	**CacUpC1**. IF D18F4x15C[BoostLock] THEN Read-only. ELSE Read-write. ENDIF. Reset: Product-specific. 1=Cac interface is up on C1 (non XC6) state. 0=Cac interface is down and Cstate scalers are used in place of Cac reads.
13	**CstateCores**. IF D18F4x15C[BoostLock] THEN Read-only. ELSE Read-write. ENDIF. Reset: Product-specific. Specifies how CstateCnt determines Cstate boost conditions. Bit — Description 0h — CstateCnt specifies the number of compute units. 1h — CstateCnt specifies the number of cores.
12	Reserved.
11:9	**CstateCnt: C-state count**. IF D18F4x15C[BoostLock] THEN Read-only. ELSE Read-write. ENDIF. Reset: Product-specific. Specifies the number of cores or compute units (see CstateCores) that must be in CC6 before a transition can occur to a boosted P-state that is higher performance than the P-state specified by CstateBoost. A value of 0 disables access to P-states above CstateBoost.
8:6	**CstateBoost**. Read-write. Reset: Product-specific. Specifies the P-state which requires the number of cores or compute units (see CstateCores) specified in CstateCnt to be in CC6 before a transition to a higher performance (lower numbered) boosted P-state is allowed. CstateBoost must be less than or equal to D18F4x15C[NumBoostStates] otherwise undefined behavior results. If D18F4x15C[BoostLock]==1, CstateBoost can only be written with values that are greater than or equal to the reset value. Attempts to write values less than the reset value are ignored. A value of 0 indicates that the C-state boost feature is not supported. This field uses hardware P-state numbering. See 2.5.3.1.1.2 [Hardware P-state Numbering].
5	**ApmTdpLimitSts: APM TDP limit status**. Read; set-by-hardware; write-1-to-clear. Reset: 0. This bit is set by hardware when D18F5xE8[ApmTdpLimit] changes.
4	**ApmTdpLimitIntEn: APM TDP limit interrupt enable**. Read-write. Reset: 0. BIOS: 1. 1=Enables the generation of an interrupt using APIC330 of each core when D18F5xE8[ApmTdpLimit] changes.
3	**TdpLimitDis**. IF D18F4x15C[BoostLock] THEN Read-only. ELSE Read-write. ENDIF. Reset: 0. 1=Disables TDP limit checking and allows the processor to transition to higher performance P-states.
2:0	Reserved.

D18F4x1C0 Node Cac Register 1

Bits	Description
31:12	Reserved.
11:0	**NodeCacLatest**. Read-only; updated-by-hardware. Reset: 0. Specifies the sum of all instantaneous power credits on each compute unit. NodeCacLatest is reset to 0 when D18F4x15C[ApmMasterEn]==0.

D18F4x250 TDP Limit 8

Bits	Description
31	Reserved.
30:28	**TdpLimitPstate**. Read-write. Reset: 0. Specifies the highest performance P-state that has a power consumption less than or equal to the TDP limit. This field is programmed by BIOS and uses software P-state numbering. See 2.5.3.1.1.1 [Software P-state Numbering].
27:12	Reserved.
11:0	**NodeTdpLimit**. Read-write; Same-for-all. Reset: Product-specific. Specifies the maximum allowed sum of TDPs from all cores on a node. If the consumed power exceeds the NodeTdpLimit, a P-state limit is applied to all cores on the processor to reduce the powerconsumption so that it remains within the TDP limit. If D18F4x15C[BoostLock]==1, NodeTdpLimit can only be written with values that are less than or equal to the reset value. Attempts to write an invalid value are ignored. See 2.5.9.2 [TDP Limiting].

3.14 Device 18h Function 5 Configuration Registers

See 3.1 [Register Descriptions and Mnemonics]. See 2.7 [Configuration Space].

D18F5x00 Device/Vendor ID

Bits	Description
31:16	**DeviceID: device ID**. Read-only. Value: 141Fh.
15:0	**VendorID: vendor ID**. Read-only. Value: 1022h.

D18F5x04 Status/Command

Bits	Description
31:16	**Status**. Read-only. Value: 0000h.
15:0	**Command**. Read-only. Value: 0000h.

D18F5x08 Class Code/Revision ID

Bits	Description
31:8	**ClassCode**. Read-only. Value: 06_0000h. Provides the host bridge class code as defined in the PCI specification.
7:0	**RevID: revision ID**. Read-only. Value: 00h.

D18F5x0C Header Type

Bits	Description
31:0	**HeaderTypeReg**. Read-only. Reset: 0080_0000h. These bits are fixed at their default values. The header type field indicates that there are not multiple functions present in this device.

D18F5x34 Capabilities Pointer

Bits	Description
31:8	Reserved.
7:0	**CapPtr: capabilities pointer**. Read-only. Value: 00h.

D18F5x[70,60,50,40] Northbridge Performance Event Select Low

Bits	Description
31:0	MSRC001_024[6,4,2,0][31:0] is an alias of D18F5x[70,60,50,40].

D18F5x[74,64,54,44] Northbridge Performance Event Select High

Bits	Description
31:0	MSRC001_024[6,4,2,0][63:32] is an alias of D18F5x[74,64,54,44].

D18F5x[78,68,58,48] Northbridge Performance Event Counter Low

See 2.6.1.2 [NB Performance Monitor Counters] for proper read sequence.

Bits	Description
31:0	MSRC001_024[7,5,3,1][31:0] is an alias of D18F5x[78,68,58,48].

D18F5x[7C,6C,5C,4C] Northbridge Performance Event Counter High

See 2.6.1.2 [NB Performance Monitor Counters] for proper read sequence.

Bits	Description
31:0	MSRC001_024[7,5,3,1][63:32] is an alias of D18F5x[7C,6C,5C,4C].

D18F5x80 Compute Unit Status 1

See 2.4.4 [Processor Cores and Downcoring].
Software associates core ID to the cores of the compute units according to the following table. All combinations not listed are reserved.

Table 189: D18F5x80[Enabled, DualCore] Definition

Enabled	DualCore	Definition
1h	1h	1 compute unit is enabled; both cores of the compute unit are enabled.
3h	3h	2 compute units are enabled; both cores of each compute unit are enabled.

Bits	Description
31:24	Reserved.
23:16	**DualCore: both cores of a compute unit are enabled**. Read-only. Reset: Product-specific. 1=Both cores of a compute unit are enabled. See Table 189 [D18F5x80[Enabled, DualCore] Definition]. Bit — Description [0] — Compute unit 0 [1] — Compute unit 1 [7:2] — Reserved

15:8	Reserved.
7:0	**Enabled: at least one core of a compute unit is enabled**. Read-only. Reset: Product-specific. 1=At least one core is enabled in a compute unit. See Table 189 [D18F5x80[Enabled, DualCore] Definition]. Bit Description [0] Compute unit 0 [1] Compute unit 1 [7:2] Reserved

D18F5x84 Northbridge Capabilities 2

Unless otherwise specified, 1=The feature is supported by the processor; 0=The feature is not supported.

Bits	Description
31:29	Reserved.
28:24	**DdrMaxRateEnf: enforced maximum DDR rate**. Read-only. Value: Product-specific. See: DdrMaxRate. Specifies the maximum DRAM data rate that the processor is designed to support. Writes to D18F2x94_dct[3:0][MemClkFreq] that specify a frequency greater than specified by DdrMaxRateEnf will result in the D18F2x94_dct[3:0][MemClkFreq] being set to DdrMaxRateEnf.
23:21	Reserved.
20:16	**DdrMaxRate: maximum DDR rate**. Read-only. Value: Product-specific. Specifies the maximum DRAM data rate that the processor is designed to support. DdrMaxRate is defined by Table 141 [Valid Values for Memory Clock Frequency Value Definition]; except that 00h is defined as no limit. See D18F2x94_dct[3:0][MemClkFreq], and DdrMaxRateEnf.
15:12	**DctEn[3:0]: DCT[3:0] enabled**. Read-only. Value: Product-specific. Specifies which DCT controllers are enabled. 1=Enabled. 0=Disabled. Bit Description [0] DCT 0 [1] Reserved [2] Reserved [3] DCT 3
11:8	Reserved.
7:0	**CmpCap: CMP capable**. Read-only. Value: Product-specific. Number of cores on the node is CmpCap+1. CmpCap does not reflect cores disabled by D18F3x190[DisCore].

D18F5x88 NB Configuration 4 (NB_CFG4)

Bits	Description
31:25	Reserved.
24	**DisHbNpReqBusLock**. Read-write. Reset: 0. BIOS: 1. 0=While bus locks are in progress, all non-posted commands from I/O, including atomics, are blocked until the core has completed the locked transaction and releases the bus. 1=All non-posted commands except atomics do not honor bus locks and are allowed to proceed. This bit may be set to achieve better DMA performance in the presence of bus locks.

23:21	Reserved.
20	**DisSraCamXbarAddrMatch**. Read-write. Reset: 0. BIOS: 1. 1=Allow reads from ONION+ with SeqId=0 to be re-ordered by XCS.
19	Reserved.
18	**EnCstateBoostBlockCC6Exit**. Read-write. Reset: 0. BIOS: 1. 1=Cores cannot exit CC6 until VDD is less than or equal to the voltage of the P-state indexed by D18F4x16C[CstateBoost].
17:15	Reserved.
14	**DisHldRegRdRspChk**. Read-write. Reset: 0. BIOS: 1. 1=Disable primary holding register CPU or I/O read response checks.
13:1	Reserved.
0	Reserved.

D18F5x8C NB Configuration 5 (NB_CFG5)

Bits	Description
31:27	Reserved.
26	**DisSrqPickNcReqThrtl**. Read-write. Reset: 1. 1=Disable throttling SRQ picker for requests sourced from the links.
25:16	Reserved.
15	**EnSrqAllocGt31**. Read-write. Cold reset: 0. BIOS: 1. 1=Enables allocation of SRA entries to above the lower 32 entries.
14:2	Reserved.
1	Reserved.
0	Reserved.

D18F5xE0 Processor TDP Running Average

Bits	Description
31:4	Reserved.
3:0	**RunAvgRange: running average range**. Read-write; Same-for-all. Reset: 0. BIOS: 2h. Specifies the interval over which the processor averages power consumption estimates from the cores for boosting. Time interval = 2^(RunAvgRange + 1) * FreeRunSampleTimer rate. A value of 0 disables the TDP running average accumulator capture function. See 2.5.9 [Application Power Management (APM)].

D18F5xE8 TDP Limit 3

Bits	Description
31:29	Reserved.

28:16	**ApmTdpLimit**. Read-only; updated-by-hardware. Value: D18F4x250[NodeTdpLimit]. If the consumed node power exceeds the ApmTdpLimit on an single node processor or the ApmTdpLimit/2 on a multi-node processor, a P-state limit is applied to all cores on all nodes to reduce the power consumption to remain within the TDP limit. See 2.5.9.2 [TDP Limiting].
15:10	Reserved.
9:0	**Tdp2Watt**. Read-only. Value: Product-specific. Specifies in watts/TDP units the conversion factor for converting TDP units to watts. Tdp2Watt is a fixed point integer with 10 bits to the right of the decimal point and 0 bits to the left of the decimal point.

D18F5xEC Load Step Throttle Control

Bits	Description
31:19	Reserved.
18:7	**LSCacThreshold: load step Cac threshold**. IF D18F4x15C[BoostLock] THEN Read-only. ELSE Read-write. ENDIF. Cold reset: Product-specific. Specifies the power consumption threshold required for load step throttling. D18F4x1C0[NodeCacLatest] must be less than LSCacThreshold prior to load step throttling.
6:4	**LSPstate: load step P-state**. Cold reset: Product-specific. IF D18F4x15C[BoostLock] THEN Read-only. ELSE Read-write. ENDIF. Specifies the P-state threshold required for load step throttling. This field uses hardware P-state numbering. See 2.5.3.1.1.2 [Hardware P-state Numbering].
3:1	**LSCpNum: load step compute unit number**. Cold reset: Product-specific. IF D18F4x15C[BoostLock] THEN Read-only. ELSE Read-write. ENDIF. Specifies the compute unit threshold required for load step throttling. The number of compute units in C0 must be greater than LSCpNum prior to load step throttling. See LSPstate.
0	**LSThrottleEn: load step throttle enable**. Cold reset: Product-specific. Read-write. 1=Enable the load step throttle controllers when the requirements in LSCpNum, LSPstate, and LSCacThreshold are met.

D18F5x128 Clock Power/Timing Control 3

Bits	Description
31	Reserved.
30	**NbFidChgCpuOpEn**. Read-write. Cold reset: 0. BIOS: 1.
29:28	Reserved.
27	Reserved.
26:23	Reserved.
22	**NbPllPwrDwnRegEn: NB PLL power down**. Read-write. Cold reset: Product-specific. 1=The NB PLL is powered down when the NB is power gated and DRAM is placed into self-refresh (see 2.5.4.2 [NB C-states]). 0=The NB PLL is not powered down during NB C-states.
21	**PC6Vid[7]**. Read-write. Cold reset: Product-specific. See PC6Vid[6:0].
20:18	Reserved.
17	**PwrGateDis: power-gate disable**. Read-write. Cold reset: 0. 1=NB power gating is disabled. 0=NB power gating is enabled. See 2.5.4.2 [NB C-states].

16	Reserved.
15	**CC6PwrDwnRegEn: CC6 power down regulator enable**. Read-write. Cold reset: Product-specific. 1=Power down the VDDA regulator on CC6 entry. See PllRegTime.
14	**PC6PwrDwnRegEn: PC6 power down regulator enable**. Read-write. Cold reset: Product-specific. 1=Power down the VDDA regulator on PC6 entry. See PllRegTime.
13:12	**PwrGateTmr: power gate timer**. Read-write. Cold reset: 01b. BIOS: 01b. Specifies the minimum delay time required from the power gating or ungating of one Compute Unit to the power gating or ungating of the same Compute Unit or another Compute Unit. Bits Description Bits Description 00b 500 ns 10b Reserved. 01b 1 us 11b Reserved.
11:10	**PllVddOutUpTime**. Read-write. Cold reset: 0. The VDD regulator may be powered down when the processor transitions to PC6. If the regulator is powered down, this field specifies the time required to initialize the core PLL logic once the regulator is powered back up. Bits Description Bits Description 00b 100 ns 10b 400 ns 01b 200 ns 11b 800 ns
9	**FastSlamTimeDown**. Read-write. Cold reset: 0. BIOS: 1. Specifies the time the processor waits for downward voltage transitions to complete. This field only effects transitions from D18F4x16C[CstateBoost] or lower performance P-states. 0=D18F3xD8[VSRampSlamTime]. 1=10 us.
8:7	**PllRegTime: Pll regulator time**. Read-write. Cold reset: 10b. The VDDAregulator may be powered down when the processor transitions to PC6 or CC6. See PC6PwrDwnRegEn and CC6PwrDwnRegEn. If CC6PwrDwnRegEn==1, the VDDA regulator is powered down during CC6. If PC6PwrDwnRegEn==1, the VDDA regulator is powered down during PC6. Ifthe VDDA regulator is powered down during CC6 and the core transitions from CC6 to PC6, the regulator remains powered down during PC6 regardless of the PC6PwrDwnRegEn setting. This field specifies the time required for the VDDA regulator to power back up and initialize the core PLL logic that is powered by the VDDA regulator. Bits Description Bits Description 00b Reserved. 10b 1.5 us 01b Reserved. 1 1b 2.0 us
6:0	**PC6Vid[6:0]: package C6 vid**. Read-write. Cold reset: Product-specific. PC6Vid[7:0] = {PC6Vid[7], PC6Vid[6:0]}. PC6Vid[7:0] specifies the VID driven in the PC6 state. See 2.5.3.2.3.4 [Package C6 (PC6) State]. See 2.5.1.3.2 [Low Power Voltages].

D18F5x12C Clock Power/Timing Control 4

See the *AMD Serial VID Interface 2.0 (SVI2) Specification*.

Bits	Description

31	**Svi2CmdBusy**. Read-only; updated-by-hardware. Cold reset: 0. 1=SVI2 command in progress. This bit is set by hardware when any SVI2 command is sent to the voltage regulator. Software must wait for this bit to clear to 0 before writing any of the following fields: D18F5x12C[CorePsi1En, CoreLoadLineTrim, CoreOffsetTrim], D18F5x188[NbPsi1, NbLoadLineTrim, NbOffsetTrim], D18F5x18C[CoreTfn, NbTfn]. This bit is cleared by hardware when the SVI2 command is complete. On a voltage change, this bit is cleared when the voltage transition is completed. See 2.5.1.4.1 [Hardware-Initiated Voltage Transitions]. On a telemetry or PSIx_L change, this bit is cleared as soon as the SVI2 command is sent to the voltage regulator. See 2.5.1.1.1 [SVI2 Features] and 2.5.1.3.1 [PSIx_L Bit].
30	**WaitVidCompDis: wait VID completion disable**. IF (D18F2x1B4[SmuCfgLock]) THEN Read-only; updated-by-hardware. ELSE Read-write. ENDIF. Cold reset: 0. 0=Hardware waits for the VOTF complete indicator from the voltage regulator before clearing Svi2CmdBusy or making additional voltage change requests. 1=Hardware clears Svi2CmdBusy 500us after changes to CoreLoadLineTrim, CoreOffsetTrim, or D18F5x188[NbLoadLineTrim, NbOffsetTrim] are made; hardware clears Svi2CmdBusy and additional voltage changes are allowed after the time specified by D18F3xD8[VSRampSlamTime] . See 2.5.1.4 [Voltage Transitions].
29:6	RAZ.
5	**CorePsi1En: Core PSI1_L enable**. If D18F2x1B4[SmuCfgLock] THEN Read-only; updated-by-hardware. ELSE Read-write. ENDIF Cold reset: 0. BIOS: 1. 0=PSI1_L for VDD is deasserted. 1=PSI1_L for VDD is asserted when all cores are in CC6. See 2.5.3.2.3.4 [Package C6 (PC6) State], 2.5.1.3.1 [PSIx_L Bit], and Svi2CmdBusy.
4:2	**CoreLoadLineTrim: Core load line trim**. IF (D18F2x1B4[SmuCfgLock]) THEN Read-only; updated-by-hardware. ELSE Read-write. ENDIF. Cold reset: 011b. BIOS: D0F0xBC_xC010_40A0[SviLoadLineTrimVdd]. CoreLoadLineTrim and NbLoadLineTrim specify a percentage change relative to the initial load line slope for VDD and VDDNB, respectively. See Svi2CmdBusy. Bits Description Bits Description 000b Load line disabled 100b +20% 001b -40% 101b +40% 010b -20% 110b +60% 011b 0% 111b +80%
1:0	**CoreOffsetTrim: Core offset trim**. IF (D18F2x1B4[SmuCfgLock]) THEN Read-only; updated-by-hardware. ELSE Read-write. ENDIF. Cold reset: 10b. BIOS: D0F0xBC_xC010_40A0[SviLoadLineOffsetVdd]. CoreOffsetTrim and NbOffsetTrim specify a voltage offset relative to the initial load line offset for VDD and VDDNB, respectively. See Svi2CmdBusy. Bits Description Bits Description 00b Load line offset disabled 10b 0mV 01b -25mV 11b +25mV

D18F5x16[C:0] Northbridge P-state [3:0]

Each of these registers specify the frequency and voltage associated with each of the NB P-states.

Table 190: Register Mapping for D18F5x16[C:0]

Register	Function
D18F5x160	NB P-state 0

Table 190: Register Mapping for D18F5x16[C:0]

D18F5x164	NB P-state 1
D18F5x168	NB P-state 2
D18F5x16C	NB P-state 3

The NbVid field is allowed to be different between processors in a multi-processor system. All other fields are required to be programmed to the samevalue for all processors in the coherent fabric. See 2.5.4.1 [NB P-states] for more information about these registers.

Table 191: NB P-state Definitions

Term	Definition
NBCOF	NB current operating frequency in MHz. NBCOF = 100 * (D18F5x16[C:0][NbFid] + 4h) / (2^D18F5x16[C:0][NbDid]).
NBCOF[0]	NB current operating frequency in MHz for NB P-state 0. NBCOF[0] = (100 * (D18F5x160[NbFid] + 4h) / (2^D18F5x160[NbDid])).
NBCOF[1]	NB current operating frequency in MHz for NB P-state 1. NBCOF[1] = (100 * (D18F5x164[NbFid] + 4h) / (2^D18F5x164[NbDid])).
NBCOF[2]	NB current operating frequency in MHz for NB P-state 2. NBCOF[2] = (100 * (D18F5x168[NbFid] + 4h) / (2^D18F5x168[NbDid])).
NBCOF[3]	NB current operating frequency in MHz for NB P-state 3. NBCOF[3] = (100 * (D18F5x16C[NbFid] + 4h) / (2^D18F5x16C[NbDid])).

Bits	Description
31:24	**NbIddValue: Northbridge current value**. Read-write. Cold reset: Product-specific. See NbIddDiv.
23:22	**NbIddDiv: Northbridge current divisor**. Read-write. Cold reset: Product-specific. After reset, NbIddDiv and NbIddValue combine to specify the expected maximum current drawn on the VDDNB power plane at a given VDDNB voltage. These values are intended to be used by 2.5.1.3.1.1 [BIOS Requirements for PSI0_L]. These values are not intended to convey final product power levels and may not match the power levels specified in the Power and Thermal Datasheet. These fields may be subsequently altered by software; they do not affect the hardware behavior. Bits — Description 00b — IddValue / 1 A, Range: 0 to 255 A. 01b — IddValue / 10 A, Range: 0 to 25.5 A. 10b — IddValue / 100 A, Range: 0 to 2.55 A. 11b — Reserved.
21	**NbVid[7]**. Read-write. Cold reset: Product-specific. See NbVid[6:0].
20	Reserved.
19	Reserved.

18	**MemPstate: Memory P-state**. Read-write. Cold reset: Product-specific. 1=The Northbridge P-state specified by this register maps to memory P-state 1. 0=The Northbridge P-state specified by this register maps to memory P-state 0. Memory P-states may be globally disabled by programming D18F5x170[MemPstateDis]. See 2.5.7.1 [Memory P-states].
17	Reserved.
16:10	**NbVid[6:0]: Northbridge VID**. Read-write. Cold reset: Product-specific. NbVid[7:0] = {NbVid[7], NbVid[6:0]}. NbVid[7:0] specifies the Northbridge voltage.
9:8	Reserved.
7	**NbDid: Northbridge divisor ID**. Read-write. Cold reset: Product-specific. Specifies the Northbridge frequency divisor. See NbFid[5:0].
6:1	**NbFid[5:0]: Northbridge frequency ID**. Read-write. Cold reset: Product-specific. Specifies the Northbridge frequency multiplier. The NB COF is a function of NbFid and NbDid, and defined by NBCOF. NbFid and NbDid are not changed on a write if the value written results in a frequency greater than MSRC001_0071[MaxNbCof]. See 2.5.3.1.5 [Core P-state Transition Behavior].
0	**NbPstateEn: Northbridge P-state enable**. Read-write. Cold reset: Product-specific. 1=The Northbridge P-state specified by this register is valid. 0=The Northbridge P-state specified by this register is not valid. This bit must be set to 1 in order for the Northbridge P-state specified by this register to be programmed in D18F5x170[NbPstateHi, NbPstateLo].

D18F5x170 Northbridge P-state Control

See also 2.5.4.1 [NB P-states].

<table>
<tr><th>Bits</th><th>Description</th></tr>
<tr><td>31</td><td>MemPstateDis: memory P-state disable. IF (D18F3xE8[MemPstateCap] && D18F2x1B4[SmuCfgLock]==0) THEN Read-write; updated-by-hardware; Updated-by-SMU. ELSE Read-only; updated-by-hardware; Updated-by-SMU. Reset: Product-specific. 1=Memory P-state transitions are disabled. The current P-state is not changed by programming this bit. The memory P-state will be forced to M0 on the next NB P-state transition. On processors where memory P-states are enabled, programming this bit may result in a violation of bandwidth requirementsstated in 2.5.3.1.5. Software must ensure that NB P-states which violate those requirements are forced disabled. 0=Memory P-state transitions are enabled if D18F2x90_dct[3:0][DisDllShutdownSR]==0.</td></tr>
<tr><td>30</td><td>NbPstateFidVidSbcEn. IF (D18F5x174[NbPstateDis] || D18F2x1B4[SmuCfgLock]) THEN Read-only. ELSE Read: Write-1-only. ENDIF. Reset: 0. BIOS: 1. NB P-state transitions are blocked until this field is set to a 1.</td></tr>
<tr><td>29:27</td><td>NbPstateHiRes: NB P-state high residency timer. If D18F2x1B4[SmuCfgLock] THEN Read-only; updated-by-hardware. ELSE Read-write. ENDIF. Reset: 0. Specifies the minimum time the processor must spend in the high NB P-state before transitions to the low NB P-state are allowed. See 2.5.4.1 [NB P-states].
<table>
<tr><th>Bits</th><th>Description</th><th>Bits</th><th>Description</th></tr>
<tr><td>000b</td><td>0us</td><td>100b</td><td>1ms</td></tr>
<tr><td>001b</td><td>10us</td><td>101b</td><td>5ms</td></tr>
<tr><td>010b</td><td>100us</td><td>110b</td><td>10ms</td></tr>
<tr><td>011b</td><td>500us</td><td>111b</td><td>50ms</td></tr>
</table>
</td></tr>
</table>

26:24	**NbPstateLoRes: NB P-state low residency timer**. If D18F2x1B4[SmuCfgLock] THEN Read-only; updated-by-hardware. ELSE Read-write. ENDIF. Reset: 0. Specifies the minimum time the processor must spend in the low NB P-state before transitions to the high NB P-state are allowed. See 2.5.4.1 [NB P-states]. See: NbPstateHiRes.
23	**NbPstateGnbSlowDis**. If D18F2x1B4[SmuCfgLock] THEN Read-only; updated-by-hardware. ELSE Read-write. ENDIF. Reset: 0. Specifies whether NBP-state transitions take the GnbSlow signal into account. 0=Take GnbSlow into account. 1=Ignore GnbSlow. See 2.5.4.1 [NB P-states].
22:15	Reserved.
14	**SwNbPstateLoDis: software NB P-state low disable**. IF (D18F5x174[NbPstateDis] | D18F2x1B4[SmuCfgLock]) THEN Read-only. ELSE Read-write. ENDIF. Reset: 0. 1=Transition to NbPstateHi and disable transitions to NbPstateLo.
13	**NbPstateDisOnP0: NB P-state disable on P0**. IF (D18F5x174[NbPstateDis] | D18F2x1B4[SmuCfgLock]) THEN Read-only. ELSE Read-write. ENDIF. Reset: 0. 1=Transition to NbPstateHi and disable transitions to NbPstateLo if any compute unit is in P0 or a boosted P-state. This field uses software P-state numbering. See 2.5.3.1.1.1 [Software P-state Numbering].
12:9	**NbPstateThreshold: NB P-state threshold**. If D18F2x1B4[SmuCfgLock] THEN Read-only; updated-by-hardware. ELSE Read-write. ENDIF. Reset: Product-specific. BIOS: COUNT(D18F5x80[Enabled]). Specifies the minimum number of compute units that must be in a P-state with MSRC001_00[6B:64][NbPstate]==1 before transitions to lower performance NB P-states are allowed. See NbPstateLo and NbPstateHi.
8	Reserved.
7:6	**NbPstateHi: NB P-state high**. IF (D18F2x1B4[SmuCfgLock]) THEN Read-only; updated-by-hardware. ELSE Read-write. ENDIF. Cold reset: Product-specific. If NB P-states are enabled, this field specifies the NB P-state that is used when the number of compute units in a P-state with MSRC001_00[6B:64][NbPstate]==1 is less than NbPstateThreshold. This field must be programmed to the same value for all processors in the coherent fabric. This field is not changed on a write if the value written is greater than the NbPstateMaxVal value written or greater than the current NbPstateLo value. See also NbPstateDisOnP0, SwNbPstateLoDis, NbPstateLo, D18F5x174[NbPstateDis], and D18F5x16[C:0][NbPstateEn].
5	Reserved.
4:3	**NbPstateLo: NB P-state low**. IF (D18F2x1B4[SmuCfgLock]) THEN Read-only; updated-by-hardware. ELSE Read-write. ENDIF. Cold reset: Product-specific. If NB P-states are enabled, this field specifies the NB P-state that is used when the number of compute units in a P-state with MSRC001_00[6B:64][NbPstate]==1 is greater than or equal to NbPstateThreshold. NbPstateLo must be greater than or equal to NbPstateHi. This field must be programmed to the same value for all processors in the coherent fabric. This field is not changed on a write if the value written is greater than the NbPstateMaxVal value written or less than the current NbPstateHi value. See also NbPstateDisOnP0, SwNbPstateLoDis, D18F5x174[NbPstateDis], and D18F5x16[C:0][NbPstateEn].
2	Reserved.
1:0	**NbPstateMaxVal: NB P-state maximum value**. IF (D18F2x1B4[SmuCfgLock]) THEN Read-only; updated-by-hardware. ELSE Read-write. ENDIF. Cold reset: specified by the reset state of D18F5x16[C:0][NbPstateEn]; the cold reset value is the highest NB P-state number corresponding to the register in which NbPstateEn is set (e.g., if D18F5x160 and D18F5x164 have this bit set and the others do not, then NbPstateMaxVal=1; if NbPstateEn is only set in D18F5x160, then NbPstateMaxVal=0). This specifies the highest NB P-state value (lowest performance state) supported by the hardware.

D18F5x174 Northbridge P-state Status

Bits	Description
31	**NbPstateReqBusy**. Read-only; updated-by-hardware. Reset: 0. 1=NB P-state request is pending. 0=No NB P-state requests are outstanding.
30:25	Reserved.
24	**CurMemPstate: current memory P-state**. Read-only; updated-by-hardware. Reset: 0. Specifies the current memory P-state. 1=Memory P-state 1. 0=Memory P-state 0. See 2.5.7.1 [Memory P-states].
23	**CurNbVid[7]: current northbridge voltage ID[7]**. MSRC001_0071[CurNbVid[7]] is an alias of D18F5x174[CurNbVid[7]]. VDDNB voltage.
22	**CurNbPstateLo.** Read-only; updated-by-hardware. Reset: 0. 1=Current NB Pstate maps to D18F5x170[NbPstateLo]. 0=Current NB Pstate maps to D18F5x170[NbPstateHi].
21	Reserved.
20:19	**CurNbPstate: current northbridge P-state**. Read-only; updated-by-hardware. Reset: 0. Provides the NB P-state that corresponds to the current frequency component of the NB. The value of this field is updated when the COF transitions to a new value associated with an NB P-state. Bits — Description 00b — NB P0 01b — NB P1 10b — NB P2 11b — NB P3
18:12	**CurNbVid[6:0]: current northbridge voltage ID**. MSRC001_0071[CurNbVid[6:0]] is an alias of D18F5x174[CurNbVid[6:0]]. VDDNB voltage.
11	Reserved.
10	Reserved.
9	**CurNbDid: current northbridge divisor ID**. Read-only; updated-by-hardware. Reset: 0.
8:3	**CurNbFid[5:0]: current northbridge frequency ID**. Read-only; updated-by-hardware. Reset: 0.
2:1	**StartupNbPstate: startup northbridge P-state number**. Read-only. Cold reset: Product-specific. Specifies the cold reset VID, FID and DID for the Northbridge based on the NB P-state number selected.
0	**NbPstateDis: northbridge P-state disable**. Read-only. Value: Product-specific. MSRC001_0071[NbPstateDis] is an alias of D18F5x174[NbPstateDis].

D18F5x178 Northbridge Fusion Configuration

Bits	Description
31:20	Reserved.
19	**SwGfxDis**. Read-write. Reset: 1. BIOS: IF (GpuEnabled) THEN 0. ELSE 1. ENDIF. 1=Hardware handshakes for NB P-state transitions and DRAM self-refresh entry are ignored. See 2.5.4.1.2 [NB P-state Transitions]. See 2.5.7.2 [DRAM Self-Refresh].
18	**CstateFusionHsDis: C-state fusion handshake disable**. Read-write. Reset: 0. BIOS: 1. 1=Ignore the FCH handshake response for PC6 transitions. 0=Use the FCH handshake response for PC6 entry. See 2.5.3.2.4.1 [FCH Messaging].

17	**Dis2ndGnbAllowPsWait**. Read-write. Reset: 0. BIOS: 1. 1=Do not do a second check of AllowNb-Trans after quiescing the cores when transitioning NB P-states. See 2.5.4.1.2 [NB P-state Transitions].
16	**ProcHotToGnbEn**. Read-write. Reset: 0. BIOS: 1. 1=The GPU is placed into a low-power state when PROCHOT_L is asserted. Note: the GPU power-state transitions associated with PROCHOT_L nominally occur every 1 millisecond; PROCHOT_L assertions and deassertions for less than this period may not result in GPU state changes.
15:12	Reserved.
11	**AllowSelfRefrS3Dis: allow self-refresh S3 disable**. Read-write. Reset: 0. BIOS: 1. 1=The NB does not wait for handshake before placing DRAM into self-refresh (see 2.5.7.2 [DRAM Self-Refresh]) on S3 entry (see 2.5.8.1.1 [ACPI Suspend to RAM State (S3)]). 0=The NB waits for handshake before placing DRAM into self-refresh on S3 entry.
10	**InbWakeS3Dis: InbWake S3 disable**. Read-write. Reset: 0. BIOS: 1. 1=The NB does not wait for handshake before placing DRAM into self-refresh (see 2.5.7.2 [DRAM Self-Refresh]) on S3 entry (see 2.5.8.1.1 [ACPI Suspend to RAM State (S3)]). 0=The NB waits for handshake before placing DRAM into self-refresh on S3 entry.
9:4	Reserved.
3	**CstateThreeWayHsEn: C-state three way handshake enable**. Read-write. Reset: 0. 1=Enable the three way handshake with the FCH when entering a C-state. 0=Only a two way handshake with FCH is used. There is no message about the resulting package state sent to FCH. See 2.5.3.2.4.1 [FCH Messaging].
2	**CstateFusionDis: C-state fusion disable**. Read-write. Reset: 0. 1=All HALT or C-state requests are forwarded to the FCH. 0=HALT and C-state requests are forwarded to the FCH when each core has made a request. See 2.5.3.2.4.1 [FCH Messaging].
1:0	Reserved.

D18F5x17C Miscellaneous Voltages

Bits	Description
31	**NbPsi0VidEn: Northbridge PSI0_L VID enable**. Read-write. Reset: 0. This bit specifies how PSI0_L is controlled for VDDNB. See D18F3xA0[PsiVidEn] and 2.5.1.3.1 [PSIx_L Bit].
30:23	**NbPsi0Vid[7:0]: Northbridge PSI0_L VID threshold**. Read-write. Reset: 0. When enabled by NbPsi0VidEn, NbPsi0Vid specifies the threshold value of the VID code generated by the Northbridge, which in turn determines the state of PSI0_L. See D18F3xA0[PsiVid[6:0]] and 2.5.1.3.1 [PSIx_L Bit].
22:18	Reserved.
17:10	**MinVid: minimum voltage**. Read-only. Reset: Product-specific. Specifies the VID code corresponding to the minimum voltage (highest VID code) that the processor drives. 00h indicates that no minimum VID code is specified. See 2.5.1 [Processor Power Planes And Voltage Control].
9:8	Reserved.
7:0	**MaxVid: maximum voltage**. Read-only. Reset: Product-specific. Specifies the VID code corresponding to the maximum voltage (lowest VID code) that the processor drives. 00h indicates that no maximum VID code is specified. See 2.5.1 [Processor Power Planes And Voltage Control].

D18F5x188 Clock Power/Timing Control 5

See the *AMD Serial VID Interface 2.0 (SVI2) Specification*.

Bits	Description
31:6	RAZ.
5	**NbPsi1: Northbridge PSI1_L**. IF D18F2x1B4[SmuCfgLock] THEN Read-only; updated-by-hardware. ELSE Read-write. ENDIF Cold reset: 0. Specifies how PSI1_L is controlled for VDDNB. 1=PSI1_L is low. 0=PSI1_L is high. See 2.5.1.3.1 [PSIx_L Bit].
4:2	**NbLoadLineTrim: Northbridge load line trim**. IF D18F2x1B4[SmuCfgLock] THEN Read-only; updated-by-hardware. ELSE Read-write. ENDIF. Cold reset: 011b. BIOS: D0F0xBC_xC010_40A0[SviLoadLineTrimVddNb]. See D18F5x12C[CoreLoadLineTrim].
1:0	**NbOffsetTrim: Northbridge offset trim**. IF D18F2x1B4[SmuCfgLock] THEN Read-only; updated-by-hardware. ELSE Read-write. ENDIF. Cold reset: 10b. BIOS: D0F0xBC_xC010_40A0[SviLoadLineOffsetVddNb]. See D18F5x12C[CoreOffsetTrim].

D18F5x18C Clock Power/Timing Control 6

See the *AMD Serial VID Interface 2.0 (SVI2) Specification*.

Bits	Description
31:2	RAZ.
1	**CoreTfn: Core telemetry functionality**. If D18F2x1B4[SmuCfgLock] THEN Read-only; updated-by-hardware. ELSE Read-write. ENDIF Cold reset: 0. BIOS: 1. See NbTfn.
0	**NbTfn: Northbridge telemetry functionality**. If D18F2x1B4[SmuCfgLock] THEN Read-only; updated-by-hardware. ELSE Read-write. ENDIF. Cold reset: 0. See D18F5x12C[Svi2CmdBusy]. CoreTfn and NbTfn specify the telemetry mode as follows: CoreTfn / NbTfn / Description 0 / 0 / Telemetry enabled in voltage-only mode. 0 / 1 / Telemetry enabled in voltage and current mode. 1 / 0 / Telemetry disabled. 1 / 1 / Reserved.

D18F5x194 Name String Address Port

D18F5x194 and D18F5x198 provide BIOS with a read-only name string that may be copied to MSRC001_00[35:30] at warm reset. Each of D18F5x198_x[B:0] is read as follows:

1. Write D18F5x194[Index].
2. Read D18F5x198.

Bits	Description
31:4	Reserved.
3:0	**Index: name string register index**. Read-write. Reset: 0. Bits / Description Bh-0h / Name String Registers. See D18F5x198_x[B:0]. Fh-Ch / Reserved.

D18F5x198 Name String Data Port

See D18F5x194 for register access information. Address: D18F5x194[Index].

Bits	Description
31:0	**Data**. Reset: 0.

D18F5x198_x[B:0] Name String Data

Bits	Description
31:24	**NameStringByte3: name string ASCII character 3**. Read-only. Value: Product-specific.
23:16	**NameStringByte2: name string ASCII character 2**. Read-only. Value: Product-specific.
15:8	**NameStringByte1: name string ASCII character 1**. Read-only. Value: Product-specific.
7:0	**NameStringByte0: name string ASCII character 0**. Read-only. Value: Product-specific.

D18F5x240 ECC Exclusion Base Address Low

- Transaction addresses are within the defined range if: EccExclBaseAddr[47:6] <= address[47:6] <= EccExclLimitAddr[47:6].
- BIOS must quiesce all other forms of DRAM traffic when configuring this range. See MSRC001_001F[DisDramScrub].
- When initializing the base/limit pair, the BIOS must write the limit register before the EccExclEn bit is set. BIOS should clear EccExclEn before changing the address range.
- BIOS should re-initialize memory with valid ECC when resizing this region.

Bits	Description
31:6	**EccExclBaseAddr[31:6]: ECC exclusion base address register bits[31:6]**. Read-write. Reset: 0. EccExclBaseAddr[47:6]={D18F5x244[EccExclBaseAddr[47:32]], EccExclBaseAddr[31:6]}. The ECC Exclusion Base/Limit Address registers setup a contiguous range in DRAM where ECC check and error reporting is disabled. BIOS configures the ECC exclusion range code to cover the frame buffer region in ECC UMA systems with internal GPUs. The GPU is configured as MC_SHARED:MC_VM_STEERING [DEFAULT_STEERING]=1 (system traffic to onion).
5:1	Reserved.
0	**EccExclEn**. Read-write. Reset: 0. 1=Enable ECC Exclusion Range. See D18F5x240[EccExclBaseAddr].

D18F5x244 ECC Exclusion Base Address High

Bits	Description
31:16	Reserved.
15:0	**EccExclBaseAddr[47:32]: ECC exclusion base address register bits[47:32]**. Read-write. Reset: 0. See D18F5x240[EccExclBaseAddr].

D18F5x248 ECC Exclusion Limit Address Low

Bits	Description
31:6	**EccExclLimitAddr[31:6]: ECC exclusion limit address register bits[31:6]**. Read-write. Reset: 0. EccExclLimitAddr[47:6]={D18F5x24C[EccExclLimitAddr[47:32]], EccExclLimitAddr[31:6]}. See D18F5x240[EccExclBaseAddr].
5:0	Reserved.

D18F5x24C ECC Exclusion Limit Address High

Bits	Description
31:16	Reserved.
15:0	**EccExclLimitAddr[47:32]: ECC exclusion limit address register bits[47:32]**. Read-write. Reset: 0. See D18F5x240[EccExclBaseAddr].

D18F5x260 Clock Power/Timing Control 8

Bits	Description
31:4	Reserved.
3:1	**ClkStretchPercent: clock stretch percent**. Read-only. Reset: Product-specific. Specifies the percentage of clock stretching. Bits — Description 000b — 0% 001b — 5% 010b — 7% 111b-011b — Reserved.
0	**ClkStretchEn: clock stretch enable**. Read-only. Reset: Product-specific. 1=Clock stretch enable. 0=Clock stretch disable.

3.15 Northbridge IOAPIC Registers

The Northbridge IOAPIC is accessed through the Northbridge IOAPIC base address specified by D0F0xFC_x01 [IOAPIC Base Address Lower] and D0F0xFC_x02 [IOAPIC Base Address Upper].

NBIOAPICx00 IO Register Select

Bits	Description
31:8	Reserved.
7:0	**IndirectAddressOffset**. Read-write. Reset: 0. Specifies the indexed register accessed via NBIOAPICx10 [IO Window].

NBIOAPICx10 IO Window

Bits	Description
31:0	**IoapicData**.

NBIOAPICx10_x00 IOAPIC ID

This register is not used in IOxAPIC PCI bus delivery mode.

Bits	Description
31:28	**ExtendID: extended IOAPIC device ID**. IF (D0F0xFC_x00[IoapicIdExtEn]==0) THEN Read-only. ELSE Read-write. ENDIF. Reset: 0.
27:24	**ID: IOAPIC device ID**. Read-write. Reset: 0.
23:0	Reserved.

NBIOAPICx10_x01 IOAPIC Version

Bits	Description
31:24	Reserved.
23:16	**MaxRedirectionEntries**. Value: 1Fh. Indicates 32 entries [31:0].
15	**PRQ**. Value: 1. IRQ pin assertion supported.
14:8	Reserved.
7:0	**Version**. Value: 21h. PCI 2.2 compliant.

NBIOAPICx10_x02 IOAPIC Arbitration

Bits	Description
31:28	Reserved.
27:24	**ArbitrationID**. Read-only. Reset: 0.
23:0	Reserved.

NBIOAPICx10_x[4E:10:step2] Redirection Table Entry [31:0]

Bits	Description
63:56	**DestinationID**. Read-write. Reset: 0. Bits [19:12] of the address field of the interrupt message.
55:32	Reserved.
31:17	Reserved.
16	**Mask**. Read-write. Reset: 1. 1=Mask the interrupt injection at the input of this device. 0=Unmask.
15	**TriggerMode**. Read-write. Reset: 0. 0=Edge. 1=Level.
14	**RemoteIRR**. Read-only. Reset: 0. Used for level triggered interrupts only. It is cleared by EOI special cycle transaction or write to EOI register. 1=Interrupt message is delivered.
13	**InterruptPinPolarity**. Read-write. Reset: 0. 0=High. 1=Low.
12	**DeliveryStatus**. Read-only. Reset: 0. 0=Idle. 1=Send Pending.
11	**DestinationMode**. Read-write. Reset: 0. 0=Physical. 1=Logical.
10:8	**DeliveryMode**. Read-write. Reset: 0. Bits Definition Bits Definition 000b Fixed 100b NMI 001b Lowest Priority 101b INIT 010b SMI/PMI 110b Reserved 011b Reserved 111b ExtINT
7:0	**Vector**. Read-write. Reset: 0. Interrupt vector associated with this interrupt input.

NBIOAPICx20 IRQ Pin Assertion

Bits	Description
31:8	Reserved.
7:0	**InputIrq**. Read-write. Reset: 0. IRQ number for the requested interrupt. A write to this register triggers an interrupt associated with the redirection table entry referenced by the IRQ number. Currently the redirection table has 24 entries. Writes with IRQ number greater than 17h have no effect.

NBIOAPICx40 EOI

Bits	Description
31:8	Reserved.
7:0	**Vector**. Write-only. Reset: 0. Interrupt vector. A write to this register clears the remote IRR bit in the redirection table entry found matching the interrupt vector. This provides an alternate mechanism other than PCI special cycle for EOI to reach IOxAPIC.

3.16 IOMMU Memory Mapped Registers

See 3.1 [Register Descriptions and Mnemonics] for a description of the register naming convention. See 2.12.1 [IOMMU Configuration Space].

IOMMUx00 Device Table Base Address Low

Bits	Description
31:12	**DevTblBase[31:12]: device table base address bits[31:12]**. Read-write. Reset: 0. DevTblBase[51:12] = {IOMMUx04[DevTblBase[51:32], DevTblBase[31:12]]}. DevTblBase[51:12] specifies the 4Kbyte-aligned base address of the first level device table.
11:9	Reserved.
8:0	**DevTblSize: device table size**. Read-write. Reset: 0. This field contains 1 less than the length of the device table, in multiples of 4K bytes. A minimum size of 0 corresponds to a 4K byte device table and a maximum size of 1FFh corresponds to a 2M byte device table.

IOMMUx04 Device Table Base Address High

Bits	Description
31:20	Reserved.
19:0	**DevTblBase[51:32]: device table base address bits[51:32]**. See: IOMMUx00[DevTblBase[31:12]].

IOMMUx08 Command Buffer Base Address Low

Bits	Description
31:12	**ComBase[31:12]: command buffer base address bits[31:12]**. Read-write. Reset: 0. ComBase[51:12] = {IOMMUx0C[ComBase[51:32], ComBase[31:12]]}. ComBase[51:12] specifies the 4Kbyte-aligned base address of the command buffer.
11:0	Reserved.

IOMMUx0C Command Buffer Base Address High

Bits	Description
31:28	Reserved.
27:24	**ComLen: command buffer length**. Read-write. Reset: 8h. Specifies the length of the command buffer in power of 2 increments. The minimum size is 256 entries (4K bytes); values less than 8h are reserved. Bits — Description 7h-0h — Reserved. Fh-8h — 2^ComLen entries (2^ComLen*16 bytes).
23:20	Reserved.
19:0	**ComBase[51:32]: command buffer base address bits[51:32]**. See: IOMMUx08[ComBase[31:12]].

IOMMUx10 Event Log Base Address Low

Bits	Description
31:12	**EventBase[31:12]: event log base address bits[31:12]**. Read-write. Reset: 0. EventBase[51:12] = {IOMMUx14[EventBase[51:32], EventBase[31:12]]}. EventBase[51:12] specifies the 4K-byte aligned base address of the event log.
11:0	Reserved.

IOMMUx14 Event Log Base Address High

Bits	Description
31:28	Reserved.
27:24	**EventLen: event log length**. Read-write. Reset: 8h. Specifies the length of the event log in power of 2 increments. The minimum size is 256 entries (4K bytes); values less than 8h are reserved. Bits Description 7h-0h Reserved. Fh-8h 2^EventLen entries (2^EvemtLen*16 bytes).
23:20	Reserved.
19:0	**EventBase[51:32]: event log base address bits [51:32]**. See: IOMMUx10[EventBase[31:12]].

IOMMUx18 Control Low

Bits	Description
31:30	Reserved.
29	Reserved.
28	Reserved.
27:25	Reserved.
24	**SmiFLogEn: SMI filter log enable**. Read-write. Reset: 0. Specifies if blocked SMI interrupts are reported in the IOMMU event log. When SmiFSup=00b, SmiFLogEn is ignored by hardware and may be implemented as a read-only value of 0b. 0=SMI interrupts are not logged in the IOMMU event log (same behavior as IOMMU Revision 1). 1=SMI interrupts blocked due to a match-failure with all valid (SmiDV=1b) SMI filter registers are reported in the IOMMU event log.
23	Reserved.
22	**SmiFEn: SMI filter enable**. Read-write. Reset: 0. Specifies how SMI interrupts are controlled by the IOMMU. When SmiFSup=00b, SmiFEn is ignored by hardware and may be implemented as a read-only value of 0. 0=SMI interrupts are always passed-through (same behavior as IOMMU Revision 1). 1=SMI interrupts are blocked unless otherwise controlled by the SMI Filter Registers and blocked SMI interrupts are reported in the event log as governed by SmiFLogEn.

21:18	**Tlpt**. Read-write. Reset: 0. Tlpt contains the 4-bit value matched to the PCIe TLP Type field when the PCIe TLP Fmt value indicates the field carries a prefix.
17	**GaEn**. Read-write. Reset: 0. Guest APIC enable. 1=Loose. 0=Prohibited
16	**GtEn**. Read-write. Reset: 0. 1=Guest translation may be enabled for a peripheral by programming DTE[GV]. This bit must be programmed to zero when IOMMUx30[GtSup]=0.
15	**PprEn**. Read-write. Reset: 0. 1=Peripheral page service requests are processed. 0=Peripheral page service requests are treated as invalid device requests. This bit must be programmed to zero when IOMMUx30[PprSup]=0.
14	**PprIntEn**. Read-write. Reset: 0. 1=An interrupt is generated when IOMMUx2020[PprInt]=1 or IOMMUx2020[PprOverflow]=1. The interrupt vector used is indicated in D0F2x50[IommuMsiNumPpr].This bit must be programmed to zero when IOMMUx30[PprSup]=0.
13	**PprLogEn**. Read-write. Reset: 0. 1=Peripheral page service request events are written to the PPR log when IommuEn=1. 0=Peripheral page service request logging is not enabled. Peripheral page service requests are discarded when PprLogEn=0 or IOMMUx30[PprSup]=0. When IommuEn=1 and software sets PprLogEn, the IOMMU clears IOMMUx2020[PprOverflow] and sets IOMMUx2020[PprRun]. The IOMMU can then write new entries to the event log if there are usable entries available. Software can read IOMMUx2020[PprRun] to determine the status of the peripheral page service request log. Note the peripheral page service request and event logs are independent. IOMMUx38, IOMMUx2030, and IOMMUx2038 must be programmed prior to setting PprLogEn.
12	**CmdBufEn**. Read-write. Reset: 0. 1=Start or restart command buffer processing. When CmdBufEn=1 and IommuEn=1, the IOMMU starts fetching commands and sets IOMMUx2020[CmdBufRun]. 0=Halt command buffer processing. Writing a 0 to this bit causes the IOMMU to cease fetching new commands although commands previously fetched are completed. The IOMMU stops fetching commands upon reset and after errors. See IOMMUx2020[CmdBufRun]. Writing of event log entries is independently controlled by EventLogEn. IOMMUx08, IOMMUx0C, IOMMUx2000, and IOMMUx2008 must be programmed prior to setting CmdBufEn.
11	**Isoc**. Read-write. Reset: 0. This bit controls the state of the isochronous bit in the HyperTransport read request packet when the IOMMU issues I/O page table reads and device table reads on the HyperTransport link. 1=Request packet to use isochronous channel. 0=Request packet to use standard channel. If IOMMU isoc requests are enabled, then we must ensure the isoc channel is enabled as well. See D0F0x98_x1E[HiPriEn].
10	**Coherent**. Read-write. Reset: 1. This bit controls the state of the coherent bit in the HyperTransport read request packet when the IOMMU issues device table reads on the HyperTransport link. 1=Device table requests are snooped by the processor. 0=Device table requests are not snooped by the processor.
9	**ResPassPw**. Read-write. Reset: 0. This bit controls the state of the ResPassPW bit in the HyperTransport read request packet when the IOMMU issues I/O page table reads and device table reads on the HyperTransport link. 1=Response may pass posted requests. 0=Response may not pass posted requests.
8	**PassPw**. Read-write. Reset: 0. This bit controls the state of the PassPW bit in the HyperTransport read request packet when the IOMMU issues I/O page table reads and device table reads on the HyperTransport link. 1=Request packet may pass posted requests. 0=Request packet may not pass posted requests.

7:5	**InvTimeout**. Read-write. Reset: 0. This field specifies the invalidation timeout for IOTLB invalidation requests. Bits: Description 000b: No timeout. 001b: 1 ms. 010b: 10 ms. 011b: 100 ms. 100b: 1 sec. 101b: 10 sec. 111b-110b: Reserved
4	**ComWaitIntEn**. Read-write. Reset: 0. 1=An interrupt is generated when IOMMUx2020[ComWaitInt]=1.
3	**EventIntEn**. Read-write. Reset: 0. 1=An interrupt is generated when IOMMUx2020[EventLogInt]=1 or IOMMUx2020[EventOverflow]=1.
2	**EventLogEn**. Read-write. Reset: 0. 1=All events detected are written to the event log when IommuEn=1. 0=Event logging is not enabled. Events are discarded when the event log is not enabled. When IommuEn=1 and software sets EventLogEn, the IOMMU clears IOMMUx2020[EventOverflow] and sets IOMMUx2020[EventLogRun]. IOMMUx10, IOMMUx14, IOMMUx2010, and IOMMUx2018 must be programmed prior to setting EventLogEn.
1	**HtTunEn**. Read-write. Reset: 0. 1= Upstream traffic received by the HyperTransport tunnel is translated by the IOMMU. 0=Upstream traffic received by the HyperTransport tunnel is not translated by the IOMMU. The IOMMU ignores the state of this bit while IommuEn=0. See D0F2x40[IommuHtTunnelSup].
0	**IommuEn**. Read-write. Reset: 0. 1=IOMMU enabled. All upstream transactions are translated by the IOMMU. IOMMUx00 [Device Table Base Address Low] and IOMMUx04 [Device Table Base Address High] must be configured by software before setting this bit. 0=IOMMU is disabled and no upstream transactions are translated or remapped by the IOMMU. When disabled, the IOMMU does not read any commands or create any event log entries.

IOMMUx20 Exclusion Range Base Low

Bits	Description
31:12	**ExclBase[31:12]: exclusion range base address bits[31:12]**. Read-write. Reset: 0. ExclBase[51:12] = {IOMMUx20[ExclBase[51:32]], ExclBase[31:12]}. Specifies the 4Kbyte-aligned base address of the exclusion range.
11:2	Reserved.
1	**ExAllow: exclusion allow**. Read-write. Reset: 0. 1=All accesses to the exclusion range are forwarded untranslated. 0=The EX bit in the device table entry specifies if accesses to the exclusion range are translated.
0	**ExEn: exclusion enable**. Read-write. Reset: 0. 1=The exclusion range is enabled.

IOMMUx24 Exclusion Range Base High

Bits	Description

31:20	Reserved.
19:0	**ExclBase[51:32]: exclusion range base address bits[51:32]**. See: IOMMUx20[ExclBase[31:12]].

IOMMUx28 Exclusion Range Limit Low

Bits	Description
31:12	**ExclLimit[31:12]: exclusion range limit address bits[31:12]**. Read-write. Reset: 0. ExclLimit[51:12] = {IOMMUx2C[ExclLimit[51:32]], ExclLimit[31:12]}. ExclLimit[51:12] specfies the 4Kbyte-aligned limit address of the exclusion range.
11:0	Reserved.

IOMMUx2C Exclusion Range Limit High

Bits	Description
31:20	Reserved.
19:0	**ExclLimitHi**. See: IOMMUx28[ExclLimit[31:12]].

IOMMUx30 Extended Feature Low

Bits	Description
31:30	Reserved.
29:28	Reserved.
27:26	Reserved.
25:24	Reserved.
23:21	Reserved
20:18	**SmiFRC: SMI-Filter Register Count**. Read-only. Reset: 2. Indicates the number of SMI interrupt filter registers. SmiFRC must be 000b when SmiFSup=00b. Bits — Description 000b — 1 SMI filter registers. 001b — 2 SMI filter registers. 010b — 4 SMI filter registers. 011b — 8 SMI filter registers. 100b — 16 SMI filter registers. 111b-101b — Reserved.
17:16	**SmiFSup: SMI Filter Supported**. Read-only. Reset: 0. Specifies that SMI interrupts may be filtered. Bits — Description 00b — SMI interrupts are always passed-through. 01b — SMI interrupts are filtered under the control of SmiFEn and the SMI-filter registers. 11b-10b — Reserved.

15:14	**GlxSup**. Read-only. Reset: 1. Bits — Description 00b — GLX in the DTE is ignored and the IOMMU performs only single-level guest CR3 lookups. This value is not meaningful when GtSup=0. 01b — Two-level GCR3 base address table is supported in hardware. 10b — Three-level GCR3 base address table is supported in hardware for 20-bit PASID values. 11b — Reserved.
13:12	Reserved.
11:10	**HATS: host address translation size**. Read-only. Reset: 2. The maximum number of host address translation levels supported. This value is not meaningful when GtSup=0. IOMMU behaviour is undefined if Next Level in a page directory entry exceeds the limit set by HATS. See D0F2x70[HatsW]. Bits — Description 00b — 4 levels. 01b — 5 levels. 10b — 6 levels. 11b — Reserved.
9	**PcSup: performance counters supported**. Read-only. Reset: 1. 1=performance counters are supported.
8	**HeSup: hardware error registers supported**. Read-only. Reset: 0. 0=Hardware error registers do not report error information. 1=Error information is reported in hardware error registers.
7	**GaSup: guest virtual APIC supported**. Read-only. Reset: 0. 1=Guest Virtual APIC supported.
6	**IaSup: INVALIDATE_IOMMU_ALL supported**. Read-only. Reset: 1. 1=The INVALIDATE_IOMMU_ALL command is supported.
5	Reserved.
4	**GtSup: guest translation supported**. Read-only. Reset: 1. 1=Guest address translation is supported. 0=Only nested address translation is supported. When GtSup=0, the following values in the DTE must be zero: GV, GLX and GCR3 Table Root Pointer. See IOMMUx18[GtEn].
3	**NxSup: no execute supported**. Read-only. Reset: 0. 1=No-execute protection is supported. 0=No-execute protection is not supported.
2	**XtSup: x2 apic supported**. Read-only. Reset: 0. 1=The interrupt remapping table is expanded to support x2APIC interrupt information. 0=x2APIC support is disabled.
1	**PprSup: peripheral page service request (PPR) supported**. Read-only. Reset: 1. 1=Indicates that IOMMU handles page service request events from peripherals, the IOMMU supports the page service request queue, and that the second IOMMU interrupt can be used to signal peripheral page service request events.
0	**PrefSup: prefetch support**. Read-only. Reset: 1. 1=Indicates that IOMMU will accept PREFETCH_IOMMU_PAGES commands.

IOMMUx34 Extended Feature High

Bits	Description

31:4	Reserved.
3:0	**PasMax: PASID maximum**. Read-only. Reset: 8h. This specifies the maximum PASID value supported. This field is not meaningful when IOMMUx30[GtSup]=0. See D0F2x74[PasMaxW]. Bits Description 2h-0h Reserved. Fh-3h 2^(PasMax+1)-1.

IOMMUx38 PPR Log Base Address Low

Bits	Description
31:12	**PprBase[31:12]: PPR log base address bits[31:12]**. Read-write. Reset: 0. PprBase[51:12] = {IOMMUx3C[PprBase[51:32]], PprBase[31:12]}. PprBase[51:12] specifies the 4Kbyte-aligned base address of the PPR log.
11:0	Reserved.

IOMMUx3C PPR Log Base Address High

Bits	Description
31:28	Reserved.
27:24	**PprLen: PPR log length**. Read-write. Reset: 8h. Specifies the length of the PPR log in power of two increments. Bits Description 7h-0h Reserved. Fh-8h 2^PprLen entries (2^PprLen*16 bytes).
23:20	Reserved.
19:0	**PprBase[51:32]: PPR log base address bits[51:32]**. See: IOMMUx38[31:12].

IOMMUx40 Hardware Error Upper Low

Bits	Description
31:0	**FirstEvCode[31:0]: first event code bits[31:0]**. Read-write. Reset: 0. FirstEvCode[59:0] = {IOMMUx44[FirstEvCode[59:32]], FirstEvCode[31:0]}. IOMMUx44[EvCode] and FirstEvCode[59:0] specify the upper 64 bits of the most recent hardware error detected by the IOMMU.

IOMMUx44 Hardware Error Upper High

Bits	Description
31:28	**EvCode: event code**. Read-write. Reset: 0. Event code for the type of error logged.
27:0	**FirstEvCode[59:32]: first event code bits[59:32]**. See: IOMMUx40[FirstEvCode[31:0]].

IOMMUx48 Hardware Error Lower Low

Bits	Description
31:0	**SecondEvCode[31:0]: second event code bits[31:0]**. Read-write. Reset: 0. SecondEvCode[63:0] = {IOMMUx4C[SecondEvCode[63:32]], SecondEvCode[31:0]}. SecondEvCode[63:0] specifies the lower 64 bits of the most recent hardware error detected by IOMMU.

IOMMUx4C Hardware Error Lower High

Bits	Description
31:0	**SecondEvCode[63:32]: second event code bits[63:32]**. See: IOMMUx48[SecondEvCode[31:0]].

IOMMUx50 Hardware Error Status

Bits	Description
31:2	Reserved.
1	**HEO: hardware error overflow**. Read-write. Reset: 0. Defines the contents of the IOMMU hardware error registers as having beeing overwritten. 0=Not overwritten. 1=Contents overwritten by new information. HEO is only valid when HEV==1.
0	**HEV: hardware error valid**. Read-write. Reset: 0. 1=Contents of the IOMMU hardware error registers are valid.

IOMMUx[78,70,68,60] SMI Filter Low

Table 192: Register Mapping for IOMMUx[78,70,68,60]

Register	Function
IOMMUx60	SMI Filter 0
IOMMUx68	SMI Filter 1
IOMMUx70	SMI Filter 2
IOMMUx78	SMI Filter 3

Bits	Description
31:18	Reserved.
17	**SMIFlock: SMI Filter Lock**. Read-write. Reset: 0.
16	**SMIDV: SMI Device Valid**. IF (SMIFlock==1) THEN Read-only. ELSE Read-write. ENDIF. Reset: 0. The SMI filter is enabled and the device ID specified in SmiDID is valid for SMI.
15:0	**SMIDid: SMI Device ID**. IF (SMIFlock==1) THEN Read-only. ELSE Read-write. ENDIF. Reset: 0. Specifies the device ID for which SMIs are forwarded upstream.

IOMMUx[7C,74,6C,64] SMI Filter High

Table 193: Register Mapping for IOMMUx[7C,74,6C,64]

Register	Function
IOMMUx64	SMI Filter 0
IOMMUx6C	SMI Filter 1
IOMMUx74	SMI Filter 2
IOMMUx7C	SMI Filter 3

Bits	Description
31:0	Reserved.

IOMMUx2000 Command Buffer Head Pointer

Bits	Description
31:19	Reserved.
18:4	**CmdHdptr: command buffer head pointer**. Read-write; updated-by-hardware. Reset: 0. Specifies the 128-bit aligned offset from the command buffer base address register of the next command to be fetched by the IOMMU. The IOMMU increments this register, rolling over to zero at the end of the buffer, after fetching and validating the command in the command buffer. After incrementing this register, the IOMMU cannot re-fetch the command from the buffer. If this register is written by software while IOMMUx2020[CmdBufRun]=1, the IOMMU behavior is undefined. If this register is set by software to a value outside the length specified by IOMMUx0C[ComLen], the IOMMU behavior is undefined.
3:0	Reserved.

IOMMUx2008 Command Buffer Tail Pointer

Bits	Description
31:19	Reserved.
18:4	**CmdTailptr: command buffer tail pointer**. Read-write; updated-by-hardware. Reset: 0. Specifies the 128-bit aligned offset from the command buffer base address register of the next command to be written by the software. Software must increment this field, rolling over to zero at the end of the buffer, after writing a command to the command buffer. If software advances the tail pointer equal to or beyond the head pointer after adding one or more commands to the buffer, the IOMMU behavior is undefined. If software sets the command buffer tail pointer to an offset beyond the length of the command buffer, the IOMMU behavior is undefined.
3:0	Reserved.

IOMMUx2010 Event Log Head Pointer

Bits	Description
31:19	Reserved.

18:4	**EventHdptr: event log head pointer**. Read-write. Reset: 0. Specifies the 128 bit aligned offset from the event log base address register that will be read next by software. Software must increment this field, rolling over at the end of the buffer, after reading an event from the event log. If software advances the head pointer beyond the tail pointer, the IOMMU behavior is undefined. If software sets the event log head pointer to an offset beyond the length of the event log, the IOMMU behavior is undefined.
3:0	Reserved.

IOMMUx2018 Event Log Tail Pointer

Bits	Description
31:19	Reserved.
18:4	**EventTailptr: event log tail pointer**. Read-write. Reset: 0. Specifies the 128-bit aligned offset from the event log base address register that will be written next by the IOMMU when an event is detected. The IOMMU increments this register, rolling over at the end of the buffer, after writing an event to the event log. If this register is written while IOMMUx2020[EventLogRun]==1, the IOMMU behavior is undefined. If this register is set by software to a value outside the length specified by IOMMUx14[EventLen], the IOMMU behavior is undefined.
3:0	Reserved.

IOMMUx2020 Status

Bits	Description
31:19	Reserved.
18	Reserved.
17	Reserved.
16	Reserved.
15	Reserved.
14:13	Reserved.
12	Reserved.
11	Reserved.
10	Reserved.
9	Reserved.
8	Reserved.

7	**PprRun: peripheral page service request running**. Read-only. Reset: 0. 1=Peripheral page requests are logged as they occur. 0=Peripheral page requests are discarded without logging. When PprOverflow=1, the IOMMU does not write new PPR log entries even when PprRun=1. When halted, PPR logging is restarted by using IOMMUx18[PprLogEn].
6	**PprInt: peripheral page service request interrupt**. Read-write; Write-1-to-clear. Reset: 0. 1=PPR entry written to the PPR log by the IOMMU. 0=No PPR entry written to the PPR log by the IOMMU. See IOMMUx18[PprIntEn].
5	**PprOverflow: peripheral page service request overflow**. Read-write; Write-1-to-clear. Reset: 0. 1=IOMMU PPR log overflow has occured. This bit is set when a new peripheral page service request is to be written to the PPR log and there is no usable entry in the PPR log, causing the new information to be discarded. No new PPR log entries are written while this bit is set. See IOMMUx18[PprIntEn].
4	**CmdBufRun: command buffer running**. Read-only. Reset: 0. 1=Commands may be fetched from the command buffer. 0=IOMMU has stopped fetching new commands. The IOMMU freezes command processing after COMMAND_HARDWARE_ERROR or ILLEGAL_COMMAND_ERROR errors. When frozen, command fetching is restarted by using IOMMUx18[CmdBufEn].
3	**EventLogRun: event log running**. Read-only. Reset: 0. 1=Events are logged as they occur. 0=Event reports are discarded without logging. When EventOverflow=1, the IOMMU does not write new event log entries even when EventLogRun=1. When halted, event logging is restarted by using IOMMUx18[EventLogEn].
2	**ComWaitInt: completion wait interrupt**. Read-write; Write-1-to-clear. Reset: 0. 1=COMPLETION_WAIT command completed. This bit is only set if the i bit is set in the COMPLETION_WAIT command. See IOMMUx18[ComWaitIntEn].
1	**EventLogInt: event log interrupt**. Read-write; Write-1-to-clear. Reset: 0. 1=Event entry written to the event log by the IOMMU. See IOMMUx18[EventIntEn].
0	**EventOverflow**. Read-write; Write-1-to-clear. Reset: 0. 1=IOMMU event log overflow has occurred. This bit is set when a new event is to be written to the event log and there is no usable entry in the event log, causing the new event information to be discarded. No new event log entries are written while this bit is set. See IOMMUx18[EventIntEn].

IOMMUx2030 PPR Log Head Pointer

Bits	Description
31:19	Reserved.
18:4	**PprHdptr: PPR head pointer**. Read-write. Reset: 0. Specifies the 128-bit aligned offset from the PPR log base address register that will be read next by software. Software must increment this field, rolling over at the end of the buffer, after reading a PPR entry from the PPR event log. If software advances the head pointer beyond the tail pointer, the IOMMU behavior is undefined. If software sets the PPR log head pointer to an offset beyond the length of the PPR log, the IOMMU behavior is undefined.
3:0	Reserved.

IOMMUx2038 PPR Log Tail Pointer

Bits	Description
31:19	Reserved.
18:4	**PprTailptr**. Read-write. Reset: 0. Specifies the 128-bit aligned offset from the PPR log base address register that will be written next by the IOMMU when a peripheral page request is detected. The IOMMU increments this register, rolling over at the end of the buffer, after writing a PPR entry to the PPR log. If this register is written while IOMMUx2020[PprRun]=1, the IOMMU behavior is undefined. If software sets the PPR log tail pointer to an offset beyond the length of the PPR log, defined by IOMMUx3C[PprLen], the IOMMU behavior is undefined.
3:0	Reserved.

IOMMUx4000 Counter Configuration

Bits	Description
31:18	Reserved.
17:12	**NCounterBanks: number of counter banks**. Read-only. Reset: 2h. The number of counter banks supported by the IOMMU. Each bank contains two or more counter and control registers as specified by NCounter. For each counter bank, a corresponding control bit is in IOMMUx4008, IOMMUx4010, and IOMMUx4018. Each supported event counter bank is in a distinct, consecutive 4K byte page. Bits — Description 00h — No counter banks supported. 3Fh-01h — <NCounterBanks> event counter banks are supported. Note: IOMMU event counter banks are numbered starting with 0.
11	Reserved.
10:7	**NCounter: number of counters per bank**. Read-only. Reset: 4h. Reports the number of individual counters in each IOMMU counter bank. Each counter bank contains the same number of counters. Bits — Description 0h — No counters supported. 1h — Reserved. Fh-2h — <NCounter> counters in each bank.
6:0	Reserved.

IOMMUx4008 Counter PASID Bank Lock Low

Bits	Description
31:0	**PasidLock[31:0]: pasid lock enable bits[31:0]**. Read-write. Reset: 0. PasidLock[63:0] = {IOMMUx400C[PasidLock[63:32]], PasidLock[31:0]}. For each bit in PasidLock[63:0], if the bit is set then writes to the corresponding bank in IOMMUx4[1,0][3:0]10 and IOMMUx4[1,0][3:0]14 are ignored. Bit positions above the value reported in IOMMUx4000[NCounterBanks] are ignored when written and return zero when read.

IOMMUx400C Counter PASID Bank Lock High

Bits	Description
31:0	**PasidLock[63:32]**. See: IOMMUx4008[PasidLock[31:0]].

IOMMUx4010 Domain Bank Lock Low

Bits	Description
31:0	**DomainLock[31:0]: domain lock enable bits[31:0]**. Read-write. Reset: 0. DomainLock[63:0] = {IOMMUx4014[DomainLock[63:32]], DomainLock[31:0]}. For each bit in DomainLock[63:0], if the bit is set then writes to the corresponding bank in IOMMUx4[1,0][3:0]18 and IOMMUx4[1,0][3:0]1C are ignored. Bit positions above the value reported in IOMMUx4000[NCounterBanks] are ignored when written and return zero when read.

IOMMUx4014 Domain Bank Lock High

Bits	Description
31:0	**DomainLock[63:32]**. See: IOMMUx4010[DomainLock[31:0]].

IOMMUx4018 DeviceID Bank Lock Low

Bits	Description
31:0	**DevIDLock[31:0]: deviceID lock enable bits[31:0]**. Read-write. Reset: 0. DevIDLock[63:0] = {IOMMUx401C[DevIDLock[63:32]], DevIDLock[31:0]}. For each bit in DevIDLock[63:0], if the bit is set then writes to the corresponding bank in IOMMUx4[1,0][3:0]20 and IOMMUx4[1,0][3:0]24 are ignored. Bit positions above the value reported in IOMMUx4000[NCounterBanks] are ignored when written and return zero when read.

IOMMUx401C DeviceID Bank Lock High

Bits	Description
31:0	**DevIDLock[63:32]**. See: IOMMUx4018[DevIDLock[31:0]].

IOMMUx4[1,0][3:0]00 Counter Low

Table 194: Register Mapping for IOMMUx4[1,0][3:0]00

Register	Function	Register	Function
IOMMUx40000	Bank 0 Counter 0	IOMMUx41000	Bank 1 Counter 0
IOMMUx40100	Bank 0 Counter 1	IOMMUx41100	Bank 1 Counter 1
IOMMUx40200	Bank 0 Counter 2	IOMMUx41200	Bank 1 Counter 2
IOMMUx40300	Bank 0 Counter 3	IOMMUx41300	Bank 1 Counter 3

Bits	Description
31:0	**Icounter[31:0]**. Read-write. Reset: 0. Icounter[47:0] = {IOMMUx4[1,0][3:0]04[Icounter[47:32]], Icounter[31:0]}. Icounter[47:0] reports the counter value. The counter counts up continuously, wrapping at the maximum value. There is no overflow indicator.

IOMMUx4[1,0][3:0]04 Counter High

Table 195: Register Mapping for IOMMUx4[1,0][3:0]04

Register	Function	Register	Function
IOMMUx40004	Bank 0 Counter 0	IOMMUx41004	Bank 1 Counter 0
IOMMUx40104	Bank 0 Counter 1	IOMMUx41104	Bank 1 Counter 1
IOMMUx40204	Bank 0 Counter 2	IOMMUx41204	Bank 1 Counter 2
IOMMUx40304	Bank 0 Counter 3	IOMMUx41304	Bank 1 Counter 3

Bits	Description
31:16	Reserved.
15:0	**Icounter[47:32]**. See: IOMMUx4[1,0][3:0]00[Icounter[31:0]].

IOMMUx4[1,0][3:0]08 Counter Source

Table 196: Register Mapping for IOMMUx4[1,0][3:0]08

Register	Function	Register	Function
IOMMUx40008	Bank 0 Counter 0	IOMMUx41008	Bank 1 Counter 0
IOMMUx40108	Bank 0 Counter 1	IOMMUx41108	Bank 1 Counter 1
IOMMUx40208	Bank 0 Counter 2	IOMMUx41208	Bank 1 Counter 2
IOMMUx40308	Bank 0 Counter 3	IOMMUx41308	Bank 1 Counter 3

Bits	Description
31	**Cac: counter source architectural or custom**. Read-write. Reset: 0. 0=Architectural counter input group. 1=Custom input group.
30	**CountUnits**. Read-write. Reset: 0. 0=Counter counts events (level). 1=Counter counts clocks (edges).
29:8	Reserved.
7:0	**Csource: counter source**. Read-write. Reset: 0. Counter source. Selects event counter input from the choices provided.

IOMMUx4[1,0][3:0]10 PASID Match Low

See IOMMUx4008.

Table 197: Register Mapping for IOMMUx4[1,0][3:0]10

Register	Function	Register	Function
IOMMUx40010	Bank 0 Counter 0	IOMMUx41010	Bank 1 Counter 0

Table 197: Register Mapping for IOMMUx4[1,0][3:0]10

IOMMUx40110	Bank 0 Counter 1	IOMMUx41110	Bank 1 Counter 1
IOMMUx40210	Bank 0 Counter 2	IOMMUx41210	Bank 1 Counter 2
IOMMUx40310	Bank 0 Counter 3	IOMMUx41310	Bank 1 Counter 3

Bits	Description
31	**PasMEn: PASID match enable**. Read-write. Reset: 0. 0=PASID is ignored. 1=Filtered PASID must match to count an event. An event with no PASID tag is only counted when Pasmen=0.
30:16	Reserved.
15:0	**PasidMatch**. Read-write. Reset: 0. This value is compared with the masked (filtered) value of the incoming PASID of the transaction to decide if the corresponding event is counted. The event is counted if PasidMatch is exactly equal to the masked incoming PASID.

IOMMUx4[1,0][3:0]14 PASID Match High

See IOMMUx4008.

Table 198: Register Mapping for IOMMUx4[1,0][3:0]14

Register	Function	Register	Function
IOMMUx40014	Bank 0 Counter 0	IOMMUx41014	Bank 1 Counter 0
IOMMUx40114	Bank 0 Counter 1	IOMMUx41114	Bank 1 Counter 1
IOMMUx40214	Bank 0 Counter 2	IOMMUx41214	Bank 1 Counter 2
IOMMUx40314	Bank 0 Counter 3	IOMMUx41314	Bank 1 Counter 3

Bits	Description
31:16	Reserved.
15:0	**PasidMask**. Read-write. Reset: 0. This bit-mask is ANDed with the PASID of the transaction to decide to count the corresponding event. 0=Count events for all values of incoming PASID. 0001h-FFFFh=Bit-wise mask ANDed with incoming PASID.

IOMMUx4[1,0][3:0]18 Domain Match Low

Table 199: Register Mapping for IOMMUx4[1,0][3:0]18

Register	Function	Register	Function
IOMMUx40018	Bank 0 Counter 0	IOMMUx41018	Bank 1 Counter 0
IOMMUx40118	Bank 0 Counter 1	IOMMUx41118	Bank 1 Counter 1
IOMMUx40218	Bank 0 Counter 2	IOMMUx41218	Bank 1 Counter 2
IOMMUx40318	Bank 0 Counter 3	IOMMUx41318	Bank 1 Counter 3

Bits	Description
31	**DomMEn: domain match enable**. Read-write. Reset: 0. 0=Domain is ignored. 1=Filtered Domain must match DomainMatch to count an event.

30:16	Reserved.
15:0	**DomainMatch**. Read-write. Reset: 0. This value is compared with the masked (filtered) value of the incoming Domain of the transaction to decide to count the corresponding event. The event is counted if DomainMatch is exactly equal to the masked incoming Domain.

IOMMUx4[1,0][3:0]1C Domain Match High

Table 200: Register Mapping for IOMMUx4[1,0][3:0]1C

Register	Function	Register	Function
IOMMUx4001C	Bank 0 Counter 0	IOMMUx4101C	Bank 1 Counter 0
IOMMUx4011C	Bank 0 Counter 1	IOMMUx4111C	Bank 1 Counter 1
IOMMUx4021C	Bank 0 Counter 2	IOMMUx4121C	Bank 1 Counter 2
IOMMUx4031C	Bank 0 Counter 3	IOMMUx4131C	Bank 1 Counter 3

Bits	Description
31:16	Reserved.
15:0	**DomainMask**. Read-write. Reset: 0. This bit-mask is ANDed with the Domain of the transaction to decide to count the corresponding event. 0000h=Count events for all values of incoming Domain. 0001h-FFFFh=Bit-wise mask ANDed with incoming Domain.

IOMMUx4[1,0][3:0]20 DeviceID Match Low

Table 201: Register Mapping for IOMMUx4[1,0][3:0]20

Register	Function	Register	Function
IOMMUx40020	Bank 0 Counter 0	IOMMUx41020	Bank 1 Counter 0
IOMMUx40120	Bank 0 Counter 1	IOMMUx41120	Bank 1 Counter 1
IOMMUx40220	Bank 0 Counter 2	IOMMUx41220	Bank 1 Counter 2
IOMMUx40320	Bank 0 Counter 3	IOMMUx41320	Bank 1 Counter 3

Bits	Description
31	**DidMEn: deviceID match enable**. Read-write. Reset: 0. 0=DeviceID is ignored. 1=Filtered DeviceID must match to count an event.
30:16	Reserved.
15:0	**DeviceidMatch**. Read-write. Reset: 0. This value is compared with the masked (filtered) value of the incoming DeviceID of the transaction to decide to count the corresponding event. The event is counted if DeviceidMatch is exactly equal to the masked incoming DeviceID.

IOMMUx4[1,0][3:0]24 DeviceID Match High

Table 202: Register Mapping for IOMMUx4[1,0][3:0]24

Register	Function	Register	Function
IOMMUx40024	Bank 0 Counter 0	IOMMUx41024	Bank 1 Counter 0

Table 202: Register Mapping for IOMMUx4[1,0][3:0]24

IOMMUx40124	Bank 0 Counter 1	IOMMUx41124	Bank 1 Counter 1
IOMMUx40224	Bank 0 Counter 2	IOMMUx41224	Bank 1 Counter 2
IOMMUx40324	Bank 0 Counter 3	IOMMUx41324	Bank 1 Counter 3

Bits	Description
31:16	Reserved.
15:0	**DeviceidMask**. Read-write. Reset: 0. This bit-mask is ANDed with the DeviceID of the transaction to decide to count the corresponding event. 0=Count events for all values of incoming DeviceID. 0001h-FFFFh=Bit-wise mask ANDed with incoming DeviceID.

IOMMUx4[1,0][3:0]28 Counter Report Low

Table 203: Register Mapping for IOMMUx4[1,0][3:0]28

Register	Function	Register	Function
IOMMUx40028	Bank 0 Counter 0	IOMMUx41028	Bank 1 Counter 0
IOMMUx40128	Bank 0 Counter 1	IOMMUx41128	Bank 1 Counter 1
IOMMUx40228	Bank 0 Counter 2	IOMMUx41228	Bank 1 Counter 2
IOMMUx40328	Bank 0 Counter 3	IOMMUx41328	Bank 1 Counter 3

Bits	Description
31:0	**EventNote[31:0]**. Read-write. Reset: 0. EventNote[51:0] = {IOMMUx4[1,0][3:0]2C[EventNote[51:32]], EventNote[31:0]}. When IOMMUx4[1,0][3:0]2C[CERE]==1 and the corresponding counter is incremented and wraps to zero, EventNote[51:0] is reported in the EVENT_COUNTER_ZERO event log entry.

IOMMUx4[1,0][3:0]2C Counter Report High

Table 204: Register Mapping for IOMMUx4[1,0][3:0]2C

Register	Function	Register	Function
IOMMUx4002C	Bank 0 Counter 0	IOMMUx4102C	Bank 1 Counter 0
IOMMUx4012C	Bank 0 Counter 1	IOMMUx4112C	Bank 1 Counter 1
IOMMUx4022C	Bank 0 Counter 2	IOMMUx4122C	Bank 1 Counter 2
IOMMUx4032C	Bank 0 Counter 3	IOMMUx4132C	Bank 1 Counter 3

Bits	Description
31	**CERE: counter event report enable**. Read-write. Reset: 0. Counter Event Report Enable. 0=No event report when counter wraps to zero. 1=IOMMU writes an EVENT_COUNTER_ZERO event log entry when the counter wraps to zero. The counter-wrap event is treated like any other event. Software note: the counter-wrap event is delivered promptly but without a latency assurance.
30:20	Reserved.
19:0	**EventNote[51:32]**. See: IOMMUx4[1,0][3:0]28[EventNote[31:0]].

THIS PAGE INTENTIALLY LEFT BLANK

3.17 APIC Registers

See 2.4.9.1.2 [APIC Register Space].

MMIO local APIC space is accessible in xAPIC mode.

APIC20 APIC ID

Bits	Description
31:24	**ApicId: APIC ID**. Read-write. Reset: Varies based on core number. • The initial value of APIC20[ApicId[7:0]] is {0000b, CpuCoreNum[3:0]}. See 2.4.9.1.3 [ApicId Enumeration Requirements]. See 2.4.4 [Processor Cores and Downcoring].
23:0	Reserved.

APIC30 APIC Version

Bits	Description
31	**ExtApicSpace: extended APIC register space present**. Read-only. Reset: 1. 1=Indicates the presence of extended APIC register space starting at APIC400.
30:25	RAZ.
24	**DirectedEoiSupport: directed EOI support**. Read-only. Reset: 0. 0=Directed EOI capability not supported.
23:16	**MaxLvtEntry**. Read-only. Reset: Product-specific. Specifies the number of entries in the local vector table minus one.
15:8	RAZ.
7:0	**Version**. Read-only. Reset: 10h. Indicates the version number of this APIC implementation.

APIC80 Task Priority (TPR)

Bits	Description
31:8	RAZ.
7:0	**Priority**. Read-write. Reset: 0. This field is assigned by software to set a threshold priority at which the core is interrupted.

APIC90 Arbitration Priority (APR)

Bits	Description
31:8	RAZ.
7:0	**Priority**. Read-only. Reset: 0. Indicates the current priority for a pending interrupt, or a task or interrupt being serviced by the core. The priority is used to arbitrate between cores to determine which accepts a lowest-priority interrupt request.

APICA0 Processor Priority (PPR)

Bits	Description
31:8	RAZ.
7:0	**Priority**. Reset: 0. Read-only. Indicates the core's current priority servicing a task or interrupt, and is used to determine if any pending interrupts should be serviced. It is the higher value of the task priority value and the current highest in-service interrupt.

APICB0 End of Interrupt

This register is written by the software interrupt handler to indicate the servicing of the current interrupt is complete.

Bits	Description
31:0	Unused. Write-only.

APICC0 Remote Read

Bits	Description
31:0	**RemoteReadData**. Read-only. Reset: 0. The data resulting from a valid completion of a remote read inter-processor interrupt.

APICD0 Logical Destination (LDR)

Bits	Description
31:24	**Destination**. Read-write. Reset: 0. This APIC's destination identification. Used to determine which interrupts should be accepted.
23:0	Reserved.

APICE0 Destination Format

Only supported in xAPIC mode.

Bits	Description
31:28	**Format**. Read-write. Reset: Fh. Controls which formatto use when accepting interrupts with a logical destination mode. Bits — Definition 0h — Cluster destinations are used. Eh-1h — Reserved. Fh — Flat destinations are used.
27:0	Reserved. Reset: FFF_FFFFh.

APICF0 Spurious-Interrupt Vector (SVR)

Bits	Description
31:13	RAZ.
12	**EoiBroadcastDisable: EOI broadcast disable**. Read-only. Reset: 0.
11:10	RAZ.
9	**FocusDisable**. Read-write. Reset: 0. 1=Disable focus core checking during lowest-priority arbitrated interrupts.
8	**APICSWEn: APIC software enable**. Read-write. Reset: 0. 0=SMI, NMI, INIT, LINT[1:0], and Startup interrupts may be accepted; pending interrupts in APIC[170:100] and APIC[270:200] are held, but further fixed, lowest-priority, and ExtInt interrupts are not accepted. All LVT entry mask bits are set and cannot be cleared.
7:0	**Vector**. Read-write. Reset: FFh. The vector that is sent to the core in the event of a spurious interrupt. The behavior of bits 3:0 are controlled as specified by D18F0x68[ApicExtSpur].

APIC[170:100] In-Service (ISR)

The in-service registers provide a bit per interrupt to indicate that the corresponding interrupt is being serviced by the core. APIC100[15:0] are reserved. Interrupts are mapped as follows:

Table 205: Register Mapping for APIC[170:100]

Register	Function
APIC100	Interrupts [31:16]
APIC110	Interrupts [63:32]
APIC120	Interrupts [95:64]
APIC130	Interrupts [127:96]
APIC140	Interrupts [159:128]
APIC150	Interrupts [191:160]
APIC160	Interrupts [223:192]
APIC170	Interrupts [255:224]

Bits	Description
31:0	**InServiceBits**. Reset: 0. Read-only. These bits are set when the corresponding interrupt is being serviced by the core.

APIC[1F0:180] Trigger Mode (TMR)

The trigger mode registers provide a bit per interrupt to indicate the assertion mode of each interrupt. APIC180[15:0] are reserved. Interrupts are mapped as follows:

Table 206: Register Mapping for APIC[1F0:180]

Register	Function
APIC180	Interrupts [31:16]
APIC190	Interrupts [63:32]
APIC1A0	Interrupts [95:64]
APIC1B0	Interrupts [127:96]
APIC1C0	Interrupts [159:128]
APIC1D0	Interrupts [191:160]
APIC1E0	Interrupts [223:192]
APIC1F0	Interrupts [255:224]

Bits	Description
31:0	**TriggerModeBits**. Reset: 0. Read-only. The corresponding trigger mode bit is updated when an interrupt is accepted. The values are: 0=Edge-triggered interrupt. 1=Level-triggered interrupt.

APIC[270:200] Interrupt Request (IRR)

The interrupt request registers provide a bit per interrupt to indicate that the corresponding interrupt has been accepted by the APIC. APIC200[15:0] are reserved. Interrupts are mapped as follows:

Table 207: Register Mapping for APIC[270:200]

Register	Function
APIC200	Interrupts [31:16]
APIC210	Interrupts [63:32]
APIC220	Interrupts [95:64]
APIC230	Interrupts [127:96]
APIC240	Interrupts [159:128]
APIC250	Interrupts [191:160]
APIC260	Interrupts [223:192]
APIC270	Interrupts [255:224]

Bits	Description
31:0	**RequestBits**. Read-only. Reset: 0. The corresponding request bit is set when the an interrupt is accepted by the APIC.

APIC280 Error Status

Writes to this register trigger an update of the register state. The value written by software is arbitrary. Each write causes the internal error state to be loaded into this register, clearing the internal error state. Consequently, a second write prior to the occurrence of another error causes the register to be overwritten with cleared data.

Bits	Description
31:8	RAZ.

7	**IllegalRegAddr: illegal register address**. Read-write. Reset: 0. This bit indicates that an access to a nonexistent register location within this APIC was attempted. Can only be set in xAPIC mode.
6	**RcvdIllegalVector: received illegal vector**. Read-write. Reset: 0. This bit indicates that this APIC has received a message with an illegal vector (00h to 0Fh for fixed and lowest priority interrupts).
5	**SentIllegalVector**. Read-write. Reset: 0. This bit indicates that this APIC attempted to send a message with an illegal vector (00h to 0Fh for fixed and lowest priority interrupts).
4	RAZ.
3	**RcvAcceptError: receive accept error**. Read-write. Reset: 0. This bit indicates that a message received by this APIC was not accepted by this or any other APIC.
2	**SendAcceptError**. Read-write. Reset: 0. This bit indicates that a message sent by this APIC was not accepted by any APIC.
1:0	RAZ.

APIC300 Interrupt Command Low (ICR Low)

Not all combinations of ICR fields are valid. Only the following combinations are valid:

Table 208: ICR valid combinations

Message Type	Trigger Mode	Level	Destination Shorthand
Fixed	Edge	x	x
	Level	Assert	x
Lowest Priority, SMI, NMI, INIT	Edge	x	Destination or all excluding self.
	Level	Assert	Destination or all excluding self
Startup	x	x	Destination or all excluding self

Note: x indicates a don’t care.

Bits	Description
31:20	RAZ.
19:18	**DestShrthnd: destination shorthand**. Read-write. Reset: 0. Provides a quick way to specify a destination for a message. Bits — Description 00b — No shorthand (Destination field) 01b — Self 10b — All including self 11b — All excluding self (This sends a message with a destination encoding of all 1s, so if lowest priority is used the message could end up being reflected back to this APIC.) If all including self or all excluding self is used, then destination mode is ignored and physical is automatically used.

17:16	**RemoteRdStat: remote read status**. Read-only. Reset: 0. Bits — Description 00b — Read was invalid 01b — Delivery pending 10b — Delivery complete and access was valid 11b — Reserved
15	**TM: trigger mode**. Read-write. Reset: 0. Indicates how this interrupt is triggered. 0=Edge triggered. 1=Level triggered.
14	**Level**. Read-write. Reset: 0. 0=Deasserted. 1=Asserted.
13	RAZ.
12	**DS: interrupt delivery status**. Read-only. Reset: 0. This bit is set to indicate that the interrupt has not yet been accepted by the destination core(s). 0=Idle. 1=Send pending. Software may repeatedly write ICRL without polling the DS bit; all requested IPIs will be delivered.
11	**DM: destination mode**. Read-write. Reset: 0. 0=Physical. 1=Logical.
10:8	**MsgType**. Read-write. Reset: 0. The message types are encoded as follows: Bits — Description 000b — Fixed 001b — Lowest Priority 010b — SMI 011b — Remote Read 100b — NMI 101b — INIT 110b — Startup 111b — External Interrupt
7:0	**Vector**. Read-write. Reset: 0. The vector that is sent for this interrupt source.

APIC310 Interrupt Command High (ICR High)

Bits	Description
31:24	**DestinationField**. Read-write. Reset: 0. The destination encoding used when APIC300[DestShrthnd] is 00b.
23:0	RAZ.

APIC320 LVT Timer

Bits	Description
31:18	RAZ.
17	**Mode**. Read-write. Reset: 0. 0=One-shot. 1=Periodic.
16	**Mask**. Read-write. Reset: 1. 0=Not masked. 1=Masked.
15:13	RAZ.
12	**DS: interrupt delivery status**. Read-only; updated-by-hardware. Reset: 0. 0=Idle. 1=Send pending. (Indicates that the interrupt has not yet been accepted by the core.)
11	RAZ.

10:8	**MsgType: message type**. Read-write. Reset: 000b. See 2.4.9.1.14 [Generalized Local Vector Table].
7:0	**Vector**. Read-write. Reset: 00h. Interrupt vector number.

APIC330 LVT Thermal Sensor

Interrupts for this local vector table are caused by changes in MSRC001_0061[CurPstateLimit] due to SB-RMI or HTC.

Bits	Description
31:17	RAZ.
16	**Mask**. Read-write. Reset: 1. 0=Not masked. 1=Masked.
15:13	RAZ.
12	**DS: interrupt delivery status**. Read-only; updated-by-hardware. Reset: 0. 0=Idle. 1=Send pending. (Indicates that the interrupt has not yet been accepted by the core.)
11	RAZ.
10:8	**MsgType: message type**. Read-write. Reset: 000b. See 2.4.9.1.14 [Generalized Local Vector Table].
7:0	**Vector**. Read-write. Reset: 00h. Interrupt vector number.

APIC340 LVT Performance Monitor

Interrupts for this local vector table are caused by overflows of:

- MSRC001_00[07:04] [Performance Event Counter (PERF_CTR[3:0])].
- MSRC001_020[B,9,7,5,3,1] [Performance Event Counter (PERF_CTR[5:0])].
- MSRC001_024[7,5,3,1] [Northbridge Performance Event Counter (NB_PERF_CTR[3:0])].

Bits	Description
31:17	RAZ.
16	**Mask**. Read-write. Reset: 1. 0=Not masked. 1=Masked.
15:13	RAZ.
12	**DS: interrupt delivery status**. Read-only; updated-by-hardware. Reset: 0. 0=Idle. 1=Send pending. (Indicates that the interrupt has not yet been accepted by the core.)
11	RAZ.
10:8	**MsgType: message type**. Read-write. Reset: 000b. See 2.4.9.1.14 [Generalized Local Vector Table].
7:0	**Vector**. Read-write. Reset: 00h. Interrupt vector number.

APIC3[60:50] LVT LINT[1:0]

Table 209: Register Mapping for APIC3[60:50]

Register	Function
APIC350	LINT 0
APIC360	LINT 1

Bits	Description
31:17	RAZ.
16	**Mask**. Read-write. Reset: 1. 0=Not masked. 1=Masked.
15	**TM: trigger mode**. Read-write. Reset: 0. 0=Edge. 1=Level.
14	**RmtIRR**. Read-only; updated-by-hardware. Reset: 0. If trigger mode is level, remote IRR is set when the interrupt has begun service. Remote IRR is cleared when the end of interrupt has occurred.
13	Reserved.
12	**DS: interrupt delivery status**. Read-only; updated-by-hardware. Reset: 0. 0=Idle. 1=Send pending. (Indicates that the interrupt has not yet been accepted by the core.)
11	RAZ.
10:8	**MsgType: message type**. Read-write. Reset: 000b. See 2.4.9.1.14 [Generalized Local Vector Table].
7:0	**Vector**. Read-write. Reset: 00h. Interrupt vector number.

APIC370 LVT Error

Bits	Description
31:17	RAZ.
16	**Mask**. Read-write. Reset: 1. 0=Not masked. 1=Masked.
15:13	Reserved.
12	**DS: interrupt delivery status**. Read-only; updated-by-hardware. Reset: 0. 0=Idle. 1=Send pending. (Indicates that the interrupt has not yet been accepted by the core.)
11	RAZ.
10:8	**MsgType: message type**. Read-write. Reset: 000b. See 2.4.9.1.14 [Generalized Local Vector Table].
7:0	**Vector**. Read-write. Reset: 00h. Interrupt vector number.

APIC380 Timer Initial Count

Bits	Description
31:0	**Count**. Read-write. Reset: 0. The value copied into the current count register when the timer is loaded or reloaded.

APIC390 Timer Current Count

Bits	Description
31:0	**Count**. Read-only. Reset: 0. The current value of the counter.

APIC3E0 Timer Divide Configuration

The Div bits are encoded as follows:

Table 210: Div[3,1:0] Value Table

Div[3]	Div[1:0]	Resulting Timer Divide
0	00b	2
0	01b	4
0	10b	8
0	11b	16
1	00b	32
1	01b	64
1	10b	128
1	11b	1

Bits	Description
31:4	RAZ.
3	**Div[3]**. Read-write. Reset: 0. See Table 210.
2	RAZ.
1:0	**Div[1:0]**. Read-write. Reset: 0. See Table 210.

APIC400 Extended APIC Feature

Bits	Description
31:24	RAZ.
23:16	**ExtLvtCount: extended local vector table count**. Read-only. Reset: 04h. This specifies the number of extended LVT registers (APIC[530:500]) in the local APIC.
15:3	RAZ.
2	**ExtApicIdCap: extended APIC ID capable**. Read-only. Reset: 1. 1=The processor is capable of supporting an 8-bit APIC ID, as controlled by APIC410[ExtApicIdEn].
1	**SeoiCap: specific end of interrupt capable**. Read-only. Reset: 1. 1=The APIC420 [Specific End Of Interrupt] is present.
0	**IerCap: interrupt enable register capable**. Read-only. Reset: 1. This bit indicates that the APIC[4F0:480] [Interrupt Enable] are present. See 2.4.9.1.8 [Interrupt Masking].

APIC410 Extended APIC Control

Bits	Description
31:3	RAZ.
2	**ExtApicIdEn: extended APIC ID enable**. Read-write. Reset: 0. 1=Enable 8-bit APIC ID; APIC20[ApicId] supports an 8-bit value; an interrupt broadcast in physical destination mode requires that the IntDest[7:0]=1111_1111b (instead of xxxx_1111b); a match in physical destination mode occurs when (IntDest[7:0] == ApicId[7:0]) instead of (IntDest[3:0] == ApicId[3:0]). If ExtApicIdEn=1 then program D18F0x68[ApicExtId]=1 and D18F0x68[ApicExtBrdCst]=1.

1	**SeoiEn**. Read-write. Reset: 0. 1=Enable SEOI generation when a write to APIC420 [Specific End Of Interrupt] is received.
0	**IerEn**. Read-write. Reset: 0. 1=Enable writes to the interrupt enable registers.

APIC420 Specific End Of Interrupt

Bits	Description
31:8	RAZ.
7:0	**EoiVec: end of interrupt vector**. Read-write. Reset: 0. A write to this field causes an end of interrupt cycle to be performed for the vector specified in this field. The behavior is undefined if no interrupt is pending for the specified interrupt vector.

APIC[4F0:480] Interrupt Enable

Interrupt enables range is mapped as follows:

Table 211: Register Mapping for APIC[4F0:480]

Register	Function
APIC480	IntEn[31:0]
APIC490	IntEn[63:32]
APIC4A0	IntEn[95:64]
APIC4B0	IntEn[127:96]
APIC4C0	IntEn[159:128]
APIC4D0	IntEn[191:160]
APIC4E0	IntEn[223:192]
APIC4F0	IntEn[255:224]

Bits	Description
31:0	**InterruptEnableBits**. Read-write. Reset: FFFF_FFFFh. The interrupt enable bits can be used to enable each of the 256 interrupts. See above table.

APIC[530:500] Extended Interrupt [3:0] Local Vector Table

APIC500 provides a local vector table entry for IBS; See D18F3x1CC. APIC510 provides a local vector table entry for error thresholding. The APIC[530:520] registers are unused.

Table 212: Register Mapping for APIC[530:500]

Register	Function
APIC500	Extended Interrupt 0 (IBS)
APIC510	Extended Interrupt 1 (Thresholding)
APIC520	Extended Interrupt 2
APIC530	Extended Interrupt 3

Bits	Description
31:17	RAZ.
16	**Mask**. Read-write. Reset: 1. 0=Not masked. 1=Masked.
15:13	RAZ.
12	**DS: interrupt delivery status**. Read-only; updated-by-hardware. Reset: 0. 0=Idle. 1=Send pending. (Indicates that the interrupt has not yet been accepted by the core.)
11	RAZ.
10:8	**MsgType: message type**. Read-write. Reset: 000b. See 2.4.9.1.14 [Generalized Local Vector Table].
7:0	**Vector**. Read-write. Reset: 00h. Interrupt vector number.

3.18 CPUID Instruction Registers

Processor feature capabilities and configuration information are provided through the CPUID instruction. The information is accessed by (1) selecting the CPUID function setting EAX and optionally ECX for some functions, (2) executing the CPUID instruction, and (3) reading the results in the EAX, EBX, ECX, and EDX registers. The syntax *CPUID FnXXXX_XXXX_EiX[_xYYY]* refers to the function where EAX==X, and optionally ECX==Y, and the registers specified by EiX. EiX can be any single register such as {EAX, EBX, ECX, and EDX}, or a range of registers, such as E[C,B,A]X. Undefined function numbers return 0's in all 4 registers. See 2.4.11 [CPUID Instruction].

Unless otherwise specified, single-bit feature fields are encoded as 1=Feature is supported by the processor; 0=Feature is not supported by the processor.

The following provides processor specific details about CPUID.

CPUID Fn0000_0000_EAX Processor Vendor and Largest Standard Function Number

Bits	Description
31:0	**LFuncStd: largest standard function**. Value: 0000_000Dh. The largest CPUID standard function input value supported by the processor implementation.

CPUID Fn0000_0000_E[D,C,B]X Processor Vendor

CPUID Fn0000_0000_E[D,C,B]X and CPUID Fn8000_0000_E[D,C,B]X return the same value.

Table 213: Reset Mapping for CPUID Fn8000_0000_E[D,C,B]X

Register	Value	Description
CPUID Fn0000_0000_EBX	6874_7541h	The ASCII characters "h t u A".
CPUID Fn0000_0000_ECX	444D_4163h	The ASCII characters "D M A c".
CPUID Fn0000_0000_EDX	6974_6E65h	The ASCII characters "i t n e".

Bits	Description
31:0	**Vendor**. The 12 8-bit ASCII character codes to create the string "AuthenticAMD".

CPUID Fn0000_0001_EAX Family, Model, Stepping Identifiers

Also see CPUID Fn8000_0001_EAX [Family, Model, Stepping Identifiers].

Family is an 8-bit value and is defined as: **Family[7:0] =** ({0000b,BaseFamily[3:0]} + ExtendedFamily[7:0]). E.g. If BaseFamily[3:0]=Fh and ExtendedFamily[7:0]=07h, then Family[7:0]=16h.

Model is an 8-bit value and is defined as: **Model[7:0]** = {ExtendedModel[3:0], BaseModel[3:0]}. E.g. If ExtendedModel[3:0]=Eh and BaseModel[3:0]=8h, then Model[7:0] = E8h. Model numbers vary with product.

Bits	Description
31:28	Reserved.
27:20	**ExtFamily: extended family**. Alias of D18F3xFC[ExtFamily].
19:16	**ExtModel: extended model**. Alias of D18F3xFC[ExtModel].
15:12	Reserved.
11:8	**BaseFamily**. Alias of D18F3xFC[BaseFamily].
7:4	**BaseModel**. Alias of D18F3xFC[BaseModel].
3:0	**Stepping**. Alias of D18F3xFC[Stepping].

CPUID Fn0000_0001_EBX LocalApicId, LogicalProcessorCount, CLFlush

Bits	Description
31:24	**LocalApicId: initial local APIC physical ID**. The initial APIC20[ApicId] value. See 2.4.4 [Processor Cores and Downcoring].
23:16	**LogicalProcessorCount: logical processor count**. Value: CPUID Fn8000_0008_ECX[NC] + 1. Specifies the number of cores in the processor as CPUID Fn8000_0008_ECX[NC] + 1.
15:8	**CLFlush: CLFLUSH size in quadwords**. Value: 08h.
7:0	**8BitBrandId: 8 bit brand ID**. Value: 00h. Indicates that the brand ID is in CPUID Fn8000_0001_EBX.

CPUID Fn0000_0001_ECX Feature Identifiers

These values can be over-written by MSRC001_1004.

Bits	Description
31	RAZ. Reserved for use by hypervisor to indicate guest status.
30	**RDRAND: RDRAND instruction support**. Value: 0.
29	**F16C: half-precision convert instruction support**. Value: 1.
28	**AVX: AVX instruction support**. Value: 1. Value: 1.

27	**OSXSAVE: OS enabled support for XGETBV/XSETBV**. 1=The OS has enabled support for XGETBV/XSETBV instructions to query processor extended states.
26	**XSAVE: XSAVE (and related) instruction support**. Value: 1. 1=Support provided for the XSAVE, XRSTOR, XSETBV, and XGETBV instructions and the XFEATURE_ENABLED_MASK register.
25	**AES: AES instruction support**. Value: Product-specific.
24	Reserved.
23	**POPCNT: POPCNT instruction**. Value: 1.
22	**MOVBE: MOVBE instruction support**. Value: 0.
21	**x2APIC: x2APIC capability**. Value: 0.
20	**SSE42: SSE4.2 instruction support**. Value: 1.
19	**SSE41: SSE4.1 instruction support**. Value: 1.
18	Reserved.
17	**PCID: process context identifiers support**. Value: 0.
16:14	Reserved.
13	**CMPXCHG16B: CMPXCHG16B instruction**. Value: 1.
12	**FMA: FMA instruction support**. Value: 1.
11:10	Reserved.
9	**SSSE3: supplemental SSE3 extensions**. Value: 1.
8:4	Reserved.
3	**Monitor: Monitor/Mwait instructions**. Value: ~MSRC001_0015[MonMwaitDis].
2	Reserved.
1	**PCLMULQDQ**: **PCLMULQDQ instruction support**. Value: Product-specific.
0	**SSE3: SSE3 extensions**. Value: 1.

CPUID Fn0000_0001_EDX Feature Identifiers

These values can be over-written by MSRC001_1004.

Bits	Description
31:29	Reserved.
28	**HTT: hyper-threading technology**. Value: CPUID Fn8000_0008_ECX[NC]!=0. 1=Multi core product (CPUID Fn8000_0008_ECX[NC] != 0). 0=Single core product (CPUID Fn8000_0008_ECX[NC]==0).
27	Reserved.
26	**SSE2: SSE2 extensions**. Value: 1.
25	**SSE: SSE extensions**. Value: 1.
24	**FXSR: FXSAVE and FXRSTOR instructions**. Value: 1.
23	**MMX: MMX™ instructions**. Value: 1.
22:20	Reserved.
19	**CLFSH: CLFLUSH instruction**. Value: 1.
18	Reserved.
17	**PSE36: page-size extensions**. Value: 1.
16	**PAT: page attribute table**. Value: 1.
15	**CMOV: conditional move instructions, CMOV, FCOMI, FCMOV**. Value: 1.
14	**MCA: machine check architecture, MCG_CAP**. Value: 1.
13	**PGE: page global extension, CR4.PGE**. Value: 1.
12	**MTRR: memory-type range registers**. Value: 1.
11	**SysEnterSysExit: SYSENTER and SYSEXIT instructions**. Value: 1.
10	Reserved.
9	**APIC: advanced programmable interrupt controller (APIC) exists and is enabled**. Value: MSR0000_001B[ApicEn].
8	**CMPXCHG8B: CMPXCHG8B instruction**. Value: 1.
7	**MCE: machine check exception, CR4.MCE**. Value: 1.
6	**PAE: physical-address extensions (PAE)**. Value: 1.
5	**MSR: AMD model-specific registers (MSRs), with RDMSR and WRMSR instructions**. Value: 1.
4	**TSC: time stamp counter, RDTSC/RDTSCP instructions, CR4.TSD**. Value: 1.
3	**PSE: page-size extensions (4 MB pages)**. Value: 1.
2	**DE: debugging extensions, IO breakpoints, CR4.DE**. Value: 1.
1	**VME: virtual-mode enhancements**. Value: 1.
0	**FPU: x87 floating point unit on-chip**. Value: 1.

CPUID Fn0000_000[4:2] Reserved

Bits	Description
31:0	Reserved.

CPUID Fn0000_0005_EAX Monitor/MWait

Bits	Description
31:16	Reserved.
15:0	**MonLineSizeMin: smallest monitor-line size in bytes**. Value: 40h.

CPUID Fn0000_0005_EBX Monitor/MWait

Bits	Description
31:16	Reserved.
15:0	**MonLineSizeMax: largest monitor-line size in bytes**. Value: 40h.

CPUID Fn0000_0005_ECX Monitor/MWait

Bits	Description
31:2	Reserved.
1	**IBE: interrupt break-event**. Value: 1.
0	**EMX: enumerate MONITOR/MWAIT extensions**. Value: 1.

CPUID Fn0000_0005_EDX Monitor/MWait

Bits	Description
31:0	Reserved.

CPUID Fn0000_0006_EAX Thermal and Power Management

Bits	Description
31:3	Reserved.
2	**ARAT: always running APIC timer**. Value: 0. 1=Indicates support for APIC timer always running feature.
1:0	Reserved.

CPUID Fn0000_0006_EBX Thermal and Power Management

Bits	Description
31:0	Reserved.

CPUID Fn0000_0006_ECX Thermal and Power Management

These values can be over-written by MSRC001_1003.

Bits	Description
31:1	Reserved.
0	**EffFreq: effective frequency interface**. Value: 1. 1=Indicates presence of MSR0000_00E7 [Max Performance Frequency Clock Count (MPERF)] and MSR0000_00E8 [Actual Performance Frequency Clock Count (APERF)].

CPUID Fn0000_0006_EDX Thermal and Power Management

Bits	Description
31:0	Reserved.

CPUID Fn0000_0007_EAX_x0 Structured Extended Feature Identifiers (ECX=0)

Bits	Description
31:0	Reserved.

CPUID Fn0000_0007_EBX_x0 Structured Extended Feature Identifiers (ECX=0)

Bits	Description
31:11	Reserved.
10	**INVPCID: invalidate processor context ID**. Value: 0.
9	Reserved.
8	**BMI2: bit manipulation group 2 instruction support**. Value: 0.
7	**SMEP: supervisor mode execution protection**. Value: 0.
6	Reserved.
5	**AVX2: AVX extension support**. Value: 0.
4	Reserved.
3	**BMI1: bit manipulation group 1 instruction support**. Value: 1.

2:1	Reserved.
0	**FSGSBASE: FS and GS base read write instruction support**. Value: 1.

CPUID Fn0000_0007_ECX_x0 Structured Extended Feature Identifiers (ECX=0)

Bits	Description
31:0	Reserved.

CPUID Fn0000_0007_EDX_x0 Structured Extended Feature Identifiers (ECX=0)

Bits	Description
31:0	Reserved.

CPUID Fn0000_000[A:8] Reserved

Bits	Description
31:0	Reserved.

CPUID Fn0000_000B Reserved

Bits	Description
31:0	Reserved.

CPUID Fn0000_000C Reserved

Bits	Description
31:0	Reserved.

CPUID Fn0000_000D_EAX_x0 Processor Extended State Enumeration (ECX=0)

Bits	Description
31:0	**XFeatureSupportedMask[31:0]**. Value: 0000_0007h.

CPUID Fn0000_000D_EBX_x0 Processor Extended State Enumeration (ECX=0)

Bits	Description
31:0	**XFeatureEnabledSizeMax**. Size in bytes of XSAVE/XRSTOR area for the currently enabled features in XCR0. Value: 512 + 64 + (IF (XCR0[AVX] | XCR0[LWP]) THEN 256. ELSE 0. ENDIF.) + (IF XCR0[LWP]) THEN 128. ELSE 0. ENDIF.). The components of this sum are described as follows: • 512: FPU/SSE save area (needed even if XCR0[SSE]=0). • 64: Header size (always needed). • Size of YMM area if YMM enabled. • Size of LWP area if LWP enabled.

CPUID Fn0000_000D_ECX_x0 Processor Extended State Enumeration (ECX=0)

Bits	Description
31:0	**XFeatureSupportedSizeMax**. Size in bytes of XSAVE/XRSTOR area for all features that the core supports. See XFeatureEnabledSizeMax. Value: 0000_03C0h.

CPUID Fn0000_000D_EDX_x0 Processor Extended State Enumeration (ECX=0)

Bits	Description
31:0	**XFeatureSupportedMask[63:32]**. Value: 4000_0000h.

CPUID Fn0000_000D_EAX_x1 Processor Extended State Enumeration (ECX=1)

Bits	Description
31:1	Reserved.
0	**XSAVEOPT: XSAVEOPT is available**. Value: 1.

CPUID Fn0000_000D_E[D,C,B]X_x1 Processor Extended State Enumeration (ECX=1)

Bits	Description
31:0	Reserved.

CPUID Fn0000_000D_EAX_x2 Processor Extended State Enumeration (ECX=2)

Bits	Description
31:0	**YmmSaveStateSize: YMM save state byte size**. Value: 0000_0100h.

CPUID Fn0000_000D_EBX_x2 Processor Extended State Enumeration (ECX=2)

Bits	Description
31:0	**YmmSaveStateOffset: YMM save state byte offset**. Value: 0000_0240h.

CPUID Fn0000_000D_ECX_x2 Processor Extended State Enumeration (ECX=2)

Bits	Description
31:0	Reserved.

CPUID Fn0000_000D_EDX_x2 Processor Extended State Enumeration (ECX=2)

Bits	Description
31:0	Reserved.

For CPUID Fn0000_000D, if ECX>2 and ECX<62 then EAX/EBX/ECX/EDX will return 0.

CPUID Fn0000_000D_EAX_x3E Processor Extended State Enumeration (ECX=62)

Bits	Description
31:0	**LwpSaveStateSize: LWP save state byte size**. Value: 0000_0080h.

CPUID Fn0000_000D_EBX_x3E Processor Extended State Enumeration (ECX=62)

Bits	Description
31:0	**LwpSaveStateOffset: LWP save state byte offset**. Value: 0000_0340h.

CPUID Fn0000_000D_ECX_x3E Processor Extended State Enumeration (ECX=62)

Bits	Description
31:0	Reserved.

CPUID Fn0000_000D_EDX_x3E Processor Extended State Enumeration (ECX=62)

Bits	Description
31:0	Reserved.

For CPUID Fn0000_000D, if ECX>62 then EAX/EBX/ECX/EDX will return 0.

CPUID Fn8000_0000_EAX Largest Extended Function Number

Bits	Description
31:0	**LFuncExt: largest extended function**. Value: 8000_001Eh. The largest CPUID extended function input value supported by the processor implementation.

CPUID Fn8000_0000_E[D,C,B]X Processor Vendor

CPUID Fn0000_0000_E[D,C,B]X and CPUID Fn8000_0000_E[D,C,B]X return the same value.

Table 214: CPUID Fn8000_0000_E[B,C,D]X Value

Register	Value	Description
CPUID Fn8000_0000_EBX	6874_7541h	The ASCII characters “h t u A”.
CPUID Fn8000_0000_ECX	444D_4163h	The ASCII characters “D M A c”.
CPUID Fn8000_0000_EDX	6974_6E65h	The ASCII characters “i t n e”.

Bits	Description
31:0	**Vendor**. The 12 8-bit ASCII character codes to create the string “AuthenticAMD”.

CPUID Fn8000_0001_EAX Family, Model, Stepping Identifiers

Also see CPUID Fn0000_0001_EAX [Family, Model, Stepping Identifiers].

Bits	Description
31:28	Reserved.
27:20	**ExtFamily: extended family**. CPUID Fn8000_0001_EAX[ExtFamily] is an alias of D18F3xFC[ExtFamily].
19:16	**ExtModel: extended model**. CPUID Fn8000_0001_EAX[ExtModel] is an alias of D18F3xFC[ExtModel].
15:12	Reserved.
11:8	**BaseFamily**. CPUID Fn8000_0001_EAX[BaseFamily] is an alias of D18F3xFC[BaseFamily].
7:4	**BaseModel**. CPUID Fn8000_0001_EAX[BaseModel] is an alias of D18F3xFC[BaseModel].
3:0	**Stepping**. CPUID Fn8000_0001_EAX[Stepping] is an alias of D18F3xFC[Stepping].

CPUID Fn8000_0001_EBX BrandId Identifier

Bits	Description
31:28	**PkgType: package type**. Specifies the package type. Value: Product-specific. Bits — Description 0h — FP3 (BGA) 1h — FM2r2 (uPGA) Fh-2h — Reserved.
27:0	Reserved.

CPUID Fn8000_0001_ECX Feature Identifiers

These values can be over-written by MSRC001_1005.

Bits	Description
31:29	Reserved.
28	**PerfCtrExtL2I: L2I performance counter extensions support**. Value: 0. Indicates support for MSRC001_023[6,4,2,0] and MSRC001_023[7,5,3,1].
27	**PerfTsc: performance time-stamp counter supported**. Value: 1. Indicates support for MSRC001_0280 [Performance Time Stamp Counter (CU_PTSC)].
26	**DataBreakpointExtension**. Value: 1. Indicates data breakpoint support for MSRC001_1027 and MSRC001_101[B:9].
25	Reserved.
24	**PerfCtrExtNB: NB performance counter extensions support.** Value: 1. Indicates support for MSRC001_024[6,4,2,0] and MSRC001_024[7,5,3,1].
23	**PerfCtrExtCore: core performance counter extensions support**. Value: 1. Indicates support for MSRC001_020[A,8,6,4,2,0] and MSRC001_020[B,9,7,5,3,1].
22	**TopologyExtensions: topology extensions support**. Value: 1. Indicates support for CPUID Fn8000_001D_EAX_x0-CPUID Fn8000_001E_EDX.
21	**TBM: trailing bit manipulation instruction support**. Value: 1.
20	Reserved.
19	Reserved.
18	Reserved.
17	**TCE: translation cache extension**. Value: 1.

16	**FMA4: 4-operand FMA instruction support**. Value: 1.
15	**LWP: lightweight profiling support**. Value: 1.
14	Reserved.
13	**WDT: watchdog timer support**. Value: 1.
12	**SKINIT: SKINIT and STGI support**. Value: 1.
11	**XOP: extended operation support**. Value: 1.
10	**IBS: Instruction Based Sampling**. Value: 1.
9	**OSVW: OS Visible Work-around support**. Value: 1.
8	**3DNowPrefetch: Prefetch and PrefetchW instructions**. Value: 1.
7	**MisAlignSse: Misaligned SSE Mode.** Value: 1.
6	**SSE4A: EXTRQ, INSERTQ, MOVNTSS, and MOVNTSD instruction support.** Value: 1.
5	**ABM: advanced bit manipulation**. Value: 1. LZCNT instruction support.
4	**AltMovCr8: LOCK MOV CR0 means MOV CR8**. Value: 1.
3	**ExtApicSpace: extended APIC register space**. Value: 1.
2	**SVM: Secure Virtual Mode feature**. Value: Product-specific. Indicates support for: VMRUN, VMLOAD, VMSAVE, CLGI, VMMCALL, and INVLPGA.
1	**CmpLegacy: core multi-processing legacy mode**. Value: Product-specific. 1=Multi core product (CPUID Fn8000_0008_ECX[NC] != 0). 0=Single core product (CPUID Fn8000_0008_ECX[NC] == 0).
0	**LahfSahf: LAHF/SAHF instructions**. Value: 1.

CPUID Fn8000_0001_EDX Feature Identifiers

These values can be over-written by MSRC001_1005.

Bits	Description
31	**3DNow: 3DNow!™ instructions**. Value: 0.
30	**3DNowExt: AMD extensions to 3DNow!™ instructions**. Value: 0.
29	**LM: long mode**. Value: 1.
28	Reserved.
27	**RDTSCP: RDTSCP instruction**. Value: 1.
26	**Page1GB: one GB large page support**. Value: 1.
25	**FFXSR: FXSAVE and FXRSTOR instruction optimizations**. Value: 1.
24	**FXSR: FXSAVE and FXRSTOR instructions**. Value: 1.

23	**MMX: MMX™ instructions**. Value: 1.
22	**MmxExt: AMD extensions to MMX instructions**. Value: 1.
21	Reserved.
20	**NX: no-execute page protection**. Value: 1.
19:18	Reserved.
17	**PSE36: page-size extensions**. Value: 1.
16	**PAT: page attribute table**. Value: 1.
15	**CMOV: conditional move instructions, CMOV, FCOMI, FCMOV**. Value: 1.
14	**MCA: machine check architecture, MCG_CAP**. Value: 1.
13	**PGE: page global extension, CR4.PGE**. Value: 1.
12	**MTRR: memory-type range registers**. Value: 1.
11	**SysCallSysRet: SYSCALL and SYSRET instructions**. Value: 1.
10	Reserved.
9	**APIC: advanced programmable interrupt controller (APIC) exists and is enabled**. Value: MSR0000_001B[ApicEn].
8	**CMPXCHG8B: CMPXCHG8B instruction**. Value: 1.
7	**MCE: machine check exception, CR4.MCE**. Value: 1.
6	**PAE: physical-address extensions (PAE)**. Value: 1.
5	**MSR: model-specific registers (MSRs), with RDMSR and WRMSR instructions**. Value: 1.
4	**TSC: time stamp counter, RDTSC/RDTSCP instructions, CR4.TSD**. Value:1.
3	**PSE: page-size extensions (4 MB pages)**. Value: 1.
2	**DE: debugging extensions, IO breakpoints, CR4.DE**. Value: 1.
1	**VME: virtual-mode enhancements**. Value: 1.
0	**FPU: x87 floating point unit on-chip**. Value: 1.

CPUID Fn8000_000[4:2]_E[D,C,B,A]X Processor Name String Identifier

Table 215: Valid Values for CPUID Fn8000_000[4:2]_E[D,C,B,A]X

Register	Value
CPUID Fn8000_0002_EAX	MSRC001_0030[31:0]
CPUID Fn8000_0002_EBX	MSRC001_0030[63:32]
CPUID Fn8000_0002_ECX	MSRC001_0031[31:0]
CPUID Fn8000_0002_EDX	MSRC001_0031[63:32]
CPUID Fn8000_0003_EAX	MSRC001_0032[31:0]
CPUID Fn8000_0003_EBX	MSRC001_0032[63:32]
CPUID Fn8000_0003_ECX	MSRC001_0033[31:0]
CPUID Fn8000_0003_EDX	MSRC001_0033[63:32]
CPUID Fn8000_0004_EAX	MSRC001_0034[31:0]

Table 215: Valid Values for CPUID Fn8000_000[4:2]_E[D,C,B,A]X

CPUID Fn8000_0004_EBX	MSRC001_0034[63:32]
CPUID Fn8000_0004_ECX	MSRC001_0035[31:0]
CPUID Fn8000_0004_EDX	MSRC001_0035[63:32]

Bits	Description
31:0	**ProcName: processor name**. These return the ASCII string corresponding to the processor name, stored in MSRC001_00[35:30] [Processor Name String].

CPUID Fn8000_0005_EAX L1 TLB 2M/4M Identifiers

This function provides the processor's first level cache and TLB characteristics for each core.

Bits	Description
31:24	**L1DTlb2and4MAssoc: data TLB associativity for 2 MB and 4 MB pages**. Value: FFh. See: CPUID Fn8000_0005_ECX[L1DcAssoc].
23:16	**L1DTlb2and4MSize: data TLB number of entries for 2 MB and 4 MB pages**. Value: 64. The value returned is for the number of entries available for the 2 MB page size; 4 MB pages require two 2 MB entries, so the number of entries available for the 4 MB page size is one-half the returned value.
15:8	**L1ITlb2and4MAssoc: instruction TLB associativity for 2 MB and 4 MB pages**. Value: FFh. See: CPUID Fn8000_0005_ECX[L1DcAssoc].
7:0	**L1ITlb2and4MSize: instruction TLB number of entries for 2 MB and 4 MB pages**. Value: 24. The value returned is for the number of entries available for the 2 MB page size; 4 MB pages require two 2 MB entries, so the number of entries available for the 4 MB page size is one-half the returned value.

CPUID Fn8000_0005_EBX L1 TLB 4K Identifiers

See: CPUID Fn8000_0005_EAX.

Bits	Description
31:24	**L1DTlb4KAssoc: data TLB associativity for 4 KB pages**. Value: FFh. See: CPUID Fn8000_0005_ECX[L1DcAssoc].
23:16	**L1DTlb4KSize: data TLB number of entries for 4 KB pages**. Value: 64.
15:8	**L1ITlb4KAssoc: instruction TLB associativity for 4 KB pages**. Value: FFh. ITLB associativity for 4 KB pages is reported by CPUID Fn8000_0006_EBX[L2ITlb4KAssoc].
7:0	**L1ITlb4KSize: instruction TLB number of entries for 4 KB pages**. Value: 48. ITLB size for 4 KB pages is reported by CPUID Fn8000_0006_EBX[L2ITlb4KSize].

CPUID Fn8000_0005_ECX L1 Data Cache Identifiers

This function provides first level cache characteristics for each core.

Bits	Description
31:24	**L1DcSize: L1 data cache size in KB**. Value: 16.
23:16	**L1DcAssoc: L1 data cache associativity**. Value: 4. Bits / Description 00h: Reserved 01h: 1 way (direct mapped) 02h: 2 way 03h: 3 way FEh-04h: [L1IcAssoc] way FFh: Fully associative
15:8	**L1DcLinesPerTag: L1 data cache lines per tag**. Value: 1.
7:0	**L1DcLineSize: L1 data cache line size in bytes**. Value: 64.

CPUID Fn8000_0005_EDX L1 Instruction Cache Identifiers

This function provides first level cache characteristics for each core.

Bits	Description
31:24	**L1IcSize: L1 instruction cache size KB**. Value: 96.
23:16	**L1IcAssoc: L1 instruction cache associativity**. Value: 3. See: CPUID Fn8000_0005_ECX[L1DcAssoc].
15:8	**L1IcLinesPerTag: L1 instruction cache lines per tag**. Value: 1.
7:0	**L1IcLineSize: L1 instruction cache line size in bytes**. Value: 64.

CPUID Fn8000_0006_EAX L2 TLB 2M/4M Identifiers

This function provides the processor's second level cache and TLB characteristics for each core.

Bits	Description
31:28	**L2DTlb2and4MAssoc: L2 data TLB associativity for 2 MB and 4 MB pages**. Value: 6. See: CPUID Fn8000_0006_ECX[L2Assoc].
27:16	**L2DTlb2and4MSize: L2 data TLB number of entries for 2 MB and 4 MB pages**. Value: 1024. The value returned is for the number of entries available for the 2 MB page size; 4 MB pages require two 2 MB entries, so the number of entries available for the 4 MB page size is one-half the returned value.

15:12	**L2ITlb2and4MAssoc: L2 instruction TLB associativity for 2 MB and 4 MB pages**. Value: 6. See: CPUID Fn8000_0006_ECX[L2Assoc].
11:0	**L2ITlb2and4MSize: L2 instruction TLB number of entries for 2 MB and 4 MB pages**. Value: 1024. The value returned is for the number of entries available for the 2 MB page size; 4 MB pages require two 2 MB entries, so the number of entries available for the 4 MB page size is one-half the returned value.

CPUID Fn8000_0006_EBX L2 TLB 4K Identifiers

This function provides second level TLB characteristics for 4K pages shared by each core on a Compute Unit.

Bits	Description
31:28	**L2DTlb4KAssoc: L2 data TLB associativity for 4 KB pages**. Value: 6. See: CPUID Fn8000_0006_ECX[L2Assoc].
27:16	**L2DTlb4KSize: L2 data TLB number of entries for 4 KB pages**. Value: 1024.
15:12	**L2ITlb4KAssoc: L2 instruction TLB associativity for 4 KB pages**. Value: 4. See: CPUID Fn8000_0006_ECX[L2Assoc].
11:0	**L2ITlb4KSize: L2 instruction TLB number of entries for 4 KB pages**. Value: 512.

CPUID Fn8000_0006_ECX L2 Cache Identifiers

Bits	Description
31:16	**L2Size: L2 cache size in KB**. Value: Product-specific. Bits: Description 03FFh-0000h: Reserved 0400h: 1 MB 07FFh-0401h: Reserved 0800h: 2 MB FFFFh-0801h: Reserved
15:12	**L2Assoc: L2 cache associativity**. Value: 8. 0h: Disabled 1h: 1 way (direct mapped) 2h: 2 ways 3h: Reserved 4h: 4 ways 5h: Reserved 6h: 8 ways 7h: Reserved 8h: 16 ways 9h: Reserved Ah: 32 ways Bh: 48 ways Ch: 64 ways Dh: 96 ways Eh: 128 ways Fh: Fully associative

11:8	**L2LinesPerTag: L2 cache lines per tag**. Value: 1.
7:0	**L2LineSize: L2 cache line size in bytes**. Value: 64.

CPUID Fn8000_0006_EDX L3 Cache Identifiers

This function provides third level cache characteristics shared by all cores.

Bits	Description
31:18	**L3Size: L3 cache size**. Value: 0.
17:16	Reserved.
15:12	**L3Assoc: L3 cache associativity**. Value: 0.
11:8	**L3LinesPerTag: L3 cache lines per tag**. Value: 0.
7:0	**L3LineSize: L3 cache line size in bytes**. Value: 0.

CPUID Fn8000_0007_EAX Processor Feedback Capabilities

Bits	Description
31:16	**MaxWrapTime**. Value: 0000h. Specifies the maximum time between reads that software should use to avoid two wraps. A read of at least once every MaxWrapTime seconds will result in either zero or one wrap during that interval.
15:8	**Version**. Value: 00h. Specifies the processor feedback capabilities version.
7:0	**NumberOfMonitors**. Value: 00h. Specifies the number of processor feedback MSR pairs supported. Valid if (CPUID Fn8000_0007_EDX[ProcFeedbackInterface]==1).

CPUID Fn8000_0007_EBX RAS Capabilities

Bits	Description
31:3	Reserved.
2	**HWA: hardware assert supported**. 1=Indicates support for MSRC001_10[DF:C0]. Value: 0.
1	**SUCCOR: Software uncorrectable error containment and recovery capability**. Value: 0.
0	**McaOverflowRecov: MCA overflow recovery support**. Value: 1. 1=MCA overflow conditions (MCi_STATUS[Overflow]=1) are not fatal; software may safely ignore such conditions. 0=MCA overflow conditions require software to shut down the system. See 2.15.1.6 [Handling Machine Check Exceptions].

CPUID Fn8000_0007_ECX Advanced Power Management Information

Bits	Description
31:0	Reserved.

CPUID Fn8000_0007_EDX Advanced Power Management Information

This function provides advanced power management feature identifiers.

Bits	Description
31:13	Reserved.
12	Reserved.
11	**ProcFeedbackInterface: processor feedback interface**. Value: 0. 1=Indicates support for processor feedback interface; CPUID Fn8000_0007_EAX.
10	**EffFreqRO: read-only effective frequency interface**. Value: 1. 1=Indicates presence of MSRC000_00E7 [Read-Only Max Performance Frequency Clock Count (MPerfReadOnly)] and MSRC000_00E8 [Read-Only Actual Performance Frequency Clock Count (APerfReadOnly)].
9	**CPB: core performance boost**. Value: Product-specific. 1=Indicates presence of MSRC001_0015[CpbDis] and support for core performance boost. See 2.5.9 [Application Power Management (APM)].
8	**TscInvariant: TSC invariant**. Value: 1. The TSC rate is invariant.
7	**HwPstate: hardware P-state control**. Value: 1. MSRC001_0061 [P-state Current Limit], MSRC001_0062 [P-state Control] and MSRC001_0063 [P-state Status] exist.
6	**100MHzSteps: 100 MHz multiplier Control**. Value: 1.
5	Reserved.
4	**TM: hardware thermal control (HTC)**. Value: Product-specific.
3	**TTP: THERMTRIP**. Value: 1.
2	**VID: Voltage ID control**. Value: 0. Function replaced by HwPstate.
1	**FID: Frequency ID control**. Value: 0. Function replaced by HwPstate.
0	**TS: Temperature sensor**. Value: 1.

CPUID Fn8000_0008_EAX Long Mode Address Size Identifiers

This provides information about the maximum physical and linear address width supported by the processor.

Bits	Description
31:24	Reserved.
23:16	**GuestPhysAddrSize: maximum guest physical byte address size in bits**. Value: 0. 0=The maximum guest physical address size defined by PhysAddrSize.

15:8	**LinAddrSize: Maximum linear byte address size in bits**. Value: IF (CPUID Fn8000_0001_EDX[LM]) THEN 30h. ELSE 20h. ENDIF.
7:0	**PhysAddrSize: Maximum physical byte address size in bits**. Value: 30h.

CPUID Fn8000_0008_EBX Reserved

Bits	Description
31:0	Reserved.

CPUID Fn8000_0008_ECX Size Identifiers

This provides information about the number of cores supported by the processor.

Bits	Description
31:18	Reserved.
17:16	**PerfTscSize: performance time-stamp counter size**. Value: 00b. Indicates the size of MSRC001_0280[PTSC]. Valid only when (CPUID Fn8000_0001_ECX[PerfTsc]==1). Bits — Description 00b — 40 bits 01b — 48 bits 10b — 56 bits 11b — 64 bits
15:12	**ApicIdCoreIdSize: APIC ID size**. Value: 4h. The number of bits in the initial APIC20[ApicId] value that indicate core ID within a processor.
11:8	Reserved.
7:0	**NC: number of cores - 1**. Value: D18F5x84[CmpCap]-COUNT(D18F3x190[DisCore]). The number of cores in the processor is NC+1 (e.g., if NC=0, then there is one core). See 2.4.4 [Processor Cores and Downcoring].

CPUID Fn8000_0008_EDX Reserved

Bits	Description
31:0	Reserved.

CPUID Fn8000_0009 Reserved

Bits	Description
31:0	Reserved.

CPUID Fn8000_000A_EAX SVM Revision and Feature Identification

This provides SVM revision. If (CPUID Fn8000_0001_ECX[SVM]==0) then CPUID Fn8000_000A_EAX is

reserved.

Bits	Description
31:8	Reserved.
7:0	**SvmRev: SVM revision**. Value: 01h.

CPUID Fn8000_000A_EBX SVM Revision and Feature Identification

This provides SVM revision and feature information. If (CPUID Fn8000_0001_ECX[SVM]==0) then CPUID Fn8000_000A_EBX is reserved.

Bits	Description
31:0	**NASID: number of address space identifiers (ASID)**. Value: 10000h.

CPUID Fn8000_000A_ECX SVM Revision and Feature Identification

Bits	Description
31:0	Reserved.

CPUID Fn8000_000A_EDX SVM Revision and Feature Identification

This provides SVM feature information. If (CPUID Fn8000_0001_ECX[SVM]==0) then CPUID Fn8000_000A_EDX is reserved.

Bits	Description
31:14	Reserved.
13	Reserved.
12	**PauseFilterThreshold: PAUSE filter threshold**. Value: 1.
11	Reserved.
10	**PauseFilter: pause intercept filter**. Value: 1.
9:8	Reserved.
7	**DecodeAssists: decode assists**. Value: 1.
6	**FlushByAsid: flush by ASID**. Value: 1.
5	**VmcbClean: VMCB clean bits**. Value: 1.
4	**TscRateMsr: MSR based TSC rate control**. Value: 1. 1=Indicates support for TSC ratio MSRC000_0104.
3	**NRIPS: NRIP Save**. Value: 1.
2	**SVML: SVM lock**. Value: 1.

1	**LbrVirt: LBR virtualization**. Value: 1.
0	**NP: nested paging**. Value: 1.

CPUID Fn8000_00[18:0B] Reserved

Bits	Description
31:0	Reserved.

CPUID Fn8000_0019_EAX L1 TLB 1G Identifiers

This function provides first level TLB characteristics for 1G pages shared by each core on a Compute Unit.

Bits	Description
31:28	**L1DTlb1GAssoc: L1 data TLB associativity for 1 GB pages**. See: CPUID Fn8000_0006_ECX[L2Assoc]. Value: Fh.
27:16	**L1DTlb1GSize: L1 data TLB number of entries for 1 GB pages**. Value: 64.
15:12	**L1ITlb1GAssoc: L1 instruction TLB associativity for 1 GB pages**. See: CPUID Fn8000_0006_ECX[L2Assoc]. Value: Fh.
11:0	**L1ITlb1GSize: L1 instruction TLB number of entries for 1 GB pages**. Value: 24.

CPUID Fn8000_0019_EBX L2 TLB 1G Identifiers

This provides 1 GB paging information. The *associativity* fields are defined by CPUID Fn8000_0006_EAX, CPUID Fn8000_0006_EBX, CPUID Fn8000_0006_ECX and CPUID Fn8000_0006_EDX.

Bits	Description
31:28	**L2DTlb1GAssoc: L2 data TLB associativity for 1 GB pages**. See: CPUID Fn8000_0006_ECX[L2Assoc]. Value: 6.
27:16	**L2DTlb1GSize: L2 data TLB number of entries for 1 GB pages**. Value: 1024.

15:12	**L2ITlb1GAssoc: L2 instruction TLB associativity for 1 GB pages**. See: CPUID Fn8000_0006_ECX[L2Assoc]. Value: 6.
11:0	**L2ITlb1GSize: L2 instruction TLB number of entries for 1 GB pages**. Value: 1024.

CPUID Fn8000_0019_E[D,C]X Reserved

Bits	Description
31:0	Reserved.

CPUID Fn8000_001A_EAX Performance Optimization Identifiers

This function returns performance related information. For more details on how to use these bits to optimize software, see the optimization guide.

Bits	Description
31:3	Reserved.
2	**FP256**. Value: 0.
1	**MOVU**. Value: 1.
0	**FP128**. Value: 1.

CPUID Fn8000_001A_E[D,C,B]X Reserved

Bits	Description
31:0	Reserved.

CPUID Fn8000_001B_EAX Instruction Based Sampling Identifiers

This function returns IBS feature information.

Bits	Description
31:11	Reserved.
10	**IbsOpData4: IBS op data 4 MSR supported**. Value: 0.
9	**IbsFetchCtlExtd: IBS fetch control extended MSR supported**. Value: 0. 1=Indicates support for MSRC001_103C [IBS Fetch Control Extended (IC_IBS_EXTD_CTL)].

8	**OpBrnFuse: fused branch micro-op indication supported**. Value: 1. 1=Indicates support for MSRC001_1035[IbsOpBrnFuse].
7	**RipInvalidChk: invalid RIP indication supported**. Value: 1. 1=Indicates support for MSRC001_1035[IbsRipInvalid].
6	**OpCntExt: IbsOpCurCnt and IbsOpMaxCnt extend by 7 bits**. Value: 1. 1=Indicates support for MSRC001_1033[IbsOpCurCnt[26:20], IbsOpMaxCnt[26:20]].
5	**BrnTrgt: branch target address reporting supported**. Value: 1.
4	**OpCnt: op counting mode supported**. Value: 1.
3	**RdWrOpCnt: read write of op counter supported**. Value: 1.
2	**OpSam: IBS execution sampling supported**. Value: 1.
1	**FetchSam: IBS fetch sampling supported**. Value: 1.
0	**IBSFFV: IBS feature flags valid**. Value: 1.

CPUID Fn8000_001B_E[D,C,B]X Instruction Based Sampling Identifiers

Bits	Description
31:0	Reserved.

CPUID Fn8000_001C_EAX Lightweight Profiling Capabilities 0

This function returns IBS feature information; see the Lightweight Profiling Specification section titled "Detecting LWP". If (CPUID Fn8000_0001_ECX[LWP]==0) then CPUID Fn8000_001C_E[D,C,B,A]X is reserved.

Bits	Description
31	**LwpInt: interrupt on threshold overflow available**. Value: MSRC000_0105[LwpInt]. 1=Interrupt on threshold overflow is available.
30	**LwpPTSC: performance time stamp counter in event record is available**. Value: MSRC000_0105[LwpPTSC]. 1=Performance time stamp counter in event record is available.
29	**LwpCont: sampling in continuous mode is available**. Value: MSRC000_0105[LwpCont]. 1=Sampling in continuous mode is available.
28:7	Reserved.
6	**LwpRNH: core reference clocks not halted event available**. Value: MSRC000_0105[LwpRNH]. 1=Core reference clocks not halted event is available.
5	**LwpCNH: core clocks not halted event available**. Value: MSRC000_0105[LwpCNH]. 1=Core clocks not halted event is available.
4	**LwpDME: DC miss event available**. Value: MSRC000_0105[LwpDME]. 1=DC miss event is available.
3	**LwpBRE: branch retired event available**. Value: MSRC000_0105[LwpBRE]. 1=Branch retired event is available.
2	**LwpIRE: instructions retired event available**. Value: MSRC000_0105[LwpIRE]. 1=Instructions retired event is available.

1	**LwpVAL: LWPVAL instruction available**. Value: MSRC000_0105[LwpVAL]. 1=LWPVAL instruction is available.
0	**LwpAvail: LWP available**. Value: XCR0[62]. 1=LWP is available.

CPUID Fn8000_001C_EBX Lightweight Profiling Capabilities 0

See CPUID Fn8000_001C_EAX.

Bits	Description
31:24	**LwpEventOffset: offset to the EventInterval1 field**. Value: 80h. Offset from the start of the LWPCB to the EventInterval1 field.
23:16	**LwpMaxEvents: maximum EventId**. Value: 3. Maximum EventId value that is supported.
15:8	**LwpEventSize: event record size**. Value: 20h. Size in bytes of an event record in the LWP event ring buffer.
7:0	**LwpCbSize: control block size**. Value: 13h. Size in quadwords of the LWPCB.

CPUID Fn8000_001C_ECX Lightweight Profiling Capabilities 0

See CPUID Fn8000_001C_EAX.

Bits	Description
31	**LwpCacheLatency: cache latency filtering supported**. Value: 0. 1=Cache-related events can be filtered by latency.
30	**LwpCacheLevels: cache level filtering supported**. Value: 0. 1=Cache-related events can be filtered by the cache level that returned the data.
29	**LwpIpFiltering: IP filtering supported**. Value: 0. 1=IP filtering is supported.
28	**LwpBranchPrediction: branch prediction filtering supported**. Value: 0. 1=Branches Retired events can be filtered based on whether the branch was predicted properly.
27:24	Reserved.
23:16	**LwpMinBufferSize: event ring buffer size**. Value: 01h. Minimum size of the LWP event ring buffer, in units of 32 event records.
15:9	**LwpVersion: version**. Value: 000_0001b. Version of LWP implementation.
8:6	**LwpLatencyRnd: amount cache latency is rounded**. Value: 0. The amount by which cache latency is rounded.
5	**LwpDataAddress: data cache miss address valid**. Value: 0. 1=Address is valid for cache miss event records.
4:0	**LwpLatencyMax: latency counter bit size**. Value: 0. Size in bits of the cache latency counters.

CPUID Fn8000_001C_EDX Lightweight Profiling Capabilities 0

See CPUID Fn8000_001C_EAX.

Bits	Description
31	**LwpInt: interrupt on threshold overflow supported**. Value: 1. 1=Interrupt on threshold overflow is supported.

30	**LwpPTSC: performance time stamp counter in event record is available**. Value: 1. 1=Performance time stamp counter in event record is supported.
29	**LwpCont: sampling in continuous mode is available**. Value: 1. 1=Sampling in continuous mode is supported.
28:7	Reserved.
6	**LwpRNH: core reference clocks not halted event supported**. Value: 0. 1=Core reference clocks not halted event is supported.
5	**LwpCNH: core clocks not halted event supported**. Value: 0. 1=Core clocks not halted event is supported.
4	**LwpDME: DC miss event supported**. Value: 0. 1=DC miss event is supported.
3	**LwpBRE: branch retired event supported**. Value: 1. 1=Branch retired event is supported.
2	**LwpIRE: instructions retired event supported**. Value: 1. 1=Instructions retired event is supported.
1	**LwpVAL: LWPVAL instruction supported**. Value: 1. 1=LWPVAL instruction is supported.
0	**LwpAvail: lightweight profiling supported**. Value: 1. 1=Lightweight profiling is supported.

CPUID Fn8000_001D_EAX_x0 Cache Properties

CPUID Fn8000_001D_EAX_x0 reports topology information for the DC.
If (CPUID Fn8000_0001_ECX[TopologyExtensions]==0) then CPUID Fn8000_001D_E[D,C,B,A]X is reserved.

Table 216: ECX mapping to Cache Type for CPUID Fn8000_001D_E[D,C,B,A]X

ECX	Cache Type
0	DC
1	IC
2	L2
3	Null

Bits	Description
31:26	Reserved.
25:14	**NumSharingCache: number of cores sharing cache**. Value: 000h. The number of cores sharing this cache is NumSharingCache+1.
13:10	Reserved.
9	**FullyAssociative: fully associative cache**. Value: 0. 1=Cache is fully associative.
8	**SelfInitialization: cache is self-initializing**. Value: 1. 1=Cache is self initializing; cache does not need software initialization.

7:5	**CacheLevel: cache level.** Identifies the cache level. Value: 001b. Bits — Description 000b — Reserved 001b — Level 1 010b — Level 2 011b — Level 3 111b-100b — Reserved
4:0	**CacheType: cache type**. Identifies the type of cache. Value: 01h. Bits — Description 00h — Null; no more caches 01h — Data cache 02h — Instruction cache 03h — Unified cache 1Fh-04h — Reserved

CPUID Fn8000_001D_EAX_x1 Cache Properties

CPUID Fn8000_001D_EAX_x1 reports topology information for the IC. See CPUID Fn8000_001D_EAX_x0.

Bits	Description
31:26	Reserved.
25:14	**NumSharingCache: number of cores sharing cache**. See: CPUID Fn8000_001D_EAX_x0[NumSharingCache]. Value: IF (DualCoreEnabled==1) THEN 001h. ELSE 000h. ENDIF.
13:10	Reserved.
9	**FullyAssociative: fully associative cache**. Value: 0. See: CPUID Fn8000_001D_EAX_x0[FullyAssociative].
8	**SelfInitialization: cache is self-initializing**. Value: 1. See: CPUID Fn8000_001D_EAX_x0[SelfInitialization].
7:5	**CacheLevel: cache level**. Identifies the cache level. Value: 001b. See: CPUID Fn8000_001D_EAX_x0[CacheLevel].
4:0	**CacheType: cache type**. Value: 02h. See: CPUID Fn8000_001D_EAX_x0[CacheType].

CPUID Fn8000_001D_EAX_x2 Cache Properties

CPUID Fn8000_001D_EAX_x2 reports topology information for the L2. See CPUID Fn8000_001D_EAX_x0.

Bits	Description
31:26	Reserved.
25:14	**NumSharingCache: number of cores sharing cache**. See: CPUID Fn8000_001D_EAX_x0[NumSharingCache]. Value: IF (DualCoreEnabled==1) THEN 001h. ELSE 000h. ENDIF.
13:10	Reserved.
9	**FullyAssociative: fully associative cache**. Value: 0. See: CPUID Fn8000_001D_EAX_x0[FullyAssociative].

8	**SelfInitialization: cache is self-initializing**. Value: 1. See: CPUID Fn8000_001D_EAX_x0[SelfInitialization].
7:5	**CacheLevel: cache level.** Identifies the cache level. Value: 010b. See: CPUID Fn8000_001D_EAX_x0[CacheLevel].
4:0	**CacheType: cache type**. Value: 03h. See: CPUID Fn8000_001D_EAX_x0[CacheType].

CPUID Fn8000_001D_EAX_x3 Cache Properties

CPUID Fn8000_001D_EAX_x3 reports done/null. See CPUID Fn8000_001D_EAX_x0.

Bits	Description
31:5	Reserved.
4:0	**CacheType: cache type**. Value: 00h. See: CPUID Fn8000_001D_EAX_x0[CacheType].

CPUID Fn8000_001D_EBX_x0 Cache Properties

CPUID Fn8000_001D_EBX_x0 reports topology information for the DC. See CPUID Fn8000_001D_EAX_x0.

Bits	Description
31:22	**CacheNumWays: cache number of ways**. Cache number of ways is CacheNumWays+1. Value: 003h.
21:12	**CachePhysPartitions: cache physical line partitions**. Value: 000h. Cache partitions is CachePhysPartitions+1.
11:0	**CacheLineSize: cache line size in bytes**. Value: 03Fh. Cache line size in bytes is CacheLineSize+1.

CPUID Fn8000_001D_EBX_x1 Cache Properties

CPUID Fn8000_001D_EBX_x1 reports topology information for the IC. See CPUID Fn8000_001D_EAX_x0.

Bits	Description
31:22	**CacheNumWays: cache number of ways**. See: CPUID Fn8000_001D_EBX_x0[CacheNumWays]. Value: 002h.
21:12	**CachePhysPartitions: cache physical line partitions**. Value: 000h. See: CPUID Fn8000_001D_EBX_x0[CachePhysPartitions].
11:0	**CacheLineSize: cache line size in bytes**. Value: 03Fh. See: CPUID Fn8000_001D_EBX_x0[CacheLineSize].

CPUID Fn8000_001D_EBX_x2 Cache Properties

CPUID Fn8000_001D_EBX_x2 reports topology information for the L2. See CPUID Fn8000_001D_EAX_x0.

Bits	Description
31:22	**CacheNumWays: cache number of ways**. Value: 00Fh. See: CPUID Fn8000_001D_EBX_x0[CacheNumWays].
21:12	**CachePhysPartitions: cache physical line partitions**. Value: 000h. See: CPUID Fn8000_001D_EBX_x0[CachePhysPartitions].
11:0	**CacheLineSize: cache line size in bytes**. Value: 03Fh. See: CPUID Fn8000_001D_EBX_x0[CacheLineSize].

CPUID Fn8000_001D_EBX_x3 Cache Properties

CPUID Fn8000_001D_EAX_x3 reports done/null. See CPUID Fn8000_001D_EAX_x0.

Bits	Description
31:22	**CacheNumWays: cache number of ways**. Value: 0. See: CPUID Fn8000_001D_EBX_x0[CacheNumWays].
21:12	**CachePhysPartitions: cache physical line partitions**. Value: 000h. See: CPUID Fn8000_001D_EBX_x0[CachePhysPartitions].
11:0	**CacheLineSize: cache line size in bytes**. Value: 0. See: CPUID Fn8000_001D_EBX_x0[CacheLineSize].

CPUID Fn8000_001D_ECX_x0 Cache Properties

CPUID Fn8000_001D_ECX_x0 reports topology information for the DC. See CPUID Fn8000_001D_EAX_x0.

Bits	Description
31:0	**CacheNumSets: cache number of sets**. Cache number of sets is CacheNumSets+1. Value: 0000_003Fh.

CPUID Fn8000_001D_ECX_x1 Cache Properties

CPUID Fn8000_001D_ECX_x1 reports topology information for the IC. See CPUID Fn8000_001D_EAX_x0.

Bits	Description
31:0	**CacheNumSets: cache number of sets**. See: CPUID Fn8000_001D_ECX_x0[CacheNumSets]. Value: 0000_01FFh.

CPUID Fn8000_001D_ECX_x2 Cache Properties

CPUID Fn8000_001D_ECX_x2 reports topology information for the L2. See CPUID Fn8000_001D_EAX_x0.

Bits	Description
31:0	**CacheNumSets: cache number of sets**. Value: Product-specific. See: CPUID Fn8000_001D_ECX_x0[CacheNumSets].

CPUID Fn8000_001D_ECX_x3 Cache Properties

CPUID Fn8000_001D_EAX_x3 reports done/null. See CPUID Fn8000_001D_EAX_x0.

Bits	Description
31:0	Reserved. Value: 0000_0000h.

CPUID Fn8000_001D_EDX_x0 Cache Properties

CPUID Fn8000_001D_EDX_x0 reports topology information for the DC. See CPUID Fn8000_001D_EAX_x0.

Bits	Description
31:2	Reserved.
1	**CacheInclusive: cache inclusive**. Value: 0. 0=Cache is not inclusive of lower cache levels. 1=Cache is inclusive of lower cache levels.
0	**WBINVD: Write-Back Invalidate/Invalidate**. Value: 0. 0=WBINVD/INVD invalidates all lower level caches of non-originating cores sharing this cache. 1=WBINVD/INVD not ensured to invalidate all lower level caches of non-originating cores sharing this cache.

CPUID Fn8000_001D_EDX_x1 Cache Properties

CPUID Fn8000_001D_EDX_x1 reports topology information for the IC. See CPUID Fn8000_001D_EAX_x0.

Bits	Description
31:2	Reserved.
1	**CacheInclusive: cache inclusive**. Value: 0. See: CPUID Fn8000_001D_EDX_x0[CacheInclusive].
0	**WBINVD: Write-Back Invalidate/Invalidate**. Value: 0. See: CPUID Fn8000_001D_EDX_x0[WBINVD].

CPUID Fn8000_001D_EDX_x2 Cache Properties

CPUID Fn8000_001D_EDX_x2 reports topology information for the L2. See CPUID Fn8000_001D_EAX_x0.

Bits	Description
31:2	Reserved.

1	**CacheInclusive: cache inclusive**. See: CPUID Fn8000_001D_EDX_x0[CacheInclusive]. Value: 0.
0	**WBINVD: Write-Back Invalidate/Invalidate**. Value: 1. See: CPUID Fn8000_001D_EDX_x0[WBINVD].

CPUID Fn8000_001D_EDX_x3 Cache Properties

CPUID Fn8000_001D_EAX_x3 reports done/null. See CPUID Fn8000_001D_EAX_x0.

Bits	Description
31:0	Reserved. Value: 0000_0000h.

CPUID Fn8000_001E_EAX Extended APIC ID

If CPUID Fn8000_0001_ECX[TopologyExtensions]==0 then CPUID Fn8000_001E_E[D,C,B,A]X is reserved. If (MSR0000_001B[ApicEn]==0) then CPUID Fn8000_001E_EAX[ExtendedApicId] is reserved.

Bits	Description
31:0	**ExtendedApicId: extended APIC ID**. Value: IF (MSR0000_001B[ApicEn]==0) THEN 0000_0000h. ELSE APIC20[31:0]. ENDIF.

CPUID Fn8000_001E_EBX Compute Unit Identifiers

See CPUID Fn8000_001E_EAX.

Bits	Description
31:16	Reserved.
15:8	**ThreadsPerComputeUnit: threads per compute unit**. The number of threads per compute unit is ThreadsPerComputeUnit+1. Value: Product-specific.
7:0	**ComputeUnitId: compute unit ID**. Identifies the processor compute unit ID. Value: Product-specific.

CPUID Fn8000_001E_ECX Node Identifiers

See CPUID Fn8000_001E_EAX.

Bits	Description
31:0	Reserved.

CPUID Fn8000_001E_EDX Reserved

See CPUID Fn8000_001E_EAX.

Bits	Description
31:0	Reserved.

3.19 MSRs - MSR0000_xxxx

See 3.1 [Register Descriptions and Mnemonics] for a description of the register naming convention. MSRs are accessed through x86 WRMSR and RDMSR instructions.

MSR0000_0000 Load-Store MCA Address

Bits	Description
63:0	Alias of MSR0000_0402.

MSR0000_0001 Load-Store MCA Status

Bits	Description
63:0	Alias of MSR0000_0401.

MSR0000_0010 Time Stamp Counter (TSC)

Reset: 0000_0000_0000_0000h.

Bits	Description
63:32	**TSC[63:32]: time stamp counter high**. See: TSC[31:0].
31:0	**TSC[31:0]: time stamp counter low**. Read-write; updated-by-hardware. TSC[63:0] = {TSC[63:32],TSC[31:0]}. The TSC increments at the P0 frequency. This field uses software P-state numbering. See 2.5.3.1.1.1 [Software P-state Numbering]. The TSC counts at the same rate in all P-states, all C states, S0, or S1. A read of this MSR in guest mode is affected by MSRC000_0104 [Time Stamp Counter Ratio (TscRateMsr)]. The value (TSC/TSCRatio) is the TSC P0 frequency based value (as if TSCRatio==1.0) when (TSCRatio!=1.0).

MSR0000_001B APIC Base Address (APIC_BAR)

Bits	Description
63:40	MBZ.
39:12	**ApicBar[39:12]: APIC base address register**. Read-write. Reset: 00_FEE0_0h. Specifies the base address, physical address [39:12], for the APICXX register set in xAPIC mode. See 2.4.9.1.2 [APIC Register Space].
11	**ApicEn: APIC enable**. Read-write. Reset: 0. See 2.4.9.1.2 [APIC Register Space]. 1=Local APIC is enabled in xAPIC mode.
10	MBZ.
9	MBZ.
8	**BSC: boot strap core**. Read-write; updated-by-hardware. Reset: x. 1=The core is the boot core of the BSP. 0=The core is not the boot core of the BSP.
7:0	MBZ.

MSR0000_002A Cluster ID (EBL_CR_POWERON)

Read; GP-write.

Bits	Description
63:18	MBZ.
17:16	**ClusterID**. Reset: 00b. The field does not affect hardware.
15:0	MBZ.

MSR0000_00E7 Max Performance Frequency Clock Count (MPERF)

Reset: 0000_0000_0000_0000h.

Bits	Description
63:0	**MPERF: maximum core clocks counter**. Read-write; Updated-by-hardware. Incremented by hardware at the P0 frequency while the core is in C0. This register does not increment when the core is in the stop-grant state. In combination with MSR0000_00E8, this is used to determine the effective frequency of the core. A read of this MSR in guest mode is affected by MSRC000_0104 [Time Stamp Counter Ratio (TscRateMsr)]. This field uses software P-state numbering. See MSRC001_0015[EffFreqCntMwait], 2.5.3.3 [Effective Frequency], and 2.5.3.1.1.1 [Software P-state Numbering].

MSR0000_00E8 Actual Performance Frequency Clock Count (APERF)

Reset: 0000_0000_0000_0000h.

Bits	Description
63:0	**APERF: actual core clocks counter**. Read-write; Updated-by-hardware. This register increments in proportion to the actual number of core clocks cycles while the core is in C0. The register does not increment when the core is in the stop-grant state. See MSR0000_00E7.

MSR0000_00FE MTRR Capabilities (MTRRcap)

Read; GP-write. Reset: 0000_0000_0000_0508h.

Bits	Description
63:11	Reserved.
10	**MtrrCapWc: write-combining memory type**. 1=The write combining memory type is supported.
9	Reserved.
8	**MtrrCapFix: fixed range register**. 1=Fixed MTRRs are supported.
7:0	**MtrrCapVCnt: variable range registers count**. Specifies the number of variable MTRRs supported.

MSR0000_0174 SYSENTER CS (SYSENTER_CS)

Bits	Description
63:32	RAZ.

31:16	Reserved.
15:0	**SysEnterCS: SYSENTER target CS**. Read-write. Reset: 0000h. Holds the called procedure code segment.

MSR0000_0175 SYSENTER ESP (SYSENTER_ESP)

Reset: 0000_0000_0000_0000h.

Bits	Description
63:32	Reserved.
31:0	**SysEnterESP: SYSENTER target SP**. Read-write. Holds the called procedure stack pointer.

MSR0000_0176 SYSENTER EIP (SYSENTER_EIP)

Reset: 0000_0000_0000_0000h.

Bits	Description
63:32	Reserved.
31:0	**SysEnterEIP: SYSENTER target IP**. Read-write. Holds the called procedure instruction pointer.

MSR0000_0179 Global Machine Check Capabilities (MCG_CAP)

Read; GP-write.

Bits	Description
63:9	Reserved.
8	**McgCtlP: MCG_CTL register present**. Value: 1. 1=The machine check control registers (MCi_CTL) are present. See 2.15.1 [Machine Check Architecture]
7:0	**Count**. Value: 07h. Indicates the number of error reporting banks visible to each core. 06h=Error-reporting banks 0 through 5. See 2.15.1.1 [Machine Check Registers].

MSR0000_017A Global Machine Check Status (MCG_STAT)

Reset: 0000_0000_0000_0000h. See 2.15.1 [Machine Check Architecture].

Bits	Description
63:3	Reserved.
2	**MCIP: machine check in progress**. Read-write; set-by-hardware. 1=A machine check is in progress.
1	**EIPV: error instruction pointer valid**. Read-write; Updated-by-hardware. 1=The instruction pointer that was pushed onto the stack by the machine check mechanism references the instruction that caused the machine check error.
0	**RIPV: restart instruction pointer valid**. Read-write; Updated-by-hardware. 1=Program execution can be reliably restarted at the EIP address on the stack. 0=The interrupt was not precise and/or the process (task) context may be corrupt; continued operation of this process may not be possible without intervention, however system processing or other processes may be able to continue with appropriate software clean up.

MSR0000_017B Global Machine Check Exception Reporting Control (MCG_CTL)

Read-write. Reset: 0000_0000_0000_0000h. This registers controls enablement of the individual error reporting banks; see 2.15.1 [Machine Check Architecture]. When a machine check register bank is not enabled in MCG_CTL, errors for that bank are not logged or reported, and actions enabled through the MCA are not taken; each MCi_CTL register identifies which errors are still corrected when MCG_CTL[i] is disabled.

Bits	Description
63:7	Unused.
6	**MC6En: MC6 register bank enable**. 1=The MC6 machine check register bank is enabled.
5	**MC5En: MC5 register bank enable**. 1=The MC5 machine check register bank is enabled.
4	**MC4En: MC4 register bank enable**. 1=The MC4 machine check register bank is enabled for all cores of the node.
3	Unused.
2	**MC2En: MC2 register bank enable**. 1=The MC2 machine check register bank is enabled.
1	**MC1En: MC1 register bank enable**. 1=The MC1 machine check register bank is enabled.
0	**MC0En: MC0 register bank enable**. 1=The MC0 machine check register bank is enabled.

MSR0000_01D9 Debug Control (DBG_CTL_MSR)

Bits	Description
63:7	Reserved.
6	MBZ.
5:2	**PB: performance monitor pin control**. Read-write. Reset: 0. This field does not control any hardware.
1	**BTF**. Read-write. Reset: 0. 1=Enable branch single step.
0	**LBR**. Read-write. Reset: 0. 1=Enable last branch record.

MSR0000_01DB Last Branch From IP (BR_FROM)

Read; GP-write; Not-same-for-all, Updated-by-hardware. Reset: 0000_0000_0000_0000h.

Bits	Description
63:0	**LastBranchFromIP**. Loaded with the segment offset of the branch instruction.

MSR0000_01DC Last Branch To IP (BR_TO)

Read; GP-write; Not-same-for-all, Updated-by-hardware. Reset: 0000_0000_0000_0000h.

Bits	Description
63:0	**LastBranchToIP**. Holds the target RIP of the last branch that occurred before an exception or interrupt.

MSR0000_01DD Last Exception From IP

Read; GP-write; Not-same-for-all, Updated-by-hardware. Reset: 0000_0000_0000_0000h.

Bits	Description
63:0	**LastIntFromIP**. Holds the source RIP of the last branch that occurred before the exception or interrupt.

MSR0000_01DE Last Exception To IP

Read; GP-write; Not-same-for-all, Updated-by-hardware. Reset: 0000_0000_0000_0000h.

Bits	Description
63:0	**LastIntToIP**. Holds the target RIP of the last branch that occurred before the exception or interrupt.

MSR0000_020[F:0] Variable-Size MTRRs Base/Mask

Per-compute-unit.
Each MTRR (MSR0000_020[F:0] [Variable-Size MTRRs Base/Mask], MSR0000_02[6F:68,59:58,50], or MSR0000_02FF [MTRR Default Memory Type (MTRRdefType)]) specifies a physical address range and a corresponding memory type (MemType) associated with that range. Setting the memory type to an unsupported value results in a #GP.

The variable-size MTRRs come in pairs of base and mask registers (MSR0000_0200 and MSR0000_0201 are the first pair, etc.). Variables MTRRs are enabled through MSR0000_02FF[MtrrDefTypeEn]. A core access--with address CPUAddr--is determined to be within the address range of a variable-size MTRR if the following equation is true:
CPUAddr39:12] & PhyMask[39:12] == PhyBase[39:12] & PhyMask[39:12].

For example, if the variable MTRR spans 256 KB and starts at the 1 MB address. The PhyBase would be set to 0_0010_0000h and the PhyMask to F_FFFC_0000h (with zeros filling in for bits[11:0]). This results in a range from 0_0010_0000h to 0_0013_FFFF.

MSR0000_020[E,C,A,8,6,4,2,0] Variable-Size MTRRs Base

Table 217: Register Mapping for MSR0000_020[E,C,A,8,6,4,2,0]

Register	Function
MSR0000_0200	Range 0
MSR0000_0202	Range 1
MSR0000_0204	Range 2
MSR0000_0206	Range 3
MSR0000_0208	Range 4
MSR0000_020A	Range 5
MSR0000_020C	Range 6
MSR0000_020E	Range 7

Table 218: Valid Values for Memory Type Definition

Bits	Description
000b	UC or uncacheable.
001b	WC or write combining.
011b-010b	Reserved
100b	WT or write through.
101b	WP or write protect.
110b	WB or write back.
111b	Reserved

Bits	Description
63:48	MBZ.
47:12	**PhyBase: base address**. Read-write. Reset: 0.
11:3	MBZ.
2:0	**MemType: memory type**. Read-write. Reset: 0. Address range from 00000h to 0FFFFh. See: Table 218 [Valid Values for Memory Type Definition].

MSR0000_020[F,D,B,9,7,5,3,1] Variable-Size MTRRs Mask

Table 219: Register Mapping for MSR0000_020[F,D,B,9,7,5,3,1]

Register	Function
MSR0000_0201	Range 0
MSR0000_0203	Range 1
MSR0000_0205	Range 2
MSR0000_0207	Range 3
MSR0000_0209	Range 4
MSR0000_020B	Range 5
MSR0000_020D	Range 6
MSR0000_020F	Range 7

Bits	Description
63:48	MBZ.
47:12	**PhyMask: address mask**. Read-write. Reset: 0.
11	**Valid: valid**. Read-write. Reset: 0. 1=The variable-size MTRR pair is enabled.
10:0	MBZ.

MSR0000_02[6F:68,59:58,50] Fixed-Size MTRRs

Per-compute-unit.
See MSR0000_020[F:0] for general MTRR information. Fixed MTRRs are enabled through MSR0000_02FF[MtrrDefTypeFixEn, MtrrDefTypeEn]. For addresses below 1MB, the appropriate Fixed

MTRRs override the default access destination. Each fixed MTRR includes two bits, RdDram and WrDram, that determine the destination based on the access type.
See 2.4.6.1.2 [Determining The Access Destination for Core Accesses].

Table 220: Register Mapping for MSR0000_02[6F:68,59:58,50]

Register	Function
MSR0000_0250	64K Range
MSR0000_0258	16K_0 Range
MSR0000_0259	16K_1 Range
MSR0000_0268	4K_0 Range
MSR0000_0269	4K_1 Range
MSR0000_026A	4K_2 Range
MSR0000_026B	4K_3 Range
MSR0000_026C	4K_4 Range
MSR0000_026D	4K_5 Range
MSR0000_026E	4K_6 Range
MSR0000_026F	4K_7 Range

Table 221: Field Mapping for MSR0000_02[6F:68,59:58,50]

Register	Bits							
	63:56	55:48	47:40	39:32	31:24	23:16	15:8	7:0
MSR0000_0250	64K_70000	64K_60000	64K_50000	64K_40000	64K_30000	64K_20000	64K_10000	64K_00000
MSR0000_0258	16K_9C000	16K_98000	16K_94000	16K_90000	16K_8C000	16K_88000	16K_84000	16K_80000
MSR0000_0259	16K_BC000	16K_B8000	16K_B4000	16K_B0000	16K_AC000	16K_A8000	16K_A4000	16K_A0000
MSR0000_0268	4K_C7000	4K_C6000	4K_C5000	4K_C4000	4K_C3000	4K_C2000	4K_C1000	4K_C0000
MSR0000_0269	4K_CF000	4K_CE000	4K_CD000	4K_CC000	4K_CB000	4K_CA000	4K_C9000	4K_C8000
MSR0000_026A	4K_D7000	4K_D6000	4K_D5000	4K_D4000	4K_D3000	4K_D2000	4K_D1000	4K_D0000
MSR0000_026B	4K_DF000	4K_DE000	4K_DD000	4K_DC000	4K_DB000	4K_DA000	4K_D9000	4K_D8000
MSR0000_026C	4K_E7000	4K_E6000	4K_E5000	4K_E4000	4K_E3000	4K_E2000	4K_E1000	4K_E0000
MSR0000_026D	4K_EF000	4K_EE000	4K_ED000	4K_EC000	4K_EB000	4K_EA000	4K_E9000	4K_E8000
MSR0000_026E	4K_F7000	4K_F6000	4K_F5000	4K_F4000	4K_F3000	4K_F2000	4K_F1000	4K_F0000
MSR0000_026F	4K_FF000	4K_FE000	4K_FD000	4K_FC000	4K_FB000	4K_FA000	4K_F9000	4K_F8000

Bits	Description
63:61	MBZ.
60	**RdDram: read DRAM**. See: MSR0000_02[6F:68,59:58,50][4].
59	**WrDram: write DRAM**. See: MSR0000_02[6F:68,59:58,50][3].
58:56	**MemType: memory type**. See: MSR0000_02[6F:68,59:58,50][2:0].
55:53	MBZ.
52	**RdDram: read DRAM**. See: MSR0000_02[6F:68,59:58,50][4].
51	**WrDram: write DRAM**. See: MSR0000_02[6F:68,59:58,50][3].
50:48	**MemType: memory type**. See: MSR0000_02[6F:68,59:58,50][2:0].

47:45	MBZ.
44	**RdDram: read DRAM**. See: MSR0000_02[6F:68,59:58,50][4].
43	**WrDram: write DRAM**. See: MSR0000_02[6F:68,59:58,50][3].
42:40	**MemType: memory type**. See: MSR0000_02[6F:68,59:58,50][2:0].
39:37	MBZ.
36	**RdDram: read DRAM**. See: MSR0000_02[6F:68,59:58,50][4].
35	**WrDram: write DRAM**. See: MSR0000_02[6F:68,59:58,50][3].
34:32	**MemType: memory type**. See: MSR0000_02[6F:68,59:58,50][2:0].
31:29	MBZ.
28	**RdDram: read DRAM**. See: MSR0000_02[6F:68,59:58,50][4].
27	**WrDram: write DRAM**. See: MSR0000_02[6F:68,59:58,50][3].
26:24	**MemType: memory type**. See: MSR0000_02[6F:68,59:58,50][2:0].
23:21	MBZ.
20	**RdDram: read DRAM**. See: MSR0000_02[6F:68,59:58,50][4].
19	**WrDram: write DRAM**. See: MSR0000_02[6F:68,59:58,50][3].
18:16	**MemType: memory type**. See: MSR0000_02[6F:68,59:58,50][2:0].
15:13	MBZ.
12	**RdDram: read DRAM**. See: MSR0000_02[6F:68,59:58,50][4].
11	**WrDram: write DRAM**. See: MSR0000_02[6F:68,59:58,50][3].
10:8	**MemType: memory type**. See: MSR0000_02[6F:68,59:58,50][2:0].
7:5	MBZ.
4	**RdDram: read DRAM**. IF (MSRC001_0010[MtrrFixDramModEn]) THEN Read-write. ELSE MBZ. ENDIF. Reset: 0. 0=Read accesses to the range are marked as MMIO. 1=Read accesses to the range are marked as destined for DRAM. Address range from 00000h to 0FFFFh. See: MSRC001_0010[MtrrFixDramEn, MtrrFixDramModEn]).
3	**WrDram: write DRAM**. IF (MSRC001_0010[MtrrFixDramModEn]) THEN Read-write. ELSE MBZ. ENDIF. Reset: 0. 0=Write accesses to the range are marked as MMIO. 1=Write accesses to the range are marked as destined for DRAM. Address range from 00000h to 0FFFFh. See: MSRC001_0010[MtrrFixDramEn, MtrrFixDramModEn]).
2:0	**MemType: memory type**. Read-write. Reset: 0. Address range from 00000h to 0FFFFh. See: Table 218 [Valid Values for Memory Type Definition].

MSR0000_0277 Page Attribute Table (PAT)

This register specifies the memory type based on the PAT, PCD, and PWT bits in the virtual address page tables.

Bits	Description
63:59	MBZ.
58:56	**PA7MemType**. See: PA0MemType. Reset: 0h. Default UC. MemType for {PAT, PCD, PWT} = 7h.
55:51	MBZ.
50:48	**PA6MemType**. See: PA0MemType. Reset: 7h. Default UC-. MemType for {PAT, PCD, PWT} = 6h.

47:43	MBZ.
42:40	**PA5MemType**. See: PA0MemType. Reset: 4h. Default WT. MemType for {PAT, PCD, PWT} = 5h.
39:35	MBZ.
34:32	**PA4MemType**. See: PA0MemType. Reset: 6h. Default WB. MemType for {PAT, PCD, PWT} = 4h.
31:27	MBZ.
26:24	**PA3MemType**. See: PA0MemType. Reset: 0h. Default UC. MemType for {PAT, PCD, PWT} = 3h.
23:19	MBZ.
18:16	**PA2MemType**. See: PA0MemType. Reset: 7h. Default UC-. MemType for {PAT, PCD, PWT} = 2h.
15:11	MBZ.
10:8	**PA1MemType**. See: PA0MemType. Reset: 4h. Default WT. MemType for {PAT, PCD, PWT} = 1h.
7:3	MBZ.
2:0	**PA0MemType**. Read-write. Reset: 6h. MemType for {PAT, PCD, PWT} = 0h. Bits Description Bits Description 0h UC or uncacheable. 4h WT or write through. 1h WC or write combining. 5h WP or write protect. 2h MBZ. 6h WB or write back. 3h MBZ. 7h UC- or uncacheable (overridden by WC state).

MSR0000_02FF MTRR Default Memory Type (MTRRdefType)

Per-compute-unit.
See MSR0000_020[F:0] for general MTRR information.

Bits	Description
63:12	MBZ.
11	**MtrrDefTypeEn: variable and fixed MTRR enable**. Read-write. Reset: 0. 1=MSR0000_020[F:0] [Variable-Size MTRRs Base/Mask], and MSR0000_02[6F:68,59:58,50] [Fixed-Size MTRRs] are enabled. 0=Fixed and variable MTRRs are not enabled.
10	**MtrrDefTypeFixEn: fixed MTRR enable**. Read-write. Reset: 0. 1=MSR0000_02[6F:68,59:58,50] [Fixed-Size MTRRs]are enabled. This field is ignored (and the fixed MTRRs are not enabled) if MSR0000_02FF[MtrrDefTypeEn]=0.
9:8	MBZ.
7:0	**MemType: memory type**. Read-write. Reset: 0. If MtrrDefTypeEn==1 then MemType specifies the memory type for memory space that is not specified by either the fixed or variable range MTRRs. If MtrrDefTypeEn==0 then the default memory type for all of memory is UC. Valid encodings are {00000b, MSR0000_02[6F:68,59:58,50][2:0]}.

MSR0000_0400 MC0 Machine Check Control (MC0_CTL)

Read-write. Reset: 0000_0000_0000_0000h. See 2.15.1 [Machine Check Architecture]. See MSRC001_0044 [DC Machine Check Control Mask (MC0_CTL_MASK)].

Bits	Description
63:12	Unused.
11	Unused.

10	Unused.
9	**IntErrType1: internal error type 1**.
8	**IntErrType2: internal error type 2**.
7	**SRDE: read data error**. System read data errors on cache fill.
6	**LFE: line fill error**. Uncorrectable error on cache fill.
5	**SCBP: SCB parity**.
4	**SQP: store queue parity**.
3	**LQP: load queue parity**.
2	**DatP: data parity**.
1	**TLBP: TLB parity**.
0	**TagP: tag parity**.

MSR0000_0401 MC0 Machine Check Status (MC0_STATUS)

See 2.15.1 [Machine Check Architecture]. See MSRC001_0015[McStatusWrEn]. Table 222 describes each error type. Table 223 describes the error codes and status register settings for each error type. MSR0000_0001 is an alias of MSR0000_0401.

Bits	Description
63	**Val: error valid**. Read-write; set-by-hardware. Cold reset: 0. 1=This bit indicates that a valid error has been detected. This bit should be cleared to 0 by software after the register has been read.
62	**Overflow: error overflow**. Read-write; set-by-hardware. Cold reset: 0. 1=An error was detected while the valid bit (Val) was set; at least one error was not logged. Overflow is set independently of whether the existing error is overwritten. The following hierarchy identifies the error logging priorities. 1. Uncorrectable errors 2. Deferred errors 3. Correctable errors The machine check mechanism handles the contents of MC*i*_STATUS during overflow as follows: • Higher priority errors overwrite lower priority errors. • New errors of equal or lower priority do not overwrite existing errors. • Uncorrectable errors which are not logged due to overflow result in setting PCC, unless the new uncorrectable error is of the same type and in the same reportable address range as the existing error.
61	**UC: error uncorrected**. Read-write; Updated-by-hardware. Cold reset: 0. 1=The error was not corrected by hardware.
60	**En: error enable**. Read-write; Updated-by-hardware. Cold reset: 0. 1=MCA error reporting is enabled for this error, as indicated by MCi_CTL.
59	**MiscV: miscellaneous error register valid**. Read-write; Updated-by-hardware. Cold reset: 0. 1=Valid thresholding in MSR0000_0403.

58	**AddrV: error address valid**. Read-write; Updated-by-hardware. Cold reset: 0. 1=MCi_ADDR contains address information associated with the error.
57	**PCC: processor context corrupt**. Read-write; Updated-by-hardware. Cold reset: 0. 1=Hardware context held by the processor may have been corrupted. Continued operation of the system may have unpredictable results. The error is not recoverable or survivable, and the system should be reinitialized. See 2.15.1.6.1 [Differentiation Between System-Fatal and Process-Fatal Errors].
56:45	Reserved.
44	**Deferred: deferred error**. Read-write; Updated-by-hardware. Cold reset: 0. 1=A deferred error was created. A deferred error is the result of an uncorrectable data error which did not immediately cause a processor exception; the data is poisoned and an exception is deferred until the data is loaded by a core.
43	**Poison: poison error**. Read-write; Updated-by-hardware. Cold reset: 0. 1=The error was the result of attempting to consume poisoned data. This indicator does not apply to MSR0000_0411 [MC4 Machine Check Status (MC4_STATUS)].
42:40	Reserved.
39:36	**Way: cache way in error.** Read-write; Updated-by-hardware. Cold reset: 0. Indicates the cache way in error. Bits Description 0h Way 0 1h Way 1 2h Way 2 3h Way 3 Fh-4h Reserved
35:21	Reserved.
20:16	**ErrorCodeExt: extended error code**. Read-write; Updated-by-hardware. Cold reset: 0. Logs an extended error code when an error is detected. This model-specific field is used in conjunction with ErrorCode to identify the error sub-type for root cause analysis (see 2.15.1.5 [Error Code]). See Table 223 for expected values.
15:0	**ErrorCode: error code**. Read-write; Updated-by-hardware. Cold reset: 0. See 2.15.1.5 [Error Code] for details on decoding this field. See Table 223 for expected values.

Table 222: MC0 Error Descriptions

Error Type	Error Sub-type	Description[1]	CTL[2]	EAC[3]
Line Fill Error	-	An uncorrectable error occurred during a line fill from the L2 cache or the NB. (Note: For IO read, may not actually install to L1 cache.)	LineFillError	E
Data Cache Error	Data array	Error occurred in cache data array access.	DatP	D
	SCB	Error occurred in SCB access.	SCBP	D
	STQ	Error occurred in STQ access.	SQP	D

Table 222: MC0 Error Descriptions

Error Type	Error Sub-type	Description[1]	CTL[2]	EAC[3]
Tag Error	Tag array	A tag error was encountered. If uncorrectable, this errors is system fatal and results in a sync flood.	TagP	D
	STQ	Error occurred in STQ access.	SQP	D
	LDQ	Error occurred in LDQ access.	LQP	D
L1 TLB Error	TLB parity	Parity error in L1 TLB access.	TLBP	D
	TLB multimatch	Lookup hit on multiple entries.		D
	Locked TLB miss	TLB miss occurred after lock granted.		E
System Read Data Error	-	An error occurred during an attempted read of data from the NB. Possible reasons include master abort, target abort.	SRDE	E
Internal Error	IntErrType1	An internal error condition was detected which prohibits the core from continuing execution.	IntErrType1	E
	IntErrType2		IntErrType2	E

1. CID: core ID. All LS errors are reported to the affected core; see 2.15.1.3 [Error Detection, Action, Logging, and Reporting].
2. See MSR0000_0400.
3. EAC: D=Error action taken if detected. E=Error action taken if MCA bank enabled. See 2.15.1.3 [Error Detection, Action, Logging, and Reporting].

Table 223: MC0 Error Signatures

Error Type	Error	ErrorCodeExt	Error Code						UC	ADDRV	PCC	Deferred	Poison
			Type	UU/PP	T	RRRR	II/TT	LL					
Line Fill Error	-	01h	MEM	-	-	DRD	D	LG	1	1	0	-0	-1
Data Cache Error	Data array	00h				DRD	D	L1	0/1	1	0	-0	-0
	SCB	03h											
	STQ	02h											
Tag Error	Tag array	10h	MEM	- SRC	- 0	DRD, DWR, Probe	G	L1	1	0/1	1	-0	-0
	STQ	11h				DWR			0/1	1	0/1		
	LDQ	12h				DRD			0/1	1	0		
L1 TLB Error	TLB parity	00h	TLB			-	D	L1	0/1	1	0	-0	-0
	TLB Multimatch	01h							0/1	0			
	Locked TLB miss	02h							1	1			
System Read Data Error	-	00h	BUS			DRD	MEM/IO	LG	1	1	0	-0	-0
Internal Error	Type1	01h		GEN	1	GEN	GEN	LG	1	0	0	-0	-0
	Type2	02h											

MSR0000_0402 MC0 Machine Check Address (MC0_ADDR)

Read-write; Updated-by-hardware. Cold reset: 0000_0000_0000_0000h. The MCi_ADDR register contains valid data if indicated by MCi_STATUS[AddrV]. See 2.15.1 [Machine Check Architecture]. MSR0000_0000 is an alias of MSR0000_0402.

Bits	Description
63:0	**ADDR: Address**. See Table 224.

Table 224: MC0 Address Register

Error Type	Error Sub-type	Bits	Description
Line Fill Error	-	63:48	Reserved
		47:6	**PhysAddr[47:6]**.
		5:0	Reserved
Data Cache Error	Data array	63:48	Reserved
		47:4	**PhysAddr[47:4]**.
		3:0	Reserved
Data Cache Error	SCB	63:12	Reserved
		11:4	**PhysAddr[11:4]**.
		3:0	Reserved
Data Cache Error	STQ	63:5	Reserved
		4:0	**Index**.
Tag Error	Tag array	63:48	Reserved
		47:6	**PhysAddr[47:6]**.
		5:4	**PhysAddr[5:4]**. Not valid for probe errors.
		3:0	Reserved
	STQ	63:5	Reserved
		4:0	**Index**.
	LDQ	63:6	Reserved
		5:0	**Index**.
L1 TLB Error	TLB parity	63:48	Reserved
		47:12	**LinAddr[47:12]**.
		11:5	Reserved
		4:0	**TlbIndex**.
	Locked TLB miss	63:48	Reserved
		47:12	**LinAddr[47:12]**.
		11:0	Reserved
System Read Data Error	-	63:48	Reserved
		47:6	**PhysAddr[47:6]**.
		5:0	Reserved

MSR0000_0403 MC0 Machine Check Miscellaneous (MC0_MISC)

See 2.15.1.7 [Error Thresholding].

Bits	Description
63	**Valid**. IF (MSRC001_0015[McStatusWrEn]) THEN Read-write. ELSE Read-only. ENDIF. Reset: 1. 1=A valid CntP field is present in this register.
62	**CntP: counter present**. IF (MSRC001_0015[McStatusWrEn]) THEN Read-write. ELSE Read-only. ENDIF. Reset: 1. 1=A valid threshold counter is present.
61	**Locked**. IF (MSRC001_0015[McStatusWrEn]) THEN Read-write. ELSE Read-only. ENDIF.Reset: 0. 1=Writes to this register are ignored. This bit is set by BIOS to indicate that this register is not available for OS use. BIOS should set this bit if IntType is set to SMI.
60	**IntP: Interrupt support present**. IF (MSRC001_0015[McStatusWrEn] | ~Locked) THEN Read-write. ELSE Read-only. ENDIF. Reset: 1. 1=IntType can be used to generate interrupts. 0=IntType and interrupt generation are not suported.
59:56	Reserved.
55:52	**LvtOffset: LVT offset**. IF (MSRC001_0015[McStatusWrEn] | ~Locked) THEN Read-write. ELSE Read-only. ENDIF. Reset: 0000b. BIOS: 1. Specifies the address of the LVT entry in the APIC registers as follows: LVT address = (LvtOffset shifted left 4 bits) + 500h (see APIC[530:500]). Only values 0 through 3 are valid; all others reserved.
51	**CntEn: counter enable**. Read-write; Updated-by-hardware. Reset: 0. 1=Count thresholding errors. See 2.15.1.7 [Error Thresholding].
50:49	**IntType: interrupt type**. Read-write. Cold reset: 0. Specifies the type of interrupt signaled when Ovrflw is set and IntP==1. Bits — Description 00b — No Interrupt. 01b — APIC based interrupt (see LvtOffset above) to all cores. 10b — SMI trigger event (always routed to CpuCoreNum 0, as defined in 2.4.4 [Processor Cores and Downcoring]); see 2.4.10.2.3 [SMI Sources And Delivery]. 11b — Reserved.
48	**Ovrflw: overflow**. Read-write; set-by-hardware. Cold reset: 0. Set by hardware when ErrCnt transitions from FFEh to FFFh. When this field is set, ErrCnt no longer increments. When this bit is set and the IntP field==1, the interrupt selected by the IntType field is generated.
47:44	Reserved.
43:32	**ErrCnt: error counter**. Read-write; updated-by-hardware. Cold reset: 0. This is written by software to set the starting value of the error counter. This is incremented by hardware when errors are logged. When this counter overflows, it stays at FFFh (no rollover). The threshold value, written by software, is (FFFh - the desired error count (the number of errors necessary in order for an interrupt to be taken)); the desired error count of 0 (a write value of FFFh) is not supported.
31:24	**BlkPtr: Block pointer for additional MISC registers**. Read-only. Value: 00h. 00h=Extended MISC MSR block is not valid.
23:0	Reserved.

MSR0000_0404 MC1 Machine Check Control (MC1_CTL)

Per-compute-unit; Read-write.
Reset: 0000_0000_0000_0000h. See 2.15.1 [Machine Check Architecture].

Bits	Description
63:26	Unused.
25	Unused.
24	Unused.
23	**IVP: IC valid bit parity error**.
22	**L1TLBM: IC L1 TLB multi-match error**.
21	**L2TLBM: IC L2 TLB multi-match error**.
20	**DFIFOE: decoder FIFO parity error**.
19	**DPDBE: decoder predecode buffer parity error**.
18	**DEIBP: decoder instruction buffer parity error**.
17	**DEUOPQP: Decoder micro-op queue parity error**.
16	**DEPRP: microcode patch buffer parity error**.
15	**BSRP: branch status register parity error**.
14	Unused.
13	**PQP: prediction queue parity error**.
12	**PFBP: prefetch buffer parity**.
11:10	Unused.
9	**SRDE: system read data error**.
8	Unused.
7	**LFE: line fill error**. Uncorrectable error on cache line fill.
6	**L1TP: L1 TLB parity error**.
5	**L2TP: L2 TLB parity error**.
4	**ISTP: L1 cache probe tag array parity error**.
3	**IMTP: L1 cache main tag array parity error**.
2	**IDP: L1 cache data array parity errors**.
1	Unused.
0	Unused.

MSR0000_0405 MC1 Machine Check Status (MC1_STATUS)

See 2.15.1 [Machine Check Architecture]. See MSRC001_0015[McStatusWrEn]. Table 225 describes each error type. Table 226 describes the error codes and status register settings for each error type.

Bits	Description
63	**Val: error valid**. See: MSR0000_0401[Val].

62	**Overflow: error overflow**. See: MSR0000_0401[Overflow].
61	**UC: error uncorrected**. See: MSR0000_0401[UC].
60	**En: error enable**. See: MSR0000_0401[En].
59	**MiscV: miscellaneous error register valid**. Read-write; Updated-by-hardware. Cold reset: 0. See: MSR0000_0401[MiscV]. 1=Valid thresholding in MSR0000_0407.
58	**AddrV: error address valid**. See: MSR0000_0401[AddrV].
57	**PCC: processor context corrupt**. See: MSR0000_0401[PCC].
56:45	Reserved.
44	**Deferred: deferred error**. See: MSR0000_0401[Deferred].
43	**Poison: poison error**. See: MSR0000_0401[Poison].
42:40	Reserved.
39:36	**Way: cache way in error.** Read-write; Updated-by-hardware. Cold reset: 0. Indicates the cache way in error. Bits Description 0h Way 0 1h Way 1 2h Way 2 Fh-3h Reserved
35:21	Reserved.
20:16	**ErrorCodeExt: extended error code**. Read-write; Updated-by-hardware. Cold reset: 0. See MSR0000_0401[ErrorCodeExt]. See Table 226 for expected values.
15:0	**ErrorCode: error code**. Read-write; updated-by-hardware. Cold reset: 0. See 2.15.1.5 [Error Code] for details on decoding this field. See Table 226 for expected values.

Table 225: MC1 Error Descriptions

Error Type	Error	Description	CTL[3]	CID[2]	EAC[1]
Line Fill Error	-		LineFill Poison	A	E

Table 225: MC1 Error Descriptions

Error Type	Error	Description	CTL[3]	CID[2]	EAC[1]
Instruction cache read error	IC Data Load Parity	A parity error occurred during load of data from the instruction cache. The data is discarded from the IC and can be refetched.	IDP	A	D
	IC valid bit	Parity error for IC valid bit.	IVP	A	D
	Main tag	A main tag parity error occurred.	IMTP	A	D
	Prediction queue	Parity error in prediction queue.	PQP	A	E
	PFB data/address	PFB data/address had a parity error. A PFB valid bit error, PFB multimatch error, Line Fill Error, or ReadData Error may additionally cause a PFB data/address error.	PFBP	A	E
	PFB valid bit	PFB valid bit had a parity error. This error may cause subsequent errors related to the entry, but the effect can be contained to the running process.		B	E
	PFB non-cacheable bit	PFB non-cacheable bit had a parity error.		B	E
	PFB promotion address error	An address parity error was detected when promoting from the PFB to the IC.		B	E
	Branch status register	A parity error was discovered in the branch status register. This error is uncorrectable, but the effect can be contained to the running process.	BSRP	A	E
Instruction cache read error	Microcode Patch Buffer	Parity error in the microcode patch buffer. This error is uncorrectable. If a reset is not performed or the patch area is not reloaded, then it is recommended that the compute unit be removed from the running configuration by the operating system if possible. After a reset, BIST is used to determine whether there is a hard fault in the RAM. If a hard fault is not found, the error was likely a transient upset and the RAM is not broken. This error can also be caused by an error in the microcode patch region of the CC6 save area if ECC is not enabled.	DEPRP	A	E

Table 225: MC1 Error Descriptions

Error Type	Error	Description	CTL[3]	CID[2]	EAC[1]
Instruction cache read error	Decoder micro-op queue	Parity error in decode unit. This error is correctable unless the operation is for a non-cacheable operand.	DEUQ	A	E
	Decoder instruction buffer		DEIBP	A	E
	Decoder pre-decode buffer		DEPD	A	E
	Decoder fetch address FIFO		DEFF	A	E
Tag Probe	Probe tag error	A tag error was encountered during probe or victimization.	ISTP	0	D
	Probe tag valid bit	Parity error for IC probe tag valid bit.	IVP	0	D
L1 TLB	Parity	Parity error in L1 TLB.	L1TP	A	D
	Multimatch	Hit multiple entries in L1 TLB.	L1TLBM	A	D
L2 TLB	Parity	Parity error in L2 TLB.	L2TP	A	D
	Multimatch	Hit multiple entries in L2 TLB.	L2TLBM	A	D
System Read Data Error	-	An error occurred during an attempted demand read of data from the NB. Possible reasons include master abort, target abort.	SRDE	A	E

1. EAC: D=Error action taken if detected. E=Error action taken if MCA bank enabled.See 2.15.1.3 [Error Detection, Action, Logging, and Reporting].
2. CID: core ID. A=Error reported to the affected core. 0=Error reported to core 0 of the Compute Unit. B=Error reported to all cores of the Compute Unit. See 2.15.1.3 [Error Detection, Action, Logging, and Reporting].
3. See MSR0000_0404.

Table 226: MC1 Error Signatures

Error Type	Error	ErrorCodeExt	Error Code						UC	ADDRV	PCC	Deferred	Poison
			Type	UU/PP	TT	RRRR	II/TT	LL					
Line Fill Error	-	00h	MEM	-	-	IRD	I	L2	1	1	0	-0	-1
Instruction Cache Read Error	IC data load parity	01h		-	-	IRD	I	L1	0	1	0	-0	-0
	IC valid bit	02h							0	1	0	-0	-0
	Main tag	03h							0	1	0	-0	-0
	Prediction queue	04h							1	0	0	-0	-0
	PFB data/address	05h							0/1	0	0	-0	-0
	PFB valid bit	0Dh							1	0	0	-0	-0
	PFB non-cacheable bit	0Ah							0/1	0	0	-0	-0
	PFB promotion address error	07h							1	0	1	-0	-0
	Branch status register	06h							1	0	0	-0	-0
	Microcode Patch Buffer	10h						LG	1	1	1	-0	-0
	Decoder micro-op queue	11h						L1	0/1	1	0	-0	-0
	Decoder instruction buffer	12h							0/1	1	0	-0	-0
	Decoder pre-decode buffer	13h							0/1	0	0	-0	-0
	Decoder fetch address FIFO	14h							0/1	1	0	-0	-0
Tag Probe	Probe tag error	08h	MEM	-	-	Probe	I	L1	0	1	0	-0	-0
	Probe tag valid bit	09h											
L1 TLB	Parity	00h	TLB	-	-	-	I	L1	0	1	0	-0	-0
	Multimatch	01h											
L2 TLB	Parity	00h						L2					
	Multimatch	01h											
System Read Data Error	-	00h	BUS	SRC	0	IRD	MEM	LG	1	1	0	-0	-0

MSR0000_0406 MC1 Machine Check Address (MC1_ADDR)

Read-write; Updated-by-hardware. Cold reset: 0000_0000_0000_0000h. The MCi_ADDR register contains

valid data if indicated by MCi_STATUS[AddrV]. See 2.15.1 [Machine Check Architecture].

Bits	Description
63:0	**ADDR: Address**. See Table 227.

The following table defines the address register as a function of error type.

Table 227: MC1 Address Register

Error Type	Error Sub-Type	Bits	Description
Line Fill Error	-	63:48	Reserved
		47:6	**LinAddr[47:6]**.
		5:0	Reserved
Instruction cache read error	IC data load parity	63:48	Reserved
		47:3	**LinAddr[47:3]**. [7:6] Description 00b Bank 0 01b Bank 1 10b Bank 2 11b Bank 3
		2:1	**Way**. Bits Description 00b Way 0 01b Way 1 10b Way 2 11b Reserved
		0	Reserved
Instruction cache read error	IC valid bit	63:48	Reserved
		47:6	**LinAddr[47:6]**. [7:6] Description 00b Bank 0 01b Bank 1 10b Bank 2 11b Bank 3
		5:0	Reserved

Table 227: MC1 Address Register

Error Type	Error Sub-Type	Bits	Description
Instruction cache read error	Main tag	63:48	Reserved
		47:6	**LinAddr[47:6]**. [7:6] Description 00b Bank 0 01b Bank 1 10b Bank 2 11b Bank 3
		5:3	Reserved
		2:1	**Way**. Bits Description 00b Way 0 01b Way 1 10b Way 2 11b Reserved
		1:0	Reserved
Instruction Cache Read Error	Microcode Patch Buffer	63:4	Reserved
		3:0	Line group index.
Instruction cache read error	Decoder micro-op queue	63:2	Reserved
		1:0	Micro-op queue slot in error.
Instruction cache read error	Decoder instruction buffer	63:3	Reserved
		2	**PrefixMaskMismatch**. If (PrefixMaskMismatch==1) then BankAndParityBitInError=00b.
		1:0	**BankAndParityBitInError**. Bits Description 00b Bank A, parity bit 0 or 1 01b Bank B, parity bit 0 or 1 10b Bank A, parity bit 2 or 3 11b Bank B, parity bit 2 or 3
Instruction cache read error	Decoder fetch address FIFO	63:2	Reserved
		1	**BsrTagParityError**.
		0	**BankInError**. 0=Bank A. 1=Bank B.

Table 227: MC1 Address Register

Error Type	Error Sub-Type	Bits	Description
Tag Probe	Probe tag error	63:50	Reserved
		49:48	**BankBitmask**. Bit Description [0] Bank 6 [1] Bank 7
		47:6	**PhysAddr[47:6]**.
		5:0	**BankBitmask**. Bit Description [0] Bank 0 [1] Bank 1 [2] Bank 2 [3] Bank 3 [4] Bank 4 [5] Bank 5
Tag Probe	Probe tag valid bit	63:48	Reserved
		47:6	**PhysAddr[47:6]**.
		5:0	Reserved
L1 TLB	Parity, Multimatch	63:48	Reserved
		47:12	**LinAddr[47:12]**. 4-KB page: • [47:12]: LinAddr[47:12]. 2-MB page: • [47:20]: LinAddr[47:20]. • [19:12]: Reserved
		11:3	Reserved
		2:0	**BankBitmask**. Bit Description [0] Bank 0 [1] Bank 1 [2] Bank 2
L2 TLB	Parity, Multimatch	63:48	Reserved
		47:12	**LinAddr[47:12]**. (4-KB page size only)
		11:4	Reserved
		3:0	**MatchLines**.

MSR0000_0407 MC1 Machine Check Miscellaneous (MC1_MISC)

Cold reset: 0000_0000_0000_0000h.
See 2.15.1.7 [Error Thresholding].

Bits	Description
63	**Valid**. See: MSR0000_0403[Valid].
62	**CntP: counter present**. See: MSR0000_0403[CntP].

61	**Locked**. See: MSR0000_0403[Locked].
60	**IntP: Interrupt support present.** See: MSR0000_0403[IntP].
59:56	Reserved.
55:52	**LvtOffset: LVT offset**. See: MSR0000_0403[LvtOffset].
51	**CntEn: counter enable**. See: MSR0000_0403[CntEn].
50:49	**IntType: interrupt type**. See: MSR0000_0403[IntType].
48	**Ovrflw: overflow.** See: MSR0000_0403[Ovrflw].
47:44	Reserved.
43:32	**ErrCnt: error counter**. See: MSR0000_0403[ErrCnt].
31:24	**BlkPtr: Block pointer for additional MISC registers**. See: MSR0000_0403[BlkPtr].
23:0	Reserved.

MSR0000_0408 MC2 Machine Check Control (MC2_CTL)

Read-write; Per-compute-unit.
Reset: 0000_0000_0000_0000h. See 2.15.1 [Machine Check Architecture]. See MSRC001_0046 [BU Machine Check Control Mask (MC2_CTL_MASK)].

Bits	Description
63:16	Unused.
15	Unused.
14	**L2TlbPoison: TLB fill poison error from L2**.
13	**RdData: read data error from NB**.
12	**L2Tag: L2 cache tag error**.
11	**L2TlbData: L2 TLB parity error**. Parity error reading from TLB.
10	**L2Prefetch: L2 data prefetcher parity error**.
9	**XabAddr: XAB address parity error**.
8	**PrbAddr: probe buffer address parity error**.
7	**FillData: fill data parity and ECC error**.
6	**PrqAddr: post retire queue address parity error**.
5	**PrqData: post retire queue data parity error**.
4	**WccAddr: write coalescing cache address ECC error**.
3	**WccData: write coalescing cache data ECC error**.
2	**WcbData: write combining buffer data parity error**.
1	**VbData: victim buffer data parity and ECC error**.
0	**L2TagMultiHit: L2 tag multiple hit error**.

MSR0000_0409 MC2 Machine Check Status (MC2_STATUS)

See 2.15.1 [Machine Check Architecture]. See MSRC001_0015[McStatusWrEn]. Table 229 describes each

error type. Table 230 describes the error codes and status register settings for each error type.

Bits	Description
63	**Val: error valid**. See: MSR0000_0401[Val].
62	**Overflow: error overflow**. See: MSR0000_0401[Overflow].
61	**UC: error uncorrected**. See: MSR0000_0401[UC].
60	**En: error enable**. See: MSR0000_0401[En].
59	**MiscV: miscellaneous error register valid**. Read-write; Updated-by-hardware. Cold reset: 0. See: MSR0000_0401[MiscV]. 1=Valid thresholding in MSR0000_040B.
58	**AddrV: error address valid**. See: MSR0000_0401[AddrV].
57	**PCC: processor context corrupt**. See: MSR0000_0401[PCC].
56	Reserved.
55	Reserved.
54:47	**Syndrome[7:0]**. Read-write; Updated-by-hardware. Cold reset: 0. The syndrome bits when an ECC error is detected. See Table 230 for when Syndrome[11:0] is valid. Syndrome[11:0] = {Syndrome[11:8], Syndrome[7:0]}. Array — Description L2 Tag — Syndrome[7:0]. WCC Tag — Syndrome[11:0]. L2 Data — Syndrome[8:0]. WCC Data — Syndrome[8:0].
46	**CECC: correctable ECC error**. Read-write; Updated-by-hardware. Cold reset: 0. 1=The error was a correctable ECC error.
45	**UECC: uncorrectable ECC error**. Read-write; updated-by-hardware. Cold reset: 0. 1=The error was an uncorrectable ECC error.
44	**Deferred: deferred error**. See: MSR0000_0401[Deferred].
43	**Poison: poison error**. See: MSR0000_0401[Poison].
42:40	Reserved.
39:36	**Way: cache way in error**. Read-write; Updated-by-hardware.Cold reset: 0. Indicates the cache way in error. See Table 230 for when Way is valid and what ways are valid. Bits — Description 0h — Way 0 1h — Way 1 Eh-2h — Way <Way> Fh — Way 15
35:32	Reserved.
31:28	Reserved.
27:24	**Syndrome[11:8]**. See: MSR0000_0409[Syndrome[7:0]].
23:21	Reserved.

20:16	**ErrorCodeExt: extended error code**. Read-write; updated-by-hardware. Cold reset: 0. See MSR0000_0401[ErrorCodeExt]. See Table 230 for expected values.
15:0	**ErrorCode: error code**. Read-write; Updated-by-hardware. Cold reset: 0. See 2.15.1.5 [Error Code] for details on decoding this field. See Table 230 for expected values.

Table 228: MBE, SBU, and SBC Definitions

Term	Definition
MBE	Multi-bit ECC error, uncorrected.
SBU	Single-bit ECC error, not-corrected. There are some implementation specific conditions when a single bit error is not correctable.
SBC	Single-bit ECC error is detected and correctable.

Table 229: MC2 Error Descriptions

Error Type	Error	Description	CTL[3]	CID[2]	EAC[1]
System Read Data	L2Tlb Prefetch Wcc	An error occurred during an attempted read of data from the NB. Possible reasons include master abort, target abort, and receipt of read data error for TLB. Error Action[4]: None.	RdData	A	D
TLB	TlbPar	Data parity error reading from TLB. Error Action[4]: Invalidate TLB entry.	L2TlbData	A	D
	FillErr	Poison data provided for TLB fill. Error Action[4]: None.	L2TlbPoison	A	D
L2 Cache	Prefetch	Prefetcher request FIFO parity error. Error Action[4]: Invalidate entry (drop prefetch).	L2Prefetch	A	D
L2 Cache	FillEcc	Fill ECC error on data fills. CECC: Corrected data returned to destination; error remains in source. UECC: Poison data returned to destination; error remains in source. The data sources are indicated in LL field and affect what part of Way is valid: Source LL Way WCC L1 [1:0]. See Note 1. L2 L2 [3:0]. NB LG N/A. See Note 2. Notes: 1. WCC: Indicates data corrupted in WCC or Fill Buffer. 2. NB: Note: Data from NB was sent either okay (good ECC) or already poisoned. Indicates data corrupted in Fill Buffer.	FillData	A	D

Table 229: MC2 Error Descriptions

Error Type	Error	Description	CTL[3]	CID[2]	EAC[1]
L2 Cache	FillPar	Fill parity error on instruction fills. SubCase: Description NB->IC: NB to IC parity error: Error Action[4]: Invalidate data and Nack request (IC will re-request). L2->IC: L2 to IC parity error: Error Action[4]: Invalidate data and Nack request (IC will re-request. L2->LS,TLB: L2 to LS or TLB parity error: Error Action[4]: Poison data returned to destination; error remains in source.	FillData	A	D
L2 Cache	PrqAddr	Post Retire Queue address parity error. Error Action[4]: Sync flood.	PrqAddr	A	D
L2 Cache	PrqData	Post Retire Queue data parity error.Error Action[4]: Poison line WCC or line sent to NB.	PrqData	A	D
L2 Cache	WccTag	Write Coalescing Cache tag ECC error. SubCase: Error Action[4] UECC: Sync flood. CECC: Invalidate Wcc tag entry (cleans error).	WccAddr	0	D
L2 Cache	WccData	WCC data ECC error. SubCase: Error Action[4] UECC: Poison copy in WCC. CECC: Corrected copy in WCC.	WccData	A	D
L2 Cache	WcbData	WCB data parity error.Error Action[4]: Poison sent to NB.	WcbData	A	D
L2 Cache	VbData	VB data ECC or parity error. SubCase: Description Par: Parity: Parity error indicated when CECC and UECC are both clear. Error Action[4]: Poison sent to NB. UECC: Error Action[4]: Poison sent to NB. CECC: Single-bit ECC error, corrected: Error Action[4]: Corrected data sent to NB.	VbData	0	D
L2 Cache	L2TagMH	Multiple hits on L2 tag. Error Action[4]: Sync flood.	L2TagMultiHit	0	D

Table 229: MC2 Error Descriptions

Error Type	Error	Description	CTL[3]	CID[2]	EAC[1]
L2 Cache	L2Tag	A correctable or uncorrectable ECC error was seen in the L2 tag. The L2TagMH error signature supersedes the L2Tag error signature if they both occur for the same L2 tag read. SubCase — Description UECC — Error Action[4]: Sync flood. CECC — Error Action[4]: Correct error in array and retry the operation. Hard — A hard correctable error (UC, CECC) was seen in the L2 tag. Error Action[4]: Sync flood.	L2Tag	0	D
L2 Cache	XabAddr	Transaction Address Buffer (XAB) parity error. This error is system fatal; memory coherence may have been affected. Error Action[4]: Sync flood.	XabAddr	A	D
L2 Cache	PrbAddr	Probe buffer address parity error. This error is system fatal; memory coherence may have been affected. Error Action[4]: Sync flood.	PrbAddr	0	D

1. EAC: The error action is taken if detected for all CU errors. D=Error action taken if detected. E=Error action taken if MCA bank enabled. See 2.15.1.3 [Error Detection, Action, Logging, and Reporting].
2. CID: core ID. A=Error reported to the affected core. 0=Error reported to core 0 of the compute unit; see 2.15.1.3 [Error Detection, Action, Logging, and Reporting].
3. See MSR0000_0408.
4. Error Action: Sync flood=Take sync flood if PCC=1. None=No action other than that specified by MCA.

Table 230: MC2 Error Signatures

Error Type	Error Sub-Type	Sub	ErrorCodeExt	Error Code						UC	ADDRV	PCC	Syndrome	Way	CECC	UECC	Deferred	Poison
				Type	UU/PP	T	RRRR	II/TT	LL									
TLB	TlbPar	-	00h	TLB	-	-	-	G	L2	0	1	0	-	[2:0]	0	0	0	0
	FillErr	-	01h							1				-				1
System Read Data	TLB	-	00h	BUS	SRC	0	RD	MEM/IO	L2	1	1	0	-	-	0	0	0	0
	Prefetch		01h					MEM	L2	0								
	Wcc		02h				DWR		L1	1								
L2 Cache	FillEcc	-	04h	MEM	-	-	DRD	D	See[1]	0	1	0	[8:0]	See[1]	0/1	0/1	0/1	0
L2 Cache	FillPar	NB->IC	05h	MEM	-	-	IRD	I	LG	0	0	0	-	-	0	0	0	0
		L2->IC							L2									
		L2->					DRD	D		0	1	0		[3:0]			1	

Table 230: MC2 Error Signatures

Error Type	Error Sub-Type	Sub	ErrorCodeExt	Error Code						UC	ADDRV	PCC	Syndrome	Way	CECC	UECC	Deferred	Poison
				Type	UU/PP	T	RRRR	II/TT	LL									
L2 Cache	Prefetch	-	06h	MEM	-	-	Prefetch	D	L2	0	1	0	-	-	0	0	0	0
	PrqAddr	-	07h				DWR	D	L1	1	0	1	-	-	0	0	0	0
	PrqData	-	08h							0		0					1	
L2 Cache	WccTag	-	09h	MEM	-	-	DWR	D	L1	0/1	1	UC	[11:0]	[1:0]	0/1	0/1	0	0
	WccData	-	0Ah						L1	0	1	0	[8:0]	[1:0]	0/1	0/1	0/1	0
	WcbData	-	0Bh						LG	0		0	-	-	0	0	1	
L2 Cache	VbData	Par	0Ch	MEM	-	-	Probe, Evict	I	L2	0	0	0	-	-	0	0	1	0
		ECC						D					[8:0]		0/1	0/1		
Tag	L2Tag	-	10h	MEM	-	-	GEN	G	L2	0/1	1	UC	[7:0]	[3:0]	0/1	0/1	0	0
		Hard	11h							1	1	1	-	[3:0]	0	0	0	0
	L2Tag	-	12h							1	1	1	-	-	0	0	0	0
	XabAddr	-	13h															
	PrbAddr	-	14h				Probe											

1. LL and Way are specified in Table 229.

MSR0000_040A MC2 Machine Check Address (MC2_ADDR)

Read-write; Updated-by-hardware. Cold reset: 0000_0000_0000_0000h. See 2.15.1 [Machine Check Architecture]. The following table defines the address register as a function of error type.

Bits	Description
63:0	**ADDR**. Read-write; updated-by-hardware. See Table 231.

Table 231: MC2 Address Register

Error Type	Error Sub-Type	Bits	Description
System Read Data Error	-	63:48	Reserved
		47:6	**PhysAddr[47:6]**.
		5:0	Reserved
TLB	TlbPar	63:7	Reserved
		6:0	**Index[6:0]**.
	FillErr 63:48		Reserved
		47:6	**PhysAddr[47:6]**.
		5:0	Reserved
L2 Cache	Prefetch	63:5	Reserved
		4:0	Prefetch FIFO read pointer.

Table 231: MC2 Address Register

Error Type	Error Sub-Type	Bits	Description
L2 Cache	FillEcc, FillPar (SubCase=L2->LS,TLB)	63:48	Reserved
		47:3	**PhysAddr[47:3]**.
		2:0	Reserved
L2 Cache	WccTag, WccData	63:10	Reserved
		9:6	**Index[9:6]**.
		5:0	Reserved
L2 Cache	WcbData	63:48	Reserved
		47:3	**PhysAddr[47:3]**.
		2	Reserved
		1:0	Index[1:0].
Tag	L2Tag, L2TagMH	63:17	Reserved
		16:6	**PhysAddr[16:6]**. Bits Description 1 MB PhysAddr[15:6] valid; [16] Reserved. 2 MB PhysAddr[16:6] valid See CPUID Fn8000_0006_ECX[L2Size]
		5:0	Reserved
Tag	XabAddr	63:5	Reserved
		4:0	XabIndex.
Tag	PrbAddr	63:4	Reserved
		3:0	ProbeBufferIndex.

MSR0000_040B MC2 Machine Check Miscellaneous (MC2_MISC)

Cold reset: 0000_0000_0000_0000h.
See 2.15.1.7 [Error Thresholding].

Bits	Description
63	**Valid**. See: MSR0000_0403[Valid].
62	**CntP: counter present**. See: MSR0000_0403[CntP].
61	**Locked**. See: MSR0000_0403[Locked].
60	**IntP: Interrupt support present.** See: MSR0000_0403[IntP].
59:56	Reserved.
55:52	**LvtOffset: LVT offset**. See: MSR0000_0403[LvtOffset].
51	**CntEn: counter enable**. See: MSR0000_0403[CntEn].
50:49	**IntType: interrupt type**. See: MSR0000_0403[IntType].
48	**Ovrflw: overflow.** See: MSR0000_0403[Ovrflw].
47:44	Reserved.
43:32	**ErrCnt: error counter**. See: MSR0000_0403[ErrCnt].

31:24	**BlkPtr: Block pointer for additional MISC registers**. See: MSR0000_0403[BlkPtr].
23:0	Reserved.

MSR0000_040C MC3 Machine Check Control (MC3_CTL)

Reset: 0000_0000_0000_0000h. Read-only.

Bits	Description
63:0	Unused.

MSR0000_040D MC3 Machine Check Status (MC3_STATUS)

Reset: 0. See MSRC001_0015[McStatusWrEn].

Bits	Description
63:0	Reserved.

MSR0000_040E MC3 Machine Check Address (MC3_ADDR)

Reset: 0000_0000_0000_0000h. Read-only.

Bits	Description
63:0	Reserved.

MSR0000_040F MC3 Machine Check Miscellaneous (MC3_MISC)

Reset: 0000_0000_0000_0000h. Read-only.

Bits	Description
63:0	Reserved.

MSR0000_0410 MC4 Machine Check Control (MC4_CTL)

Read-write; Not-same-for-all. Reset: 0000_0000_0000_0000h.
MSR0000_0410[31:0] is an alias of D18F3x40, which is accessible through PCI configuration space. Only one of these registers exists in multi-core devices; see 3.1.1 [Northbridge MSRs In Multi-Core Products]. Accessibility of this register by non-NBC cores is affected by D18F3x44[NbMcaToMstCpuEn].

See D18F3x44 [MCA NB Configuration] for further NB MCA configuration controls. See 2.15.1 [Machine Check Architecture] for a general description of the machine check architecture. See MSRC001_0048 [NB Machine Check Control Mask (MC4_CTL_MASK)] for the corresponding error mask register.

Bits	Description
63:32	Unused.
31	**McaCpuDatErrEn: Compute Unit data error**. 1=Enables MCA reporting of CPU data errors sent to the NB.
30	Unused.

29:28	Unused.
27	Unused.
26	**NbArrayParEn: northbridge array parity error reporting enable**. IF ((D18F4x118[NbPwrGate1] || D18F4x118[NbPwrGate0] || D18F4x11C[NbPwrGate2])==1) THEN BIOS: 1. ENDIF. 1=Enables reporting of parity errors in the NB arrays.
25	**UsPwDatErrEn: upstream data error enable**. Read-write. 1=Enables MCA reporting of upstream posted writes in which the EP bit is set.
24:18	Unused.
17	**CpPktDatEn: completion packet error reporting enable**. Read-write. 1=Enables MCA reporting of completion packets with the EP bit set.
16	**NbIntProtEn: northbridge internal bus protocol error reporting enable**. Read-write. 1=Enables MCA reporting of protocol errors detected on the northbridge internal bus. When possible, this enable should be cleared before initiating a warm reset to avoid logging spurious errors due to RESET_L signal skew.
15:13	Unused.
12	**WDTRptEn: watchdog timer error reporting enable**. 1=Enables MCA reporting of watchdog timer errors. The watchdog timer checks for NB system accesses for which a response is expected but no response is received. See D18F3x44 [MCA NB Configuration] for information regarding configuration of the watchdog timer duration. This bit does not affect operation of the watchdog timer in terms of its ability to complete an access that would otherwise cause a system hang. This bit only affects whether such errors are reported through MCA.
11	**AtomicRMWEn: atomic read-modify-write error reporting enable**. 1=Enables MCA reporting of atomic read-modify-write (RMW) commands received from an IO link. Atomic RMW commands are not supported. An atomic RMW command results in a link error response being generated back to the requesting IO device. The generation of the link error response is not affected by this bit.
10	Unused.
9	**TgtAbortEn: target abort error reporting enable**. 1=Enables MCA reporting of target aborts to a link. The NB returns an error response back to the requestor with any associated data all 1s independent of the state of this bit.
8	**MstrAbortEn: master abort error reporting enable**. 1=Enables MCA reporting of master aborts to a link. The NB returns an error response back to the requestor with any associated data all 1s independent of the state of this bit.
7:6	Unused.
5	**SyncPktEn: link sync packet error reporting enable**. 1=Enables MCA reporting of link-defined sync error packets detected on link. The NB floods its outgoing link with sync packets after detectinga sync packet on the incoming link independent of the state of this bit.
4:2	Unused.
1	**UECCEn: uncorrectable ECC error reporting enable**. 1=Enables MCA reporting of DDR3 DRAM uncorrectable ECC errors which are detected in the NB. In some cases data may be forwarded to the core prior to checking ECC in which case the check takes place in one of the other error reporting banks.
0	**CECCEn: correctable ECC error reporting enable**. 1=Enables MCA reporting of DDR3 DRAM correctable ECC errors which are detected in the NB.

MSR0000_0411 MC4 Machine Check Status (MC4_STATUS)

Not-same-for-all. Cold reset: 0000_0000_0000_0000h.
MSR0000_0411[63:32] is an alias of D18F3x4C, and MSR0000_0411[31:0] is an alias of D18F3x48. Only one of these registers exists in multi-core devices; see 3.1.1 [Northbridge MSRs In Multi-Core Products]. Accessibility of this register by non-NBC cores is affected by D18F3x44[NbMcaToMstCpuEn]. See MSRC001_0015[McStatusWrEn] for information on writing to this register. See 2.15.1 [Machine Check Architecture] for machine check architecture background.

Table 232 describes each error type. Table 233 and Table 234 describe the error codes and status register settings for each error type.

Bits	Description
63	**Val: valid**. See: MSR0000_0401[Val].
62	**Overflow: error overflow**. See: MSR0000_0401[Overflow].
61	**UC: error uncorrected**. See: MSR0000_0401[UC].
60	**En: error enable**. See: MSR0000_0401[En].
59	**MiscV: miscellaneous error register valid**. Read-write; Updated-by-hardware. 1=Valid thresholding in MSR0000_0413 or MSRC000_0408.
58	**AddrV: error address valid**. See: MSR0000_0401[AddrV].
57	**PCC: processor context corrupt**. See: MSR0000_0401[PCC].
56	**ErrCoreIdVal: error core ID is valid**. Read-write; set-by-hardware. 1=The ErrCoreId field is valid.
55	Reserved.
54:47	**Syndrome[7:0]**. Read-write. The syndrome bits when an ECC error is detected. See Table 234 Valid Syndrome column for which bits are valid for each error.
46	**CECC: correctable ECC error**. Read-write; Updated-by-hardware. 1=The error was a correctable ECC error according to the restrictions of the ECC algorithm. UC indicates whether the error was actually corrected by the processor.
45	**UECC: uncorrectable ECC error**. Read-write; Updated-by-hardware. 1=The error was an uncorrectable ECC error according to the restrictions of the ECC algorithm. UC indicates whether the error was actually corrected by the processor.
44	**Deferred: deferred error**. Read-write; Updated-by-hardware. 1=A deferred error was created. A deferred error is the result of an uncorrectable data error which did not immediately cause a processor exception; the data is poisoned and an exception is deferred until the data is consumed.
43:42	Reserved.
41	**SubLink: sublink**. Read-write; set-by-hardware. For errors associated with a link, this bit indicates if the error was associated with the upper or lower byte of the link. 0=Sublink [7:0]. 1=Sublink [15:8].
40	**Scrub: error detected on a scrub**. Read-write; Set-by-hardware.
39:37	Reserved.
36	**Link**. Read-write; set-by-hardware. For errors associated with a link, this field indicates that the link was associated with the error.
35:32	**ErrCoreId: error associated with core N**. Read-write; updated-by-hardware. When ErrCoreIdVal=1 this field indicates which core within the processor is associated with the error; otherwise this field is reserved. All values greater than D18F5x84[CmpCap] are reserved.

31:24	Reserved.
23:21	Reserved.
20:16	**ErrorCodeExt: extended error code**. Read-write; Updated-by-hardware. See MSR0000_0401[ErrorCodeExt]. See Table 233 for values.
15:0	**ErrorCode: error code**. Read-write; Updated-by-hardware. See 2.15.1.5 [Error Code].

Table 232: MC4 Error Descriptions

Error Type	Description	CTL[1]	ETG[2]	EAC[4]
Sync Error	Link-defined sync error packets detected on link. The NB floods its outgoing links with sync packets after detecting a sync packet on an incoming link independent of the state of the control bits.	SyncPktEn	L	D
Master Abort	Master abort seen as result of link operation. Reasons for this error include requests to non-existent addresses. The NB returns an error response back to the requestor with any associated data all 1s independent of the state of the control bit.	MstrAbortEn	L	D
Target Abort	Target abort seen as result of link operation. The NB returns an error response back to the requestor with any associated data all 1s independent of the state of the control bit.	TgtAbortEn	L	D
RMW Error	An atomic read-modify-write (RMW) command was received from an IO link. Atomic RMW commands are not supported. An atomic RMW command results in a link error response being generated back to the requesting IO device. The generation of the link error response is not affected by the control bit.	AtomicRMWEn	L	D
WDT Error	NB WDT timeout due to lack of progress. The NB WDT monitors transaction completions. A transaction that exceeds the programmed time limit reports errors via the MCA. The cause of error may be another node or device which failed to respond.	WDTRptEn	L	D
DRAM ECC Error	A DRAM ECC error detected.	CECCEn, UECCEn	D	D
Link Data Error	Data error detected on link. If enabled for reporting and the request is sourced from a core, then PCC is set. (If not enabled for reporting, PCC is not set. If configured to allow an error response to be returned to the core, this could allow error containment to a scope smaller than the entire system.)	McaUsPwDatErrEn, CpPktDatEn	L	D

Table 232: MC4 Error Descriptions

Error Type	Description	CTL[1]	ETG[2]	EAC[4]
Protocol Error	Protocol error detected by link. These errors are distinguished from each other by the value in MSR0000_0412[ErrAddr]. See Table 236. For protocol errors, the system cannot continue operation. Protocol errors can be caused by other subcomponents than the one reporting the error. For diagnosis, collect and examine MCA registers from other banks, cores, and processors in the system.	NbIntProtEn	L[3]	D
NB Array Error	A parity error was detected in the NB internal arrays.	NbArrayParEn	-	D
Compute Unit Data Error	NB received a data error from a core and this error could not be contained. For the cause of the data error, examine the core MCA registers for deferred errors. This error may occur for the following types of data writes: • APIC • Configuration space (IO and MMIO) For these errors, sync flood will occur if D18F3x180[SyncFloodOnCpuLeakErr] is set.	McaCpuDatErrEn	-	D

1. CTL: See MSR0000_0410.
2. ETG: error threshold group. See 2.15.1.7 [Error Thresholding].
   - L=Link.
   - D=DRAM.
3. The error thresholding group is Link if link protocol error; none for non-link protocol error.
4. EAC: D=Error action taken if detected. E=Error action taken if MCA bank enabled.

The NB is capable of reporting the following errors:

Table 233: MC4 Error Signatures, Part 1

Error Type	ErrorCode-Ext	Error Code					
		Type	PP	T	RRRR	II/TT	LL
Reserved 00h		-	-	-	-	-	-
Reserved	01h	-	-	-	-	-	-
Sync Error	02h	BUS	OBS	0	GEN	GEN	LG
Mst Abort	03h	BUS	SRC/OBS	0	RD/WR	MEM/IO[1]	LG
Tgt Abort	04h	BUS	SRC/OBS	0	RD/WR	MEM/IO[1]	LG
RMW Error	06h	BUS	OBS	0	GEN	IO	LG
WDT Error	07h	BUS	GEN	1	GEN	GEN	LG
ECC Error	08h	BUS	SRC/RES	0	RD/WR	MEM	LG
Link Data Error	0Ah	BUS	SRC/OBS	0	RD/WR/ DWR	MEM/IO	LG
NB Protocol Error	0Bh		OBS	0	GEN	GEN	LG
NB Array Error	0Ch		OBS	0	GEN	GEN	LG
Compute Unit Data Error	19h	MEM	-	-	WR	Data	LG

Table 233: MC4 Error Signatures, Part 1

Error Type	ErrorCode-Ext	Error Code					
		Type	PP	T	RRRR	II/TT	LL

1. Indicates the type of link attached to the reporting NB, not the instruction type. MEM indicates coherent link, IO indicates IO link.

Table 234: MC4 Error Signatures, Part 2

Error Type	UC	AddrV	PCC	Syndrome Valid	CECC	UECC	Deferred	Scrub	Link	Err CoreId
Sync Error	1	0	1	-	0	0	0	0	Y	-
Mst Abort	1	1	Core[5]	-	0	0	0	0	Y	Y
Tgt Abort	1	1	Core[5]	-	0	0	0	0	Y	Y
RMW Error	1	1	0	-	0	0	0	0	Y	-
WDT Error	1	0[1] 1[2]	1	-	0	0	0	0	-	-
ECC Error	MS[6]	1	MS[4]& Core[5]	15:0	~MS| Hist[7]	~MS| Hist[7]	0	1/0	-	-
Link Data Error	~Deferred[11]	1	0	-	0	0	0/1	0	Y	-
NB Protocol Error	1	1/0[2]	1	-	0	0	0	0	Y	-
NB Array Error	~Deferred[6]	1[4]	~Deferred[6]	-	0	0	0/1	0	-	-
Compute Unit Data Error	1	0	1	-	0	0	0	0	-	Y

1. See Table 240 [Format of MSR0000_0412[ErrAddr[47:1]] for Watchdog Timer Errors].
2. See Table 236 [Format of MSR0000_0412[ErrAddr[47:1]] for Protocol Errors].
3. See Table 239 [Valid Values for ArrayErrorType].
4. MS: multi-symbol. 1=Multi-symbol. 0=Not multi-symbol.
5. Core: source is core. 1=Source is core. 0=Source is not core.
6. Deferred: error is deferred. 1=Error is deferred. 0=Error is not deferred.
7. Hist: Error was detected by the hardware-managed history scheme.

MSR0000_0412 MC4 Machine Check Address (MC4_ADDR)

IF (D18F3x44[NbMcaToMstCpuEn] && !NBC) THEN RAZ; Per-node; not-same-for-all. ELSE Read-write; Per-node; not-same-for-all. ENDIF. Cold reset: 0000_0000_0000_0000h. See 2.15.1 [Machine Check Architecture]. MSR0000_0412[31:0] is an alias of D18F3x50. MSR0000_0412[63:32] is an alias of D18F3x54. Only one of these registers exists in multi-core devices; see 3.1.1 [Northbridge MSRs In Multi-Core Products]. ErrAddr[47:1] carries supplemental information associated with a machine check error, generally the address being accessed. Accessibility of this register by non-NBC cores is affected by D18F3x44[NbMcaToMstCpuEn]. The format of ErrAddr[47:1] is a function of

MSR0000_0411[ErrorCodeExt]; See ErrAddr[47:1].

Bits	Description
63:48	Reserved. Value: 00h.
47:32	**ErrAddr[47:32]: Error Address Bits[47:32]**. See: ErrAddr[31:1].
31:1	**ErrAddr[31:1]: Error Address Bits[31:1]**. ErrAddr[47:0] = {MSR0000_0412[ErrAddr[47:32]], MSR0000_0412[ErrAddr[31:1]], MSR0000_0412[ErrAddr[0]]}. See the tables below for the encoding.
0	**ErrAddr[0]: Error Address Bit[0]**.

The register format depends on the type of error being logged:
- Protocol errors contain the error reason code, may contain the physical address, and are formatted according to Table 236.
- NB array errors indicate the array in error, and are formatted according to Table 238.
- NB Watchdog timer errors depend on the mode selected by D18F3x180[McaLogErrAddrWdtErr], and the format is indicated by D18F3x4C[AddrV]. If D18F3x4C[AddrV] is indicated, errors are formatted according to Table 235. If D18F3x4C[AddrV] is not indicated, errors are formatted according to Table 240.
- All other NB errors which indicate D18F3x4C[AddrV] are formatted according to Table 235.

Table 235: Format of MSR0000_0412[ErrAddr[47:1]] for All Other Errors

Bits	Description
47:1	**PhysAddr[47:1]**.

Table 236: Format of MSR0000_0412[ErrAddr[47:1]] for Protocol Errors

Bits	Description
47:6	**PhysAddr[47:6]**. Valid of (MSR0000_0411[AddrV]==1); otherwise reserved.
5:1	**ProtocolErrorType**. See Table 237 [Valid Values for ProtocolErrorType].

Table 237: Valid Values for ProtocolErrorType

Bits	Description
00h	Link: SRQ Read Response without matching request.
01h	Link: Probe Response without matching request.
02h	Link: TgtDone without matching request.
03h	Link: TgtStart without matching request.
04h	Link: Command buffer overflow.
05h	Link: Data buffer overflow.
06h	Link: Link retry packet count acknowledge overflow.
07h	Link: Data command in the middle of a data transfer.
08h	Link: Link address extension command followed by a packet other than a command with address.
09h	Link: A specific coherent-only packet from a CPU was issued to an IO link.

Table 237: Valid Values for ProtocolErrorType

Bits	Description
0Ah	Link: A command with invalid encoding was received. This error occurs when: 1. Any invalid command is received (including a command with no valid encoding or a coherent link command over an IO link or vice versa) while not in retry mode. 2. Any illegal command is received in which the CRC is correct while in retry mode (including any upstream broadcast command (link command encoding = 11101xb)).
0Bh	Link: Link CTL deassertion occurred when a data phase was not pending. This error condition may only occur when error-retry mode is not enabled (if it is enabled, this condition triggers a retry).
0Fh-0Ch	Reserved.
1Fh-10h	Reserved.

Table 238: Format of MSR0000_0412[ErrAddr[47:1]] for NB Array Errors

Bits	Description
47:6	Reserved.
5:1	**ArrayErrorType**. See Table 239 [Valid Values for ArrayErrorType].

Table 239: Valid Values for ArrayErrorType

Bits	Description
00h	SRA: System request address.
01h	SRD: System request data.
02h	SPB: System packet buffer.
03h	MCD: Memory controller data.
04h	MPB: Memory packet buffer.
05h	LPB0: Link 0 packet buffer.
08h-06h	Reserved.
09h	MPBC: Memory controller command packet buffer.
0Ah	MCDBM: Memory controller byte mask.
0Bh	MCACAM: Memory controller address array.
0Ch	DMAP: Extended DRAM address map.
0Dh	MMAP: Extended MMIO address map.
0Eh	X86MAP: Extended PCI/IO address map.
0Fh	CFGMAP: Extended config address map.
17h-10h	Reserved.
18h	SRIMCTRTE: SRI/MCT extended routing table.
1Ch-19h	Reserved.
1Dh	TCB: TCB array.
1Fh-1Eh	Reserved.

Table 240: Format of MSR0000_0412**[**ErrAddr[47:1]**] for** Watchdog Timer Errors

Bits	Description
47:40	**CoreId**. Indicates the core ID if the SourcePointer specifies Core. Bits: Description 07h-00h: CoreId FFh-08h: Reserved
39:36	**SystemResponseCount**. This field records unspecified, implementation-specific information.
35:31	**WaitCode**. records unspecified, implementation-specific information (all zeroes means no waiting condition).
30	**WaitForPostedWrite**.
29:27	**DestinationNode**. Records the Node ID of the node addressed by the transaction.
26:25	**DestinationUnit**. Bits: Description 00b: Core 01b: Extended Core 10b: Memory Controller 11b: Host
24:22	**SourceNode**. Records the Node ID of the node originating the transaction.
21:20	**SourceUnit**. (same encoding as Destination Unit)
19:15	**SourcePointer**. Identifies crossbar source: Bits: Description 00h: SRI HostBridge. 03h-01h: Reserved. 04h: Core. See CoreId. 07h-05h: Reserved. 08h: Memory controller. 0Fh-09h: Reserved. 1Fh-10h: Link. Link HH; sublink N (where N=0b for ganged links). All unused codes are reserved.
14:11	**SrqEntryState**. Records unspecified, implementation-specific information (all zeroes means idle).
10:7	**OpType**. Records unspecified, implementation-specific information.
6:1	**LinkCommand**. When the NB WDT expires, the link command of the transaction that timed out is captured here. This field is encoded identically to the “Code” field for link transactions defined in the link specification.

MSR0000_0413 NB Machine Check Misc 4 (DRAM Thresholding) 0 (MC4_MISC0)

MSR0000_0413 is the first of the NB machine check miscellaneous registers. MSR0000_0413 is associated with the DRAM error type. To see the remaining NB machine check miscellaneous registers, refer to MSRC000_0408. Only one of these registers exists in multi-core devices; see 3.1.1 [Northbridge MSRs In Multi-Core Products].

Bits	Description

63	**Valid**. IF (D18F3x44[NbMcaToMstCpuEn] && !NBC) THEN RAZ; Per-node; not-same-for-all. ELSEIF (MSRC001_0015[McStatusWrEn]) THEN Read-write; Per-node; not-same-for-all. ELSE Read-only; Per-node; not-same-for-all. Reset: 1. ENDIF. 1=The CntP field is present.
62	**CntP: counter present**. IF (D18F3x44[NbMcaToMstCpuEn] && !NBC) THEN RAZ; Per-node; not-same-for-all. ELSEIF (MSRC001_0015[McStatusWrEn]) THEN Read-write; Per-node; not-same-for-all. ELSE Read-only; Per-node; not-same-for-all. Reset: 1. ENDIF. 1=A valid threshold counter is present.
61	**Locked**. IF (D18F3x44[NbMcaToMstCpuEn] && !NBC) THEN RAZ; Per-node; not-same-for-all. ELSEIF (MSRC001_0015[McStatusWrEn]) THEN Read-write; Per-node; not-same-for-all. ELSE Read-only; Per-node; not-same-for-all. Reset: 0. ENDIF. BIOS: IF (IntType==10b) THEN 1. ELSE 0. ENDIF. 1=Writes to bits [55:32] of this register are ignored. Set by BIOS to indicate that this register is not available for OS use. When MSRC001_0015[McStatusWrEn] is set, MSR writes to this register update all bits, regardless of the state of the Locked bit.
60:56	Reserved.
55:52	**LvtOffset: LVT offset**. IF (D18F3x44[NbMcaToMstCpuEn] && !NBC) THEN RAZ; Per-node; not-same-for-all. ELSEIF (MSRC001_0015[McStatusWrEn] | ~MSR0000_0413[Locked]) THEN Read-write; Per-node; not-same-for-all. ELSE Read-only; Per-node; not-same-for-all. Reset: 0h. ENDIF. Specifies the address of the LVT entry in the APIC registers as follows: LVT address = (LvtOffset shifted left 4 bits) + 500h (see APIC[530:500]). Bits — Description 3h-0h — See APIC[530:500]. Fh-4h — Reserved
51	**CntEn: counter enable**. IF (D18F3x44[NbMcaToMstCpuEn] && !NBC) THEN RAZ; Per-node; not-same-for-all. ELSEIF (MSRC001_0015[McStatusWrEn] | ~Locked) THEN Read-write; Per-node; not-same-for-all. ELSE Read-only; Per-node; not-same-for-all. Reset: 0. ENDIF. 1=Count thresholding errors. See 2.15.1.7 [Error Thresholding].
50:49	**IntType: interrupt type**. IF (D18F3x44[NbMcaToMstCpuEn] && !NBC) THEN RAZ; Per-node; not-same-for-all. ELSEIF (MSRC001_0015[McStatusWrEn] | ~MSR0000_0413[Locked]) THEN Read-write; Per-node; not-same-for-all. ELSE Read-only; Per-node; not-same-for-all. Cold reset: 0. ENDIF. Specifies the type of interrupt signaled when Ovrflw is set. Bits — Description 00b — No Interrupt. 01b — APIC. APIC based interrupt (see LvtOffset above) to all cores. 10b — SMI. SMI trigger event (always routed to CpuCoreNum 0, as defined in 2.4.4 [Processor Cores and Downcoring]); see 2.4.10.2.3 [SMI Sources And Delivery]. 11b — Reserved.
48	**Ovrflw: overflow.** IF (D18F3x44[NbMcaToMstCpuEn] && !NBC) THEN RAZ; Per-node; not-same-for-all. ELSEIF (MSRC001_0015[McStatusWrEn] | ~Locked) THEN Read-write; Per-node; not-same-for-all; set-by-hardware. ELSE Read-only; Per-node; not-same-for-all; set-by-hardware. Cold reset: 0. ENDIF. Set by hardware when ErrCnt transitions from FFEh to FFFh. When this bit is set, the interrupt selected by the IntType field is generated.
47:44	Reserved.

43:32	**ErrCnt: error counter**. IF (D18F3x44[NbMcaToMstCpuEn] && !NBC) THEN RAZ; Per-node; not-same-for-all. ELSEIF (MSRC001_0015[McStatusWrEn] | ~Locked) THEN Read-write; Per-node; not-same-for-all; updated-by-hardware. ELSE Read-only; Per-node; not-same-for-all; updated-by-hardware. Cold reset: 0. ENDIF. Written by software to set the starting value of the error counter. Incremented by hardware when errors are logged. Saturates at FFFh (no rollover). The threshold value, written by software, is (FFFh - the desired error count (the number of errors necessary in order for an interrupt to be taken)).
31:24	**BlkPtr: Block pointer for additional MISC registers**. Read-only. Value: 01h. 01h=Extended MC4_MISC MSR block is valid. See MSRC000_0408.
23:0	Reserved.

MSR0000_0414 MC5 Machine Check Control (MC5_CTL)

Read-write. Reset: 0000_0000_0000_0000h. See 2.15.1 [Machine Check Architecture]. See MSRC001_0049 [EX Machine Check Control Mask (MC5_CTL_MASK)].

Bits	Description
63:16	Unused.
15	Unused.
14	Unused.
13	**STATQ: retire status queue parity**.
12	**DE: DE error**.
11	**FRF: flag register file parity**.
10	**AG1PRF: physical register file AG1 port parity**.
9	**AG0PRF: physical register file AG0 port parity**.
8	**EX1PRF: physical register file EX1 port parity**.
7	**EX0PRF: physical register file EX0 port parity**.
6	**MAP: mapper checkpoint array parity**.
5	**RETDISP: retire dispatch queue parity**.
4	**IDF: IDRF array parity**.
3	**PLDEX: EX payload array parity**.
2	**PLDAG: AG payload array parity**.
1	Reserved.
0	**WDT: core watchdog timer**. See MSRC001_0074 [CPU Watchdog Timer (CpuWdtCfg)].

MSR0000_0415 MC5 Machine Check Status (MC5_STATUS)

Cold reset: 0000_0000_0000_0000h. See 2.15.1 [Machine Check Architecture]. See MSRC001_0015[McStatusWrEn]. Table 241 describes each error type. Table 242 describes the error codes and status register settings for each error type.

Bits	Description
63	**Val: error valid**. See: MSR0000_0401[Val].
62	**Overflow: error overflow**. See: MSR0000_0401[Overflow].
61	**UC: error uncorrected**. See: MSR0000_0401[UC].
60	**En: error enable**. See: MSR0000_0401[En].
59	**MiscV: miscellaneous error register valid**. Read-write; Updated-by-hardware. See: MSR0000_0401[MiscV]. 1=Valid thresholding in MSR0000_0417.
58	**AddrV: error address valid**. See: MSR0000_0401[AddrV]. 1=Valid address in MSR0000_0416.
57	**PCC: processor context corrupt**. See: MSR0000_0401[PCC].
56:24	Reserved.
23:21	Reserved.
20:16	**ErrorCodeExt: extended error code**. Read-write; Updated-by-hardware. See MSR0000_0401[ErrorCodeExt]. See Table 242 for values.
15:0	**ErrorCode: error code**. Read-write; Updated-by-hardware. See 2.15.1.5 [Error Code]. See Table 242.

Table 241: MC5 Error Descriptions

Error Type	Error Sub-type	Description	CTL[1]	EAC[3]
WDT error	-	The WDT timer has expired. See MSRC001_0074 [CPU Watchdog Timer (CpuWdtCfg)].	WDT	E
Internal	Wakeup array dest tag parity	A parity error occurred in the wakeup array.	PICWAK	D

Table 241: MC5 Error Descriptions

Error Type	Error Sub-type	Description	CTL[1]	EAC[3]
Internal	AG payload array parity	A parity error occurred in the address generator payload array.	PLDAG	D
	EX payload array parity	A parity error occurred in the EX payload array.	PLDEX	D
	IDRF array parity	A parity error occurred in the immediate displacement register file.	IDF	D
	Retire dispatch queue parity	A parity error occured in the retire dispatch queue. This error causes the processor to enter the Shutdown state; 2.15.1.3.1 [MCA conditions that cause Shutdown].	RETDISP	E
	Mapper checkpoint array parity	A parity error occured in the mapper checkpoint array. This error causes the processor to enter the Shutdown state if UC=1; 2.15.1.3.1 [MCA conditions that cause Shutdown].	MAP	D
	EX0PRF parity	A parity error occurred in the physical register file's EX0 port.	EX0PRF	D
	EX1PRF parity	A parity error occurred in the physical register file's EX1 port.	EX1PRF	D
	AG0PRF parity	A parity error occurred in the physical register file's AG0 port.	AG0PRF	D
	AG1PRF parity	A parity error occurred in the physical register file's AG1 port.	AG1PRF	D
	Flag register file parity	A parity error occurred in the flag register file.	FRF	D
	DE error	A DE error occurred.	DE	E
Internal	Retire status queue parity	A parity error occurred in the retire status queue. This error causes the processor to enter the Shutdown state; 2.15.1.3.1 [MCA conditions that cause Shutdown]	STATQ	D

1. CTL: See MSR0000_0414.
2. CID: core ID. All EX errors are reported to the affected core; see 2.15.1.3 [Error Detection, Action, Logging, and Reporting].
3. EAC: D=Error action taken if detected. E=Error action taken if MCA bank enabled.See 2.15.1.3 [Error Detection, Action, Logging, and Reporting].

Table 242: MC5 Error Signatures

Error Type	Error Sub-Type	ErrorCodeExt	Error Code						UC	ADDRV	MISCV	PCC	CECC	UECC
			Type	UU/PP	TT	RRRR	II/TT	LL						
WDT error	-	00h	BUS	GEN	1	GEN	GEN	LG	1	1	1	1	0	0
Internal error	Wakeup array dest tag parity	01h	BUS	GEN	0	GEN	GEN	LG	1/0	0	0	0	0	0

Table 242: MC5 Error Signatures

Error Type	Error Sub-Type	ErrorCodeExt	Error Code						UC	ADDRV	MISCV	PCC	CECC	UECC
			Type	UU/PP	TT	RRRR	II/TT	LL						
Internal error	AG payload array parity	02h	BUS	GEN	0	GEN	GEN	LG	1/0	1	0	0	0	0
	EX payload array parity	03h							1/0	1	0	0	0	0
	IDRF array parity	04h							1/0	1	0	0	0	0
	Retire dispatch queue parity	05h							1[1]	1	0	0	0	0
	Mapper checkpoint array parity	06h							1/0[2]	1	0	0	0	0
	EX0PRF parity	07h							1/0	0	0	0	0	0
	EX1PRF parity	08h							1/0	0	0	0	0	0
	AG0PRF parity	09h							1/0	0	0	0	0	0
	AG1PRF parity	0Ah							1/0	0	0	0	0	0
	Flag register file parity	0Bh							1/0	0	0	0	0	0
	DE error	0Ch							1/0[2]	0	0	0	0	0
Internal error	Retire status queue parity	0Dh	BUS	GEN	0	GEN	GEN	LG	1[1]	1	0	1/0[3]	0	0

1. Causes shutdown.
2. Causes shutdown if UC=1.
3. STATQ sets PCC=1 if a store retired in last 3 cycles or FpTokenRet bits mismatch.

MSR0000_0416 MC5 Machine Check Address (MC5_ADDR)

Read-write; Updated-by-hardware. Cold reset: 0000_0000_0000_0000h. The MCi_ADDR register contains valid data if indicated by MCi_STATUS[AddrV]. See 2.15.1 [Machine Check Architecture]. The register format depends on the type of error being logged.

Bits	Description
63:0	**ADDR**. See Table 243.

The following tables define the address register as a function of error type.

Table 243: MC5 Address Register

Error Type	Error Sub-Type	Bits	Description
WDT	- (ErrorCodeExt=00h)	63:48	Reserved
		47:0	**LogAddr[47:0]**. Logical address of the next instruction after the last instruction retired.

Table 243: MC5 Address Register

Error Type	Error Sub-Type	Bits	Description
Internal	AG payload array parity (ErrorCodeExt=02h), EX payload array parity (ErrorCodeExt=03h), IDRF array parity (ErrorCodeExt=04h)	63:6	Reserved
		5:0	**SchedulerQID**.
Internal	Retire dispatch queue parity (ErrorCodeExt=05h)	63:7	Reserved
		6:0	**RetirementID**.
Internal	STATQ parity (ErrorCodeExt=0Dh)	63:7	Reserved
		6:0	**RetirementID**.
Internal	Mapper checkpoint array parity (ErrorCodeExt=06h)	63:6	Reserved
		5:0	**CheckpointID**.

MSR0000_0417 MC5 Machine Check Miscellaneous (MC5_MISC)

Cold reset: 0000_0000_0000_0000h. This register records unspecified, implementation-specific status bits when an FR machine check error is logged.
See 2.15.1.7 [Error Thresholding].

Bits	Description
63	**Valid**. See: MSR0000_0403[Valid].
62	**CntP: counter present**. See: MSR0000_0403[CntP].
61	**Locked**. See: MSR0000_0403[Locked].
60	**IntP: Interrupt support present.** See: MSR0000_0403[IntP].
59:56	Reserved.
55:52	**LvtOffset: LVT offset**. See: MSR0000_0403[LvtOffset].
51	**CntEn: counter enable**. See: MSR0000_0403[CntEn].
50:49	**IntType: interrupt type**. See: MSR0000_0403[IntType].
48	**Ovrflw: overflow.** See: MSR0000_0403[Ovrflw].
47:44	Reserved.
43:32	**ErrCnt: error counter**. See: MSR0000_0403[ErrCnt].
31:24	**BlkPtr: Block pointer for additional MISC registers**. See: MSR0000_0403[BlkPtr].
23:0	Reserved.

MSR0000_0418 MC6 Machine Check Control (MC6_CTL)

Per-compute-unit; Read-write. Reset: 0000_0000_0000_0000h. See 2.15.1 [Machine Check Architecture]. See MSRC001_004A [FP Machine Check Control Mask (MC6_CTL_MASK)].

Bits	Description
63:7	Unused.

6	Unused.
5	**SRF: status register file parity error**.
4	**RetireQ: retire queue parity error**.
3	Unused.
2	**Sched: scheduler table parity error**.
1	**FreeList: free list parity error**.
0	**PRF: physical register file parity error**.

MSR0000_0419 MC6 Machine Check Status (MC6_STATUS)

See 2.15.1 [Machine Check Architecture]. See MSRC001_0015[McStatusWrEn]. Table 244 describes each error type. Table 245 describes the error codes and status register settings for each error type.

Bits	Description
63	**Val: valid**. See: MSR0000_0401[Val].
62	**Overflow: error overflow**. See: MSR0000_0401[Overflow].
61	**UC: error uncorrected**. See: MSR0000_0401[UC].
60	**En: error enable**. See: MSR0000_0401[En].
59	**MiscV: miscellaneous error register valid**. Read-only. Value: 0. See: MSR0000_0401[MiscV].
58	**AddrV: error address valid**. Read-only. Value: 0. See: MSR0000_0401[AddrV].
57	**PCC: processor context corrupt**. See: MSR0000_0401[PCC].
56:21	Reserved.
20:16	**ErrorCodeExt: extended error code**. Read-write; Updated-by-hardware. Logs an extended error code when an error is detected. This model-specific field is used in conjunction with ErrorCode to identify the error sub-type for root cause analysis (see 2.15.1.5 [Error Code]). See Table 245 for expected values.
15:0	**ErrorCode: error code**. Read-write; Updated-by-hardware. See 2.15.1.5 [Error Code] for details on decoding this field. See Table 245 for expected values.

Table 244: MC6 Error Descriptions

Error Type	Error	Description[2]	CTL[4]	CID[3]	EAC[1]
Floating Point Unit	Physical Register File	A parity error occurred in the Physical Register File (PRF).	PRF	0	E
	Status Register File	A parity error occurred in the Status Register File (SRF).	SRF	A	E
	Free List	A parity error occurred on the Free List.	FreeList	0	E
	Retire Queue	A parity error occurred in the Retire Queue.	RetireQ	0	E
	Scheduler	A parity error occurred in the Scheduler table.	Sched	0	E

Table 244: MC6 Error Descriptions

Error Type	Error	Description[2]	CTL[4]	CID[3]	EAC[1]
1. EAC: D=Error action taken if detected. E=Error action taken if MCA bank enabled. See 2.15.1.3 [Error Detection, Action, Logging, and Reporting]. 2. All FP errors are system fatal and result in a sync flood. 3. CID: core ID. A=Error reported to the affected core. 0=Error reported to core 0 of the compute unit; see 2.15.1.3 [Error Detection, Action, Logging, and Reporting]. 4. See MSR0000_0418.					

Table 245: MC6 Error Signatures

Error Type	Error Sub-Type	ErrorCodeExt	Error Code						UC	ADDRV	PCC
			Type	UU/PP	T	RRRR	II	LL			
Floating Point Unit	Status Register File	00101b	BUS	GEN	0	GEN	GEN	LG	1	0	1
	Physical Register File	00010b									
	Free List	00001b									
	Retire Queue	00011b									
	Scheduler	00100b									

MSR0000_041A MC6 Machine Check Address (MC6_ADDR)

Reset: 0000_0000_0000_0000h. Read-only. See 2.15.1 [Machine Check Architecture].

Bits	Description
63:0	Reserved.

MSR0000_041B MC6 Machine Check Miscellaneous (MC6_MISC)

Reset: 0000_0000_0000_0000h. Read-only. See 2.15.1 [Machine Check Architecture].

Bits	Description
63:0	Reserved.

3.20 MSRs - MSRC000_0xxx

MSRC000_0080 Extended Feature Enable (EFER)

SKINIT Execution: 0000_0000_0000_0000h.

Bits	Description
63:16	MBZ.
15	**TCE: translation cache extension enable**. Read-write. Reset: 0. 1=Translation cache extension is enabled.
14	**FFXSE: fast FXSAVE/FRSTOR enable**. Read-write. Reset: 0. 1=Enables the fast FXSAVE/FRSTOR mechanism. A 64-bit operating system may enable the fast FXSAVE/FRSTOR mechanism if (CPUID Fn8000_0001_EDX[FFXSR]==1)). This bit is set once by the operating system and its value is not changed afterwards.
13	**LMSLE: long mode segment limit enable**. Read-write. Reset: 0. 1=Enables the long mode segment limit check mechanism.
12	**SVME: secure virtual machine (SVM) enable**. IF (MSRC001_0114[SvmeDisable]==1) THEN MBZ. ELSE Read-write. ENDIF. Reset: 0. 1=SVM features are enabled.
11	**NXE: no-execute page enable**. Read-write. Reset: 0. 1=The no-execute page protection feature is enabled.
10	**LMA: long mode active**. Read-only. Reset: 0. 1=Indicates that long mode is active.
9	MBZ.
8	**LME: long mode enable**. Read-write. Reset: 0. 1=Long mode is enabled.
7:1	RAZ.
0	**SYSCALL: system call extension enable**. Read-write. Reset: 0. 1=SYSCALL and SYSRET instructions are enabled. This adds the SYSCALL and SYSRET instructions which can be used in flat addressed operating systems as low latency system calls and returns.

MSRC000_0081 SYSCALL Target Address (STAR)

Reset: 0000_0000_0000_0000h. This register holds the target address used by the SYSCALL instruction and the code and stack segment selector bases used by the SYSCALL and SYSRET instructions.

Bits	Description
63:48	**SysRetSel: SYSRET CS and SS**. Read-write.
47:32	**SysCallSel: SYSCALL CS and SS**. Read-write.
31:0	**Target: SYSCALL target address**. Read-write.

MSRC000_0082 Long Mode SYSCALL Target Address (STAR64)

Reset: 0000_0000_0000_0000h.

Bits	Description
63:0	**LSTAR: long mode target address**. Read-write. Target address for 64-bit mode calling programs. The address stored in this register must be in canonical form (if not canonical, a #GP fault occurs).

MSRC000_0083 Compatibility Mode SYSCALL Target Address (STARCOMPAT)

Reset: 0000_0000_0000_0000h.

Bits	Description
63:0	**CSTAR: compatibility mode target address**. Read-write. Target address for compatibility mode. The address stored in this register must be in canonical form (if not canonical, a #GP fault occurs).

MSRC000_0084 SYSCALL Flag Mask (SYSCALL_FLAG_MASK)

Bits	Description
63:32	RAZ.
31:0	**Mask: SYSCALL flag mask**. Read-write. Reset: 0000_0000h. This register holds the EFLAGS mask used by the SYSCALL instruction. 1=Clear the corresponding EFLAGS bit when executing the SYSCALL instruction.

MSRC000_00E7 Read-Only Max Performance Frequency Clock Count (MPerfReadOnly)

Reset: 0000_0000_0000_0000h.

Bits	Description
63:0	**MPerfReadOnly: read-only maximum core clocks counter**. IF (MSRC001_0015[EffFreqReadOnlyLock]) THEN Read-only; Updated-by-hardware. ELSE Read-write; Updated-by-hardware. ENDIF. Incremented by hardware at the P0 frequency while the core is in C0. This register does not increment when the core is in the stop-grant state. In combination with MSRC000_00E8, this is used to determine the effective frequency of the core. A read of this MSR in guest mode is affected by MSRC000_0104 [Time Stamp Counter Ratio (TscRateMsr)]. This field uses software P-state numbering. See MSRC001_0015[EffFreqCntMwait], 2.5.3.3 [Effective Frequency], and 2.5.3.1.1.1 [Software P-state Numbering]. This register is not affected by writes to MSR0000_00E7.

MSRC000_00E8 Read-Only Actual Performance Frequency Clock Count (APerfReadOnly)

Reset: 0000_0000_0000_0000h.

Bits	Description
63:0	**APerfReadOnly: read-only actual core clocks counter**. IF (MSRC001_0015[EffFreqReadOnlyLock]) THEN Read-only; Updated-by-hardware. ELSE Read-write; Updated-by-hardware. ENDIF. This register increments in proportion to the actual number of core clocks cycles while the core is in C0. The register does not increment when the core is in the stop-grant state. See MSRC000_00E7. This register is not affected by writes to MSR0000_00E8.

MSRC000_0100 FS Base (FS_BASE)

Reset: 0000_0000_0000_0000h.

Bits	Description
63:0	**FSBase: expanded FS segment base**. Read-write; not-same-for-all. This register provides access to the expanded 64-bit FS segment base. The address stored in this register must be in canonical form (if not canonical, a #GP fault fill occurs).

MSRC000_0101 GS Base (GS_BASE)

Reset: 0000_0000_0000_0000h.

Bits	Description
63:0	**GSBase: expanded GS segment base**. Read-write; not-same-for-all. This register provides access to the expanded 64-bit GS segment base. The address stored in this register must be in canonical form (if not canonical, a #GP fault fill occurs).

MSRC000_0102 Kernel GS Base (KernelGSbase)

Reset: 0000_0000_0000_0000h.

Bits	Description
63:0	**KernelGSBase: kernel data structure pointer**. Read-write. This register holds the kernel data structure pointer which can be swapped with the GS_BASE register using the SwapGS instruction. The address stored in this register must be in canonical form (if not canonical, a #GP fault occurs).

MSRC000_0103 Auxiliary Time Stamp Counter (TSC_AUX)

Reset: 0000_0000_0000_0000h.

Bits	Description
63:32	Reserved.
31:0	**TscAux: auxiliary time stamp counter data**. Read-write. It is expected that this is initialized by privileged software to a meaningful value, such as a processor ID. This value is returned in the RDTSCP instruction.

MSRC000_0104 Time Stamp Counter Ratio (TscRateMsr)

MSRC000_0104 [Time Stamp Counter Ratio (TscRateMsr)] allows the hypervisor to control the guest's view of the Time Stamp Counter. It provides a multiplier that scales the value returned when MSR0000_0010[TSC], MSR0000_00E7[MPERF], and MSRC000_00E7[MPerfReadOnly] are read by a guest running under virtualization. This allows the hypervisor to provide a consistent TSC, MPERF, and MPerfReadOnly rate for a guest process when moving that process between cores that have a differing P0 rate. The TSC Ratio MSR does not affect the value read from the TSC, MPERF, and MPerfReadOnly MSRs when read when in host mode or when virtualization is not being used or when accessed by code executed in system management mode (SMM) unless the SMM code is executed within a guest container. The TSC Ratio value does not affect the rate of the underlying TSC, MPERF, and MPerfReadOnly counters, or the value that gets written to the TSC, MPERF, and MPerfReadOnly MSRs counters on a write by either the host or the guest. The TSC Ratio MSR contains a fixed-point number in 8.32 format, which is 8 bits of integer and 32 bits of fraction. This number is the ratio of the desired P0 frequency to the P0 frequency of the core. The reset value of the TSC Ratio MSR is 1.0, which results in a guest frequency matches the core P0 frequency.

Bits	Description
63:40	MBZ.
39:32	**TscRateMsrInt: time stamp counter rate integer**. Read-write. Reset: 01h. Specifies the integer part of the MSR TSC ratio value.
31:0	**TscRateMsrFrac: time stamp counter rate fraction**. Read-write. Reset: 0000_0000h. Specifies the fractional part of the MSR TSC ratio value.

MSRC000_0105 Lightweight Profile Configuration (LWP_CFG)

Bits	Description
63:48	Reserved.
47:40	**LwpVector: threshold interrupt vector**. Read-write. Reset: 0. Interrupt vector number used by LWP Threshold interrupts. Must be provided if LwpInt is set to 1.
39:32	**LwpCoreId: core ID**. Read-write; not-same-for-all. Reset: 0. Core identification stored into the trace record. BIOS: CPUID Fn0000_0001_EBX[LocalApicId]. Software is recommended to set this to CPUID Fn0000_0001_EBX[LocalApicId].
31	**LwpInt: interrupt on threshold overflow**. Read-write. Reset: 0. 1=Enable LWP to interrupt on threshold overflow. CPUID Fn8000_001C_EAX[LwpInt] is an alias of MSRC000_0105[LwpInt].
30	**LwpPTSC: performance time stamp counter in event record**. Read-write. Reset: 0. 1=Enable storing performance time stamp in event record. CPUID Fn8000_001C_EAX[LwpPTSC] is an alias of MSRC000_0105[LwpPTSC].
29	**LwpCont: sampling in continuous mode**. Read-write. Reset: 0. 1=Enable continuous mode. 0=Enable synchronized mode. CPUID Fn8000_001C_EAX[LwpCont] is an alias of MSRC000_0105[LwpCont].
28:7	MBZ.
6	**LwpRNH: core reference clocks not halted event support**. MBZ. Reset: 0. 1=Enable LWP to count core reference clocks not halted. CPUID Fn8000_001C_EAX[LwpRNH] is an alias of MSRC000_0105[LwpRNH].
5	**LwpCNH: core clocks not halted event support**. MBZ. Reset: 0. 1=Enable LWP to count core clocks not halted. CPUID Fn8000_001C_EAX[LwpCNH] is an alias of MSRC000_0105[LwpCNH].
4	**LwpDME: DC miss event support**. MBZ. Reset: 0. 1=Enable LWP to count DC misses. CPUID Fn8000_001C_EAX[LwpDME] is an alias of MSRC000_0105[LwpDME].
3	**LwpBRE: branch retired event support**. Read-write. Reset: 0. 1=Enable LWP to count branches retired. CPUID Fn8000_001C_EAX[LwpBRE] is an alias of MSRC000_0105[LwpBRE].
2	**LwpIRE: instructions retired event support**. Read-write. Reset: 0. 1=Enable LWP to count instructions retired. CPUID Fn8000_001C_EAX[LwpIRE] is an alias of MSRC000_0105[LwpIRE].
1	**LwpVAL: LWPVAL instruction support**. Read-write. Reset: 0. 1=LWPVAL instruction is enabled. CPUID Fn8000_001C_EAX[LwpVAL] is an alias of MSRC000_0105[LwpVAL].
0	Reserved.

MSRC000_0106 Lightweight Profile Control Block Address (LWP_CBADDR)

Access to the internal copy of the LWPCB logical line/64 byte address. A read returns the current LWPCB address without performing any of the operations described for the SLWPCB instruction. A write to this regis-

ter with a non-zero value will cause a #GP fault. Use LLWPCB or XRSTOR to load an LWPCB address. Writing a zero to LWP_CBADDR will immediately disable LWP, discarding any internal state. For instance, an operating system can write a zero to stop LWP when it terminates a thread. All references to the LWPCB implicitly use the DS segment register. Must be 64 byte aligned.

Bits	Description
63:6	**LwpCbAddr[63:6]: control block logical address**. Read-write. Reset: 0. LwpCbAddr[63:0] = {LwpCbAddr[63:6], 000000b}.
5:0	RAZ.

MSRC000_0408 NB Machine Check Misc 4 (Link Thresholding) 1 (MC4_MISC1)

Per-node. MSRC000_0408 is associated with the link error type. See 2.15.1.7 [Error Thresholding]. Accessibility of this register by non-NBC cores is affected by D18F3x44[NbMcaToMstCpuEn].

Bits	Description
63	**Valid**. IF (D18F3x44[NbMcaToMstCpuEn] && !NBC) THEN RAZ; Per-node; not-same-for-all. ELSEIF (MSRC001_0015[McStatusWrEn]) THEN Read-write; Per-node; not-same-for-all. ELSE Read-only; Per-node; not-same-for-all. Reset: 1. ENDIF. 1=The CntP field is present.
62	**CntP: counter present**. IF (D18F3x44[NbMcaToMstCpuEn] && !NBC) THEN RAZ; Per-node; not-same-for-all. ELSEIF (MSRC001_0015[McStatusWrEn]) THEN Read-write; Per-node; not-same-for-all. ELSE Read-only; Per-node; not-same-for-all. Reset: 1. ENDIF. 1=A valid threshold counter is present.
61	**Locked**. IF (D18F3x44[NbMcaToMstCpuEn] && !NBC) THEN RAZ; Per-node; not-same-for-all. ELSEIF (MSRC001_0015[McStatusWrEn]) THEN Read-write; Per-node; not-same-for-all. ELSE Read-only; Per-node; not-same-for-all. Reset: 0. ENDIF. BIOS: IF (IntType==10b) THEN 1. ELSE 0. ENDIF. 1=Writes to bits [55:32] of this register are ignored. Set by BIOS to indicate that this register is not available for OS use. When MSRC001_0015[McStatusWrEn] is set, MSR writes to this register update all bits, regardless of the state of the Locked bit.

60:56	Reserved.
55:52	**LvtOffset: LVT offset**. IF (D18F3x44[NbMcaToMstCpuEn] && !NBC) THEN RAZ; Per-node; not-same-for-all. ELSEIF (MSRC001_0015[McStatusWrEn] | ~MSRC000_0408[Locked]) THEN Read-write; Per-node; not-same-for-all. ELSE Read-only; Per-node; not-same-for-all. Reset: 0. ENDIF. Specifies the address of the LVT entry in the APIC registers as follows: LVT address = (LvtOffset shifted left 4 bits) + 500h (see APIC[530:500]). Bits Description 3h-0h See APIC[530:500]. Fh-4h Reserved
51	**CntEn: counter enable**. IF (D18F3x44[NbMcaToMstCpuEn] && !NBC) THEN RAZ; Per-node; not-same-for-all. ELSEIF (MSRC001_0015[McStatusWrEn] | ~Locked) THEN Read-write; Per-node; not-same-for-all. ELSE Read-only; Per-node; not-same-for-all. Reset: 0. ENDIF. 1=Count thresholding errors. See 2.15.1.7 [Error Thresholding].
50:49	**IntType: interrupt type**. IF (D18F3x44[NbMcaToMstCpuEn] && !NBC) THEN RAZ; Per-node; not-same-for-all. ELSEIF (MSRC001_0015[McStatusWrEn] | ~MSRC000_0408[Locked]) THEN Read-write; Per-node; not-same-for-all. ELSE Read-only; Per-node; not-same-for-all. Cold reset: 0. ENDIF. Specifies the type of interrupt signaled when Ovrflw is set. Bits Description 00b No Interrupt. 01b APIC. APIC based interrupt (see LvtOffset above) to all cores. 10b SMI. SMI trigger event (always routed to CpuCoreNum 0, as defined in 2.4.4 [Processor Cores and Downcoring]); see 2.4.9.2.3 [SMI Sources And Delivery]. 11b Reserved.
48	**Ovrflw: overflow.** IF (D18F3x44[NbMcaToMstCpuEn] && !NBC) THEN RAZ; Per-node; not-same-for-all. ELSEIF (MSRC001_0015[McStatusWrEn] | ~Locked) THEN Read-write; Per-node; not-same-for-all; set-by-hardware. ELSE Read-only; Per-node; not-same-for-all; set-by-hardware. Cold reset: 0. ENDIF. Set by hardware when ErrCnt transitions from FFEh to FFFh. When this bit is set, the interrupt selected by the IntType field is generated.
47:44	Reserved.
43:32	**ErrCnt: error counter**. IF (D18F3x44[NbMcaToMstCpuEn] && !NBC) THEN RAZ; Per-node; not-same-for-all. ELSEIF (MSRC001_0015[McStatusWrEn] | ~Locked) THEN Read-write; Per-node; not-same-for-all; updated-by-hardware. ELSE Read-only; Per-node; not-same-for-all; updated-by-hardware. Cold reset: 0. ENDIF. Written by software to set the starting value of the error counter. Incremented by hardware when errors are logged. Saturates at FFFh (no rollover). The threshold value, written by software, is (FFFh - the desired error count (the number of errors necessary in order for an interrupt to be taken)).
31:0	Reserved.

MSRC000_0409 Reserved

Bits	Description
63:0	Reserved.

MSRC000_040[F:A] Reserved

Bits	Description
63:0	RAZ.

3.21 MSRs - MSRC001_0xxx

MSRC001_00[03:00] Performance Event Select (PERF_CTL[3:0])

Reset: 0000_0000_0000_0000h. See 2.6.1 [Performance Monitor Counters].
The legacy alias of MSRC001_020[6,4,2,0]. See MSRC001_020[A,8,6,4,2,0].

Table 246: Register Mapping for MSRC001_00[03:00]

Register	Function
MSRC001_0000	Counter 0
MSRC001_0001	Counter 1
MSRC001_0002	Counter 2
MSRC001_0003	Counter 3

Bits	Description
63:0	MSRC001_00[03:00] is an alias of MSRC001_020[6,4,2,0].

MSRC001_00[07:04] Performance Event Counter (PERF_CTR[3:0])

The legacy alias of MSRC001_020[7,5,3,1]. See MSRC001_020[B,9,7,5,3,1].

Table 247: Register Mapping for MSRC001_00[07:04]

Register	Function
MSRC001_0004	Counter 0
MSRC001_0005	Counter 1
MSRC001_0006	Counter 2
MSRC001_0007	Counter 3

Bits	Description
63:0	MSRC001_00[07:04] is an alias of MSRC001_020[7,5,3,1].

MSRC001_0010 System Configuration (SYS_CFG)

Bits	Description
63:23	Reserved.
22	**Tom2ForceMemTypeWB: top of memory 2 memory type write back**. Read-write; Per-compute-unit. Reset: 0. 1=The default memory type of memory between 4GB and TOM2 is write back instead of the memory type defined by MSR0000_02FF[MemType]. For this bit to have any effect, MSR0000_02FF[MtrrDefTypeEn] must be 1. MTRRs and PAT can be used to override this memory type.
21	**MtrrTom2En: MTRR top of memory 2 enable**. Read-write; Per-compute-unit. Reset: 0. 0=MSRC001_001D [Top Of Memory 2 (TOM2)] is disabled. 1=This register is enabled. See D0F0x64_x19[TomEn].

20	**MtrrVarDramEn: MTRR variable DRAM enable**. Read-write; Per-compute-unit. Reset: 0. BIOS: 1. 0=MSRC001_001A [Top Of Memory (TOP_MEM)] and IORRs are disabled. 1=These registers are enabled.
19	**MtrrFixDramModEn: MTRR fixed RdDram and WrDram modification enable**. Read-write. Reset: 0. Controls access to MSR0000_02[6F:68,59:58,50][RdDram, WrDram]. 0=Access type is MBZ; writing 00b does not change the hidden value of MSR0000_02[6F:68,59:58,50][RdDram, WrDram]. 1=Access type is Read-write. BIOS: This bit should be set to 1 during BIOS initialization of the fixed MTRRs, then cleared to 0 for operation.
18	**MtrrFixDramEn: MTRR fixed RdDram and WrDram attributes enable**. Read-write; Per-compute-unit. Reset: 0. BIOS: 1. 1=Enables the RdDram and WrDram attributes in MSR0000_02[6F:68,59:58,50].
17	Reserved.
16	**ChgToDirtyDis: change to dirty disable**. Read-write; Per-compute-unit. Reset: 0. 1=Disables Change-to-Dirty command; The change-to-dirty condition is handled by evicting the line and then fetching it with a RdBlkM command.
15:0	Reserved.

MSRC001_0015 Hardware Configuration (HWCR)

Bits	Description
63:32	Reserved.
31:30	Reserved.
29	**CSEnable: connected standby enable**. Read-write. Reset: 0. 0=Connected standby feature is disabled. No Local APIC writes to NB PCI space or C6 save space will occur on C6 entry. No Local APIC restore from C6 save space will occur on C6 exit. No C6 state save skip will occur. 1=Connected standby feature is enabled. Local APIC writes to NB PCI Space and C6 save space can occur if MSR0000_001B[ApicEn] is set. Local APIC restore from C6 save space on C6 exit can occur if MSR0000_001B[ApicEn].
28	Reserved.
27	**EffFreqReadOnlyLock: read-only effective frequency counter lock**. Write-1-only. Reset: 0. BIOS: 1. 1=MSRC000_00E7 and MSRC000_00E8 are read-only.
26	**EffFreqCntMwait: effective frequency counting during mwait**. Read-write. Reset: 0. Specifies whether MSR0000_00E7 [Max Performance Frequency Clock Count (MPERF)] and MSR0000_00E8 [Actual Performance Frequency Clock Count (APERF)] increment while the core is in the monitor event pending state. 0=The registers do not increment. 1=The registers increment. See 2.5.3.3 [Effective Frequency].
25	**CpbDis: core performance boost disable**. Read-write. Reset: 0. Specifies whether core performance boost is requested to be enabled or disabled. 0=CPB is requested to be enabled. 1=CPB is disabled. See 2.5.9 [Application Power Management (APM)]. If core performance boost is disabled while a core is in a boosted P-state, the core will automatically transition to the highest performance non-boosted P-state.
24	**TscFreqSel: TSC frequency select**. Read-only. Reset: 1. 1=The TSC increments at the P0 frequency. This field uses software P-state numbering. See 2.5.3.1.1.1 [Software P-state Numbering].

23	**ForceRdWrSzPrb: force probes for RdSized and WrSized**. Read-write. Reset: 0. A read returns a 1 if this field is set on any core of the node. 1=Forces probes on read-sized and write-sized transactions, except those that are display refresh.
22:21	Reserved.
20	**IoCfgGpFault: IO-space configuration causes a GP fault**. Read-write. Reset: 0. 1=IO-space accesses to configuration space cause a GP fault. The fault is triggered if any part of the IO read/write address range is between CF8h and CFFh, inclusive. These faults only result from single IO instructions, not to string and REP IO instructions. This fault takes priority over the IO trap mechanism described by MSRC001_0054 [IO Trap Control (SMI_ON_IO_TRAP_CTL_STS)].
19	Reserved.
18	**McStatusWrEn: machine check status write enable**. Read-write. Reset: 0. McStatusWrEn can be used to debug machine check exception and interrupt handlers. See 2.15.3 [Error Injection and Simulation]. See 2.15.1 [Machine Check Architecture]. • 1=MCi_STATUS registers are read-write, including reserved fields; do not cause general protection faults; such writes update all implemented bits in these registers; All fields of all threshold registers are Read-write when accessed from MSR space, including Locked, except BlkPtr which is always read-only; McStatusWrEn does not change the access type for the thresholding registers accessed via configuration space. • 0=MCi_STATUS registers are readable; writing a non-zero pattern to these registers causes a general protection fault. • The MCi_STATUS registers are: MSR0000_0401, MSR0000_0405, MSR0000_0409, MSR0000_040D, MSR0000_0411, MSR0000_0415, MSR0000_0419. McStatusWrEn does not affect the writability of MSR0000_0001; MSR0000_0001 is always writable. • The thresholding registers affected by McStatusWrEn are: MSR0000_0403, MSR0000_0407, MSR0000_040B, MSR0000_0413, MSR0000_0417, MSRC000_0408.
17	**Wrap32Dis: 32-bit address wrap disable**. Read-write. Reset: 0. 1=Disable 32-bit address wrapping. Software can use Wrap32Dis to access physical memory above 4 Gbytes without switching into 64-bit mode. To do so, software should write a greater-than 4 Gbyte address to MSRC000_0100 [FS Base (FS_BASE)] and MSRC000_0101 [GS Base (GS_BASE)]. Then it would address ±2 Gbytes from one of those bases using normal memory reference instructions with a FS or GS override prefix. However, the INVLPG, FST, and SSE store instructions generate 32-bit addresses in legacy mode, regardless of the state of Wrap32Dis.
16:15	Reserved.
14	**RsmSpCycDis: RSM special bus cycle disable**. IF MSRC001_0015[SmmLock] THEN Read-only ELSE Read-write ENDIF. Reset: 0. 0=A link special bus cycle, SMIACK, is generated on a resume from SMI.
13	**SmiSpCycDis: SMI special bus cycle disable**. IF MSRC001_0015[SmmLock] THEN Read-only ELSE Read-write ENDIF. Reset: 0. 0=A link special bus cycle, SMIACK, is generated when an SMI interrupt is taken.
12	**HltXSpCycEn: halt-exit special bus cycle enable**. Read-write. Reset: 0. BIOS: 1. Read-write. Specifies whether a halt exit special bus cycle is sent to the Northbridge when exiting from the halt state. 1=Messages are sent. 0=Messages are not sent. See 2.5.3.2.4.1 [FCH Messaging].
11	Reserved.

10	**MonMwaitUserEn: MONITOR/MWAIT user mode enable**. Read-write. Reset: 0. 1=The MONITOR and MWAIT instructions are supported in all privilege levels. 0=The MONITOR and MWAIT instructions are supported only in privilege level 0; these instructions in privilege levels 1 to 3 cause a #UD exception. The state of this bit is ignored if MonMwaitDis is set.
9	**MonMwaitDis: MONITOR and MWAIT disable**. Read-write. Reset: 0. 1=The MONITOR and MWAIT opcodes become invalid. This affects what is reported back through CPUID Fn0000_0001_ECX[Monitor].
8	**IgnneEm: IGNNE port emulation enable**. Read-write. Reset: 0. 1=Enable emulation of IGNNE port.
7:6	Reserved.
5	Reserved.
4	**INVDWBINVD: INVD to WBINVD conversion**. Read-write. Reset: 1. 1=Convert INVD to WBINVD. BIOS: See 2.3.3 [Using L2 Cache as General Storage During Boot]. This bit is required to be set for normal operation when both cores of a compute unit are enabled and thus share the L2 cache or when an L3 exists.
3	**TlbCacheDis: cacheable memory disable**. Read-write. Reset: 0. 1=Disable performance improvement that assumes that the PML4, PDP, PDE and PTE entries are in cacheable WB DRAM. Operating systems that maintain page tables in any other memory type must set the TlbCacheDis bit to insure proper operation. • TlbCacheDis does not override the memory type specified by the SMM ASeg and TSeg memory regions. See 2.4.9.2.7 [The Protected ASeg and TSeg Areas].
2	Reserved.
1	Reserved.
0	**SmmLock: SMM code lock**. Read; write-1-only. Reset: 0. SBIOS: 1. 1=SMM code in the ASeg and TSeg range and the SMM registers are read-only and SMI interrupts are not intercepted in SVM. See 2.4.9.2.9 [Locking SMM].

MSRC001_00[18,16] IO Range Base (IORR_BASE[1:0])

Per-compute-unit. Reset: X. MSRC001_0016 and MSRC001_0017 combine to specify the first IORR range and MSRC001_0018 and MSRC001_0019 combine to specify the second IORR range. A core access, with address CPUAddr, is determined to be within IORR address range if the following equation is true: CPUAddr[47:12] & PhyMask[47:12] == PhyBase[47:12] & PhyMask[47:12].
BIOS can use the IORRs to create an IO hole within a range of addresses that would normally be mapped to DRAM. It can also use the IORRs to re-assert a DRAM destination for a range of addresses that fall within a bigger IO hole that overlays DRAM. See 2.4.6.1.2 [Determining The Access Destination for Core Accesses].

Bits	Description
63:48	RAZ.
47:12	**PhyBase: physical base address**. Read-write.
11:5	RAZ.
4	**RdMem: read from memory**. Read-write. 1=Read accesses to the range are directed to system memory. 0=Read accesses to the range are directed to IO.

3	**WrMem: write to memory**. Read-write. 1=Write accesses to the range are directed to system memory. 0=Write accesses to the range are directed to IO.
2:0	RAZ.

MSRC001_00[19,17] IO Range Mask (IORR_MASK[1:0])

Per-compute-unit.
Reset: 0000_0000_0000_0000h. See MSRC001_00[18,16].

Bits	Description
63:48	RAZ.
47:12	**PhyMask: physical address mask**. Read-write.
11	**Valid**. Read-write. 1=The pair of registers that specifies an IORR range is valid.
10:0	RAZ.

MSRC001_001A Top Of Memory (TOP_MEM)

Per-compute-unit.
Reset: 0000_0000_0000_0000h.

Bits	Description
63:48	RAZ.
47:23	**TOM[47:23]: top of memory**. Read-write. Specifies the address that divides between MMIO and DRAM. This value is normally placed below 4G. From TOM to 4G is MMIO; below TOM is DRAM. See 2.4.6 [System Address Map] and 2.9.13 [DRAM CC6/PC6 Storage].
22:0	RAZ.

MSRC001_001D Top Of Memory 2 (TOM2)

Per-compute-unit.
Reset: 0000_0000_0000_0000h.

Bits	Description
63:48	RAZ.
47:23	**TOM2[47:23]: second top of memory**. Read-write. Specifies the address divides between MMIO and DRAM. This value is normally placed above 4G. From 4G to TOM2 - 1 is DRAM; TOM2 and above is MMIO. See 2.4.6 [System Address Map] and 2.9.13 [DRAM CC6/PC6 Storage]. This register is enabled by MSRC001_0010[MtrrTom2En].
22:0	RAZ.

MSRC001_001F Northbridge Configuration 1 (NB_CFG1)

Read-write; Per-node. Only one of these registers exists in multi-core devices; see 3.1.1 [Northbridge MSRs In Multi-Core Products]. MSRC001_001F[31:0] is an alias of D18F3x88. MSRC001_001F[63:32] is an alias of D18F3x8C.

Bits	Description
63	Reserved.
62	**DisStpClkAbortFlush**. Reset: 0. 1=Disable aborting flush for core when the other core has a pending architectural interrupt.
61:56	Reserved.
55	**EnaDiv1CpuLowPwr**. Reset: 0. Enables power management actions in the core even when the requested clock divisor is /1. Normally a /1 clock divisor does not generate power management actions.
54	**InitApicIdCpuIdLo**. Reset: 0. BIOS: 1. 0=Reserved. 1=Selects the format for ApicId; see APIC20.
53:52	Reserved.
51	**DisDatFwdVic**. Reset: 0. 1=Disables data forwarding from victims to reads.
50	**DisOrderRdRsp**. Reset: 0. 1=Disables ordered responses to IO link read requests.
49:47	Reserved.
46	**EnableCf8ExtCfg: enable CF8 extended configuration cycles**. Reset: 0. 1=Allows the IO configuration space access method, IOCF8 and IOCFC, to be used to generate extended configuration cycles by enabling IOCF8[27:24].
45	**DisUsSysMgtReqToNcHt: disable upstream system management request to link**. Reset: 0. 1=Disables downstream reflection of upstream STPCLK and x86 legacy input system management commands (in order to work around potential deadlock scenarios related to reflection regions).
44:37	Reserved.
36	**DisDatMsk: disable data mask**. Reset: 0. BIOS: IF (DataMaskMbType!=1) THEN 1. ELSE 0. ENDIF. 1=Disables DRAM data masking function; all write requests that are less than one cacheline, a DRAM read is performed before writing the data. Data masking is supported in ECC mode; the NB performs a minimum write size of 16B.
35:32	Reserved.
31	**DisCohLdtCfg: disable coherent link configuration accesses**. Reset: 0. 1=Disables automatic routing of PCI configuration accesses to the processor configuration registers; PCI configuration space accesses which fall within the hard-coded range reserved for processor configuration-space registers are instead routed to the IO link specified by D18F1x[1DC:1D0,EC:E0] [Configuration Map]. This can be used to effectively hide the configuration registers from software. It can also be used to provide a means for an external chip to route processor configuration accesses according to a scheme other than the hard-coded version. When used, this bit needs to be set on all processors in a system. PCI configuration accesses should not be generated if this bit is not set on all processors.
30:28	Reserved.

27	**DisDramScrub**. Reset: 0. BIOS: 1. 1=Disable DRAM ECC scrubbing; this overrides the settings in D18F3x58 [Scrub Rate Control], D18F3x5C [DRAM Scrub Address Low].
26:19	Reserved.
18	**DisCstateBoostBlockPstateUp**. Read-write. Reset: 0. BIOS: 1. 1=Allow cores that are waking up out of a non-C0 C-state to transition to the last requested Pstate without having to wait for cores in the boosted P-state to transition out of the boosted P-state.
17:0	Reserved.

MSRC001_0022 Machine Check Exception Redirection

Reset: 0000_0000_0000_0000h. This register can be used to redirect machine check exceptions (MCEs) to SMIs or vectored interrupts. If both RedirSmiEn and RedirVecEn are set, then undefined behavior results.

Bits	Description
63:32	Reserved.
31:10	Reserved.
9	**RedirSmiEn**. Read-write. 1=Redirect MCEs (that are directed to this core) to generate an SMI-trigger IO cycle via MSRC001_0056. The status is stored in SMMFEC4[MceRedirSts].
8	**RedirVecEn**. Read-write. 1=Redirect MCEs (that are directed to this core) to generate a vectored interrupt, using the interrupt vector specified in RedirVector.
7:0	**RedirVector**. Read-write. See RedirVecEn.

MSRC001_00[35:30] Processor Name String

Per-compute-unit; SharedNC.
Reset: 0000_0000_0000_0000h. BIOS: Table 249. These registers holds the CPUID name string in ASCII. The state of these registers are returned by CPUID instructions, CPUID Fn8000_000[4:2]_E[D,C,B,A]X. BIOS should set these registers to the product name for the processor as provided by AMD. Each register contains a block of 8 ASCII characters; the least byte corresponds to the first ASCII character of the block; the most-significant byte corresponds to the last character of the block. MSRC001_0030 contains the first block of the name string; MSRC001_0035 contains the last block of the name string.

Table 248: Register Mapping for MSRC001_00[35:30]

Register	Function
MSRC001_0030	Characters 7-0
MSRC001_0031	Characters 15-8
MSRC001_0032	Characters 23-16
MSRC001_0033	Characters 31-24
MSRC001_0034	Characters 39-32
MSRC001_0035	Characters 47-40

See D18F5x194 for the access method to D18F5x198_x[B:0].

Table 249: BIOS Recommendations for MSRC001_00[35:30]

Register	BIOS
MSRC001_0030	{D18F5x198_x1, D18F5x198_x0}
MSRC001_0031	{D18F5x198_x3, D18F5x198_x2}
MSRC001_0032	{D18F5x198_x5, D18F5x198_x4}
MSRC001_0033	{D18F5x198_x7, D18F5x198_x6}
MSRC001_0034	{D18F5x198_x9, D18F5x198_x8}
MSRC001_0035	{D18F5x198_xB, D18F5x198_xA}

Bits	Description
63:0	**CpuNameString**. Read-write.

MSRC001_003E Hardware Thermal Control (HTC)

Only one of these registers exists in multi-core devices; see 3.1.1 [Northbridge MSRs In Multi-Core Products]. Uses hardware P-state numbering. See 2.5.3.1.1.2 [Hardware P-state Numbering].

Bits	Description
63:32	Reserved.
31	Reserved.
30:28	**HtcPstateLimit: HTC P-state limit select**. MSRC001_003E[HtcPstateLimit] is an alias of D18F3x64[HtcPstateLimit]. MSRC001_003E[HtcPstateLimit] is an alias of D18F3x64[HtcPstateLimit].
27:24	**HtcHystLmt: HTC hysteresis**. MSRC001_003E[HtcHystLmt] is an alias of D18F3x64[HtcHystLmt].
23	**HtcSlewSel: HTC slew-controlled temperature select**. MSRC001_003E[HtcSlewSel] is an alias of D18F3x64[HtcSlewSel].
22:16	**HtcTmpLmt: HTC temperature limit**. MSRC001_003E[HtcTmpLmt] is an alias of D18F3x64[HtcTmpLmt].
15:8	Reserved.
7	**PslApicLoEn: P-state limit lower value change APIC interrupt enable**. MSRC001_003E[PslApicLoEn] is an alias of D18F3x64[PslApicLoEn].
6	**PslApicHiEn: P-state limit higher value change APIC interrupt enable**. MSRC001_003E[PslApicHiEn] is an alias of D18F3x64[PslApicHiEn].
5	**HtcActSts: HTC-active status**. MSRC001_003E[HtcActSts] is an alias of D18F3x64[HtcActSts].
4	**HtcAct: HTC-active state**. MSRC001_003E[HtcAct] is an alias of D18F3x64[HtcAct].
3:1	Reserved.
0	**HtcEn: HTC enable**. MSRC001_003E[HtcEn] is an alias of D18F3x64[HtcEn].

MSRC001_0044 DC Machine Check Control Mask (MC0_CTL_MASK)

Read-write. Reset: 0000_0000_0000_0000h. BIOS: 0000_0000_0000_0000h. See 2.15.1 [Machine Check Architecture]. See MSR0000_0400 [MC0 Machine Check Control (MC0_CTL)].

Bits	Description
63:12	Reserved.
11	Reserved.
10	Reserved.
9	Reserved.
8	**IntErrType2: internal error type 2**.
7	**SRDE: read data errors**. System read data errors on cache fill.
6	**LFE: line fill error**. Uncorrectable error on cache fill.
5	**SCBP: SCB parity**.
4	**SQP: store queue parity**.
3	**LQP: load queue parity**.
2	**DatP: data parity**.
1	**TLBP: TLB parity**.
0	**TagP: tag parity**.

MSRC001_0045 IC Machine Check Control Mask (MC1_CTL_MASK)

Read-write; Per-compute-unit. Reset: 0000_0000_0000_0080h. BIOS: 0000_0000_0000_0080h. See 2.15.1 [Machine Check Architecture]. See MSR0000_0404 [MC1 Machine Check Control (MC1_CTL)].

Bits	Description
63:26	Reserved.
25	Unused.
24	Reserved.
23	**IVP: IC valid bit parity error**.
22	**L1TLBM: IC L1 TLB multi-match error**.
21	**L2TLBM: IC L2 TLB multi-match error**.
20	**DFIFOE: decoder FIFO parity error**.
19	**DPDBE: decoder predecode buffer parity error**.
18	**DEIBP: decoder instruction buffer parity error**.
17	**DEUOPQP: Decoder micro-op queue parity error**.
16	**DEPRP: microcode patch buffer parity error**.
15	**BSRP: branch status register parity error**.
14	Reserved.
13	**PQP: prediction queue parity error**.
12	**PFBP: prefetch buffer parity**.
11:10	Reserved.

9	**SRDE: system read data error**.
8	Reserved.
7	**LineFillPoison: line fill poison error**.
6	**L1TP: L1 TLB parity error**.
5	**L2TP: L2 TLB parity error**.
4	**ISTP: L1 cache probe tag array parity error**.
3	**IMTP: L1 cache main tag array parity error**.
2	**IDP: L1 cache data array parity error**.
1:0	Reserved.

MSRC001_0046 BU Machine Check Control Mask (MC2_CTL_MASK)

Read-write; Per-compute-unit. Reset: 0000_0000_0000_0000h. BIOS: 0000_0000_0000_0000h. See 2.15.1 [Machine Check Architecture]. See MSR0000_0408 [MC2 Machine Check Control (MC2_CTL)].

Bits	Description
63:15	Reserved.
14	**L2TlbFill: TLB fill error enable**. Data with uncorrectable error provided to TLB.
13	**RdData: read data error from NB**.
12	**L2Tag: L2 cache tag error**.
11	**L2TlbData: L2 TLB parity error**. Parity error reading from TLB.
10	**L2Prefetch: L2 data prefetcher parity error**.
9	**XabAddr: XAB address parity error**.
8	**PrbAddr: probe buffer address parity error**.
7	**FillData: fill data parity and ECC error**.
6	**PrqAddr: post retire queue address parity error**.
5	**PrqData: post retire queue data parity error**.
4	**WccAddr: write coalescing cache address ECC error**.
3	**WccData: write coalescing cache data ECC error**.
2	**WcbData: write combining buffer data parity error**.
1	**VbData: victim buffer data parity and ECC error**.
0	**L2TagMultiHit: L2 tag multiple hit error**.

MSRC001_0047 Reserved (MC3_CTL_MASK)

Reset: 0000_0000_0000_0000h.

Bits	Description
63:0	Reserved.

MSRC001_0048 NB Machine Check Control Mask (MC4_CTL_MASK)

IF (D18F3x44[NbMcaToMstCpuEn] && !NBC) THEN RAZ. ELSE Read-write; Per-node. ENDIF. The

format of MC4_CTL_MASK corresponds to MSR0000_0410 [MC4 Machine Check Control (MC4_CTL)]. For each defined bit position, 1=Disable logging. Only one of these registers exists in multi-core devices; see 3.1.1 [Northbridge MSRs In Multi-Core Products]. See 2.15.1 [Machine Check Architecture]. Accessibility of this register by non-NBC cores is affected by D18F3x44[NbMcaToMstCpuEn]. See MSR0000_0410 [MC4 Machine Check Control (MC4_CTL)].

Bits	Description
63:32	Reserved.
31	**McaCpuDatErrEn**. Reset: 0. BIOS: 0.
30	Reserved.
29	**UCRCEn**. Reset: 0. BIOS: 0.
28	**CCRCEn**. Reset: 0. BIOS: 0.
27	Reserved.
26	**NbArrayPar**. Reset: 0. IF (D18F4x118[NbPwrGate0]==1 || D18F4x118[NbPwrGate1]==1 || D18F4x11C[NbPwrGate2]==1) BIOS: 1. ELSE BIOS: 0. ENDIF.
25	**UsPwDatErrEn**. Reset: 0. BIOS: 0.
24:18	Reserved.
17	**CpPktDatEn**. Reset: 0. BIOS: 0.
16	**NbIntProtEn**. Reset: 0. BIOS: 0.
15:13	Reserved.
12	**WDTRptEn**. Reset: 0. BIOS: 0.
11	**AtomicRMWEn**. Reset: 0. BIOS: 0.
10	Reserved.
9	**TgtAbortEn**. Reset: 0. BIOS: 0.
8	**MstrAbortEn**. Reset: 0. BIOS: 0.
7:6	Reserved.
5	**SyncPktEn**. Reset: 0. BIOS: 0.
4:2	Reserved.
1	**UECCEn**. Reset: 0. BIOS: 0.
0	**CECCEn**. Reset: 0. BIOS: 0.

MSRC001_0049 EX Machine Check Control Mask (MC5_CTL_MASK)

Reset: 0000_0000_0000_0000h. BIOS: 0000_0000_0000_0000h. See 2.15.1 [Machine Check Architecture]. See MSR0000_0414 [MC5 Machine Check Control (MC5_CTL)].

Bits	Description
63:0	See: MSR0000_0414. The format of MC5_CTL_MASK corresponds to MC5_CTL.

MSRC001_004A FP Machine Check Control Mask (MC6_CTL_MASK)

Per-compute-unit. Reset: 0000_0000_0000_0000h. BIOS: 0000_0000_0000_0000h. See 2.15.1 [Machine Check Architecture]. See MSR0000_0418 [MC6 Machine Check Control (MC6_CTL)].

Bits	Description
63:0	See: MSR0000_0418. The format of MC6_CTL_MASK corresponds to MC6_CTL.

MSRC001_00[53:50] IO Trap (SMI_ON_IO_TRAP_[3:0])

Per-compute-unit; SharedNC.
Reset: 0000_0000_0000_0000h.

MSRC001_00[53:50] and MSRC001_0054 provide a mechanism for executing the SMI handler if a an access to one of the specified addresses is detected. Access address and access type checking is performed before IO instruction execution. If the access address and access type match one of the specified IO address and access types, then: (1) the IO instruction is not executed; (2) any breakpoint, other than the single-step breakpoint, set on the IO instruction is not taken (the single-step breakpoint is taken after resuming from SMM); and (3) the SMI-trigger IO cycle specified by MSRC001_0056. The status is stored in SMMFEC4[IoTrapSts].

IO-space configuration accesses are special IO accesses. An IO access is defined as an IO-space configuration access when IO instruction address bits[31:0] are CFCh, CFDh, CFEh, or CFFh when IO-space configuration is enabled (IOCF8[ConfigEn]). The access address for a configuration space access is the current value of IOCF8[BusNo, Device, Function, RegNo]. The access address for an IO access that is not a configuration access is equivalent to the IO instruction address, bits[31:0].

The access address is compared with SmiAddr, and the instruction access type is compared with the enabled access types defined by ConfigSMI, SmiOnRdEn, and SmiOnWrEn. Access address bits[23:0] can be masked with SmiMask.

IO and configuration space trapping to SMI applies only to single IO instructions; it does not apply to string and REP IO instructions.

The conditional GP fault described by MSRC001_0015[IoCfgGpFault] takes priority over this trap.

Table 250: Register Mapping for MSRC001_00[53:50]

Register	Function
MSRC001_0050	Range 0
MSRC001_0051	Range 1
MSRC001_0052	Range 2
MSRC001_0053	Range 3

Bits	Description
63	**SmiOnRdEn: enable SMI on IO read**. Read-write. 1=Enables SMI generation on a read access.
62	**SmiOnWrEn: enable SMI on IO write**. Read-write. 1=Enables SMI generation on a write access.
61	**ConfigSmi: configuration space SMI**. Read-write. 1=Configuration access. 0=IO access (that is not an IO-space configuration access).
60:56	Reserved.
55:32	**SmiMask[23:0]**. Read-write. SMI IO trap mask. 0=Mask address bit. 1=Do not mask address bit.
31:0	**SmiAddr[31:0]**. Read-write. SMI IO trap address.

MSRC001_0054 IO Trap Control (SMI_ON_IO_TRAP_CTL_STS)

Per-compute-unit; SharedNC.
For each of the SmiEn bits below, 1=The trap specified by the corresponding MSR is enabled. See MSRC001_00[53:50].

Bits	Description
63:32	RAZ.
31:16	Reserved.
15	**IoTrapEn: IO trap enable**. Read-write. Reset: 0. 1=Enable IO and configuration space trapping specified by MSRC001_00[53:50] and MSRC001_0054.
14:8	Reserved.
7	**SmiEn3: SMI enable for the trap specified by MSRC001_0053**. Read-write. Reset: 0.
6	Reserved.
5	**SmiEn2: SMI enable for the trap specified by MSRC001_0052**. Read-write. Reset: 0.
4	Reserved.
3	**SmiEn1: SMI enable for the trap specified by MSRC001_0051**. Read-write. Reset: 0.
2	Reserved.
1	**SmiEn0: SMI enable for the trap specified by MSRC001_0050**. Read-write. Reset: 0.
0	Reserved.

MSRC001_0055 Interrupt Pending

Per-compute-unit; SharedNC. This register is used to specify messages that the processor generates under certain conditions, that target the IO hub. One purpose is to ensure that the IO hub can wake the processor out of the stop-grant state when there is a pending interrupt. Otherwise, it is possible for the processor to remain in the stop-grant state while an interrupt is pending in the processor. This is accomplished by sending a message to the IO hub to indicate that the interrupt is pending. There are two message types: a programmable IO-space message and the link INT_PENDING message defined by the link specification.

If the IO hub does not support the INT_PENDING message, the IO space message should be selected by IntPndMsg. When this is enabled, the check for a pending interrupt is performed at the end of each IO instruction. If there is a pending interrupt and STPCLK is asserted, the processor executes a byte-size IO access as specified by IORd, IOMsgAddr, and IOMsgData.

If the IO hub supports the INT_PENDING message, it should be selected by IntPndMsg. The check for a pending interrupt is performed while in the stop-grant state or when entering the stop-grant state. If there is a pending interrupt, the processor broadcasts the INT_PENDING message. An INT_PENDING message may not be generated for arbitrated interrupts in multi-node systems.

Bits	Description
63:32	RAZ.
31	Reserved.
30	**EnablePmTmrCheckLoop**. Read-write. Reset: 0. 1=The core loops on IO-spaœ read accesses to the address specified by IOMsgAddr until the data value has incremented from the previous read access.
29:27	Reserved.

26	**IORd: IO Read**. Read-write. Reset: 0. 1=IO read. 0=IO write.
25	**IntPndMsg: interrupt pending message**. Read-write. Reset: 0. Selects the interrupt pending message type. 0=Link-defined INT_PENDING message; 1=Programmable SMI-trigger IO-space message. The status is stored in SMMFEC4[IntPendSmiSts].
24	**IntPndMsgDis: interrupt pending message disable**. Read-write. Reset: 0. Disable generating the interrupt pending message specified by IntPndMsg.
23:16	**IOMsgData: IO message data**. Read-write. Reset: 0. IO write message data. This field is only used if IORd specifies an IO write message.
15:0	**IOMsgAddr: IO message address**. Read-write. Reset: 0. IO space message address.

MSRC001_0056 SMI Trigger IO Cycle

Not-same-for-all. Reset: 0000_0000_0000_0000h. See 2.4.9.2.3 [SMI Sources And Delivery]. This register specifies an IO cycle that may be generated when a local SMI trigger event occurs. If IoCycleEn is set and there is a local SMI trigger event, then the IO cycle generated is a byte read or write, based on IoRd, to address IoPortAddress. If the cycle is a write, then IoData contains the data written. If the cycle is a read, the value read is discarded. If IoCycleEn is clear and a local SMI trigger event occurs, then undefined behavior results.

Bits	Description
63:32	Reserved.
31:27	Reserved.
26	**IoRd: IO Read**. Read-write. 1=IO read. 0=IO write.
25	**IoCycleEn: IO cycle enable**. Read-write. 1=The SMI trigger IO cycle is enabled to be generated.
24	Reserved.
23:16	**IoData**. Read-write.
15:0	**IoPortAddress**. Read-write.

MSRC001_0058 MMIO Configuration Base Address

Same-for-all. See 2.7 [Configuration Space] for a description of MMIO configuration space.

Bits	Description
63:48	RAZ.
47:20	**MmioCfgBaseAddr[47:20]: MMIO configuration base address bits[47:20]**. Read-write. Reset: X. Specifies the base address of the MMIO configuration range.
19:6	RAZ.

5:2	**BusRange: bus range identifier**. Read-write. Reset: 0. Specifies the number of buses in the MMIO configuration space range. The size of the MMIO configuration space is 1 MB times the number of buses. Bits Description Bits Description 0h 1 5h 32 1h 2 6h 64 2h 4 7h 128 3h 8 8h 256 4h 16 Fh-9h Reserved
1	Reserved.
0	**Enable**. Read-write. Reset: 0. 1=MMIO configuration space is enabled.

MSRC001_0060 BIST Results

Read; GP-write. Reset: 0000_0000_xxxx_xxxxh. This register provides BIST results after each reset. The results provided here are identical to the values provided in EAX.
If (MSRC001_0060[31:0]=0000_0000h) then no BIST failures were detected.

Bits	Description
63:32	Reserved.
31:0	**BistResults**.

MSRC001_0061 P-state Current Limit

Read; GP-write; Per-compute-unit; updated-by-hardware. See 2.5.3 [CPU Power Management].

Bits	Description
63:7	RAZ.
6:4	**PstateMaxVal: P-state maximum value**. Specifies the lowest-performance non-boosted P-state (highest non-boosted value) allowed. Attempts to change MSRC001_0062[PstateCmd] to a lower-performance P-state (higher value) are clipped to the value of this field. This field uses software P-state numbering. See 2.5.3.1.1.1 [Software P-state Numbering].
3	RAZ.
2:0	**CurPstateLimit: current P-state limit**. Specifies the highest-performance non-boosted P-state (lowest value) allowed. CurPstateLimit is always bounded by MSRC001_0061[PstateMaxVal]. Attempts to change the CurPstateLimit to a value greater (lower performance) than MSRC001_0061[PstateMaxVal] leaves CurPstateLimit unchanged. This field uses software P-state numbering. See MSRC001_0071[CurPstateLimit] and 2.5.3.1.1.1 [Software P-state Numbering].

MSRC001_0062 P-state Control

Bits	Description
63:3	MBZ.
2:0	**PstateCmd: P-state change command**. Read-write; Not-same-for-all. Cold reset value varies by product; after a warm reset, value initializes to the P-state the core was in prior to the reset. Writes to this field cause the core to change to the indicated non-boosted P-state number, specified by MSRC001_00[6B:64]. 0=P0, 1=P1, etc. P-state limits are applied to any P-state requests made through this register. Reads from this field return the last written value, regardless of whether any limits are applied. This field uses software P-state numbering. See 2.5.3 [CPU Power Management] and 2.5.3.1.1.1 [Software P-state Numbering].

MSRC001_0063 P-state Status

Read; GP-write; Per-compute-unit; Updated-by-hardware.

Bits	Description
63:3	RAZ.
2:0	**CurPstate: current P-state**. Cold reset: Varies by product. This field provides the frequency component of the current non-boosted P-state of the core (regardless of the source of the P-state change, including MSRC001_0062[PstateCmd]; 0=P0, 1=P1, etc. The value of this field is updated when the COF transitions to a new value associated with a P-state. This field uses software P-state numbering. See 2.5.3 [CPU Power Management] and 2.5.3.1.1.1 [Software P-state Numbering].

MSRC001_00[6B:64] P-state [7:0]

Per-node. Cold reset: Varies by product. Each of these registers specify the frequency and voltage associated with each of the core P-states.

Table 251: Register Mapping for MSRC001_00[6B:64]

Register	Function
MSRC001_0064	P-state 0
MSRC001_0065	P-state 1
MSRC001_0066	P-state 2
MSRC001_0067	P-state 3
MSRC001_0068	P-state 4
MSRC001_0069	P-state 5
MSRC001_006A	P-state 6
MSRC001_006B	P-state 7

The CpuVid field in these registers is required to be programmed to the same value in all cores of a processor, but are allowed to be different between processors in a multi-processor system. All other fields in these registers are required to be programmed to the same value in each core of the coherent fabric. See 2.5.3 [CPU Power Management].

When D18F4x15C[BoostLock]=1, MSRC001_00[6B:64][CpuVid, CpuDid, CpuFid] have special write requirements associated with them.

Table 252: P-state Definitions

Term	Definition
CoreCOF	Core current operating frequency in MHz. CoreCOF = 100 * (MSRC001_00[6B:64][CpuFid[5:0]] + 10h) / (2^MSRC001_00[6B:64][CpuDid]).

Bits	Description
63	**PstateEn**. Read-write. 1=The P-state specified by this MSR is valid. 0=The P-state specified by this MSR is not valid. The purpose of this register is to indicate if the rest of the P-state information in the register is valid after a reset; it controls no hardware.
62:42	RAZ.
41:40	**IddDiv: current divisor**. Read-write. See IddValue.
39:32	**IddValue: current value**. Read-write. After a reset, IddDiv and IddValue combine to specify the expected maximum current dissipation of a single core that is in the P-state corresponding to the MSR number. These values are intended to be used to create ACPI-defined _PSS objects (see 2.5.3.1.8.3 [ACPI Processor P-state Objects]) and to perform the 2.5.3.1.7 [Processor-Systemboard Power Delivery Compatibility Check]. The values are expressed in amps; they are not intended to convey final product power levels; they may not match the power levels specified in the Power and Thermal Datasheets. These fields are encoded as follows: IddDiv — Description 00b — IddValue / 1 A, Range: 0 to 255 A. 01b — IddValue / 10 A, Range: 0 to 25.5 A. 10b — IddValue / 100 A, Range: 0 to 2.55 A. 11b — Reserved.
31:23	RAZ.
22	**NbPstate: Northbridge P-state**. IF (MSRC001_0071[NbPstateDis]) THEN Read-only. ELSE Read-write. ENDIF. 1=Low performance NB P-state. 0=High performance NB P-state. If this bit is set in any given P-state register, then it must also be set in all enabled lower performance P-state registers as well. Equivalent P-states in each core must program this bit to the same value. See 2.5.4.1 [NB P-states] and D18F5x170[NbPstateThreshold, NbPstateLo, NbPstateHi].
21	RAZ.
20:17	RAZ.
16	**CpuVid[7]: core VID bit[7]**. Read-write. Except as required by 2.5.3.1.7 [Processor-Systemboard Power Delivery Compatibility Check], software should not modify this field. See CpuVid[6:0].
15:9	**CpuVid[6:0]: core VID**. Read-write. Except as required by 2.5.3.1.7 [Processor-Systemboard Power Delivery Compatibility Check], software should not modify this field. See 2.5.1 [Processor Power Planes And Voltage Control].

8:6	**CpuDid: core divisor ID**. Read-write. Except as required by 2.5.3.1.7 [Processor-Systemboard Power Delivery Compatibility Check], software should not modify this field. Specifies the core frequency divisor; see CpuFid. Bits: Description 0h: Divide-by 1 1h: Divide-by 2 2h: Divide-by 4 3h: Divide-by 8 4h: Divide-by 16 7h-5h: Reserved
5:0	**CpuFid[5:0]: core frequency ID**. Read-write. Except as required by 2.5.3.1.7 [Processor-Systemboard Power Delivery Compatibility Check], software should not modify this field. Specifies the core frequency multiplier. The core COF is a function of CpuFid and CpuDid, and defined by CoreCOF.

MSRC001_0070 COFVID Control

Cold reset: Product-specific. There is one register implemented for each core. This register includes several fields that are identical to MSRC001_00[6B:64]. It is controlled by hardwarefor P-state transitions. It may also be used by software to directly control the current COF or VID.
Accesses to this register that result in invalid COFs or VIDs are ignored. See 2.5.3 [CPU Power Management].

Bits	Description
63:32	RAZ.
31:24	**NbVid: Northbridge VID**. IF (MSRC001_0071[NbPstateDis]) THEN Read-only. ELSE Read-write. ENDIF. See D18F5x16[C:0][NbVid].
23	RAZ.
22	**NbPstate: Northbridge P-state**. IF (MSRC001_0071[NbPstateDis]) THEN Read-only. ELSE Read-write. ENDIF. See MSRC001_00[6B:64][NbPstate].
21	RAZ.
20	**CpuVid[7]**. Read-write. See CpuVid[6:0].
19	RAZ.
18:16	**PstateId: P-state identifier**. Read-write. This field is required to provide the P-state number that is associated with the values of the other fields in this register. This value is used by the logic to determine if the P-state is increasing or decreasing. This field uses hardware P-state numbering. See 2.5.3.1.1.2 [Hardware P-state Numbering].
15:9	**CpuVid[6:0]: core VID**. Read-write. See MSRC001_00[6B:64][CpuVid]. CpuVid[7:0] = {CpuVid[7], CpuVid[6:0]}.
8:6	**CpuDid: core divisor ID**. Read-write. See MSRC001_00[6B:64][CpuDid]. The PstateId field must be updated to cause a new CpuDid value to take effect.
5:0	**CpuFid[5:0]: core frequency ID**. Read-write. See MSRC001_00[6B:64][CpuFid]. The PstateId field must be updated to cause a new CpuFid value to take effect.

MSRC001_0071 COFVID Status

See 2.5.3 [CPU Power Management].

Bits	Description
63:59	**MaxNbCof: maximum NB COF**. Read-only. Cold reset: Product-specific. Specifies the maximum NB COF supported by the processor. If MaxNbCof is greater than zero, the maximum frequency is 100 MHz * MaxNbCof; if MaxNbCof = 00h, then there is no frequency limit. Any attempt to change the NB COF to a frequency greater than specified by this field is ignored.
58:56	**CurPstateLimit: current P-state limit**. Read-only; updated-by-hardware. Provides the current highest-performance P-state limit number. This register uses hardware P-state numbering. See MSRC001_0061[CurPstateLimit] and 2.5.3.1.1.2 [Hardware P-state Numbering].
55	Reserved.
54:49	**MaxCpuCof: maximum core COF**. Read-only. Cold reset: Product-specific. Specifies the maximum CPU COF supported by the processor. The maximum frequency is 100 MHz * MaxCpuCof, if MaxCpuCof is greater than zero; if MaxCpuCof = 00h, then there is no frequency limit. Any attempt to change a CPU COF to a frequency greater than specified by this field is ignored.
48:35	Reserved.
34:32	**StartupPstate: startup P-state number**. Read-only. Cold reset: Product-specific. Specifies the cold reset VID, FID and DID for the core based on the P-state number selected. StartupPstate uses hardware P-state numbering. See MSRC001_00[6B:64] and 2.5.3.1.1.2 [Hardware P-state Numbering].
31:24	**CurNbVid[7:0]: current NB VID**. Read-only; updated-by-hardware. Cold reset: Product-specific. This field specifies the current VDDNB voltage. MSRC001_0071[CurNbVid[7:0]] is an alias of D18F5x174[CurNbVid[7:0]].
23	**NbPstateDis: NB P-states disabled**. Value: D18F5x174[NbPstateDis]. MSRC001_0071[NbPstateDis] is an alias of D18F5x174[NbPstateDis]. 0=NB P-state frequency and voltage changes are supported. See D18F5x170[SwNbPstateLoDis, NbPstateDisOnP0]. 1=NB P-state frequency and voltage changes are disabled.
22	Reserved.
21	Reserved.
20	**CurCpuVid[7]**. Read-only; updated-by-hardware; not-same-for-all. Cold reset: Product-specific. See CurCpuVid[6:0].
19	Reserved.
18:16	**CurPstate: current P-state**. Read-only; updated-by-hardware; not-same-for-all. Cold reset: Product-specific. Specifies the current P-state requested by the core. This field uses hardware P-state numbering. See MSRC001_0063[CurPstate] and 2.5.3.1.1.2 [Hardware P-state Numbering]. When a P-state change is requested, the value in this field is updated once all required frequency and voltage transitions are completed.
15:9	**CurCpuVid[6:0]: current core VID**. Read-only; updated-by-hardware; not-same-for-all. Cold reset: Product-specific. CurCpuVid = {CurCpuVid[7], CurCpuVid[6:0]}. This field specifies the current VDD voltage.

8:6	**CurCpuDid: current core divisor ID**. Read-only; updated-by-hardware. Cold reset: Product-specific. Specifies the current CpuDid of the core. See MSRC001_00[6B:64]. When a P-state change is requested, the value in this field is updated once all required frequency and voltage transitions are completed.
5:0	**CurCpuFid: current core frequency ID**. Read-only; updated-by-hardware. Cold reset: Product-specific. Specifies the current CpuFid of the core. See MSRC001_00[6B:64]. When a P-state change is requested, the value in this field is updated once all required frequency and voltage transitions are completed.

MSRC001_0073 C-state Base Address

Reset: 0000_0000_0000_0000h.

Bits	Description
63:32	Reserved.
31:16	Reserved.
15:0	**CstateAddr: C-state address.** Read-write. Specifies the IO addresses trapped by the core for C-state entry requests. A value of 0 in this field specifies that the core does not trap any IO addresses for C-state entry. Writing values greater than FFF8h into this field result in undefined behavior. All other values cause the core to trap IO addresses CstateAddr through CstateAddr+7. See 2.5.3.2.2 [C-state Request Interface], D18F4x11[C:8], and D18F4x11C.

MSRC001_0074 CPU Watchdog Timer (CpuWdtCfg)

Read-write; Same-for-all. Reset: 0000_0000_0000_0000h.

The CPU watchdog timer (WDT) is implemented as a counter that counts out the time periods specified. The counter starts counting when CpuWdtEn is set. The counter does not count during halt or stop-grant. It restarts the count each time an operation of an instruction completes. If no operation completes by the specified time period, then a machine check error may be recorded if enabled (see MSR0000_0414 through MSR0000_0417). If a watchdog timer error overflow occurs (MSR0000_0415[Overflow]), a sync flood can be generated if enabled in D18F3x180[SyncFloodOnCpuLeakErr].

The CPU watchdog timer must be set higher than the NB watchdog timer (D18F3x44 [MCA NB Configuration]) in order to allow remote requests to complete. The CPU watchdog timer must be set the same for all CPUs in a system.

Bits	Description
63:7	Reserved.

<table>
<tr><td>6:3</td><td>CpuWdtCountSel: CPU watchdog timer count select. CpuWdtCountSel and CpuWdtTimeBase together specify the time period required for the WDT to expire. The time period is ((the multiplier specified by CpuWdtCountSel) * (the time base specified by CpuWdtTimeBase)). The actual timeout period may be anywhere from zero to one increments less than the values specified, due to non-deterministic behavior.
<table>
<tr><th>Bits</th><th>Multiplier</th><th>Bits</th><th>Multiplier</th></tr>
<tr><td>0h</td><td>4095</td><td>6h</td><td>63</td></tr>
<tr><td>1h</td><td>2047</td><td>7h</td><td>31</td></tr>
<tr><td>2h</td><td>1023</td><td>8h</td><td>8191</td></tr>
<tr><td>3h</td><td>511</td><td>9h</td><td>16383</td></tr>
<tr><td>4h</td><td>255</td><td>Fh-Ah</td><td>Reserved</td></tr>
<tr><td>5h</td><td>127</td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2:1</td><td>CpuWdtTimeBase: CPU watchdog timer time base. Specifies the time base for the timeout period specified in CpuWdtCountSel.
<table>
<tr><th>Bits</th><th>Description</th></tr>
<tr><td>00b</td><td>1.31 ms</td></tr>
<tr><td>01b</td><td>1.28 us</td></tr>
<tr><td>10b</td><td>Reserved</td></tr>
<tr><td>11b</td><td>Reserved</td></tr>
</table></td></tr>
<tr><td>0</td><td>CpuWdtEn: CPU watchdog timer enable. 1=The WDT is enabled.</td></tr>
</table>

MSRC001_0111 SMM Base Address (SMM_BASE)

Reset: 0000_0000_0003_0000h. This holds the base of the SMM memory region. The value of this register is stored in the save state on entry into SMM (see 2.4.9.2.5 [SMM Save State]) and it is restored on returning from SMM. The 16-bit CS (code segment) selector is loaded with SmmBase[19:4] on entering SMM. SmmBase[3:0] is required to be 0. The SMM base address can be changed in two ways:

- The SMM base address, at offset FF00h in the SMM state save area, may be changed by the SMI handler. The RSM instruction updates SmmBase with the new value.
- Normal WRMSR access to this register.

Bits	Description
63:32	Reserved.
31:0	**SmmBase**. IF MSRC001_0015[SmmLock] THEN Read-only; Not-same-for-all. ELSE Read-write; Not-same-for-all. ENDIF.

MSRC001_0112 SMM TSeg Base Address (SMMAddr)

Reset: 0000_0000_0000_0000h.

See 2.4.9.2 [System Management Mode (SMM)] and 2.4.6.1 [Memory Access to the Physical Address Space]. See MSRC001_0113 for more information about the ASeg and TSeg address ranges.

Each CPU access, directed at CPUAddr, is determined to be in the TSeg range if the following is true:

CPUAddr[47:17] & TSegMask[47:17] == TSegBase[47:17] & TSegMask[47:17].

For example, if TSeg spans 256 KB and starts at the 1 MB address. The MSRC001_0112[TSegBase] would be set to 0010_0000h and the MSRC001_0113[TSegMask] to FFFC_0000h (with zeros filling in for bits[16:0]).

This results in a TSeg range from 0010_0000 to 0013_FFFFh.

Bits	Description
63:48	Reserved.
47:17	**TSegBase[47:17]: TSeg address range base**. IF MSRC001_0015[SmmLock] THEN Read-only ELSE Read-write ENDIF.
16:0	Reserved.

MSRC001_0113 SMM TSeg Mask (SMMMask)

Reset: 0000_0000_0000_0000h. See 2.4.9.2 [System Management Mode (SMM)].
The ASeg address range is located at a fixed address from A0000h–BFFFFh. The TSeg range is located at a variable base (specified by MSRC001_0112[TSegBase]) with a variable size (specified by MSRC001_0113[TSegMask]). These ranges provide a safe location for SMM code and data that is not readily accessible by non-SMM applications. The SMI handler can be located in one of these two ranges, or it can be located outside these ranges. These ranges must never overlap each other.

This register specifies how accesses to the ASeg and TSeg address ranges are controlled as follows:

- If [A,T]Valid=1, then:
  - If in SMM, then:
    - If [A, T]Close=0, then the accesses are directed to DRAM with memory type as specified in [A, T]MTypeDram.
    - If [A, T]Close=1, then instruction accesses are directed to DRAM with memory type as specified in [A, T]MTypeDram and data accesses are directed at MMIO space and with attributes based on [A, T]MTypeIoWc.
  - If not in SMM, then the accesses are directed at MMIO space with attributes based on [A,T]MTypeIoWc.
- See 2.4.6.1.1 [Determining Memory Type].

Bits	Description
63:48	Reserved.
47:17	**TSegMask[47:17]: TSeg address range mask**. IF MSRC001_0015[SmmLock] THEN Read-only ELSE Read-write ENDIF. See MSRC001_0112.
16:15	Reserved.
14:12	**TMTypeDram: TSeg address range memory type**. IF MSRC001_0015[SmmLock] THEN Read-only. ELSE Read-write. ENDIF. Specifies the memory type for SMM accesses to the TSeg range that are directed to DRAM. See: Table 218 [Valid Values for Memory Type Definition].
11	Reserved.
10:8	**AMTypeDram: ASeg Range Memory Type**. IF MSRC001_0015[SmmLock] THEN Read-only. ELSE Read-write. ENDIF. Specifies the memory type for SMM accesses to the ASeg range that are directed to DRAM. See: Table 218 [Valid Values for Memory Type Definition].
7:6	Reserved.
5	**TMTypeIoWc: non-SMM TSeg address range memory type**. IF MSRC001_0015[SmmLock] THEN Read-only. ELSE Read-write. ENDIF. Specifies the attribute of TSeg accesses that are directed to MMIO space. 0=UC (uncacheable). 1=WC (write combining).

4	**AMTypeIoWc: non-SMM ASeg address range memory type**. IF MSRC001_0015[SmmLock] THEN Read-only. ELSE Read-write. ENDIF. Specifies the attribute of ASeg accesses that are directed to MMIO space. 0=UC (uncacheable). 1=WC (write combining).
3	**TClose: send TSeg address range data accesses to MMIO**. Read-write. 1=When in SMM, direct data accesses in the TSeg address range to MMIO space. See AClose.
2	**AClose: send ASeg address range data accesses to MMIO**. Read-write. 1=When in SMM, direct data accesses in the ASeg address range to MMIO space. [A, T]Close allows the SMI handler to access the MMIO space located in the same address region as the [A, T]Seg. When the SMI handler is finished accessing the MMIO space, it must clear the bit. Failure to do so before resuming from SMM causes the CPU to erroneously read the save state from MMIO space.
1	**TValid: enable TSeg SMM address range**. IF MSRC001_0015[SmmLock] THEN Read-only. ELSE Read-write. ENDIF. 1=The TSeg address range SMM enabled.
0	**AValid: enable ASeg SMM address range**. IF MSRC001_0015[SmmLock] THEN Read-only. ELSE Read-write. ENDIF. 1=The ASeg address range SMM enabled.

MSRC001_0114 Virtual Machine Control (VM_CR)

Bits	Description
63:32	Reserved.
31:5	MBZ.
4	**SvmeDisable: SVME disable**. See Lock for the access type of this field. Reset: 0. 1=MSRC000_0080[SVME] is MBZ. 0=MSRC000_0080[SVME] is read-write. Attempting to set this field when (MSRC000_0080[SVME]==1) causes a #GP fault, regardless of the state of Lock. See the APM2 section titled “Enabling SVM” for software use of this field.
3	**Lock: SVM lock**. Read-only; write-1-only; cleared-by-hardware. Reset: 0. See MSRC001_0118[SvmLockKey] for the condition that causes hardware to clear this field. 1=SvmeDisable is read-only. 0=SvmeDisable is read-write.
2	**DisA20m: disable A20 masking**. Read-write; set-by-hardware. Reset: 0. 1=Disables A20 masking. This bit is set by hardware when the SKINIT instruction is executed.
1	**InterceptInit: intercept INIT**. Read-write; set-by-hardware. Reset: 0. This bit controls how INIT is delivered in host mode. This bit is set by hardware when the SKINIT instruction is executed. 0=INIT delivered normally. 1=INIT translated into a SX interrupt.
0	**DPD: debug port disable**. Read-write; set-by-hardware. Reset: 0. Set by hardware when the SKINIT instruction is executed. This bit controls if debug facilities such as JTAG and HDT have access to the processor state information. 1=HDT is disabled. 0=HDT may be enabled.

MSRC001_0115 IGNNE

Bits	Description
63:32	Reserved.
31:1	MBZ.
0	**IGNNE: current IGNNE state**. Read-write. Reset: 0. This bit controls the current state of the processor internal IGNNE signal.

MSRC001_0116 SMM Control (SMM_CTL)

IF (MSRC001_0015[SmmLock]) THEN GP-read-write. ELSE GP-read; write-only. ENDIF.
The bits in this register are processed in the order of: SmmEnter, SmiCycle, SmmDismiss, RsmCycle and SmmExit. However, only the following combination of bits may be set in asingle write (all other combinations result in undefined behavior):

- SmmEnter and SmiCycle.
- SmmEnter and SmmDismiss.
- SmmEnter, SmiCycle and SmmDismiss.
- SmmExit and RsmCycle.

Software is responsible for ensuring that SmmEnter and SmmExit operations are properly matched and are not nested.

Bits	Description
63:5	MBZ.
4	**RsmCycle: send RSM special cycle**. 1=Send a RSM special cycle.
3	**SmmExit: exit SMM**. 1=Exit SMM.
2	**SmiCycle: send SMI special cycle**. 1=Send a SMI special cycle.
1	**SmmEnter: enter SMM**. 1=Enter SMM.
0	**SmmDismiss: clear SMI**. 1=Clear the SMI pending flag.

MSRC001_0117 Virtual Machine Host Save Physical Address (VM_HSAVE_PA)

Bits	Description
63:48	MBZ.
47:12	**VM_HSAVE_PA: physical address of host save area**. Read-write. Reset: 0. This register contains the physical address of a 4-KB region where VMRUN saves host state and where vm-exit restores host state from. Writing this register causes a #GP if (FF_FFFF_Fh>=VM_HSAVE_PA>=FD_0000_0h).
11:0	MBZ.

MSRC001_0118 SVM Lock Key

Reset: 0000_0000_0000_0000h.

Bits	Description
63:0	**SvmLockKey: SVM lock key**. RAZ; write. Writes to this register when MSRC001_0114[Lock]==0 modify SvmLockKey. If ((MSRC001_0114[Lock]==1) && (SvmLockKey!=0) && (The write value==The value stored in SvmLockKey)) for a write to this register then hardware updates MSRC001_0114[Lock]=0.

MSRC001_011A Local SMI Status

Reset: 0000_0000_0000_0000h. This registers returns the same information that is returned in SMMFEC4 [Local SMI Status] portion of the SMM save state. The information in this register is only updated when MSRC001_0116[SmmDismiss] is set by software.

Bits	Description
63:32	Reserved.
31:0	Alias of SMMFEC4 [Local SMI Status].

MSRC001_0140 OS Visible Work-around MSR0 (OSVW_ID_Length)

Reset: 0000_0000_0000_0000h.

Bits	Description
63:16	Reserved.
15:0	**OSVWIdLength: OS visible work-around ID length**. Read-write. See the Revision Guide for the definition of this field; see 1.2 [Reference Documents].

MSRC001_0141 OS Visible Work-around MSR1 (OSVW Status)

Reset: 0000_0000_0000_0000h.

Bits	Description
63:0	**OsvwStatusBits: OS visible work-around status bits**. Read-write. See the Revision Guide for the definition of this field; see 1.2 [Reference Documents].

MSRC001_020[A,8,6,4,2,0] Performance Event Select (PERF_CTL[5:0])

Reset: 0000_0000_0000_0000h. See 2.6.1 [Performance Monitor Counters]. MSRC001_00[03:00] is an alias of MSRC001_020[6,4,2,0].

Table 253: Register Mapping for MSRC001_020[A,8,6,4,2,0]

Register	Function
MSRC001_0200	Counter 0
MSRC001_0202	Counter 1
MSRC001_0204	Counter 2

Table 253: Register Mapping for MSRC001_020[A,8,6,4,2,0]

MSRC001_0206	Counter 3
MSRC001_0208	Counter 4
MSRC001_020A	Counter 5

Bits	Description
63:42	Reserved.
41:40	**HostGuestOnly: count only host/guest events**. Read-write. Bits: Description 00b: Count all events, irrespective of guest/host. 01b: Count guest events if MSRC000_0080[SVME]==1. 10b: Count host events if MSRC000_0080[SVME]==1. 11b: Count all guest and host events if MSRC000_0080[SVME]==1.
39:36	Reserved.
35:32	**EventSelect[11:8]: performance event select**. See: EventSelect[7:0].
31:24	**CntMask: counter mask**. Read-write. Controls the number of events counted per clock cycle. Bits: Description 00h: The corresponding PERF_CTR[5:0] register increments by the number of events occurring in a clock cycle. Maximum number of events in one cycle is 32. 7Fh-01h: When Inv==0, the corresponding PERF_CTR[5:0] register increments by 1, if the number of events occurring in a clock cycle is greater than or equal to the CntMask value. When Inv==1, the corresponding PERF_CTR[5:0] register increments by 1, if the number of events occurring in a clock cycle is less than CntMask value. FFh-80h: Reserved.
23	**Inv: invert counter mask**. Read-write. See CntMask.
22	**En: enable performance counter**. Read-write. 1=Performance event counter is enabled.
21	Reserved.
20	**Int: enable APIC interrupt**. Read-write. 1=APIC performance counter LVT interrupt is enabled to generate an interrupt via APIC340 [LVT Performance Monitor] when the performance counter overflows.
19	Reserved.
18	**Edge: edge detect**. Read-write. 0=Level detect. 1=Edge detect. The edge count mode increments the counter when a transition happens on the monitored event. If the event selected is changed without disabling the counter, an extra edge is falsely detected when the first event is a static 0 and the second event is a static one. To avoid this false edge detection, disable the counter when changing the event and then enable the counter with a second MSR write.
17:16	**OsUserMode: OS and user mode**. Read-write. Bits: Description 00b: Count no events. 01b: Count user events (CPL>0). 10b: Count OS events (CPL=0). 11b: Count all events, irrespective of the CPL.

15:8	**UnitMask: event qualification**. Read-write. Each UnitMask bit further specifies or qualifies the event specified by EventSelect. All events selected by UnitMask are simultaneously monitored. Unless otherwise stated, the UnitMask values shown may be combined (logically ORed) to select any desired combination of the sub-events for a given event. In some cases, certain combinations can result in misleading counts, or the UnitMask value is an ordinal rather than a bit mask. These situations are described where applicable, or should be obvious from the event descriptions. For events where no UnitMask table is shown, the UnitMask is Unused.
7:0	**EventSelect[7:0]: event select**. Read-write. EventSelect[11:0] = {EventSelect[11:8], EventSelect[7:0]}. EventSelect specifies the event or event duration in a processor unit to be counted by the corresponding PERF_CTR[5:0] register. The events are specified in 3.23 [Core Performance Counter Events]. Some events are reserved; when a reserved event is selected, the results are undefined.

MSRC001_020[B,9,7,5,3,1] Performance Event Counter (PERF_CTR[5:0])

See MSRC001_020[A,8,6,4,2,0] [Performance Event Select (PERF_CTL[5:0])]. MSRC001_00[07:04] is an alias of MSRC001_020[7,5,3,1].

Table 254: Register Mapping for MSRC001_020[B,9,7,5,3,1]

Register	Function
MSRC001_0201	Counter 0
MSRC001_0203	Counter 1
MSRC001_0205	Counter 2
MSRC001_0207	Counter 3
MSRC001_0209	Counter 4
MSRC001_020B	Counter 5

Bits	Description
63:48	RAZ.
47:0	**CTR: performance counter value**. Read-write. Reset: 0.

MSRC001_024[6,4,2,0] Northbridge Performance Event Select (NB_PERF_CTL[3:0])

Per-node. See 2.6.1 [Performance Monitor Counters]. MSRC001_024[6,4,2,0][31:0] is an alias of D18F5x[70,60,50,40]. MSRC001_024[6,4,2,0][63:32] is an alias of D18F5x[74,64,54,44].

Table 255: Register Mapping for MSRC001_024[6,4,2,0]

Register	Function
MSRC001_0240	Counter 0
MSRC001_0242	Counter 1
MSRC001_0244	Counter 2
MSRC001_0246	Counter 3

Note: To get meaningful data, each of the counters should be similiarly programmed across events selected.

Bits	Description
63:36	Reserved.
35:32	**EventSelect[11:8]: performance event select**. Read-write. Reset: 0. See EventSelect[7:0].
31:23	Reserved.
22	**En: enable performance counter**. Read-write. Reset: 0. 1=Performance event counter is enabled.
21	Reserved.
20	**Int: enable APIC interrupt**. Read-write. Reset: 0. 1=APIC performance counter LVT interrupt is enabled to generate an interrupt via APIC340 [LVT Performance Monitor] to all local APIC's on this node when the performance counter overflows.
19	Reserved.
18:16	Reserved.
15:8	**UnitMask: event qualification**. Read-write. Reset: 0. Each UnitMask bit further specifies or qualifies the event specified by EventSelect. All events selected by UnitMask are simultaneously monitored. Unless otherwise stated, the UnitMask values shown may be combined (logically ORed) to select any desired combination of the sub-events for a given event. In some cases, certain combinations can result in misleading counts, or the UnitMask value is an ordinal rather than a bit mask. These situations are described where applicable, or should be obvious from the event descriptions. For events where no UnitMask table is shown, the UnitMask is Unused.
7:0	**EventSelect[7:0]: event select**. Read-write. Reset: 0. This field, along with EventSelect[11:8] above, combine to form the 12-bit event select field, EventSelect[11:0]. EventSelect specifies the event or event duration in a processor unit to be counted by the corresponding NB_PERF_CTR[3:0] register. The events are specified in 3.24 [NB Performance Counter Events]. Some events are reserved; when a reserved event is selected, the results are undefined.

MSRC001_024[7,5,3,1] Northbridge Performance Event Counter (NB_PERF_CTR[3:0])

Per-node. See MSRC001_024[6,4,2,0] [Northbridge Performance Event Select (NB_PERF_CTL[3:0])]. MSRC001_024[7,5,3,1][31:0] is an alias of D18F5x[78,68,58,48]. MSRC001_024[7,5,3,1][63:32] is an alias of D18F5x[7C,6C,5C,4C].
See 2.6.1.2 [NB Performance Monitor Counters] for proper read sequence.

Table 256: Register Mapping for MSRC001_024[7,5,3,1]

Register	Function
MSRC001_0241	Counter 0
MSRC001_0243	Counter 1
MSRC001_0245	Counter 2
MSRC001_0247	Counter 3

Bits	Description
63:48	RAZ.
47:32	**CTR[47:32]: performance counter value[47:32]**. See: CTR[31:0].
31:0	**CTR[31:0]: performance counter value[31:0]**. Read-write. Reset: 0. CTR[47:0] = {CTR[47:32], CTR[31:0]}. Returns the current value of the event counter.

MSRC001_0280 Performance Time Stamp Counter (CU_PTSC)

Support for MSRC001_0280 [Performance Time Stamp Counter (CU_PTSC)] indicated by CPUID Fn8000_0001_ECX[PerfTsc]. The size of PTSC indicated by CPUID Fn8000_0008_ECX[PerfTscSize]. Increments at a 100 MHz rate in all P-states, all C states, S0, or S1. Each core on a node at the same instant in time will vary by +/- 3 100 MHz clocks. The value of PTSC[31:0] will be inserted into each record produced.

Bits	Description
63:40	RAZ.
39:0	**PTSC: global timestamp counter**. Read-only; updated-by-hardware. Reset: 0.

3.22 MSRs - MSRC001_1xxx

MSRC001_1002 CPUID Features for CPUID Fn0000_0007_E[B,A]X_x0

Read-write. Reset: {CPUID Fn0000_0007_EAX_x0, CPUID Fn0000_0007_EBX_x0}. MSRC001_1002[63:32] provides control over values read from CPUID Fn0000_0007_EAX_x0; MSRC001_1002[31:0] provides control over values read from CPUID Fn0000_0007_EBX_x0.

Bits	Description
63:9	Reserved.
8	Reserved.
7	Reserved.
6	Reserved.
5	Reserved.
4	Reserved.
3	**BMI1**.
2:1	Reserved.
0	Reserved.

MSRC001_1003 Thermal and Power Management CPUID Features

MSRC001_1003 provides control over values read from CPUID Fn0000_0006_ECX.

Bits	Description
63:32	Reserved.
31:0	**FeaturesEcx**. Read-write. Reset: CPUID Fn0000_0006_ECX. Provides control over the features reported in CPUID Fn0000_0006_ECX.

MSRC001_1004 CPUID Features (Features)

Read-write. Reset: {CPUID Fn0000_0001_ECX, CPUID Fn0000_0001_EDX}. MSRC001_1004[63:32] provides control over values read from CPUID Fn0000_0001_ECX; MSRC001_1004[31:0] provides control over

values read from CPUID Fn0000_0001_EDX.

Bits	Description
63	Reserved.
62	**RDRAND.**
61	**F16C**.
60	**AVX**.
59	**OSXSAVE**. Modifies CPUID Fn0000_0001_ECX[OSXSAVE] only if CR4[OSXSAVE].
58	**XSAVE**.
57	**AES**. Modifies CPUID Fn0000_0001_ECX[AES] only if the reset value is 1 .
56	Reserved.
55	**POPCNT**.
54	Reserved.
53	**x2APIC**.
52	**SSE42**.
51	**SSE41**.
50:46	Reserved.
45	**CMPXCHG16B**.
44:42	Reserved.
41	**SSSE3**.
40:36	Reserved.
35	**Monitor**. Modifies CPUID Fn0000_0001_ECX[Monitor] only if ~MSRC001_0015[MonMwaitDis].
34	Reserved.
33	**PCLMULQDQ**. Modifies CPUID Fn0000_0001_ECX[PCLMULQDQ] only if the reset value is 1.
32	**SSE3**.
31:29	Reserved.
28	**HTT**.
27	Reserved.
26	**SSE2**.
25	**SSE**.
24	**FXSR**.
23	**MMX**.
22:20	Reserved.
19	**CLFSH**.
18	Reserved.
17	**PSE36**.
16	**PAT**.
15	**CMOV**.
14	**MCA**.

13	**PGE**.
12	**MTRR**.
11	**SysEnterSysExit**.
10	Reserved.
9	**APIC**. Modifies CPUID Fn0000_0001_EDX[APIC] only if MSR0000_001B[ApicEn].
8	**CMPXCHG8B**.
7	**MCE**.
6	**PAE**.
5	**MSR**.
4	**TSC**.
3	**PSE**.
2	**DE**.
1	**VME**.
0	**FPU**.

MSRC001_1005 Extended CPUID Features (ExtFeatures)

Read-write. Reset: {CPUID Fn8000_0001_ECX, CPUID Fn8000_0001_EDX}. MSRC001_1005[63:32] provides control over values read from CPUID Fn8000_0001_ECX; MSRC001_1005[31:0] provides control over values read from CPUID Fn8000_0001_EDX.

Bits	Description
63:61	Reserved.
60	**PerfCtrExtL2I**.
59	**PerfTsc**.
58	**DataBreakpointExtension**.
57	Reserved.
56	**PerfCtrExtNB**.
55	**PerfCtrExtCore**.
54	**TopologyExtensions**. BIOS: IF (CPUID Fn8000_0001_EBX[PkgType]==0001b) THEN 1. ELSE 0. ENDIF.
53	**TBM**.
52	Reserved.
51	**NodeId**. BIOS: 1.
50	Reserved.
49	Reserved.
48	**FMA4**.
47	**LWP**.
46	Reserved.

45	**WDT**.
44	**SKINIT**.
43	**XOP**.
42	**IBS**.
41	**OSVW**.
40	**3DNowPrefetch**.
39	**MisAlignSse**.
38	**SSE4A**.
37	**ABM**.
36	**AltMovCr8**.
35	**ExtApicSpace**.
34	**SVM**. Modifies CPUID Fn8000_0001_ECX[SVM] only if D18F3xE8[SvmCapable].
33	**CmpLegacy**.
32	**LahfSahf**.
31	**3DNow**.
30	**3DNowExt**.
29	**LM**. Read-write.
28	Reserved.
27	**RDTSCP**.
26	**Page1GB**.
25	**FFXSR**.
24	**FXSR**.
23	**MMX**.
22	**MmxExt**.
21	Reserved.
20	**NX**.
19:18	Reserved.
17	**PSE36**.
16	**PAT**.
15	**CMOV**.
14	**MCA**.
13	**PGE**.
12	**MTRR**.
11	**SysCallSysRet**.
10	Reserved.
9	**APIC**.
8	**CMPXCHG8B**.

7	**MCE**.
6	**PAE**.
5	**MSR**.
4	**TSC**.
3	**PSE**.
2	**DE**.
1	**VME**.
0	**FPU**.

MSRC001_101[B:9] Address Mask For DR[3:1] Breakpoints

Reset: 0000_0000_0000_0000h. Support indicated by CPUID Fn8000_0001_ECX[DataBreakpointExtension]. See MSRC001_1027.

Table 257: Register Mapping for MSRC001_101[B:9]

Register	Function
MSRC001_1019	DR1_ADDR_MASK
MSRC001_101A	DR2_ADDR_MASK
MSRC001_101B	DR3_ADDR_MASK

Table 258: Field Mapping for MSRC001_101[B:9]

Register	Bits
	31:0
MSRC001_1019	DR1
MSRC001_101A	DR2
MSRC001_101B	DR3

Bits	Description
63:32	Reserved.
31:0	**AddrMask: mask for DR linear address data breakpoint**. Read-write. This field qualifies the DR linear address data breakpoint, allowing the DR[3:1] data breakpoint on a range of addresses in memory. The mask bits are active high; 0=Include bit into address compare; 1=Exclude bit into address compare. AddrMask is always used, and it can be used in conjunction with any debug function that uses DR[3:1]. The legacy DR breakpoint function is provided by AddrMask[31:0]==0000_0000h).

MSRC001_1020 Load-Store Configuration (LS_CFG)

Bits	Description
63:29	Reserved.

28	**DisSS**. Read-write; Same-for-all. Reset: 0. BIOS: See 2.3.3 [Using L2 Cache as General Storage During Boot]. 1=Disable streaming store functionality.
27:0	Reserved.

MSRC001_1021 Instruction Cache Configuration (IC_CFG)

Per-compute-unit.

Bits	Description
63:10	Reserved.
9	**DisSpecTlbRld**. Read-write. Reset: 0. 1=Disable speculative IC TLB reload request; the request is not made to the TLB walker until the fetch is non-speculative. BIOS: See 2.3.3 [Using L2 Cache as General Storage During Boot].
8:0	Reserved.

MSRC001_1022 Data Cache Configuration (DC_CFG)

Bits	Description
63:16	Reserved.
15	**DisPfHwForSw**. Read-write. Reset: 0. 1=Disable hardware prefetches for software prefetches.
14	Reserved.
13	**DisHwPf**. Read-write. Reset: 0. 1=Disable the DC hardware prefetcher. BIOS: See 2.3.3 [Using L2 Cache as General Storage During Boot].
12:5	Reserved.
4	**DisSpecTlbRld**. Read-write. Reset: 0. 1=Disable speculative TLB reloads. BIOS: See 2.3.3 [Using L2 Cache as General Storage During Boot].
3:0	Reserved.

MSRC001_1023 Combined Unit Configuration (CU_CFG)

Per-compute-unit.

Bits	Description
63:52	Reserved.
51	Reserved.
50	Reserved.
49	**ProcFeedbackEn: processor feedback interface enable**. Read-write. Reset: 0. BIOS: 1. 1=Enable processor feedback interface; CPUID Fn8000_0007_EAX.
48:35	Reserved.
34	**WbinvdFlushClean**. Read-write. Reset: 0. BIOS: 1. 1=Flush all L2 lines on CC6 entry in microcode loop, including clean lines. 0=Flush only dirty lines on CC6 entry in microcode loop, leaving L2 clean line invalidation to the CU invalidation state machine.

33:24	Reserved.
23	**L2WayLock: L2 way lock enable**. Read-write. Reset: 0. 1=Allocations and evictions for the L2 ways >= L2FirstLockedWay are disabled. Probes can still invalidate a line in a locked way. Cache lines in the locked ways of the L2 are still accessible by software. See 2.3.3 [Using L2 Cache as General Storage During Boot].
22:19	**L2FirstLockedWay: first L2 way locked**. Read-write. Reset: 0. See L2WayLock. Bits — Description 0h — Reserved. Eh-1h — Ways <L2FirstLockedWay> to 15 locked. Fh — Way 15 locked.
18:0	Reserved.

MSRC001_1027 Address Mask For DR0 Breakpoints (DR0_ADDR_MASK)

Reset: 0000_0000_0000_0000h. Support for AddrMaskDR0[31:12] is indicated by CPUID Fn8000_0001_ECX[DataBreakpointExtension]. See MSRC001_101[B:9].

Bits	Description
63:32	Reserved.
31:0	**AddrMaskDR0: mask for DR0 linear address data breakpoint**. Read-write. This field qualifies the DR0 linear address data breakpoint, allowing the DR0 data breakpoint on a range of addresses in memory. The mask bits are active high. 0=Include bit into address compare. 1=Exclude bit into address compare. AddrMaskDR0 is always used, and it can be used in conjunction with any debug function that uses DR0. AddrMaskDR0[31:12] is only valid for data breakpoints. The legacy DR0 breakpoint function is provided by AddrMaskDR0[31:0]==0000_0000h).

MSRC001_1028 Floating Point Configuration (FP_CFG)

Per-compute-unit.

Bits	Description
63:45	Reserved.
44:41	**DiDtCfg4**. Read-write. Reset: 1111b. BIOS: D18F3x1FC[DiDtCfg4].
40	**DiDtCfg3**. Read-write. Reset: 0. BIOS: D18F3x1FC[DiDtCfg3].
39:35	Reserved.
34:27	**DiDtCfg1**. Read-write. Reset: 1001_1011b. BIOS: D18F3x1FC[DiDtCfg1].
26:25	**DiDtCfg2**. Read-write. Reset: 00b. BIOS: D18F3x1FC[DiDtCfg2].
24:23	Reserved.

22:18	**DiDtCfg0**. Read-write. Reset: 1_1111b. BIOS: D18F3x1FC[DiDtCfg0].
17	Reserved.
16	**DiDtMode**. Read-write. Reset: 0. BIOS: D18F3x1FC[DiDtMode].
15:0	Reserved.

MSRC001_102A Combined Unit Configuration 2 (CU_CFG2)

Per-compute-unit.

Bits	Description
63:57	Reserved.
56:52	**L2UpsizeCUCT: L2 upsize detector Commited Micro-op Counter Threshold**. Read-write. Reset: 0. BIOS: 19h.
51	Reserved.
50	**RdMmExtCfgQwEn: read mmio extended config quadword enable**. Read-write. Reset: 0. BIOS: 1. 1=MMIO reads to extended config space do not need to be doubleword aligned and may be up to quadword sized. This is to support 64-bit MMIO reads to extended config space. 0=MMIO reads to extended config space need to be doubleword aligned and may be up to doubleword sized. MMIO reads to extended config space that are either not doubleword aligned or greater than doubleword sized are treated as plain MMIO reads.
49:38	Reserved.
37:36	**ThrottleNbInterface[3:2]**. Read-write. Reset: 01b. BIOS: 00b. See ThrottleNbInterface[1:0].
35:26	Reserved.
25	Reserved.
24	Reserved.
23:22	Reserved.
21:18	**L2UpsizeCSWT[4:1]: L2 upsize context switch warmup threshold [4:1]**. Read-write. Reset: 0. BIOS. 0000b. See L2UpsizeCSWT[0].
17:15	Reserved.
14	Reserved.
13:11	Reserved.
10	**VicResyncChkEn**. Read-write. Reset: 0. BIOS: 1. 1=Generate an internal probe to NB for non-shared victims. Required to be set for the Monitor/MWait instructions.

9	**L2UpsizeCSWT[0]: L2 upsize context switch warmup threshold [0]**. Read-write. Reset: 0. BIOS. 0b. L2UpsizeCSWT[4:0] = {L2UpsizeCSWT[4:1], L2UpsizeCSWT[0]}. The L2UpsizeCSWT defines the context switch warmup threshold for L2 cache upsizing. When non-zero, both the internal eviction count and the internal committed uop count are cleared when either a context switch occurs (indicated by MOV CR3) or the committed uop count exceeds the L2UpsizeCSWT[4:0]*8K following a context switch. This defines a period where many rapid evictions can occur without causing an L2 cache upsize following a context switch.
8	**SpecNbReqDis**. Read-write. Reset: 0. 1=Disables speculative NB requests.
7:6	**ThrottleNbInterface[1:0]**. Read-write. ThrottleNbInterface[3:0] = {ThrottleNbInterface[3:2], ThrottleNbInterface[1:0]}. Reset: 11b. BIOS: NumOfCompUnits-1. Specifies how many clocks the CU needs to wait before sending the next packet of information to the NB. This applies to the CU->NB request interface and the CU->NB probe response interface. This field must be programmed to a value greater than or equal to the number of compute units in the node that have at least one enabled core minus 1. See 2.4.4 [Processor Cores and Downcoring]. Bits: Description 0h: 0 Clocks. 1h: 1 Clock. 2h: 2 Clocks. 3h: 3 Clocks. Fh-4h: Reserved.
5	Reserved.
4:0	**L2UpsizeERT: L2 upsize evict rate threshold**. Read-write. Reset: 0. BIOS: 1_0001b. The L2UpsizeERT defines the eviction rate threshold that can cause an L2 cache upsize after a CC6 exit. When L2UpsizeERT is zero, the L2 cache upsize mechanism is disabled. When L2UpsizeERT is non-zero, L2 cache upsizes can be triggered after the internal committed uop counter interval expires (defined by L2UpsizeCUCT) if the internal eviction counter equals or exceeds the L2UpsizeERT[4:0]*64. Ratios of the L2UpsizeERT and L2UpsizeCUCT support a range of 0.00024 through 0.25 evictions per committed uop for L2 cache upsize tuning.

MSRC001_102B Combined Unit Configuration 3 (CU_CFG3)

Per-compute-unit.

Bits	Description
63:61	Reserved.
60:59	**PcidDecrScaleFactor**. Read-write. Reset: 00b. Specifies the decrement rate for the PCID replacement counter for PCIDs not currently in use; The larger the value programmed the slower the counter decrements. Bits: Description 00b: Inactive PCID replacement counter decrements every 64 TLB replacements. 01b: Inactive PCID replacement counter decrements every 128 TLB replacements. 10b: Inactive PCID replacement counter decrements every 256 TLB replacements. 11b: Inactive PCID replacement counter decrements every 512 TLB replacements.

58:57	**PcidIncrScaleFactor**. Read-write. Reset: 00b. Specifies the increment rate for the PCID replacement counter for PCIDs currently in use; The larger the value programmed the slower the counter increments. Bits — Description 00b — Active PCID replacement counter increments every 16 TLB inserts. 01b — Active PCID replacement counter increments every 32 TLB inserts. 10b — Active PCID replacement counter increments every 64 TLB inserts. 11b — Active PCID replacement counter increments every 128 TLB inserts.
56:55	**AsidIncrScaleFactor**. Read-write. Reset: 00b. Specifies the increment rate for the ASID replacement counter for ASIDs currently in use; The larger the value programmed the slower the counter increments. Bits — Description 00b — Active ASID replacement counter increments every 16 TLB inserts. 01b — Active ASID replacement counter increments every 32 TLB inserts. 10b — Active ASID replacement counter increments every 64 TLB inserts. 11b — Active ASID replacement counter increments every 128 TLB inserts.
54:53	Reserved.
52:51	**AsidDecrScaleFactor**. Read-write. Reset: 00b. Specifies the decrement rate for the ASID replacement counter for ASIDs not currently in use; The larger the value programmed the slower the counter decrements. Bits — Description 00b — Inactive ASID replacement counter decrements every 64 TLB replacements. 01b — Inactive ASID replacement counter decrements every 128 TLB replacements. 10b — Inactive ASID replacement counter decrements every 256 TLB replacements. 11b — Inactive ASID replacement counter decrements every 512 TLB replacements.
50	Reserved.
49	**CombineCr0Cd: combine CR0[CD] for both cores of a compute unit**. Read-write. Reset: 0. BIOS: 1. BIOS: Must not be set when using L2 cache as general storage during boot; See 2.3.3 [Using L2 Cache as General Storage During Boot]; Must be set before passing control to the OS. 0=The effective-CR0[CD] is not affected by the hCR0[CD] on other cores. 1=The effective CR0[CD], for all modes, is forced to 1 if the logical OR of the hCR0[CD] for all other cores on the compute unit is 1. Note that the logical OR does not include the local core hCR0[CD].
48:43	Reserved.
42	**PwcDisableWalkerSharing**. Read-write. Reset: 0. BIOS: 0. 1=Page table walker sharing is disabled. Core 0 uses page walker 0 and Core 1 uses page walker 1.
41:23	Reserved.
22	**PfcDoubleStride**. Read-write. Reset: 0. BIOS: 1. 1=Prefetch N and N+1 offsets ahead of a stride miss instead of just N. N is configurable by PfcStrideMul.
21:20	**PfcStrideMul**. Read-write. Reset: 01b. Specifies the number of stride offsets that are prefetched. Bits — Description 00b — 3 01b — 4 10b — 5 11b — 6
19	Reserved.

18	**PfcDis**. Read-write. Reset: 0. 1=Prefetcher disabled.
17	**PfcStrideDis**. Read-write. Reset: 0. 1=Stride prefetch generation disabled.
16	**PfcRegionDis**. Read-write. Reset: 0. 1=Region prefetch generation disabled.
15:4	Reserved.
3	**PfcL1TrainDis: stride training to L1 disable**. Read-write. Reset: 0. 1=L1 prefetch training disabled.
2:0	Reserved.

MSRC001_102F Prefetch Throttling Configuration (CU_PFTCFG)

Read-write; Per-compute-unit. Reset: 0000_0000_0000_0000h.
The prefetch throttle mechanism, described as follows, is enabled when (PrefetchThrottlingEn==1), otherwise all L2 prefetches will be sent to the NB.

A tracking structure is defined that holds 4 NB prefetches. Each of the 4 prefetches in this structure stores a hashed physical address (PAHash[13:0]), computed as (PA[47:34] ^ PA[33:20] ^ PA[19:6]). Every Nth prefetch sent to the NB, where N is specified by CaptureThreshold, will replace the oldest entry in the tracking structure. Each entry in the tracking structure implements a DemandHit indication, that is initialized as 0 when inserted and set to 1 if a demand L2 hit also hits on that entry, where a hit is defined as when the L2 hit PAHash matches the entry PAHash.

Two counters are defined, a current accuracy count (AccCntCurrent[5:0]), warm reset to 0, and a previous accuracy count (AccCntPrevious[5:0]), warm reset to 3Fh. AccCntCurrent is incremented if the entry that is replaced by a tracking structure insertion is DemandHit==1. After TrackThreshold insertions to the tracking structure, AccCntCurrent is written to AccCntPrevious and AccCntCurrent=0. All throttling decisions are based on the value of AccCntPrevious.

DCT channel utilization also factors into the decision to throttle prefetches. DCT utilization is indicated by a code called DramBwLevel, ranging from 0 (low utilization) to 2 (high utilization). If DRAM prefetch watermark 2 has been reached then DramBwLevel=2, else if DRAM prefetch watermark 1 has been reached then DramBwLevel=1, else DramBwLevel=0. See D18F2x1B4[DcqBwThrotWm2, DcqBwThrotWm1]. Throttling occurs according to ThrottleLevel as a function of DramBwLevel:

- If ((DramBwLevel==0) && (AccCntPrevious < AccThresh0)) then throttle.
- If ((DramBwLevel==1) && (AccCntPrevious < AccThresh1)) then throttle.
- If ((DramBwLevel==2) && (AccCntPrevious < AccThresh2)) then throttle.

Bits	Description
63:37	Reserved.
36	**PrefetchThrottlingEn: prefetch throttling enable**. BIOS: 0. 1=Prefetch throttling enabled.
35:30	**ThrottleLevel: throttling level**. BIOS: 0. Drop ThrottleLevel prefetches out of every every ThrottleLevel+1 prefetches. Bits — Description 00h — Reserved. 01h — Drop 1 prefetch out of every every 2 prefetches. 3Eh-02h — Drop <ThrottleLevel> prefetches out of every every <ThrottleLevel+1> prefetches. 3Fh — Drop 63 prefetches out of every every 64 prefetches.

29:24	**AccThresh2: accuracy threshold level 2**. BIOS: 0. Throttle prefetches if (DramBwLevel==2) and (AccCntPrevious < AccThresh2). AccThresh2 must be programmed to be greater than AccThresh1.
23:18	**AccThresh1: accuracy threshold level 1**. BIOS: 0. Throttle prefetches if (DramBwLevel==1) and (AccCntPrevious < AccThresh1). AccThresh1 must be programmed to be greater than AccThresh0.
17:12	**AccThresh0: accuracy threshold level 0**. BIOS: 0. Throttle prefetches if (DramBwLevel==0) and (AccCntPrevious < AccThresh0).
11:6	**TrackThreshold: prefetch throttling tracking threshold**. BIOS: 0Fh. Specifies how many tracking structure writes will occur before the current accuracy count (AccCntCurrent[5:0]) replaces the previous accuracy count (AccCntPrevious[5:0]).
5:0	**CaptureThreshold: prefetch throttling capture threshold**. BIOS: 0Fh. Specifies that 1 out of every CaptureThreshold prefetches that are sent to the NB will be inserted into the tracking structure.

MSRC001_1030 IBS Fetch Control (IbsFetchCtl)

Reset: 0000_0000_0000_0000h. See 2.6.2 [Instruction Based Sampling (IBS)].
The IBS fetch sampling engine is described as follows:

- The periodic fetch counter is an internal 20-bit counter:
  - The periodic fetch counter [19:4] is set to IbsFetchCnt[19:4] and the periodic fetch counter [3:0] is set according to IbsRandEn when IbsFetchEn is changed from 0 to 1.
  - It increments for every fetch cycle that completes when IbsFetchEn==1 and IbsFetchVal==0.
    - The periodic fetch counter is undefined when IbsFetchEn==0 or IbsFetchVal==1.
  - When IbsFetchCnt[19:4] is read it returns the current value of the periodic fetch counter [19:4].
- When the periodic fetch counter reaches {IbsFetchMaxCnt[19:4],0h} and the selected instruction fetch completes or is aborted:
  - IbsFetchVal is set to 1.
    - Drivers can't assume that IbsFetchCnt[19:4] is 0 when IbsFetchVal==1.
  - The status of the operation is written to the IBS fetch registers (this register, MSRC001_1031 and MSRC001_1032).
  - An interrupt is generated as specified by MSRC001_103A. The interrupt service routine associated with this interrupt is responsible for saving the performance information stored in IBS execution registers.

Bits	Description
63:59	Reserved.
58	Reserved.
57	**IbsRandEn: random instruction fetch tagging enable**. Read-write. 1=Bits[3:0] of the fetch counter are randomized when IbsFetchEn is set to start the fetch counter. 0=Bits[3:0] of the fetch counter are set to 0h when IbsFetchEn is set to start the fetch counter.
56	**IbsL2TlbMiss: instruction cache L2TLB miss**. Read-only; set-by-hardware. 1=The instruction fetch missed in the L2 TLB.
55	**IbsL1TlbMiss: instruction cache L1TLB miss**. Read-only; set-by-hardware. 1=The instruction fetch missed in the L1 TLB.

54:53	**IbsL1TlbPgSz: instruction cache L1TLB page size**. Read-only; updated-by-hardware. Indicates the page size of the translation in the L1 TLB. This field is only valid if IbsPhyAddrValid==1. Bits: Description 00b: 4 KB 01b: 2 MB 10b: 1 GB 11b: Reserved
52	**IbsPhyAddrValid: instruction fetch physical address valid**. Read-only; set-by-hardware. 1=The physical address in MSRC001_1032 and the IbsL1TlbPgSz field are valid for the instruction fetch.
51	**IbsIcMiss: instruction cache miss**. Read-only; set-by-hardware. 1=The instruction fetch missed in the instruction cache.
50	**IbsFetchComp: instruction fetch complete**. Read-only; set-by-hardware. 1=The instruction fetch completed and the data is available for use by the instruction decoder.
49	**IbsFetchVal: instruction fetch valid**. Read-only; set-by-hardware. 1=New instruction fetch data available. When this bit is set, the fetch counter stops counting and an interrupt is generated as specified by MSRC001_103A. This bit must be cleared for the fetch counter to start counting. When clearing this bit, software can write 0000h to IbsFetchCnt[19:4] to start the fetch counter at IbsFetchMaxCnt[19:4].
48	**IbsFetchEn: instruction fetch enable**. Read-write. 1=Instruction fetch sampling is enabled.
47:32	**IbsFetchLat: instruction fetch latency**. Read-only; set-by-hardware. Indicates the number of clock cycles from when the instruction fetch was initiated to when the data was delivered to the core. If the instruction fetch is abandoned before the fetch completes, this field returns the number of clock cycles from when the instruction fetch was initiated to when the fetch was abandoned.
31:16	**IbsFetchCnt[19:4]**. Read-write; updated-by-hardware. Provides read/write access to bits[19:4] of the periodic fetch counter. Programming this field to a value greater than or equal to IbsFetchMaxCnt[19:4] results in undefined behavior.
15:0	**IbsFetchMaxCnt[19:4]**. Read-write. Specifies bits[19:4] ofthe maximum count value of the periodic fetch counter. Programming this field to 0000h and setting IbsFetchEn results in undefined behavior. Bits[3:0] of the maximum count are always 0000b.

MSRC001_1031 IBS Fetch Linear Address (IbsFetchLinAd)

Reset: 0000_0000_0000_0000h.

Bits	Description
63:0	**IbsFetchLinAd: instruction fetch linear address**. Read-write; updated-by-hardware. Provides the linear address in canonical form for the tagged instruction fetch.

MSRC001_1032 IBS Fetch Physical Address (IbsFetchPhysAd)

Reset: 0000_0000_0000_0000h.

Bits	Description
63:0	**IbsFetchPhysAd: instruction fetch physical address**. Read-write; updated-by-hardware. Provides the physical address for the tagged instruction fetch. The lower 12 bits are not modified by address translation, so they are always the same as the linear address. This field contains valid data only if MSRC001_1030[IbsPhyAddrValid] is asserted.

MSRC001_1033 IBS Execution Control (IbsOpCtl)

Reset: 0000_0000_0000_0000h. See 2.6.2 [Instruction Based Sampling (IBS)].
The IBS execution sampling engine is described as follows for IbsOpCntCtl==1. If IbsOpCntCtl==1n then references to "periodic op counter" mean "periodic cycle counter".

- The periodic op counter is an internal 27-bit counter:
  - It is set to IbsOpCurCnt[26:0] when IbsOpEn is changed from 0 to 1.
  - It increments every dispatched op when IbsOpEn==1 and IbsOpVal==0.
    - The periodic op counter is undefined when IbsOpEn==0 or IbsOpVal==1.
  - When IbsOpCurCnt[26:0] is read then it returns the current value of the periodic micro-op counter [26:0].
- When the periodic micro-op counter reaches IbsOpMaxCnt:
  - The next dispatched micro-op is tagged if IbsOpCntCtl==1. A valid op in the next dispatched line is tagged if IbsOpCntCtl==0. See IbsOpCntCtl.
  - The periodic micro-op counter [26:7]=0; [6:0] is randomized by hardware.
- The periodic micro-op counter is not modified when a tagged micro-op is flushed.
- When a tagged micro-op is retired:
  - IbsOpVal is set to 1.
    - Drivers can't assume that IbsOpCurCnt is 0 when IbsOpVal==1.
  - The status of the operation is written to the IBS execution registers (this register, MSRC001_1034, MSRC001_1035, MSRC001_1036, MSRC001_1037, MSRC001_1038 and MSRC001_1039).
  - An interrupt is generated as specified by MSRC001_103A. The interrupt service routine associated with this interrupt is responsible for saving the performance information stored in IBS execution registers.

Bits	Description
63:59	Reserved.
58:32	**IbsOpCurCnt[26:0]: periodic op counter current count**. Read-write; updated-by-hardware. Returns the current value of the periodic op counter.
31:27	Reserved.
26:20	**IbsOpMaxCnt[26:20]: periodic op counter maximum count**. Read-write. See IbsOpMaxCnt[19:4].
19	**IbsOpCntCtl: periodic op counter count control**. Read-write. 1=Count dispatched Micro-ops; when a roll-over occurs, the counter is preloaded with a pseudorandom 7 bit value between 1 and 127. 0=Count clock cycles; a 1-of-4 round robin counter selects an op in the next dispatch line; if the op pointed to by the round robin counter is invalid, then the next younger valid op is selected.
18	**IbsOpVal: micro-op sample valid**. Read-write; set-by-hardware. 1=New instruction execution data available; the periodic op counter is disabled from counting. An interrupt may be generated when this bit is set as specified by MSRC001_103A[LvtOffset].
17	**IbsOpEn: micro-op sampling enable**. Read-write. 1=Instruction execution sampling enabled.

16	Reserved.
15:0	**IbsOpMaxCnt[19:4]: periodic op counter maximum count**. Read-write. IbsOpMaxCnt[26:0] = {IbsOpMaxCnt[26:20], IbsOpMaxCnt[19:4], 0000b}. Specifies maximum count value of the periodic op counter. Bits [3:0] of the maximum count are always 0000b. Bits Description 0008h-0000h Reserved FFFFh-0009h <IbsOpMaxCnt[19:4]*16> ops

MSRC001_1034 IBS Op Logical Address (IbsOpRip)

Reset: 0000_0000_0000_0000h.

Bits	Description
63:0	**IbsOpRip: micro-op linear address**. Read-write; updated-by-hardware. Linear address in canonical form for the instruction that contains the tagged micro-op.

MSRC001_1035 IBS Op Data (IbsOpData)

Bits	Description
63:41	Reserved.
40	**IbsOpMicrocode**. Value: 0. 1=Tagged operation from microcode.
39	**IbsOpBrnFuse: fused branch micro-op**. Read-write; updated-by-hardware. Reset: 0. 1=Tagged operation was a fused branch micro-op. Support indicated by CPUID Fn8000_001B_EAX[OpBrnFuse].
38	**IbsRipInvalid: RIP is invalid**. Read-write; updated-by-hardware. Reset: 0. 1=Tagged operation RIP is invalid. Support indicated by CPUID Fn8000_001B_EAX[RipInvalidChk].
37	**IbsOpBrnRet: branch micro-op retired**. Read-write; updated-by-hardware. Reset: 0. 1=Tagged operation was a branch micro-op that retired.
36	**IbsOpBrnMisp: mispredicted branch micro-op**. Read-write; updated-by-hardware. Reset: 0. 1=Tagged operation was a branch micro-op that was mispredicted. Qualified by IbsOpBrnRet==1.
35	**IbsOpBrnTaken: taken branch micro-op**. Read-write; updated-by-hardware. Reset: 0. 1=Tagged operation was a branch micro-op that was taken. Qualified by IbsOpBrnRet==1.
34	**IbsOpReturn: return micro-op**. Read-write; updated-by-hardware. Reset: 0. 1=Tagged operation was return micro-op. Qualified by IbsOpBrnRet==1.
33:32	Reserved.

31:16	**IbsTagToRetCtr: micro-op tag to retire count**. Read-write; updated-by-hardware. Reset: 0. This field returns the number of cycles from when the micro-op was tagged to when the micro-op was retired. This field is equal to IbsCompToRetCtr when the tagged micro-op is a NOP.
15:0	**IbsCompToRetCtr: micro-op completion to retire count**. Read-write; updated-by-hardware. Reset: 0. This field returns the number of cycles from when the micro-op was completed to when the micro-op was retired.

MSRC001_1036 IBS Op Data 2 (IbsOpData2)

Reset: 0000_0000h. Northbridge data is only valid for load operations that miss both the L1 data cache and the L2 cache. If a load operation crosses a cache line boundary, the data returned in this register is the data for the access to the lower cache line.

Bits	Description
63:32	Reserved.
31:6	Reserved.
5	**NbIbsReqCacheHitSt**: **IBS cache hit state**. Read-write; updated-by-hardware. Valid when the data source type is Cache(2h). 0=M State. 1=O State.
4	**NbIbsReqDstNode**: **IBS request destination node**. Read-write; updated-by-hardware. 0=The request is serviced by the NB in the same node as the core. 1=The request is serviced by the NB in a different node than the core. Valid when NbIbsReqSrc is non-zero.
3	Reserved.
2:0	**NbIbsReqSrc: northbridge IBS request data source**. Read-write. Bits — Description 0h — No valid status. 1h — Reserved. 2h — Cache: data returned from another compute-unit cache. 3h — DRAM: data returned from DRAM. 4h — Reserved for remote cache. 5h — Reserved. 6h — Reserved. 7h — Other: data returned from MMIO/Config/PCI/APIC.

MSRC001_1037 IBS Op Data 3 (IbsOpData3)

Reset: 0000_0000_0000_0000h. If a load or store operation crosses a 128-bit boundary, the data returned in this register is the data for the access to the data below the 128-bit boundary.

Bits	Description
63:48	**IbsTlbRefillLat: L1 DTLB refill latency**. Read-only. Value: 0. The number of cycles from when a L1 DTLB refill is triggered by a tagged op to when the L1 DTLB fill has been completed.

47:32	**IbsDcMissLat: data cache miss latency**. Read-write; updated-by-hardware. Indicates the number of clock cycles from when a miss is detected in the data cache to when the data was delivered to the core. The value returned by this counter is not valid for data cache writes or prefetch instructions.
31:26	**IbsOpDcMissOpenMemReqs: outstanding memory requests on DC fill**. Read-only. Value: 0. The number of allocated, valid DC MABs when the MAB corresponding to a tagged DC miss op is deallocated. Includes the MAB allocated by the sampled op. 0_0000b=No information provided.
25:22	**IbsOpMemWidth: load/store size in bytes**. Read-only. Value: 0. Report the number of bytes the load or store is attempting to access. Bits — Description 0h — No information provided. 1h — Byte. 2h — Word. 3h — DW. 4h — QW. 5h — OW. Fh-6h — Reserved.
21	**IbsSwPf: software prefetch**. Read-only. Value: 0. 1=The op is a software prefetch.
20	**IbsL2Miss: L2 cache miss for the sampled operation**. Read-only. Value: 0. 1=The operation missed in the L2, regardless of whether the op initiated the request to the L2.
19	**IbsDcL2TlbHit1G: data cache L2TLB hit in 1G page**. Read-write; updated-by-hardware. 1=The physical address for the tagged load or store operation was present in a 1G page table entry in the data cache L2TLB.
18	**IbsDcPhyAddrValid: data cache physical address valid**. Read-write; updated-by-hardware. 1=The physical address in MSRC001_1039 is valid for the load or store operation.
17	**IbsDcLinAddrValid: data cache linear address valid**. Read-write; updated-by-hardware. 1=The linear address in MSRC001_1038 is valid for the load or store operation.
16	**DcMissNoMabAlloc: DC miss with no MAB allocated**. Read-write; updated-by-hardware. 1=The tagged load or store operation hit on an already allocated MAB.
15	**IbsDcLockedOp: locked operation**. Read-write; updated-by-hardware. 1=Tagged load or store operation is a locked operation.
14	**IbsDcUcMemAcc: UC memory access**. Read-write; updated-by-hardware. 1=Tagged load or store operation accessed uncacheable memory.
13	**IbsDcWcMemAcc: WC memory access**. Read-write; updated-by-hardware. 1=Tagged load or store operation accessed write combining memory.
12:11	Reserved.
10	Reserved.
9	Reserved.

8	**IbsDcMisAcc: misaligned access**. Read-write; updated-by-hardware. 1=The tagged load or store operation crosses a 128-bit address boundary.
7	**IbsDcMiss: data cache miss**. Read-write; updated-by-hardware. 1=The cache line used by the tagged load or store was not present in the data cache.
6	**IbsDcL2tlbHit2M: data cache L2TLB hit in 2M page**. Read-write; updated-by-hardware. 1=The physical address for the tagged load or store operation was present in a 2M page table entry in the data cache L2TLB.
5	**IbsDcL1TlbHit1G: data cache L1TLB hit in 1G page**. Read-write; updated-by-hardware. 1=The physical address for the tagged load or store operation was present in a 1G page table entry in the data cache L1TLB.
4	**IbsDcL1TlbHit2M: data cache L1TLB hit in 2M page**. Read-write; updated-by-hardware. 1=The physical address for the tagged load or store operation was present in a 2M page table entry in the data cache L1TLB.
3	**IbsDcL2TlbMiss: data cache L2TLB miss**. Read-write; updated-by-hardware. 1=The physical address for the tagged load or store operation was not present in the data cache L2TLB.
2	**IbsDcL1tlbMiss: data cache L1TLB miss**. Read-write; updated-by-hardware. 1=The physical address for the tagged load or store operation was not present in the data cache L1TLB.
1	**IbsStOp: store op**. Read-write; updated-by-hardware. 1=Tagged operation is a store operation.
0	**IbsLdOp: load op**. Read-write; updated-by-hardware. 1=Tagged operation is a load operation.

MSRC001_1038 IBS DC Linear Address (IbsDcLinAd)

Reset: 0000_0000_0000_0000h.

Bits	Description
63:0	**IbsDcLinAd**. Read-write; updated-by-hardware. Provides the linear address in canonical form for the tagged load or store operation. This field contains valid data only if MSRC001_1037[IbsDcLinAddrValid] is asserted.

MSRC001_1039 IBS DC Physical Address (IbsDcPhysAd)

Bits	Description
63:48	RAZ.
47:0	**IbsDcPhysAd: load or store physical address**. Read-write; updated-by-hardware. Reset: 0. Provides the physical address for the tagged load or store operation. The lower 12 bits are not modified by address translation, so they are always the same as the linear address. This field contains valid data only if MSRC001_1037[IbsDcPhyAddrValid] is asserted.

MSRC001_103A IBS Control

GP-write.

Bits	Description
63:32	Reserved.
31:9	Reserved.

8	**LvtOffsetVal: local vector table offset valid**. MSRC001_103A[LvtOffsetVal] is an alias of D18F3x1CC[LvtOffsetVal].
7:4	Reserved.
3:0	**LvtOffset: local vector table offset**. MSRC001_103A[LvtOffset] is an alias of D18F3x1CC[LvtOffset].

MSRC001_103B IBS Branch Target Address (BP_IBSTGT_RIP)

Reset: 0000_0000_0000_0000h. Support for this register indicated by CPUID Fn8000_001B_EAX[BrnTrgt].

Bits	Description
63:0	**IbsBrTarget**. Read-write; updated-by-hardware. The logical address in canonical form for the branch target. Contains a valid target if non-0. Qualified by MSRC001_1035[IbsOpBrnRet]==1.

MSRC001_1090 Processor Feedback Constants 0

Read-write; Per-compute-unit.

Bits	Description
63:32	Reserved.
31:16	Reserved.
15:8	**RefCountScale**. Reset: Product-specific.
7:0	**ActualCountScale**. Reset: Product-specific.

THIS PAGE INTENTIALLY LEFT BLANK

3.23 Core Performance Counter Events

This section provides the core performance counter events that may be selected through MSRC001_020[A,8,6,4,2,0][EventSelect,UnitMask]. See that register and MSRC001_020[B,9,7,5,3,1] [Performance Event Counter (PERF_CTR[5:0])].

For NB performance counter events see 2.6.1.2 [NB Performance Monitor Counters] and 3.24 [NB Performance Counter Events].

3.23.1 PMCx0[1F:00] Events (FP)

PMCx000 FPU Pipe Assignment

PERF_CTL[3]. . The number of operations (uops) and dual-pipe uops dispatched to each of the 3 FPU execution pipelines. This event reflects how busy the FPU pipelines are and may be used for workload characterization. This includes all operations performed by x87, MMX, and SSE instructions, including moves. Each increment represents a one-cycle dispatch event. This event is a speculative event. (See PMCx0CB). Since this event includes non-numeric operations it is not suitable for measuring MFLOPS. The number of events logged per cycle can vary from 0 to 6 and must use PERF_CTL[3].

UnitMask	Description
7	Reserved.
6	Total number dual-pipe uops assigned to Pipe 2.
5	Total number dual-pipe uops assigned to Pipe 1.
4	Total number dual-pipe uops assigned to Pipe 0.
3	Reserved.
2	Total number uops assigned to Pipe 2.
1	Total number uops assigned to Pipe 1.
0	Total number uops assigned to Pipe 0.

PMCx001 FP Scheduler Empty

PERF_CTL[5:3]. This is a speculative event. The number of cycles in which the FPU scheduler is empty. Note that some ops like FP loads bypass the scheduler; see the FP MAS for the full list of “no pipe” ops that bypass the scheduler. Invert this (MSRC001_020[A,8,6,4,2,0][Inv]==1) to count cycles in which at least one FPU operation is present in the FPU.

PMCx003 Retired SSE/AVX Operations

PERF_CTL[3]. This is a retire-based event. The number of retired SSE/AVX FLOPS. The number of events logged per cycle can vary from 0 to 32.

UnitMask	Description
7	Double precision multiply-add FLOPS. Multiply-add counts as 2 FLOPS.
6	Double precision divide/square root FLOPS.
5	Double precision multiply FLOPS.
4	Double precision add/subtract FLOPS.

3	Single precision multiply-add FLOPS. Multiply-add counts as 2 FLOPS.
2	Single-precision divide/square root FLOPS.
1	Single-precision multiply FLOPS.
0	Single-precision add/subtract FLOPS.

PMCx004 Number of Move Elimination and Scalar Op Optimization

PERF_CTL[3]. This is a dispatch based speculative event, and is useful for measuring the effectiveness of the Move elimination and Scalar code optimization schemes. The number of events logged per cycle can vary from 0 to 8 and must use PERF_CTL[3].

UnitMask	Description
7:4	Reserved.
3	Number of Scalar ops optimized.
2	Number of Ops that are candidates for optimization (have Z-bit either set or pass).
1	Number of SSE Move Ops eliminated.
0	Number of SSE Move Ops.

PMCx005 Retired Serializing Ops

PERF_CTL[5:3]. The number of serializing ops retired.

UnitMask	Description
7:4	Reserved.
3	x87 control word mispredict traps due to mispredictions in RC or PC, or changes in mask bits.
2	x87 bottom-executing uops retired.
1	SSE control word mispredict traps due to mispredictions in RC, FTZ or DAZ, or changes in mask bits.
0	SSE bottom-executing uops retired.

PMCx006 Number of Cycles that a Bottom-Execute uop is in the FP Scheduler

PERF_CTL[5:3]. This is a speculative event.

3.23.2 PMCx0[3F:20] Events (LS)

PMCx020 Segment Register Loads

PERF_CTL[5:0]. The number of segment register loads performed.

UnitMask	Description
7	Reserved.
6	HS.
5	GS.
4	FS.

3	DS.
2	SS.
1	CS.
0	ES.

PMCx021 Pipeline Restart Due to Self-Modifying Code

PERF_CTL[5:0]. The number of pipeline restarts that were caused by self-modifying code (a store that hits any instruction that's been fetched for execution beyond the instruction doing the store).

PMCx022 Pipeline Restart Due to Probe Hit

PERF_CTL[5:0]. The number of pipeline restarts caused by an invalidating probe hitting on a speculative out-of-order load.

PMCx023 Load Queue/Store Queue Full

PERF_CTL[2:0]. The number of cycles that the load queue (LDQ) or store queue (STQ) is full. The load queue holds loads that missed the data cache and are waiting on a refill; the store queue holds stores waiting to retire. This condition stalls further data cache accesses, although such stalls may be overlapped by independent instruction execution.

UnitMask	Description
7:2	Reserved.
1	The number of cycles that the store buffer is full.
0	The number of cycles that the load buffer is full.

PMCx024 Locked Operations

PERF_CTL[5:0]. This event covers locked operations performed and their non-speculative execution time.

PMCx026 Retired CLFLUSH Instructions

PERF_CTL[5:0]. The number of retired CLFLUSH instructions. This is a non-speculative event.

PMCx027 Retired CPUID Instructions

PERF_CTL[5:0]. The number of CPUID instructions retired.

PMCx029 LS Dispatch

PERF_CTL[5:0]. Counts the number of operations dispatched to the LS unit.

UnitMask	Description
7:3	Reserved.
2	Load-op-Stores.

1	Stores.
0	Loads.

PMCx02A Canceled Store to Load Forward Operations

PERF_CTL[5:0]. Counts the number of canceled store to load forward operations.

UnitMask	Description
7:2	Reserved.
1	Physical tag mismatch.
0	Either “store is smaller than load” or “different starting byte but partial overlap”.

PMCx02B SMIs Received

PERF_CTL[5:0]. Counts the number of SMIs received.

PMCx030 Executed CLFLUSH Instructions

PERF_CTL[5:0]. The number of executed CLFLUSH instructions. This is a speculative event.

PMCx032 Misaligned Stores

PERF_CTL[5:0]. The number of misaligned stores.

PMCx034 FP +Load Buffer Stall

PERF_CTL[5:0]. The number of loads stalled due to buffer full.

PMCx035 STLF

PERF_CTL[5:0]. Number of STLF hits.

3.23.3 PMCx0[5F:40] Events (DC)

PMCx040 Data Cache Accesses

PERF_CTL[5:0]. The number of accesses to the data cache for load and store references. This may include certain microcode scratchpad accesses, although these are generally rare. This event is a speculative event. The number of events logged per cycle can vary from 0 to 2.

PMCx041 Data Cache Misses

PERF_CTL[5:0]. The number of data cache references which missed in the data cache. This event is a speculative event. Only the first miss for a given line is included; access attempts by other instructions while the refill is still pending are not included in this event. Each event reflects one 64 B cache line refill, and counts of this event are the same as, or very close to, the combined count for PMCx042. The number of events logged per

cycle can vary from 0 to 2.

UnitMask	Description
7:2	Reserved.
1	First streaming store to a 64 B cache line.
0	First data cache miss or streaming store to a 64 B cache line.

PMCx042 Data Cache Refills from L2 or System

PERF_CTL[5:0]. The number of data cache refills satisfied from the L2 cache and/or the system. Each increment reflects a 64 B transfer. This event is a speculative event.

UnitMask	Description
7:5	Reserved.
4	No-acknowledge fill response.
3	Fill with read data error.
2	Reserved.
1	Early valid status turned out to be invalid.
0	Fill with good data. (Final valid status is valid)

PMCx043 Data Cache Refills from System

PERF_CTL[2:0]. The number of L1 cache refills satisfied fromthe system (system memory or another cache), as opposed to the L2. Each increment reflects a 64 B transfer. This event is a speculative event.

PMCx045 Unified TLB Hit

PERF_CTL[2:0]. The number of TLB accesses that miss in the L1 DTLB or L1 and L2 ITLBs and hit in the unified TLB (UCTLB). This event is a speculative event.

UnitMask	Description
7	Reserved.
6	1 GB unified TLB hit for instruction.
5	2 MB unified TLB hit for instruction.
4	4 KB unified TLB hit for instruction.
3	Reserved.
2	1 GB unified TLB hit for data.
1	2 MB unified TLB hit for data.
0	4 KB unified TLB hit for data.

PMCx046 Unified TLB Miss

PERF_CTL[2:0]. The number of TLB accesses that miss in all TLBs. This event is a speculative event.

UnitMask	Description
7	Reserved.
6	1 GB unified TLB miss for instruction.
5	2 MB unified TLB miss for instruction.
4	4 KB unified TLB miss for instruction.
3	Reserved.
2	1 GB unified TLB miss for data.
1	2 MB unified TLB miss for data.
0	4 KB unified TLB miss for data.

PMCx047 Misaligned Accesses

PERF_CTL[5:0]. The number of data cache accesses that are misaligned. These are accesses which cross an 8 B boundary. They incur an extra cache access (reflected in PMCx040), and an extra cycle of latency on reads. This event is a speculative event.

PMCx04B Prefetch Instructions Dispatched

PERF_CTL[5:0]. The number of prefetch instructions dispatched by the decoder. Such instructions may or may not cause a cache line transfer. Any Dcache and L2 accesses, hits and misses by prefetch instructions are included in these types of events. This event is a speculative event.

UnitMask	Description
7:3	Reserved.
2	NTA (PrefetchNTA).
1	Store (PrefetchW).
0	Load (Prefetch, PrefetchT0/T1/T2).

PMCx052 Ineffective Software Prefetchs

PERF_CTL[5:0]. The number of software prefetches that did not fetch data outside of the processor core.

UnitMask	Description
7:4	Reserved.
3	Software prefetch hit in the L2.
2:1	Reserved.
0	Software prefetch hit in the L1.

3.23.4 PMCx[1:0][7F:60] Events (CU)

PMCx060 Command Related to Victim Buffers

PERF_CTL[2:0].

UnitMask	Description
7	Lock
6:5	Reserved.
4	Clean Victim Command
3	Write Victim Block
2:0	Reserved.

PMCx061 Command Related to Masked Operations

PERF_CTL[2:0]. Count Masked Byte and DW reads and writes to the NB. Byte sized read and write commands can request the transfer of up to 32 bytes. DW sized read and write commands can request the transfer of up to 32 DW's. Combining of the WC memory type can cause 1 B/DW write to represent multiple stores.

UnitMask	Description
7:6	Reserved.
5	Write Double-word
4	Write yte B
3	Reserved.
2	Read Double-word
1	Reserved.
0	Read yte B

PMCx062 Command Related to Read Block Operations

PERF_CTL[2:0].

UnitMask	Description
7	Reserved.
6	Read Block Speculative Shared.
5	RdBlkSpecMod.
4	RdBlkSpec.
3	Reserved.
2	Read Block Shared.
1	RdBlkMod.
0	Read Block.

PMCx063 Command Related to Change to Dirty Operations

PERF_CTL[2:0].

UnitMask	Description
7:5	Reserved.
4	Change to Dirty.
3:0	Reserved.

PMCx064 Dram System Request

PERF_CTL[2:0].

PMCx065 Memory Requests by Type

PERF_CTL[2:0]. These events reflect accesses to uncacheable (UC), write-combining (WC), and streaming store (SS) activity to WB memory.

UnitMask	Description
7	Requests to non-cacheable (WC+/SS, but not WC) memory, consisting of reads and 64 B sized buffer flushes.
6:2	Reserved.
1	Requests to non-cacheable (WC, but not WC+/SS) memory, consisting of reads and 64 B sized buffer flushes.
0	Requests to non-cacheable (UC) memory.

PMCx067 Data Cache Prefetches

UnitMask	Description
7:2	Reserved.
1	Prefetch attempts.
0	Reserved.

PMCx068 MAB Requests

PERF_CTL[2:0]. Events PMCx068 and PMCx069 reflect utilization of the Miss Address buffers (MABs), which handle IC, DC, TLB, WCC, and WCB related requests. The UnitMask[BufferID] is an encoded value which selects one of the MABs. PMCx068 counts the number of cacheable L2 misses handled by the selected MAB; PMCx069 counts the number of cycles the selected MAB is busy waiting for the NB response. The average latency seen by the selected MAB is the number of cycles spent waiting (PMCx069) divided by the number of requests (PMCx068).

UnitMask	Description
7:0	**BufferID**. Bits — Description 27-0 — MAB ID. 255-28 — Reserved.

PMCx069 MAB Wait Cycles

PERF_CTL[2:0].
See PMCx068.

UnitMask	Description
7:0	**BufferID**. See: PMCx068[BufferID].

PMCx06C System Response by Coherence State

PERF_CTL[2:0]. The number of responses from the system for cache refill requests. The UnitMask may be used to select specific cache coherency states. Each increment represents one 64 B cache line transferred from the system (DRAM or another cache, including another core on the same node) to the data cache, instruction cache or L2 cache (for data prefetcher and TLB table walks). Modified-state responses may be for Dcache store miss refills, PrefetchW software prefetches, hardware prefetches for a store-miss stream, or Change-to-Dirty requests that get a dirty (Owned) probe hit in another cache. Exclusive responses may be for any Icache refill, Dcache load miss refill, other software prefetches, hardware prefetches for a load-miss stream, or TLB table walks that miss in the L2 cache; Shared responses may be for any of those that hit a clean line in another cache.

UnitMask	Description
7:6	Reserved.
5	Modified unwritten.
4	Data rror.E
3	Owned.
2	Shared.
1	Modified.
0	Exclusive.

PMCx06D Octwords Written to System

PERF_CTL[2:0]. The number of OW (16 B) data transfers from the processor to the system. These may be part of a 64 B cache line writeback or a 64 B dirty probe hit response, each of which would cause four increments; or a partial or complete Write Combining buffer flush (Sized Write), which could cause from one to four increments.

UnitMask	Description
7:6	Reserved.
5:1	Reserved.
0	OW write transfer.

PMCx075 Cache Cross-invalidates

These reflect internal probes for Icache or Dcache misses that hit in the Dcache or Icache, causing the line to be invalidated. These may result from code modification, data being located too close to code, or virtual address aliasing. The aliasing cases arise when a physical memory location is referenced via two or more virtual

addresses which differ in bits 14:12. Such aliasing cases are generally uncommon.

UnitMask	Description
7:4	Reserved.
3	IC Invalidates DC (execution of recently modified code, or modified data too close to code).
2	IC Invalidates IC (aliasing).
1	DC Invalidates DC (aliasing).
0	DC Invalidates IC (modification of cached instructions, or of data located too close to code).

PMCx076 CPU Clocks not Halted

PERF_CTL[2:0].
The number of clocks that the CPU is not in a halted state (due to STPCLK or a HLT instruction). Note: this event allows system idle time to be automatically factored out from IPC (or CPI) measurements, providing the OS halts the CPU when going idle. If the OS goes into an idle loop rather than halting, such calculations are influenced by the IPC of the idle loop.

PMCx07D Requests to L2 Cache

PERF_CTL[2:0]. The number of requests to the L2 cache for Icache or Dcache fills, or page table lookups for the TLB. These events reflect only read requests to the L2; writes to the L2 are indicated by PMCx07E. See PMCx081, PMCx082, PMCx083, PMCx041, PMCx042, PMCx043.

UnitMask	Description
7	Reserved.
6	L2 cache prefetcher request.
5	Reserved.
4	Canceled request.
3	NB probe request.
2	TLB fill (page table walks).
1	DC fill.
0	IC fill.

PMCx07E L2 Cache Misses

PERF_CTL[2:0]. The number of requests that miss in the L2 cache. This may include some amount of speculative activity. The IC-fill-miss and DC-fill-miss events tend to mirror the Icache and Dcache refill-from-system PMCx083 and PMCx043, and tend to include more speculative activity than those events.

UnitMask	Description
7:6	Reserved.
5	Reserved.
4	L2 Cache Prefetcher request.
3	Reserved.

2	TLB page table walk.
1	DC fill (includes possible replays, whereas PMCx041 does not).
0	IC fill.

PMCx07F L2 Fill/Writeback

PERF_CTL[2:0]. Each increment represents a 64 B cache line transfer.

UnitMask	Description
7:3	Reserved.
2	**L2CleanWritebacks**. L2 Clean Writebacks to system.
1	**L2Writebacks**. L2 Writebacks to system (Clean and Dirty).
0	**L2Fills**. L2 fills from system. Note: Fills for non-temporal software prefetch and WP-memtype fills also are counted in this event even though they don't get cached in L2.

PMCx165 Page Splintering

PERF_CTL[2:0]. Counts the number of TLB reloads where a large page is installed into the TLB as a smaller page size.

UnitMask	Description
7:3	Reserved.
2	Host page size is larger than the guest page size.
1	Splintering due to MTRRs, IORRs, APIC, TOMs or other special address region.
0	Guest page size is larger than the host page size when nested paging is enabled.

PMCx16C L2 Prefetcher Trigger Events

PERF_CTL[2:0].

UnitMask	Description
7:2	Reserved.
1	Store L1 miss seen by prefetcher.
0	Load L1 miss seen by prefetcher.

3.23.5 PMCx[1:0][9F:80] Events (IC)

Note: All instruction cache events are speculative events unless specified otherwise.

PMCx080 Instruction Cache Fetches

PERF_CTL[2:0].
The number of successful instruction cache accesses by the instruction fetcher that result in data being sent to the decoder. Each access is an aligned 32 byte read, from which a varying number of instructions may be decoded.

PMCx081 Instruction Cache Misses

PERF_CTL[2:0].
The number of instruction fetches and prefetch requests that miss in the instruction cache. This is typically equal to or very close to the sum of events 82h and 83h. Each miss results in a 64-byte cache line refill.

PMCx082 Instruction Cache Refills from L2

PERF_CTL[2:0].
The number of instruction cache refills satisfied from the L2 cache. Each increment represents one 64-byte cache line transfer.

PMCx083 Instruction Cache Refills from System

PERF_CTL[2:0].
The number of instruction cache refills from system memory (or another cache). Each increment represents one 64-byte cache line transfer.

PMCx084 L1 ITLB Miss, L2 ITLB Hit

PERF_CTL[2:0].
The number of instruction fetches that miss in the L1 ITLB but hit in the L2 ITLB.

PMCx085 L1 ITLB Miss, L2 ITLB Miss

PERF_CTL[2:0]. The number of instruction fetches that miss in both the L1 and L2 TLBs.

UnitMask	Description
7:3	Reserved.
2	Instruction fetches to a 1 GB page.
1	Instruction fetches to a 2 MB page.
0	Instruction fetches to a 4 KB page.

PMCx086 Pipeline Restart Due to Instruction Stream Probe

PERF_CTL[2:0]. The number of pipeline restarts caused by invalidating probes that hit on the instruction stream currently being executed. This would happen if the active instruction stream was being modified by another processor in an MP system - typically a highly unlikely event.

PMCx087 Instruction Fetch Stall

PERF_CTL[2:0]. The number of cycles the instruction fetcher is stalled for the core. This may be for a variety of reasons such as branch predictor updates, unconditional branch bubbles, far jumps and cache misses, instruction fetching for the other core while instruction fetch for this core is stalled, among others. May be overlapped by instruction dispatch stalls or instruction execution, such that these stalls don't necessarily impact performance.

PMCx088 Return Stack Hits

PERF_CTL[2:0].
The number of near return instructions (RET or RET Iw) that get their return address from the return address stack (i.e. where the stack has not gone empty) for the core. This may include cases where the address is incorrect (return mispredicts). This may also include speculatively executed false-path returns. Return mispredicts are typically caused by the return address stack underflowing, however they may also be caused by an imbalance in calls vs. returns, such as doing a call but then popping the return address off the stack.

This event cannot be reliably compared with events C9h and CAh (such as to calculate percentage of return mispredicts due to an empty return address stack), since it may include speculatively executed false-path returns that are not included in those retire-time events.

PMCx089 Return Stack Overflows

PERF_CTL[2:0]. The number of (near) call instructions that cause the return address stack to overflow. When this happens, the oldest entry is discarded. This count may include speculatively executed calls.

PMCx08B Instruction Cache Victims

PERF_CTL[2:0]. The number of cachelines evicted from the instruction cache that cause an L2 write due to changed predecode (start bits); the L2 write due to changed predecode doesn't write the instruction bytes. This event does not count IC evictions with unchanged predecode, which are silently dropped without an L2 write. This event is not core specific and for either core counts the IC victims caused by both cores of the compute unit.

PMCx08C Instruction Cache Lines Invalidated

PERF_CTL[2:0]. The number of instruction cache lines invalidated. A non-SMC event is CMC (cross modifying code), either from the other core of the compute unit or another compute compute unit.

UnitMask	Description
7:4	Reserved.
3	SMC invalidating probe that hit on in-flight instructions.
2	SMC invalidating probe that missed on in-flight instructions.
1	Non-SMC invalidating probe that hit on in-flight instructions.
0	Non-SMC invalidating probe that missed on in-flight instructions.

PMCx099 ITLB Reloads

PERF_CTL[2:0]. The number of ITLB reload requests.

PMCx09A ITLB Reloads Aborted

PERF_CTL[2:0]. The number of ITLB reloads aborted.

PMCx186 Uops Dispatched From Decoder

PERF_CTL[2:0]. Counts uops that are dispatched from the decoder each cycle. The number of events logged per cycle can vary from 0 to 4. Note that when microcode dispatches between 1 to 4 uops in a cycle then 4 uops are counted in that cycle.

UnitMask	Description
7:1	Reserved.
0	**UopsDispatched: Uops Dispatched From Decoder**. **AllOps**. Ops dispatched from the decoder. Bits Description 0h AllOps: Ops dispatched from the decoder.

3.23.6 PMCx[1,0][DF:C0] Events (EX, DE)

PMCx0C0 Retired Instructions

PERF_CTL[5:0]. The number of instructions retired (execution completed and architectural state updated). This count includes exceptions and interrupts - each exception or interrupt is counted as one instruction.

PMCx0C1 Retired uops

PERF_CTL[5:0]. The number of micro-ops retired. This includes all processor activity (instructions, exceptions, interrupts, microcode assists, etc.). The number of events logged per cycle can vary from 0 to 4.

PMCx0C2 Retired Branch Instructions

PERF_CTL[5:0]. The number of branch instructions retired. This includes all types of architectural control flow changes, including exceptions and interrupts.

PMCx0C3 Retired Mispredicted Branch Instructions

PERF_CTL[5:0]. The number of branch instructions retired, of any type, that were not correctly predicted. This includes those for which prediction is not attempted (far control transfers, exceptions and interrupts).

PMCx0C4 Retired Taken Branch Instructions

PERF_CTL[5:0]. The number of taken branches that were retired. This includes all types of architectural control flow changes, including exceptions and interrupts.

PMCx0C5 Retired Taken Branch Instructions Mispredicted

PERF_CTL[5:0]. The number of retired taken branch instructions that were mispredicted.

PMCx0C6 Retired Far Control Transfers

PERF_CTL[5:0]. The number of far control transfers retired including far call/jump/return, IRET, SYSCALL and SYSRET, plus exceptions and interrupts. Far control transfers are not subject to branch prediction.

PMCx0C7 Retired Branch Resyncs

PERF_CTL[5:0]. The number of resync branches. These reflect pipeline restarts due to certain microcode assists and events such as writes to the active instruction stream, among other things. Each occurrence reflects a restart penalty similar to a branch mispredict. This is relatively rare.

PMCx0C8 Retired Near Returns

PERF_CTL[5:0]. The number of near return instructions (RET or RET Iw) retired.

PMCx0C9 Retired Near Returns Mispredicted

PERF_CTL[5:0]. The number of near returns retired that were not correctly predicted by the return address predictor. Each such mispredict incurs the same penalty as a mispredicted conditional branch instruction.

PMCx0CA Retired Mispredicted Taken Branch Instructions due to Target Mismatch

PERF_CTL[5:0]. The number of indirect branch instructions retired where the target address was not correctly predicted.

PMCx0CB Retired MMX™/FP Instructions

PERF_CTL[5:0]. The number of MMX, SSE or x87 instructions retired. The UnitMask allows the selection of the individual classes of instructions as given in the table. Each increment represents one complete instruction. Since this event includes non-numeric instructions it is not suitable for measuring MFLOPS.

UnitMask	Description
7:3	Reserved.
2	SSE instructions (SSE, SSE2, SSE3, SSSE3, SSE4A, SSE4.1, SSE4.2, AVX, XOP, FMA4).
1	MMX™ instructions.
0	x87 instructions.

PMCx0CD Interrupts-Masked Cycles

PERF_CTL[5:0]. The number of cycles where interrupts are masked (EFLAGS.IF==0). Using edge-counting with this event gives the number of times IF is cleared; dividing the cycle-count value by this value gives the average length of time that interrupts are disabled on each instance. Compare the edge count with PMCx0CF to determine how often interrupts are disabled for interrupt handling vs. other reasons (e.g. critical sections).

PMCx0CE Interrupts-Masked Cycles with Interrupt Pending

PERF_CTL[5:0]. The number of cycles where interrupts are masked (EFLAGS.IF==0) and an interrupt is pending. Using edge-counting with this event and comparing the resulting count with the edge count for PMCx0CD gives the proportion of interrupts for which handling is delayed due to prior interrupts being serviced, critical sections, etc. The cycle count value gives the total amount of time for such delays. The cycle count divided by the edge count gives the average length of each such delay.

PMCx0CF Interrupts Taken

PERF_CTL[5:0]. The number of hardware interrupts taken. This does not include software interrupts (INT n instruction).

PMCx0D0 Decoder Empty

PERF_CTL[2:0]. The number of cycles where the decoder has nothing to dispatch (typically waiting on an instruction fetch that missed the Icache, or for the target fetch after a branch mispredict).

PMCx0D1 Dispatch Stalls

PERF_CTL[2:0]. The number of cycles where the decoder is stalled for any reason (has one or more instructions ready but can't dispatch them due to resource limitations in execution). This event counts even when dispatch selects the other core of the compute-unit. This is the combined effect of events PMCx0D3 to PMCx0D9, some of which may overlap; this event reflects the net stall cycles. The more common stall conditions (events PMCx0D5, PMCx0D6, PMCx0D7, PMCx0D8) may overlap considerably. The occurrence of these stalls is highly dependent on the nature of the code being executed (instruction mix, memory reference patterns, etc.).

PMCx0D3 Microsequencer Stall due to Serialization

PERF_CTL[2:0]. The number of cycles the microsequencer is stalled due to a serializing operation, which waits for the execution pipeline to drain. Relatively rare; mainly associated with system instructions. See PMCx0D1.

PMCx0D5 Dispatch Stall for Instruction Retire Queue Full

PERF_CTL[2:0]. The number of cycles the decoder is stalled because the instruction retire Q is full. This event counts even when dispatch selects the other core of the compute-unit. May occur simultaneously with certain other stall conditions; see PMCx0D1.

PMCx0D6 Dispatch Stall for Integer Scheduler Queue Full

PERF_CTL[2:0]. The number of cycles the decoder is stalled because a required integer unit scheduler queue is full. This event counts even when dispatch selects the other core of the compute-unit. May occur simultaneously with certain other stall conditions; see PMCx0D1.

PMCx0D7 Dispatch Stall for FP Scheduler Queue Full

PERF_CTL[2:0]. The number of cycles the decoder is stalled because the scheduler for the Floating Point scheduler queue is full. This event counts even when dispatch selects the other core of the compute-unit. This condition can be caused by a lack of parallelism in FP-intensive code, or by cache misses on FP operand loads (which could also show up as PMCx0D8 instead, depending on the nature of the instruction sequences). May occur simultaneously with certain other stall conditions; see PMCx0D1.

PMCx0D8 Dispatch Stall for LDQ Full

PERF_CTL[2:0]. The number of cycles the decoder is stalled because the load queue is full. This event counts

even when dispatch selects the other core of the compute-unit. This generally occurs due to heavy cache miss activity. May occur simultaneously with certain other stall conditions; see PMCx0D1.

PMCx0D9 Microsequencer Stall Waiting for All Quiet

PERF_CTL[2:0]. The number of cycles the microsequencer is stalled waiting for all outstanding requests to the system to be resolved. Relatively rare; associated with certain system instructions and types of interrupts. May partially overlap certain other stall conditions; see PMCx0D1.

PMCx0DB FPU Exceptions

PERF_CTL[5:0]. The number of floating point unit exceptions for microcode assists. The UnitMask may be used to isolate specific types of exceptions.

UnitMask	Description
7:5	Reserved.
4	Bypass faults.
3	Ext2Int faults.
2	Int2Ext faults.
1	Total microtraps.
0	Total microfaults.

PMCx0D[F:C] DR[3:0] Breakpoint Matches

PERF_CTL[5:0].

Table 259: Register Mapping for PMCx0D[F:C]

Register	Function
PMCx0DC	DR0
PMCx0DD	DR1
PMCx0DE	DR2
PMCx0DF	DR3

The number of matches on the address in breakpoint register DR[3:0], per the breakpoint type specified in DR7. Matches occur if the access becomes becomes non-speculative, but not necessarily retired. Each instruction breakpoint match incurs an overhead of about 120 cycles; load/store breakpoint matches do not incur any overhead.

PMCx1C0 Retired x87 Floating Point Operations

PERF_CTL[5:3]. The number of x87 floating point ops that have retired.

UnitMask	Description
7:3	Reserved.
2	Divide and square root ops.

1	Multiply ops.
0	Add/subtract ops.

PMCx1CF Tagged IBS Ops

PERF_CTL[5:0].

UnitMask	Description
7:3	Reserved.
2	Number of times an op could not be tagged by IBS because of a previous tagged op that has not retired.
1	Number of ops tagged by IBS that retired.
0	Number of ops tagged by IBS.

PMCx1D0 Retired Fused Branch Instructions

PERF_CTL[5:0]. Implemented by EX. The number of fused retired branch instructions retired per cycle. The number of events logged per cycle can vary from 0 to 3.

PMCx1D8 Dispatch Stall for STQ Full

PERF_CTL[5:0]. The number of cycles the decoder is stalled because the store queue is full. This event counts even when dispatch selects the other core of the compute-unit. This generally occurs due to heavy cache miss activity. May occur simultaneously with certain other stall conditions.

PMCx1DD Cycles Without Dispatch Due To Integer PRF Tokens

PERF_CTL[2:0]. The number of cycles a core has valid ops for dispatch and one of the reasons for a dispatch stall is the absence of sufficient integer PRF tokens. This event counts even when dispatch selects the other core of the compute-unit.

PMCx1DE Cycles Without Dispatch Due to FP PRF Tokens

PERF_CTL[2:0]. The number of cycles a core has valid ops for dispatch and one of the reasons for a dispatch stall is the absence of sufficient FP PRF tokens. This event requires that the other core of the compute unit is in the Halt state. This event counts even when dispatch selects the other core of the compute-unit.

PMCx1DF FP Dispatch Contention

PERF_CTL[2:0]. Cycles in which there is contention between the two threads for FP dispatch.

UnitMask	Description
7:2	Reserved.
1:0	**ContentionSel**. Bits Description 00b The other selected thread did not dispatch; this not selected thread could not have dispatched. 01b The other selected thread did not dispatch; this not selected thread could have dispatched. 10b The other selected thread did dispatch; this not selected thread could not have dispatched. 11b The other selected thread did dispatch; this not selected thread could have dispatched.

3.24 NB Performance Counter Events

This section provides the performance counter events that may be selected through MSRC001_024[6,4,2,0][EventSelect,UnitMask]. See that register and MSRC001_024[7,5,3,1] [Northbridge Performance Event Counter (NB_PERF_CTR[3:0])].

3.24.1 PMCx0E[7:4] Events (Memory Controller)

NBPMCx0E4 Memory Controller Bypass Counter Saturation

UnitMask	Description
7:6	Reserved.
5	DCQ Bypass Saturated. The DCT is selected by the field NBPMCx0E4[4:2].
4:2	Select DCQ bypass: Bits Description 000b Select DCT0 DCQ bypass. 001b Select DCT1 DCQ bypass. 111b-010b Reserved.
1	Memory controller medium priority bypass.
0	Memory controller high priority bypass.

3.24.2 PMCx0E[F:8] Events (Crossbar)

NBPMCx0E8 Thermal Status

UnitMask	Description
7	Reserved.
6	Number of clocks HTC P-state is active.
5	Number of clocks HTC P-state is inactive.
4	Reserved.
3	Reserved.

2	Number of times the HTC trip point is crossed.
1:0	Reserved.

NBPMCx0E9 CPU/IO Requests to Memory/IO

These events reflect request flow between units and nodes, as selected by the UnitMask. The UnitMask is divided into two fields: request type (CPU or IO access to IO or Memory) and source/target location (local vs. remote). One or more requests types must be enabled via bits 3:0, and at least one source and one target location must be selected via bits 7:4. Each event reflects a request of the selected type(s) going from the selected source(s) to the selected target(s).

Not all possible paths are supported. The following table shows the UnitMask values that are valid for each request type:

Source/Target	CPU to Mem	CPU to IO	IO to Mem	IO to IO
Local -> Local	A8h	A4h	A2h	A1h
Local -> Remote	98h	94h	92h	91h
Remote -> Local	-	64h	-	61h
Remote > emote	- R	-	-	-

Any of the mask values shown may be logically ORed to combine the events. For instance, local CPU requests to both local and remote nodes would be A8h | 98h = B8h. Any CPU to any IO would be A4h | 94h | 64h = F4h (but remote CPU to remote IO requests would not be included).

Note: It is not possible to tell from these events how much data is going in which direction, as there is no distinction between reads and writes. Also, particularly for IO, the requests may be for varying amounts of data, anywhere from one to sixty-four bytes. For a direct measure of the amount and direction of data flowing between nodes, use events F6h, F7h and F8h.

UnitMask	Description
7	From local node.
6	From remote node.
5	To local node.
4	To remote node.
3	CPU o Metm.
2	CPU o IO.t
1	IO o Metm.
0	IO o IO.t

NBPMCx0EA Cache Block Commands

The number of requests made to the system for cache line transfers or coherency state changes, by request type. Each increment represents one cache line transfer, except for Change-to-Dirty. If a Change-to-Dirty request hits on a line in another processor's cache that's in the Owned state, it causes a cache line transfer, otherwise there is no data transfer associated with Change-to-Dirty requests.

UnitMask	Description
7:6	Reserved.
5	Change-to-Dirty (first store to clean block already in cache).
4	Read Block Modified (Dcache store miss refill).
3	Read Block Shared (Icache refill).
2	Read Block (Dcache load miss refill).
1	Reserved.
0	Victim Block (Writeback).

NBPMCx0EB Sized Commands

The number of Sized Read/Write commands handled by the System Request Interface (local processor and hostbridge interface to the system). These commands may originate from the processor or hostbridge. Typical uses of the various Sized Read/Write commands are given in the UnitMask table. See NBPMCx0EC, which provides a separate measure of Hostbridge accesses.

UnitMask	Description
7:6	Reserved.
5	SzRd DW (1-16 DWORDs). Typical Usage: Block-oriented DMA reads, typically cache-line size.
4	SzRd Byte (4 bytes). Typical Usage: Legacy or mapped IO.
3	Posted SzWr DW (1-16 DWORDs). Typical Usage: Block-oriented DMA writes, often cache-line sized; also processor Write Combining buffer flushes.
2	Posted SzWr Byte (1-32 bytes). Typical Usage: Sub-cache-line DMA writes, size varies; also flushes of partially-filled Write Combining buffer.
1	Non-Posted SzWr DW (1-16 DWORDs). Typical Usage: Legacy or mapped IO, typically 1 DWORD.
0	Non-Posted SzWr Byte (1-32 bytes). Typical Usage: Legacy or mapped IO, typically 1-4 bytes.

NBPMCx0EC Probe Responses and Upstream Requests

This covers two unrelated sets of events: cache probe results, and requests received by the hostbridge from devices on non-coherent links.

Probe results: These events reflect the results of probes sent from a memory controller to local caches. They provide an indication of the degree data and code is shared between processors (or moved between processors due to process migration). The dirty-hit events indicate the transfer of a 64-byte cache line to the requestor (for a read or cache refill) or the target memory (for a write). The system bandwidth used by these, in terms of bytes per unit of time, may be calculated as 64 times the event count, divided by the elapsed time. Sized writes to memory that cover a full cache line do not incur this cache line transfer -- they simply invalidate the line and are reported as clean hits. Cache line transfers occur for Change2Dirty requests that hit cache lines in the Owned state. (Such cache lines are counted as Modified-state refills for PMCx06C, System Read Responses.)

Upstream requests: The upstream read and write events reflect requests originating from a device on a local IO link.

UnitMask	Description
7	Upstream non-ISOC writes.
6	Upstream ISOC writes.
5	Upstream non-display refresh reads.
4	Upstream display refresh/ISOC reads.
3	Probe hit dirty with memory cancel (probed by DMA read or cache refill request).
2	Probe hit dirty without memory cancel (probed by Sized Write or Change2Dirty).
1	Probe hit clean.
0	Probe miss.

3.24.3 PMCx0F[F:0] Events (Crossbar)

3.24.4 NBPMCx1E[F:0] Events (Crossbar)

NBPMCx1E0 CPU to DRAM Requests to Target Node

This event counts all DRAM reads and writes generated by cores on the local node to the targeted node in the coherent fabric. This counter can be used to observe processor data affinity in NUMA aware operating systems.

UnitMask	Description
7	From Local node to Node 7.
6	From Local node to Node 6.
5	From Local node to Node 5.
4	From Local node to Node 4.
3	From Local node to Node 3.
2	From Local node to Node 2.
1	From Local node to Node 1.
0	From Local node to Node 0.

NBPMCx1E1 IO to DRAM Requests to Target Node

This event counts all DRAM reads and writes generated by IO devices attached to the IO links of the local node the targeted node in the coherent fabric. This counter can be used to observe IO device data affinity in NUMA aware operating systems.

UnitMask	Description
7	From Local node to Node 7.
6	From Local node to Node 6.
5	From Local node to Node 5.
4	From Local node to Node 4.
3	From Local node to Node 3.
2	From Local node to Node 2.

1	From Local node to Node 1.
0	From Local node to Node 0.

NBPMCx1E2 CPU Read Command Latency to Target Node 0-3

This event counts the number of NB clocks from when the targeted command is received in the NB to when the targeted command completes. This event only tracks one outstanding command at a time. To determine latency between the local node and a remote node set UnitMask[7:4] to select the node and UnitMask[3:0] to select the read command type. The count returned by the counter should be divided by the count returned by NBPMCx1E3 do determine the average latency for the command type.

UnitMask	Description
7	From Local node to Node 3.
6	From Local node to Node 2.
5	From Local node to Node 1.
4	From Local node to Node 0.
3	Change-to-Dirty.
2	Read block modified.
1	Read block shared.
0	Read block.

NBPMCx1E3 CPU Read Command Requests to Target Node 0-3

This event counts the number of requests that a latency measurement is made for using NBPMCx1E2. To determine the number of commands that a latency measurement are made for between the local node and a remote node set UnitMask[7:4] to select the node and UnitMask[3:0] to select the read command type.

UnitMask	Description
7	From Local node to Node 3.
6	From Local node to Node 2.
5	From Local node to Node 1.
4	From Local node to Node 0.
3	Change-to-Dirty.
2	Read block modified.
1	Read block shared.
0	Read block.

NBPMCx1E4 CPU Read Command Latency to Target Node 4-7

This event counts the number of NB clocks from when the targeted command is received in the NB to when the targeted command completes. This event only tracks one outstanding command at a time. To determine latency between the local node and a remote node set UnitMask[7:4] to select the node and UnitMask[3:0] to select the read command type. The count returned by the counter should be divided by the count returned by NBPMCx1E5 do determine the average latency for the command type.

UnitMask	Description
7	From Local node to Node 7.
6	From Local node to Node 6.
5	From Local node to Node 5.
4	From Local node to Node 4.
3	Change-to-Dirty.
2	Read block modified.
1	Read block shared.
0	Read block.

NBPMCx1E5 CPU Read Command Requests to Target Node 4-7

This event counts the number of requests that a latency measurement is made for using NBPMCx1E4. To determine the number of commands that a latency measurement are made for between the local node and a remote node set UnitMask[7:4] to select the node and UnitMask[3:0] to select the read command type.

UnitMask	Description
7	From Local node to Node 7.
6	From Local node to Node 6.
5	From Local node to Node 5.
4	From Local node to Node 4.
3	Change-to-Dirty.
2	Read block modified.
1	Read block shared.
0	Read block.

NBPMCx1E6 CPU Command Latency to Target Node 0-3/4-7

This event counts the number of NB clocks from when the targeted command is received in the NB to when the targeted command completes. This event only tracks one outstanding command at a time. To determine latency between the local node and a remote node set UnitMask[7:4] to select the node, UnitMask[3] to select the node group and UnitMask[3:0] to select the command type. The count returned by the counter should be divided by the count returned by NBPMCx1E7 do determine the average latency for the command type.

UnitMask	Description
7	From Local node to Node 3/7.
6	From Local node to Node 2/6.
5	From Local node to Node 1/5.
4	From Local node to Node 0/4.
3	Node Group Select. 0=Nodes 0-3. 1= Nodes 4-7.
2	Victim Block.
1	Write izedS
0	Read Sized.

NBPMCx1E7 CPU Requests to Target Node 0-3/4-7

This event counts the number of requests that a latency measurement is made for using NBPMCx1E6. To determine the number of commands that a latency measurement are made for between the local node and a remote node set UnitMask[7:4] to select the node, UnitMask[3] to select the node group and UnitMask[3:0] to select the command type.

UnitMask	Description
7	From Local node to Node 3/7.
6	From Local node to Node 2/6.
5	From Local node to Node 1/5.
4	From Local node to Node 0/4
3	Node Group Select. 0=Nodes 0-3. 1= Nodes 4-7.
2	Victim Block.
1	Write izedS
0	Read Sized.

NBPMCx1EB Request Cache Status 1

The probe response type for RdBlkM or ChgToDirty request type.

UnitMask	Description
7	Track Cache Stat for RdBlkM.
6	Track Cache Stat for ChgToDirty.
5	Directed Probe.
4	Probe Miss.
3	Probe Hit M.
2	Probe Hit MuW or O.
1	Probe Hit E.
0	Probe Hit S.

3.24.5 NBPMCx1F[F:0] Events (Memory Controller, Crossbar)

NBPMCx1F0 Memory Controller Requests

Read/Write requests: The read/write request events reflect the total number of commands sent to the DRAM controller.
Sized Read/Write activity: The Sized Read/Write events reflect 32- or 64-byte transfers (as opposed to other sizes which could be anywhere between 1 and 64 bytes), from either the processor or the Hostbridge (on any node in an MP system). Such accesses from the processor would be due only to write combining buffer flushes, where 32-byte accesses would reflect flushes of partially-filled buffers. PMCx065 provides a count of sized write requests associated with WC buffer flushes; comparing that with counts for these events (providing there is very little Hostbridge activity at the same time) gives an indication of how efficiently the write combining buffers are being used. PMCx065 may also be useful in factoring out WC flushes when comparing these events with the Upstream Requests component of PMCx06C.

UnitMask	Description
7	Read requests sent to the DCT while writes requests are pending in the DCT.
6	64 Byte Sized Reads.
5	32 Bytes Sized Reads.
4	64 Bytes Sized Writes.
3	32 Bytes Sized Writes.
2	Prefetch requests sent to the DCT.
1	Read requests (including prefetch requests) sent to the DCT.
0	Write requests sent to the DCT.

NBPMCx3EC DRAM Accesses

The number of memory accesses performed by the local DRAM controller. UnitMask[7:0] may be used to isolate the different DRAM page access cases. Page miss cases incur an extra latency to open a page; page conflict cases incur both a page-close as well as page-open penalties. These penalties may be overlapped by DRAM accesses for other requests and don't necessarily represent lost DRAM bandwidth. The associated penalties are as follows:

Page miss: Trcd (DRAM RAS-to-CAS delay)
Page conflict: Trp + Trcd (DRAM row-precharge time plus RAS-to-CAS delay)

Each DRAM access represents one 64-byte block of data transferred if the DRAM is configured for 64-byte granularity, or one 32-byte block if the DRAM is configured for 32-byte granularity. (The latter is only applicable to single-channel DRAM systems, which may be configured either way.)

UnitMask	Description
7:6	Reserved.
5	DCT1 Page Conflict.
4	DCT1 age Miss.
3	DCT1 age Hit.
2	DCT0 Page Conflict.
1	DCT0 age Miss.
0	DCT0 age Hit.

NBPMCx3ED DRAM Controller Page Table Overflows

The number of page table overflows in the local DRAM controller. This table maintains information about which DRAM pages are open. An overflow occurs when a request for a new page arrives when the maximum number of pages are already open. Each occurrence reflects an access latency penalty equivalent to a page conflict.

UnitMask	Description
7:2	Reserved.

1	DCT1 Page Table Overflow.
0	DCT0 Page Table Overflow.

NBPMCx3EE Memory Controller DRAM Command Slots Missed

UnitMask	Description
7:2	Reserved.
1	DCT1 Command Slots Missed (in MEMCLKs).
0	DCT0 Command Slots Missed (in MEMCLKs).

NBPMCx3EF Memory Controller Turnarounds

The number of turnarounds on the local DRAM data bus. UnitMask[7:0] may be used to isolate the different cases. These represent lost DRAM bandwidth, which may be calculated as follows (in bytes per occurrence):

DIMM turnaround: DRAM_width_in_bytes * 2 edges_per_memclk * 2
R/W turnaround: DRAM_width_in_bytes * 2 edges_per_memclk * 1
R/W turnaround: DRAM_width_in_bytes * 2 edges_per_memclk * (Tcl-1)

where DRAM_width_in_bytes is 8 or 16 (for single- or dual-channel systems), and Tcl is the CAS latency of the DRAM in memory system clock cycles (where the memory clock for DDR-400, or PC3200 DIMMS, for example, would be 200 MHz).

UnitMask	Description
7:6	Reserved.
5	DCT1 Write to Read turnaround.
4	DCT1 Read to Write turnaround.
3	DCT1 DIMM (chip select) turnaround.
2	DCT0 Write to Read turnaround.
1	DCT0 Read to Write turnaround.
0	DCT0 DIMM (chip select) turnaround.

3.24.6 3F[F:0] Events (Memory Controller)

NBPMCx3FC DRAM Accesses

The number of memory accesses performed by the local DRAM controller. UnitMask[7:0] may be used to isolate the different DRAM page access cases. Page miss cases incur an extra latency to open a page; page conflict cases incur both a page-close as well as page-open penalties. These penalties may be overlapped by DRAM accesses for other requests and don't necessarily represent lost DRAM bandwidth. The associated penalties are as follows:

Page miss: Trcd (DRAM RAS-to-CAS delay)
Page conflict: Trp + Trcd (DRAM row-precharge time plus RAS-to-CAS delay)

Each DRAM access represents one 64-byte block of data transferred if the DRAM is configured for 64-byte granularity, or one 32-byte block if the DRAM is configured for 32-byte granularity. (The latter is only applicable to single-channel DRAM systems, which may be configured either way.)

UnitMask	Description
7:6	Reserved.
5	DCT3 Page Conflict.
4	DCT3 age Miss.
3	DCT3 age Hit.
2	DCT2 Page Conflict.
1	DCT2 age Miss.
0	DCT2 age Hit.

NBPMCx3FD DRAM Controller Page Table Overflows

The number of page table overflows in the local DRAM controller. This table maintains information about which DRAM pages are open. An overflow occurs when a request for a new page arrives when the maximum number of pages are already open. Each occurrence reflects an access latency penalty equivalent to a page conflict.

UnitMask	Description
7:2	Reserved.
1	DCT3 Page Table Overflow.
0	DCT2 Page Table Overflow.

NBPMCx3FE Memory Controller DRAM Command Slots Missed

UnitMask	Description
7:2	Reserved.
1	DCT3 Command Slots Missed (in MEMCLKs).
0	DCT2 Command Slots Missed (in MEMCLKs).

NBPMCx3FF Memory Controller Turnarounds

The number of turnarounds on the local DRAM data bus. UnitMask[7:0] may be used to isolate the different cases. These represent lost DRAM bandwidth, which may be calculated as follows (in bytes per occurrence):

DIMM turnaround: DRAM_width_in_bytes * 2 edges_per_memclk * 2
R/W turnaround: DRAM_width_in_bytes * 2 edges_per_memclk * 1
R/W turnaround: DRAM_width_in_bytes * 2 edges_per_memclk * (Tcl-1)

where DRAM_width_in_bytes is 8 or 16 (for single- or dual-channel systems), and Tcl is the CAS latency of the DRAM in memory system clock cycles (where the memory clock for DDR-400, or PC3200 DIMMS, for example, would be 200 MHz).

UnitMask	Description
7:6	Reserved.
5	DCT3 Write to Read turnaround.
4	DCT3 Read to Write turnaround.
3	DCT3 DIMM (chip select) turnaround.
2	DCT2 Write to Read turnaround.
1	DCT2 Read to Write turnaround.
0	DCT2 DIMM (chip select) turnaround.

4 Register List

The following is a list of all storage elements, context, and registers provided in this document. Page numbers, register mnemonics, and register names are provided.